

Neusoft

东软应用交付安全网关 V1.3

用户使用指南

版本 1.1

2019 年 9 月

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。

Copyright © 2017-2019 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。

联系信息

网站: <http://www.neusoft.com>

电子信箱: servicedesk@neusoft.com

服务电话: 400 655 6789

目录

前言	1
文本约定	2
图标约定	2
第 1 章 产品简介	3
1.1. 部署方式	3
1.2. 工作原理	4
1.2.1. 服务器负载均衡	4
1.2.2. 出站链路负载均衡	5
1.2.3. 入站链路负载均衡	6
1.2.4. 全局负载均衡	6
1.3. 主要功能	8
1.3.1. 应用交付	8
1.3.2. 应用安全	10
1.3.3. 日志和报表	11
1.3.4. Nginx 脚本编辑器	11
1.3.5. 虚拟系统	11
第 2 章 快速向导	12
2.1. 修改缺省管理 IP	12

2.1.1. 通过 Console 修改缺省管理 IP.....	12
2.1.2. 通过 WebUI 修改缺省管理 IP.....	15
2.2. WebUI 介绍.....	16
2.3. 配置逻辑.....	18
2.4. 配置步骤.....	19
第 3 章 虚拟服务.....	24
3.1. 七层流量管理.....	25
3.1.1. 配置基础框架.....	26
3.1.2. SSL 加密.....	33
3.1.3. URL 重写.....	36
3.1.4. 内容缓存.....	38
3.1.5. 内容压缩.....	39
3.1.6. 反向代理.....	40
3.1.7. 负载均衡.....	43
3.1.8. 会话保持.....	44
3.1.9. 持久连接.....	45
3.1.10. 域名解析（容错）.....	46
3.1.11. 自动负载均衡.....	47
3.1.12. 延迟停机.....	48
3.1.13. 云服务.....	49
3.2. 四层流量管理.....	52
3.2.1. 配置四层流量管理基础框架.....	52

3.2.2. 会话保持	57
3.2.3. 负载均衡	58
3.2.4. 自动负载均衡	60
3.2.5. 延迟停机	61
3.3. 健康状态监控	62
第 4 章 Web 安全	65
4.1. 安全策略	66
4.1.1. 添加和引用安全策略	66
4.1.2. 编辑安全策略	68
4.1.2.1. 攻击签名	68
4.1.2.2. 网页防篡改	69
4.1.2.3. 信息泄露防护	70
4.1.2.4. 访问控制	72
4.1.2.5. HTTP 协议约束	75
4.1.2.6. 全局白名单	76
4.1.2.7. 机器人防御	77
4.1.2.8. 访问速率限制	78
4.1.2.9. 访问连接限制	79
4.2. 主动防御	80
4.3. DDoS 防御	83
4.4. 漏洞扫描	85
第 5 章 公共对象	87
5.1. IP 地址集	87
5.2. ISP 地址集	88

5.3.	用户地域	89
5.4.	自定义错误页面	90
5.5.	自定义 IPS 规则	91
第 6 章	DNS 代理	93
6.1.	网关 DNS	94
6.2.	透明代理	95
6.3.	前置调度	96
6.4.	内网记录	98
第 7 章	智能 DNS	100
7.1.	DNS 服务器	101
7.2.	站点集合	102
7.3.	LDNS 集合	104
7.4.	虚拟 IP 池	105
7.5.	DNS 映射	108
7.6.	静态就近性	109
7.7.	全局配置同步	111
第 8 章	网络配置	112
8.1.	接口	112
8.1.1.	以太网接口	112
8.1.2.	WAN	113
8.1.3.	LAN	114
8.2.	VLAN	115

8.3.	静态路由	116
8.4.	智能路由	117
8.5.	DNS	120
8.6.	端口映射	120
8.7.	源地址转换	122
8.8.	ACL 配置	123
第 9 章	系统配置	127
9.1.	配置向导	127
9.2.	系统维护	131
9.2.1.	备份恢复	131
9.2.2.	许可	132
9.2.3.	重启和关闭	134
9.2.4.	诊断工具	134
9.2.5.	技术支持	135
9.3.	管理设置（Web 和 SSH）	136
9.4.	管理用户	137
9.4.1.	修改 admin/root 密码	138
9.4.2.	添加根系统管理员	139
9.4.3.	添加根系统审计员	139
9.5.	日志设置	141
9.6.	报警设置	142
9.7.	升级设置	143

9.8.	报表设置	144
9.9.	高可用性	147
9.10.	系统参数	151
9.11.	SNMP	152
9.12.	日期/时间设置	153
第 10 章	虚拟系统	154
10.1.	创建虚拟系统	154
10.2.	添加虚拟系统管理员	155
10.3.	管理虚拟系统	156
第 11 章	监控	157
11.1.	首页	157
11.2.	版权信息	159
11.3.	监控	159
11.4.	统计	162
11.5.	日志	164
11.5.1.	七层流量日志	164
11.5.2.	四层流量日志	165
11.5.3.	攻击日志	165
11.5.4.	事件日志	167
11.5.5.	访问统计	167
11.5.6.	自定义显示的日志信息	168
11.6.	报表	169

第 12 章 范例	170
12.1. 服务器负载均衡.....	171
12.2. Web 安全防护.....	174
12.3. 主动防御.....	178
12.4. 入站链路负载均衡（智能 DNS，单数据中心）.....	181
12.5. 全局负载均衡（多数据中心）.....	184
12.6. 出站链路负载均衡.....	189
12.7. 出站链路负载均衡（启用 DNS 透明代理）.....	191
12.8. 出站、入站复合链路负载均衡（地址映射，出站负载）.....	195
12.9. 某城市轨道交通用户配置实例.....	196
12.10. 电力网正反向虚拟隔离（虚拟系统）.....	207
附录 A: 术语表	212
附录 B: 日志信息	213

前言

本手册介绍东软应用交付安全网关（Neusoft Application Delivery Security Gateway，以下简称 ADSG）的功能、配置和监控。

本手册的编写面向配置和管理 ADSG 的管理用户，阅读本手册的管理用户需具有一定的网络基础知识，并了解 TCP/IP 协议。

本手册内容由以下部分组成：

- [第 1 章，产品简介](#)，概要介绍 ADSG 的部署场景、工作原理及主要功能。
- [第 2 章，快速向导](#)，介绍如何使用 WebUI 快速配置 ADSG。
- [第 3 章，虚拟服务](#)，介绍如何通过配置虚拟服务器、资源路径、服务器组和静态/云服务器以及各种应用交付功能，以保证客户业务快速、稳定、可靠地交付。
- [第 4 章，Web 安全](#)，介绍如何通过配置针对性的安全策略以及全局性的主动防御、DDoS 防御和漏洞扫描，过滤客户端流量，保护后端服务器不受攻击威胁，并保证 Web 应用的安全交付。
- [第 5 章，公共对象](#)，介绍如何添加用户自定义 IP 地址集、ISP 地址集和用户地域，用于 ACL 访问控制和智能 DNS 配置。
- [第 6 章，DNS 代理](#)，介绍如何配置 DNS 透明代理，使 ADSG 代理内网 PC 进行域名解析，从而优化内网用户访问外网时的 DNS 解析过程。
- [第 7 章，智能 DNS](#)，介绍如何通过配置智能 DNS 功能，实现入站链路负载均衡和全局负载均衡。
- [第 8 章，网络配置](#)，介绍如何配置接口、VLAN、路由、DNS 等网络信息，以及端口映射、源地址转换、ACL 等策略信息。
- [第 9 章，系统配置](#)，介绍如何使用 ADSG 的配置向导、系统维护、管理访问控制、管理用户、日志设置、报警设置、报表设置、系统升级、时间同步、系统加速、高可用性、SNMP 服务等功能。
- [第 10 章，虚拟系统](#)，介绍如何创建虚拟系统和虚拟系统管理员，以及如何配置和管理虚拟系统。
- [第 11 章，状态监控](#)，介绍如何监控 ADSG 系统状态，查看日志和报表结果信息。管理员可以通过图形或图表化的系统监控信息、日志和报表直观地了解系统当前的运行状况、网络性能，发现网络中存在的问题，以便更好地维护系统性能和安全性。
- [第 12 章，范例](#)，通过范例说明如何配置 ADSG 的几种应用场景，包括服务器负载均衡、入站链路负载均衡、出站链路负载均衡、Web 安全防护和主动防御。

- [附录 A, 术语表](#), 说明手册中使用的各种术语的含义。
- [附录 B, 日志信息](#), 介绍 AD SG 系统日志和事件的描述、含义和处理方法。




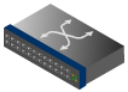




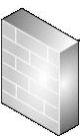

文本约定

文本约定

文本格式	描述
	菜单命令以半角大于号">"分隔。
菜单命令	例如： 选择 系统 > 维护 > 许可 。

图标约定

图标约定

图标	描述	图标	描述
	互联网		网线
	路由器		交换机
	ADSG		客户端
	物理服务器		虚拟服务器
	网络防火墙		公有云/私有云实例

第1章 产品简介

ADSG 部署在数据中心以及服务器集群前端，模拟真实服务器向客户端提供应用交付功能，同时为服务器资源提供应用级的安全防护。ADSG 的主要作用包括：

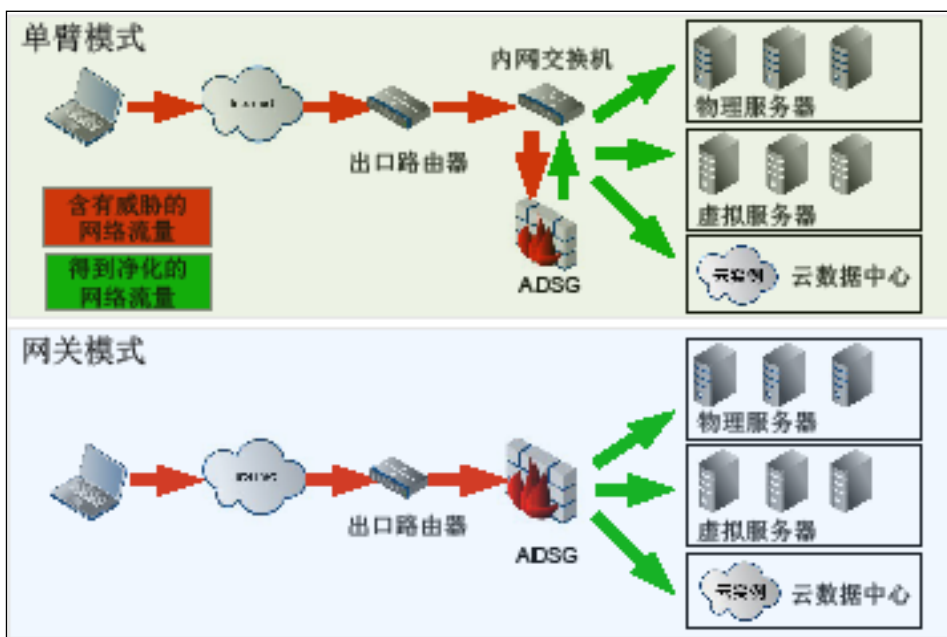
- 根据负载均衡策略将客户端流量合理地转发到真实的服务器，保证服务器端资源得到充分利用。
- 对客户端的数据流量进行安全检查，保护服务器端免受网络攻击。
- 在分流的同时，实时监听系统资源使用情况、本地流量及服务器池负载状态等指标，并且依据管理员对服务器池的属性配置，及时地增减服务器。
- 根据链路负载均衡策略为入站和出站流量选择最佳路径，充分利用链路带宽资源。

本章简单介绍 ADSG 的部署方式和主要功能，结构如下：

- [1.1 部署方式](#)
- [1.2 工作原理](#)
- [1.3 主要功能](#)

1.1. 部署方式

ADSG 主要部署在服务器前面，后端服务器可以是基于物理设备组成的数据中心、虚拟化数据中心以及云计算数据中心。ADSG 两种常见的部署方式如下图所示：



ADSG 接收客户端请求后，根据配置的负载均衡算法分发给真实的后端服务器，然后再将后端服务器的响应流量转发给客户端。

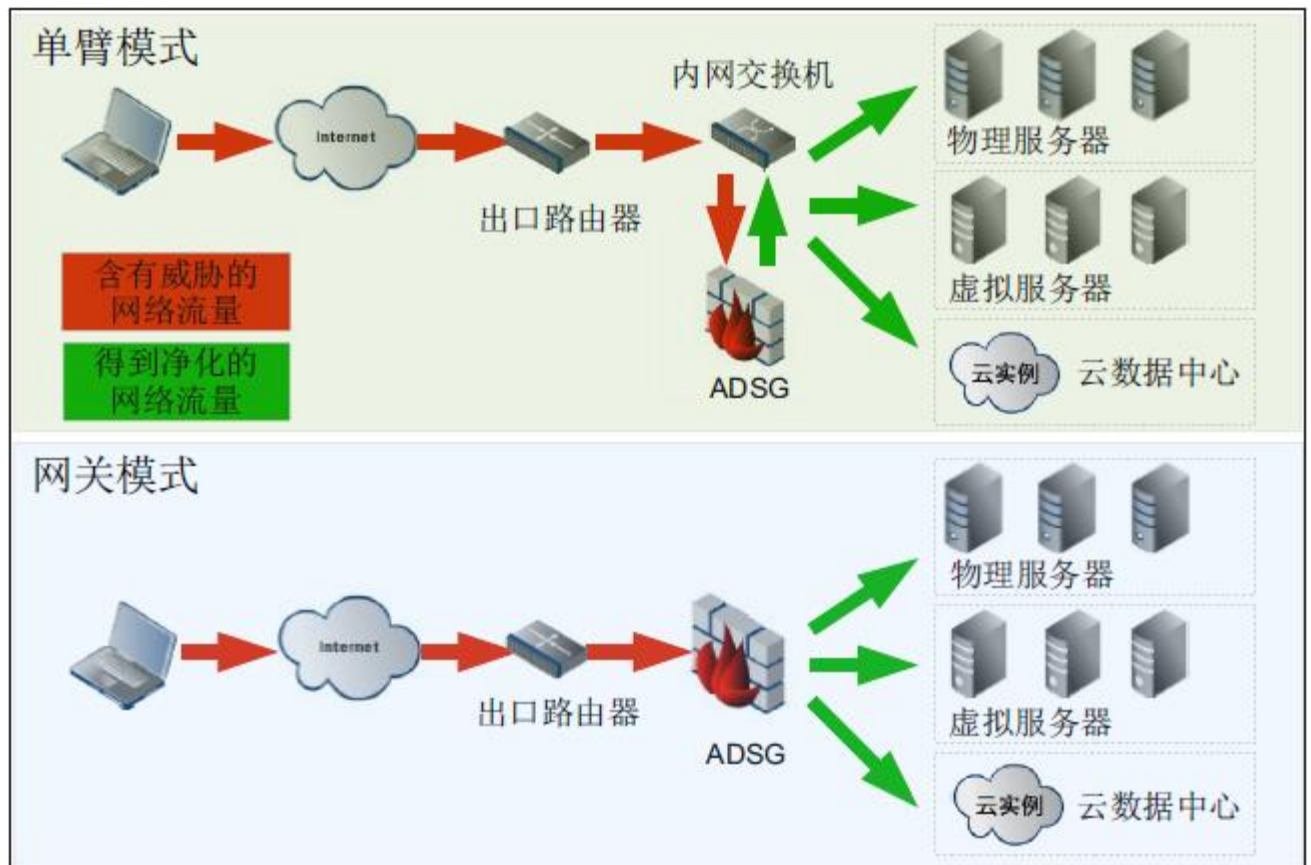
1.2.工作原理

- [1.2.1 服务器负载均衡](#)
- [1.2.2 出站链路负载均衡](#)
- [1.2.3 入站链路负载均衡](#)
- [1.2.4 全局负载均衡](#)

1.2.1. 服务器负载均衡

ADSG 的核心功能是虚拟服务，即通过创建虚拟服务器，映射、调用后端真实服务器资源，来模拟真实服务器对外提供应用交付服务。

ADSG 的虚拟服务支持七层和四层流量：



名词解释：

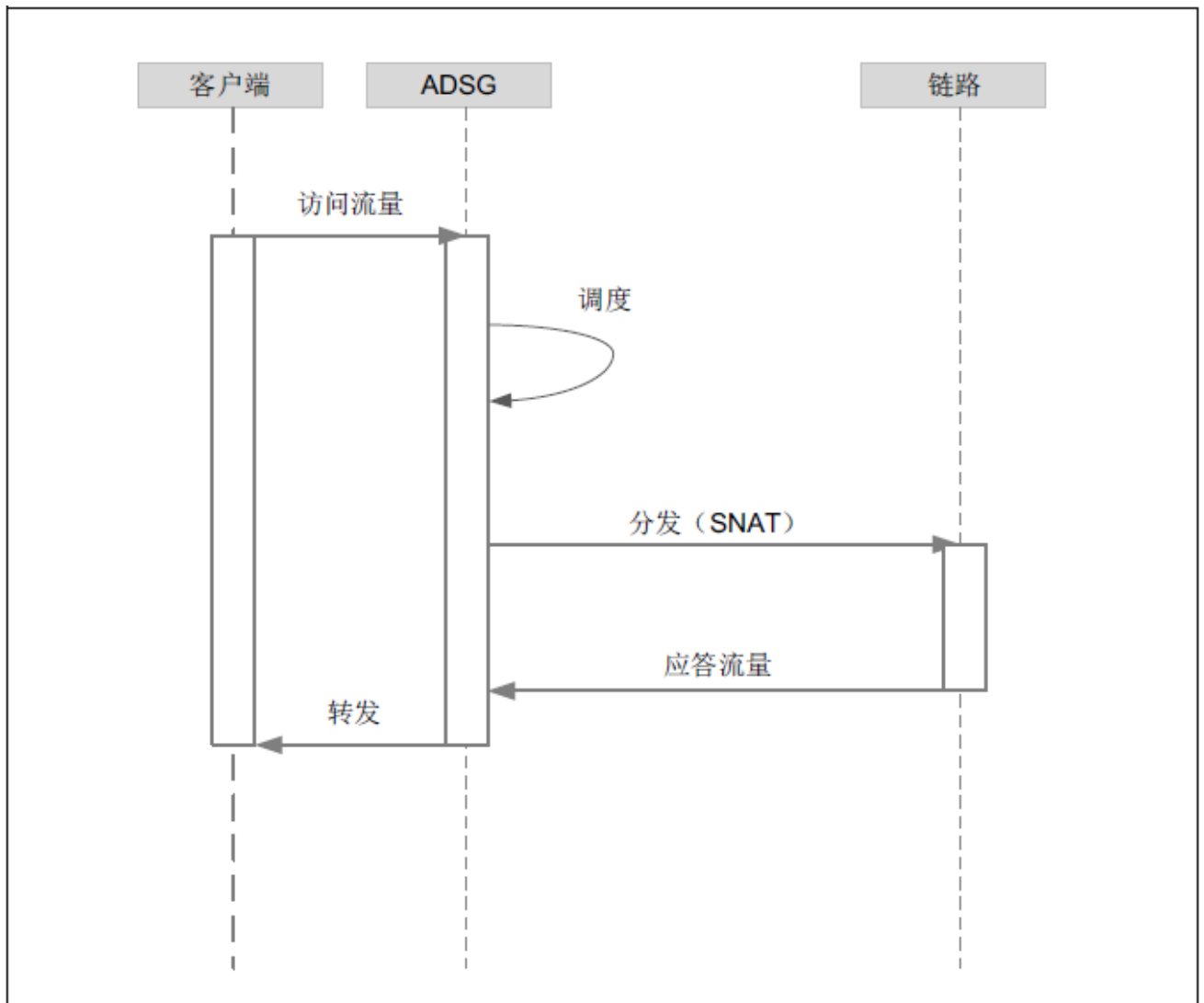
- | | |
|----------|--|
| Vserver | 虚拟服务器，代替真实服务器为终端用户提供服务。
ADSG 通过虚拟 IP 地址（VIP）对外提供服务。 |
| Location | 资源路径，终端用户要访问的资源对应的 URI 地址。
一个资源路径可映射到多个服务器组。 |

Pool	服务器组，一组静态/云服务器。
Static	静态服务器/云服务器，ADSG 保护的后端真实服务器。
Server/Cloud	静态/云服务器需要被分配到服务器组中。
Server	

1.2.2. 出站链路负载均衡

ADSG 出站链路负载均衡主要通过智能路由选取链路，再采用 SNAT 将源地址转换为链路出口的 IP 地址。工作流程如下所示：

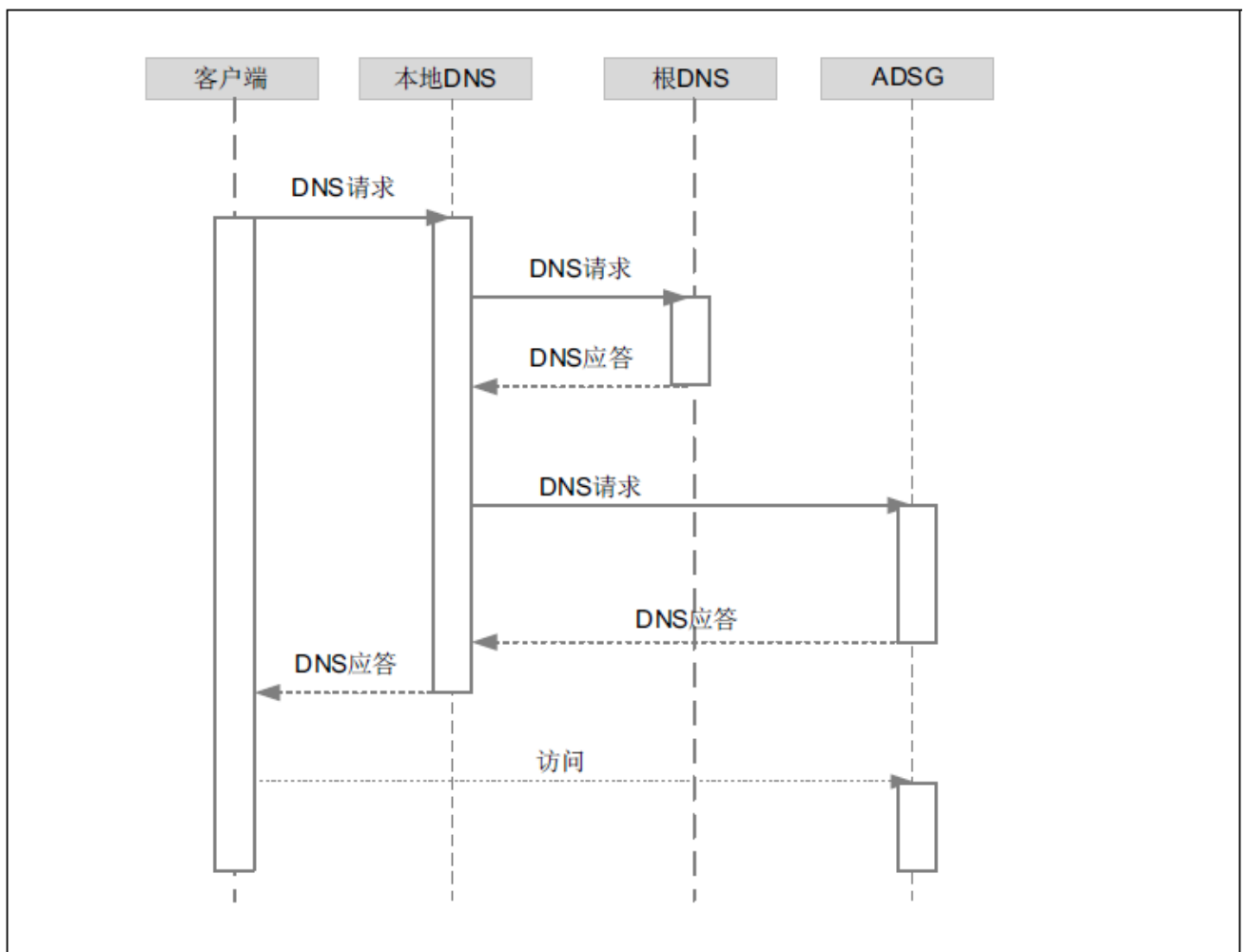
1. ADSG 接收用户访问流量；
2. 根据所访问资源和链路负载均衡算法将流量分配到相应链路，并做 SNAT；
3. 接收目的地址返回的应答流量并转发给用户。



1.2.3. 进站链路负载均衡

ADSG 通过智能 DNS 提供进站链路负载均衡服务，智能 DNS 的工作流程如下所示：

1. 用户向其本地 DNS 服务器发起域名解析请求；
2. 本地 DNS 服务器通过递归查询向根 DNS 发起查询；
3. 根 DNS 服务器回复本地 DNS 服务器，应向 ADSG 发起域名解析请求；
4. 本地 DNS 服务器向 ADSG 发起查询，ADSG 向本地 DNS 服务器回复最佳路径 IP 地址；
5. 本地 DNS 服务器向用户反馈路径 IP 地址；
6. 用户根据本地 DNS 服务器反馈的 IP 地址访问服务器。



1.2.4. 全局负载均衡

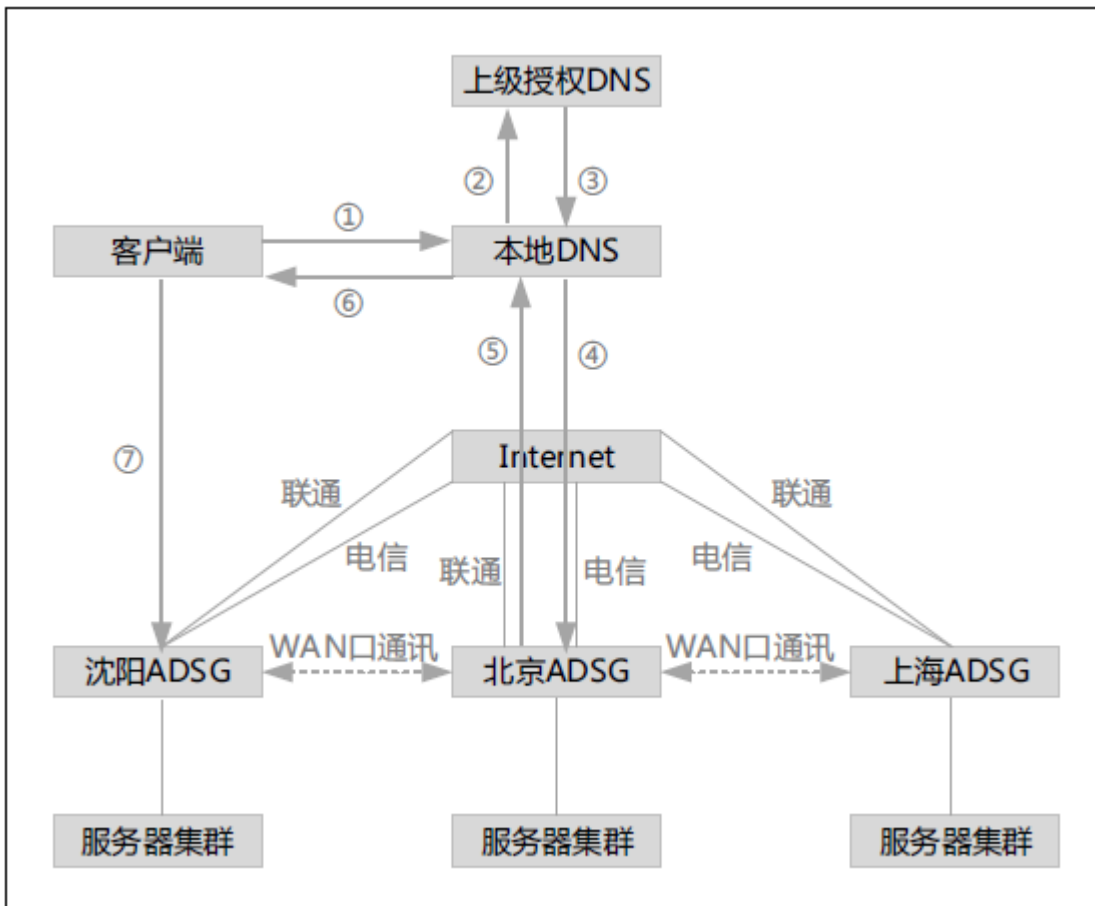
1. 用户访问服务域名，如 `www.example.com`，向本地 DNS 服务器请求域名解析，若本地 DNS 服务器有相应的记录则直接返回 IP。
2. 若本地 DNS 服务器无记录，则向其上级授权服务器发起请求。

3. 上级授权服务器给本地 DNS 服务器返回 NS 记录，告诉本地 DNS 由北京 ADSG 负责域名解析。
4. 本地 DNS 向北京 ADSG 发送对域名 www.example.com 的解析请求。

假设用户为沈阳联通 IP，则北京 ADSG 通过两级调度，将其调度至沈阳 ADSG 的联通 IP 上。对沈阳 ADSG 的联通 WAN 口进行健康和繁忙检查，决定是否返回该 IP。

（北京 ADSG 对其他位置 ADSG 的 WAN 口进行探测，以确定其健康状态，其他位置 ADSG 向北京 ADSG 发送自己 WAN 口的繁忙状态。）

5. 北京 ADSG 返回 IP 地址给本地 DNS。
6. 本地 DNS 将 IP 转发给用户，并缓存。
7. 用户获得 IP 后，访问沈阳数据中心。



1.3. 主要功能

ADSG 主要提供以下功能：

- [1.3.1 应用交付](#)
- [1.3.2 应用安全](#)
- [1.3.3 日志和报表](#)
- [1.3.4 Nginx 脚本编辑器](#)

1.3.1. 应用交付

- 链路负载均衡

ADSG 通过智能 DNS 功能提供入站链路负载均衡（单一站点）和全局负载均衡（多站点），为外网用户访问内网服务就近选择最佳访问路径；通过智能路由和源地址转换功能提供出站链路负载均衡，为内网用户访问外网选择最佳访问路径。

入站和出站链路负载均衡可以充分利用现有带宽资源，提升网络访问速度和用户访问体验，适用于存在多条运营商链路以及多地部署服务器的场景。

ADSG 出厂自带 ISP 地址集且可以自动更新，极大地提升了链路负载均衡的准确性和管理员配置的便利性。

- 服务器负载均衡

ADSG 服务器负载均衡功能是将客户端流量进行分流，对服务器端的负载进行智能调节，从而最大限度地提高服务器的工作效率。

ADSG 的服务器负载均衡支持链路探测功能，自动检测服务器的工作状态。

ADSG 还可以通过 SNMP 获取后端服务器的系统资源使用情况，用于辅助判断服务器的负载权重。

- 健康状态监控

ADSG 可以实时监控与后端服务器的链路状态：当一台服务器出现故障或被移除时，ADSG 根据负载均衡算法将流量分发给其他服务器；当故障服务器恢复工作时，ADSG 还能继续向其转发流量。此功能使 ADSG 具有高容错性。

ADSG 还可以实时监控 WAN 口链路的健康状态，原理同上。

- 会话保持

ADSG 支持基于会话的服务器负载均衡和出站链路负载均衡。管理员开启会话保持功能后，当 ADSG 接收到数据流时，首先检查该数据流是否属于已建立连接的会话。如果属于已建立连接的会

话，那么数据流仍将被转发到与该会话建立连接的服务器或出口接口；否则，会依据管理员的配置处理。

当开启会话保持功能时，管理员可以设置后端服务器的延迟停机时间，保证服务器平滑退出。

- 持久连接

ADSG 可以复用现有的 TCP 连接直接将客户端的 HTTP 请求转发给服务器，从而提高服务器的响应速度。

管理员可以设置 ADSG 与后端服务器之间的最大持久连接数。

- 反向代理

反向代理（Reverse Proxy）是指 ADSG 代表内网服务器接收来自外网客户端的请求，然后将请求转发给内网服务器，并将从服务器接收到的应答返回给客户端。此时，ADSG 对外就表现为一个服务器。

ADSG 面向客户端和服务器端分别提供反向代理功能。

- 内容缓存

ADSG 可以缓存一些后端服务器的响应，在下次相同请求到来时直接返回给客户端。

- HTTP 数据压缩

ADSG 支持对 HTTP 服务器的响应进行压缩，以提高响应速度。

- SSL 卸载和封装

SSL 加密功能使得客户端与 ADSG 之间以及 ADSG 与后端服务器之间可以使用 SSL 加密链路进行通信，避免信息明文传输带来的安全隐患。

ADSG 面向客户端提供 SSL 解封装功能。此种情况下，ADSG 将与客户端建立 HTTPS 连接，并将客户端发来的数据解密，再进行后续处理。

ADSG 面向后端服务器提供 SSL 封装功能。此种情况下，ADSG 将与后端服务器建立 HTTPS 连接，并支持双向证书认证，将客户端的数据加密后发往后端服务器。

- URL 重写

URL 重写规则用于修改 HTTP 请求中的 URL，并使用修改后的 URL 继续处理请求，最终访问后端服务器组中的 Web 资源。

- 域名解析容错

当后端服务器使用动态 IP 地址时，只能使用域名来识别服务器。这时，ADSG 需要配置 DNS 服务器用于域名解析。针对静态服务器域名解析失败的情况，用户可以设置 ADSG 的容错处理机制。

- 云计算服务器节点自动缩放

通过与云计算平台（如 AWS）联动，可以定时对云计算环境中的服务器实例进行弹性扩展；通过对服务器流量负荷的感知，可以根据管理员设定的相关阈值以及当前根据业务流量的大小完成对服务器实例的弹性扩展。

1.3.2. 应用安全

- 访问控制（ACL）

ADSG 支持包过滤功能，对用户访问进行精确控制。ADSG 不但可以控制是否允许特定流量经过，还可以限制到特定虚拟服务器的连接数。

- 全局白名单

此功能可允许一些符合条件的流量跳过某些特定的安全检查。

- 主动防御

ADSG 的主动防御功能基于主动学习模式，分为学习阶段和防御阶段：在学习阶段基于白名单的方式建立安全访问模型；在进入防御阶段后，系统将针对不符合安全模型的访问进行打分，当分值达到设定阈值后，该访问将作为恶意请求处理。

系统的安全访问模型基于东软在安全领域多年积累形成的核心威胁库构建而成，不仅能够防御诸如 SQL 注入、跨站脚本等知名攻击手段，而且基于宽泛的安全规则集合，可以防范未知攻击。

- DDoS 防御

ADSG 可以通过 TCP 半连接缓解、TCP 连接数限制、SYN Cookie、机器人识别、基于访问特征的 HTTP 访问速率限制等手段，防御和缓解 TCP SYN flood、HTTP Request flood、UDP Flood、ICMP Flood 等形式的 DDoS 攻击。

- 机器人攻击防御

很多黑客通过工具发送少量特定的应用层请求到指定网站，使服务器执行一系列杂乱、耗时的操作，最终导致服务器不堪重负，无法响应正常的请求。这种类型的攻击叫做机器人攻击（又叫“应用层 DDoS 攻击”）。

由于机器人攻击报文发送速率低，使得传统的基于网络层和传输层的 DDoS 防御模块很难检测到。ADSG 能够通过验证请求发送端是否为正常浏览器的方式，保证服务器免受防机器人攻击的困扰。

- 入侵防御

现今互联网上针对服务器的攻击事件层出不穷，常见的攻击有：跨站脚本攻击、SQL 注入攻击、缓冲区溢出、后门和木马、常见注入攻击等。ADSG 的入侵防御功能可以保护服务器免受这些常见攻击的威胁。ADSG 同时还提供攻击签名规则集检测其他类型的攻击。

- HTTP 协议约束

HTTP 协议约束主要是根据 HTTP 协议自身的属性（报文头、报文体长度等）去分析客户端请求内容，并根据分析的结果决定对客户端请求的下一步处理动作。

- 网页防篡改

ADSG 的网页防篡改功能通过预先生成网站资源指纹，并在访问请求到达时检测待访问网页的指纹是否发生变化，据此判断网页是否被异常更改。当检测到网页被异常更改后，根据预先的配置将终止本次访问或者给客户端返回事先备份的网页，从而达到防止被篡改网页外泄的目的。

- 信息泄露防护

本功能通过对后台敏感信息进行替换或者对包含敏感信息的应答进行阻断的方式，来防止后端服务器中的敏感信息泄露给客户端。

- 漏洞扫描

ADSG 可以扫描内部服务器的系统漏洞，并且将扫描结果进行文档记录以供下载，便于管理员了解内部服务器存在的漏洞。同时，ADSG 能够自动生成安全策略用来应对内部服务器的漏洞。

1.3.3. 日志和报表

ADSG 可以将流量、攻击、事件等信息以日志的形式记录下来，并且可以将指定时间段内的日志信息形成报表，以数据和图表的形式展现。

1.3.4. Nginx 脚本编辑器

ADSG 基于 SEngine 软件开发，对于熟悉 SEngine/Nginx 的用户而言，直接编辑其配置文件也是一种常用的配置手段。为此，ADSG 在 WebUI 上提供了高级配置功能，管理员可以通过手工录入 SEngine/Nginx 命令的方式来编辑其配置文件。ADSG 的高级配置功能不仅允许用户对虚拟服务模块进行配置，也允许对其他模块进行配置。

1.3.5. 虚拟系统

一个 ADSG 系统可以在逻辑上划分为多个虚拟系统，每个虚拟系统可以被看成一个独立的 ADSG 系统，拥有独立的管理 IP、负载均衡策略和安全策略。

第2章 快速向导

本章介绍如何快速完成 ADSG 的配置，内容包括：

- [2.1. 修改缺省管理 IP](#)
- [2.2. WebUI 介绍](#)
- [2.3 配置逻辑](#)
- [2.4 配置步骤](#)

2.1. 修改缺省管理 IP

ADSG 出厂默认管理 IP 和管理员信息如下：

- 管理 IP 地址：192.168.1.100/24
- 管理员名称/密码：admin/neteye

用户首次使用 ADSG 设备，可以通过两种方式修改缺省管理 IP 地址：

- [2.1.1. 通过 Console 修改缺省管理 IP](#)
- [2.1.2 通过 WebUI 修改缺省管理 IP](#)

2.1.1. 通过 Console 修改缺省管理 IP

ADSG 支持通过 Console 修改管理 IP、网关、DNS 服务器地址和打印配置信息。

要使用 Console 初始化 ADSG，请选用任何兼容标准 VT100 并带有 RS-232 接口（标准 DTE 接口）的终端或模拟终端，并进行如下配置：

- 波特率：9600
- 奇偶校验位：无
- 数据位：8
- 停止位：1

将管理主机连接 ADSG 的 Console 口，按照提示进行相关配置：

1. 打开 Console 管理界面，输入缺省用户名和密码（admin/neteye）登录：

```
Neusoft ADSG 1.3
localhost login: admin
Password:
```

2. 出现 7 个菜单选项，根据提示输入选项 1，选择修改缺省的管理 IP 地址：

```
NetEye ADSG Control Center

Please choose the number to enter each option:
1) IP Address Settings
2) Default Gateway Settings
3) DNS Settings
4) SSH Management Settings
5) Print Configuration
6) Quit and Save
7) Quit
>1_
```

3. 根据提示选择网卡：

```
IP Address Settings, choose NIC:
1) eth0
   IP: n/a
2) Go Back
>1
```

提示：管理IP地址固定配置在第一个以太网接口 eth0 上。

4. 根据提示输入新的管理 IP 地址和掩码地址：

```
Input IP Address(q to cancel)>10.1.3.108
Input Netmask(Dotted decimal notation only, q to cancel)>255.255.248.0

Set IP Address(eth0: 10.1.3.108/21) OK!
```

5. 根据提示输入菜单 2 返回主菜单：

```
IP Address Settings, choose NIC:
1) eth0
   IP: 10.1.3.108/255.255.248.0
2) Go Back
>2
```

6. 在主菜单界面选择 2，根据提示输入网关 IP 地址，然后输入 2 返回主菜单：

```
Please choose the number to enter each option:
1) IP Address Settings
2) Default Gateway Settings
3) DNS Settings
4) SSH Management Settings
5) Print Configuration
6) Quit and Save
7) Quit
>2

Default Gateway Settings, choose NIC:
1) eth0
   IP: 10.1.3.108/255.255.248.0 gw n/a
2) Go Back
>1
Input Gateway's IP(q to cancel)>10.1.1.1

Set Default Gateway(eno16777736:10.1.1.1) OK!

Default Gateway Settings, choose NIC:
1) eth0
   IP: 10.1.3.108/255.255.248.0 gw 10.1.1.1
2) Go Back
>2
```

7. 根据提示设置 DNS 服务器地址：

```
Please choose the number to enter each option:
1) IP Address Settings
2) Default Gateway Settings
3) DNS Settings
4) SSH Management Settings
5) Print Configuration
6) Quit and Save
7) Quit
>3

DNS Settings, choose option:
1) Set DNS Server()
2) Go Back
>1
Input DNS Server's IP(q to cancel)>202.107.117.11

Set DNS Server(202.107.117.11) OK!

DNS Settings, choose option:
1) Set DNS Server(202.107.117.11)
2) Go Back
>2
```

8. 在主菜单界面选择 5，打印当前配置信息：

```
Please choose the number to enter each option:
1) IP Address Settings
2) Default Gateway Settings
3) DNS Settings
4) SSH Management Settings
5) Print Configuration
6) Quit and Save
7) Quit
>5

Current Configuration:
Interfaces:
  eth0: 10.1.3.108/255.255.248.0
Default Gateway:
  eno16777736: 10.1.1.1
DNS Server:
  202.107.117.11
```

2.1.2. 通过 WebUI 修改缺省管理 IP

管理客户机要求与 ADSG 处于同一局域网，且至少安装以下任意一种浏览器：

- IE 8.0 及以上版本
- FireFox 7.0 及以上版本
- Google Chrome 26.0 及以上版本
- Opera 20.0 及以上版本

登录 WebUI 界面：

1. 为管理客户机添加 192.168.1.0/24 网段的 IP 地址，如 192.168.1.200/24。
2. 在浏览器中输入 <https://192.168.1.100:9000/>。
3. 出现如下安全提示：



4. 点击[继续浏览此网站（不推荐）](#)，出现如下登录界面：



输入缺省用户名 admin 和密码 neteye，点击[登录](#)。

如果在 5 分钟内连续登录失败 3 次，账号将被锁定 10 分钟。此处还可以修改系统语言。

登录成功后建议修改缺省密码。

点击**更改**可更改系统显示语言，可选择简体中文或 English。

5. 选择**网络>接口>接口**，双击 eth0 接口，修改缺省管理 IP 地址。

接口	WAN	LAN				
状态	名称	IP地址	MAC地址	速率	双工	备注
↑	eth0	192.168.1.100/24	00:90:fb:51:46:8b	100Mb/s	Full	
↓	eth-s1p1		08:35:71:07:e2:fc	auto	auto	
↓	eth-s1p2		08:35:71:07:e2:fd	auto	auto	

2.2.WebUI 介绍

为了便于描述，我们将 WebUI 页面分为导航区、视图区、配置区、操作按钮区、快捷菜单区、错误提示去六个区域。



导航区 通过点击导航菜单，可以打开相应功能的配置页面。

视图区 用于查看当前配置信息。






- 选中某配置项，可以在下方配置区修改其配置。
- 如果视图区空白，点击鼠标右键可以添加条目。
- 右键点击配置节点，可以选择更多配置菜单。
- 鼠标指向列表头，单击右侧出现的向下箭头，可设置列表排序属性和可见字段。再次点击向下箭头，则可取消排序。

- 直接单击列表头，可根据该列对列表条目进行排序（按首字母或数字排序）。

配置区 用于修改配置信息。和查看区选中的配置项对应。
鼠标指向某些配置参数，界面会提示该参数的解释说明和配置提示。

操作按钮区 用于对配置信息进行刷新、删除、保存等操作。

快捷菜单区 显示以下快捷菜单：

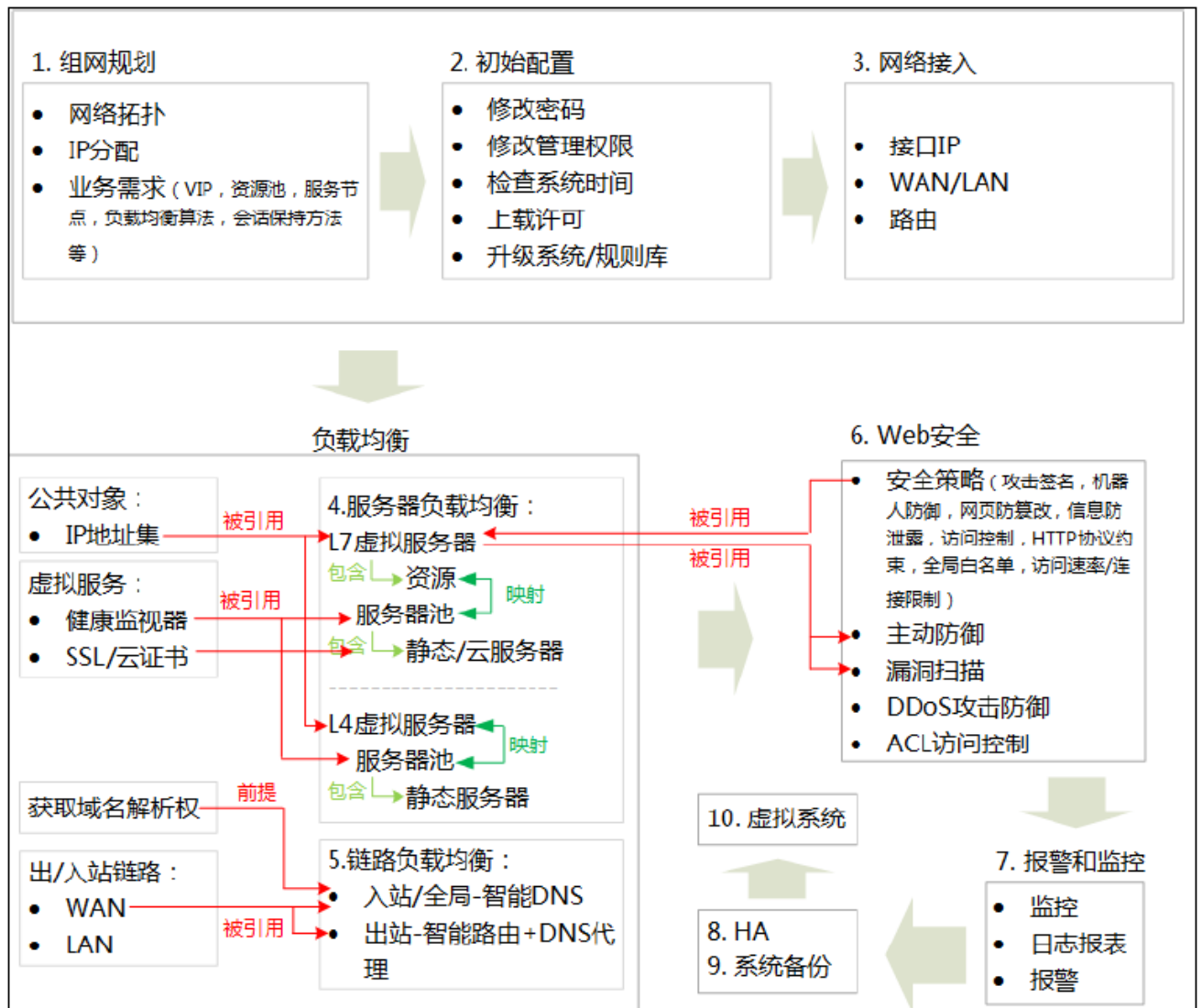
-  admin：显示当前登录的管理用户名称。
- ：点击修改当前登录的管理用户的密码。
- ：点击修改系统语言。
- ：点击使用配置向导完成七层流量管理基础框架配置。
- ：点击退出系统。

错误提示区 绿色字体表示操作成功，红色字体表示操作失败，鼠标悬浮时，显示对应错误消息。

其他区域 左上角显示系统名称，右上角显示系统时间，左下角显示软件版本，右下角显示版权信息。

2.3.配置逻辑

ADSG 的配置逻辑如下图所示：



提示：

- 服务器负载均衡是 ADSG 的核心功能，一般情况下必配。
- 链路负载均衡为增值功能，用户可选配。
- Web 安全是针对 Web 应用的防护，可配合七层服务器负载均衡使用，也可独立使用。
- HA 是避免单点故障的保障，一般必配。
- 虚拟系统的配置逻辑同根系统一致。

2.4. 配置步骤

首次登录后，推荐按照以下顺序完成系统配置：

ADSG 快速配置步骤

配置对象	配置内容	操作路径	备注
1.组网规划	1) 规划组网拓扑。		具体到网络设备物理端口、服务器网卡的分配与连接。
	2) 规划 IP 地址分配。		具体到网络设备和服务器网卡的 IP 地址分配。
	3) 确定业务需求。		具体到对外提供服务的 VIP、后端服务器成员池、服务器节点、负载均衡算法、会话保持方法等。
2.初始配置	1) 修改密码。	界面右上角的快捷菜单 	
	2) 修改管理权限。 (Web/SSH 方式)	系统>管理设置	系统默认允许所有 IP 地址的管理访问。
	3) 检查系统时间。	系统>日期/时间设置	为了使系统日志能够准确记录事件发生的时间，供管理员排错或维护时参考，需保证系统时间的准确性。
	4) 上载许可。	系统>系统维护>许可 请将系统主机 ID 号发送给 供货商，获取许可文件。	许可 (License) 限制 ADSG 的最大虚拟服务器数量及相关功能的可用性。 如未上载许可，则四层和七层默认各限制使用两个虚拟服务器；如上载许可，则虚拟服务器数量没有限制。
	5) 升级系统/规则库。	系统>升级设置	升级过程中经过 ADSG 的流量会中断，请谨慎选择升级时间。
3.网络接入	1) 根据组网规划配置接口、WAN 和 LAN。	网络 >接口	透明模式则需要划分 VLAN： 网络>VLAN
	2) 根据组网规划配置路由信息。	网络 >路由>静态路由	
4a.七层服务器负载均衡	1) 添加虚拟服务 IP 地址集。	公共对象>IP 地址集	七层服务器负载均衡针对 HTTP 和 HTTPS 流量进行智能调度。

虚拟 IP 地址集只能包含虚拟服务器的 VIP，一般设为浮动 IP。

	2) 自定义健康监视器。	虚拟服务>健康监视器	也可以使用系统自带的健康监视器。在服务器组中引用。
	3) 创建七层虚拟服务器并添加资源。	虚拟服务>流量管理（七层）>虚拟服务器	熟悉 Nginx 的用户可使用 Nginx 命令配置虚拟服务器和资源。
	4) 创建服务器组，并关联虚拟服务资源。	虚拟服务>流量管理（七层）>服务器组	右键添加服务器组，右键点击引用关联资源。
	5) 向服务器组中添加静态服务器。	虚拟服务>流量管理（七层）>服务器组>静态服务器	如果要为静态服务器设置域名，需提前设置 DNS 服务器地址。
	6) 添加云证书，向服务器组中添加云服务器。	虚拟服务>云证书 虚拟服务>流量管理（七层）>服务器组>云服务器	ADSG 可与公有云平台联动，实现服务器自动缩放，更合理地使用服务器资源。
4b.四层服务器负载均衡	1) 添加虚拟服务 IP 地址集。	公共对象>IP 地址集	四层服务器负载均衡针对 TCP 和 UDP 流量进行智能调度。
	2) 自定义健康监视器。	虚拟服务>健康监视器	在服务器组>基本配置页面选择健康监视器。
	3) 创建四层虚拟服务器。	虚拟服务>流量管理（四层）>虚拟服务器	如配置了 HA，虚拟服务的 VIP 和 Local IP 均为 HA 浮动 IP。
	4) 创建服务器组，并添加静态服务器。	虚拟服务>流量管理（四层）>服务器组	右键添加服务器组和静态服务器。
	5) 关联虚拟服务器和静态服务器组。	虚拟服务>流量管理（四层）>虚拟服务器>关联到	
5a.入站链路负载均衡（单站点）	1) 获取域名解析权。	到域名服务提供商处申请 2 个 DNS 记录：NS 记录将用户访问的域名映射到 ADSG 提供的域名；A 记录将 ADSG 提供的域名映射到虚拟服务器 IP。	入站链路负载均衡用于解决用户跨运营商访问服务时网络速度慢的问题。

	2) 配置 WAN 和 LAN，并为 WAN 指定健康监视器。	网络>接口>WAN	WAN 的上下行带宽繁忙比例用于入站链路繁忙保护。
	3) 开启智能 DNS 服务，设置监听范围，选择工作模式。	智能 DNS>DNS 服务器	单一站点入站链路负载均衡选择本地工作模式。
	4) 创建虚拟 IP 池，添加可调度的虚拟服务 IP，并指定调度策略。	智能 DNS>虚拟 IP 池	如果想按运营商链路调度，请选静态就近性策略。
	5) 添加域名与虚拟 IP 池的映射关系。	智能 DNS>DNS 映射	根据访问的域名判断可调度的虚拟 IP 池。
	6) 添加 ISP 地址段类型的 LDNS 集合。	智能 DNS>LDNS 集合	用于判断用户所属运营商链路。
	7) 添加虚拟 IP 池级别的静态就近性策略。	智能 DNS>静态就近性>虚拟 IP 池级别	根据所属运营商链路为指定用户选取地址池内虚拟 IP。
5b.入站链路全局负载均衡 (多站点)	1) 获取域名解析权。	到域名服务提供商处申请 2 个 DNS 记录：NS 记录将用户访问的域名映射到 ADNSG 提供的域名；A 记录将 ADNSG 提供的域名映射到虚拟服务器 IP。	入站链路全局负载均衡用于在多地部署服务器提供服务时实现用户就近访问，提升访问速度。
	2) 配置 WAN 和 LAN，并为 WAN 指定健康监视器。	网络>接口>WAN	WAN 的上下行带宽繁忙比例用于入站链路繁忙保护。
	3) 开启智能 DNS 服务，设置监听范围，选择工作模式。	智能 DNS>DNS 服务器	多站点入站链路负载均衡选择全局工作模式。
	4) 创建虚拟 IP 池，添加可调度的虚拟服务 IP，并指定调度策略。	智能 DNS>虚拟 IP 池	多站点入站链路负载均衡建议按用户地域添加虚拟 IP 池。 如果想按运营商链路调度，添加 IP 池时请选静态就近性策略。
	5) 添加域名与虚拟 IP 池的映射关系。	智能 DNS>DNS 映射	根据访问的域名判断可调度的虚拟 IP 池。

6) 添加用户地域类型和 ISP 地址段类型的 LDNS 集合。	智能 DNS > LDNS 集合	用于判断用户所属地域和运营商链路。
7) 添加 DNS 映射级别的静态就近性策略。	智能 DNS > 静态就近性 > DNS 映射级别	根据用户所属地域判断可调度的虚拟 IP 池。
8) 添加虚拟 IP 池级别的静态就近性策略。	智能 DNS > 静态就近性 > 虚拟 IP 池级别	根据用户所属运营商链路判断地址池内应该返回的虚拟 IP。
9) 添加本地站点和其他各地站点，指定用于站点间通讯的 IP/端口以及站点角色。	智能 DNS > 站点集合	通讯 IP/端口用于站点间同步配置信息，站点角色用于判断哪些站点负责接收 DNS 请求并调度，哪些站点仅接收访问请求。
10) 登录 None 或其他 Master 角色 ADSSG，同步配置信息： a) 配置本地站点信息； b) 同步已配 Master 的配置到本地。	智能 DNS > 站点集合 智能 DNS > 全局配置同步	如果本端为 None，仅同步对端 Master 的站点集合到本地； 如果本端为 Master，同步对端 Master 的站点集合和所有智能 DNS 配置到本地。
5c. 出站链路负载均衡	网络 > 接口 > WAN	当用户网络有多个运营商出口链路时，用于提升内网用户访问互联网的速度。 WAN 的上下行带宽繁忙比例用于出站链路繁忙保护。
	网络 > 智能路由	为用户选择出站链路。
	网络 > 源地址转换	将内网主机 IP 转换为外网 IP，使其能够访问外网。
	DNS 代理 > 网关 DNS DNS 代理 > 透明代理 DNS 代理 > 前置调度 DNS 代理 > 内网记录	先添加用于域名解析的外网 DNS 服务器，再开启并设置 DNS 透明代理。 前置调度策略和内网 DNS 记录可选配。
6.Web 安全	Web 安全 > 安全策略 虚拟服务 > 流量管理（七层） > 虚拟服务器 > 资源路径基本配置 > 安全策略	可配置以下安全策略：攻击签名、网页防篡改、信息泄露防护、访问控制、HTTP 协议约束、全局白名单、机器人防御、访问速率限制、访问链接限制。
	Web 安全 > 主动防御	需事先配置七层虚拟服务器。

	3) 配置 DDoS 防御。	Web 安全>DDoS 防御	
	4) 配置漏洞扫描。	Web 安全>漏洞扫描	仅支持对 up 状态的服务器进行漏洞扫描。
	5) 配置 ACL 访问控制。	网络> ACL 配置>基本 ACL 控制	ADSG 默认允许所有访问流量通过, ACL 访问控制列表主要用于限制外网用户对内网服务器的访问。
7.报表和监控	1) 查看系统运行状态。	查看>首页	
	2) 查看流量和统计信息。	查看>监控>监控/统计	
	3) 配置日志策略, 查看日志信息。	系统>日志设置 查看>日志	
	4) 生成报表计划, 生成报表, 查看报表结果。	系统>报表设置 查看>报表	
	5) 配置报警策略。	系统>报警设置	通过邮件接收报警信息。
8.高可用性	配置高可用性。	系统> 高可用性	在主备设备上完成高可用性配置后, 登录备设备配置接口、路由和高可用性, 然后在主设备上点击同步按钮, 同步配置信息到备设备。两端虚拟路由器 ID 和浮动 IP 相同, 角色和同步接口 IP 相反。
9.系统备份	备份系统配置信息。	系统>维护>备份/恢复	同步信息除系统日志、诊断文件和 License。
10.虚拟系统	创建和管理虚拟系统。	以 root 管理员身份登录, 创建虚拟系统和虚拟系统管理员; 以虚拟系统管理员身份登录虚拟系统配置虚拟系统。	对系统资源要求较高, 仅高端机型支持。

第3章 虚拟服务

“虚拟服务”是 ADSG 的核心功能。所谓“虚拟服务”，就是通过虚拟的服务器向用户提供服务。要使用虚拟服务，管理员需要创建虚拟服务器并将虚拟服务器映射到后端真实服务器组。

ADSG 提供的应用交付功能如下表所示：

针对七层/四层流量的应用交付功能

层级	功能名称	配置位置	系统默认	可开关	备注
七层	1. SSL 加密	虚拟服务器	空	否	客户端--(https)-->ADSG--(https)-->服务器
	2. URL 重写	虚拟服务器	空	否	
	3. 内容缓存	资源路径	关闭	是	
	4. 内容压缩	资源路径	关闭	是	
	5. 反向代理	资源路径	空	否	针对客户端和服务端分别配置。
	6. 负载均衡	服务器组	开启	否	默认使用轮询算法，不能关闭。
	7. 会话保持	服务器组	关闭	是	
	8. 持久连接	服务器组	开启	是	
	9. 域名解析容错	服务器组	关闭	是	
	10. 自动负载均衡	静态服务器	关闭	是	仅当为服务器组选择基于权重的负载均衡算法时才可用。
	11. 延迟停机	静态服务器	关闭	是	仅当为服务器组开启会话保持功能时才可用。
	12. 云服务	云证书&云服务器	空	是	支持 SSL 加密和自动缩放。
四层	1. 会话保持	虚拟服务器	空	否	
	2. 负载均衡	服务器组	开启	否	默认使用轮询算法，不能关闭。 权重在静态服务器上配置。
	3. 自动负载均衡	静态服务器	关闭	是	仅当为服务器组选择基于权重的负载均衡算法时才可用。
	4. 延迟停机	静态服务器	关闭	是	

四/	健康状态监控	健康监视器	开启	是	全局配置，然后在四层或七层服务器组中引用。
----	--------	-------	----	---	-----------------------

七层

本章介绍如下内容：

- [3.1 七层流量管理](#)
- [3.2 四层流量管理](#)
- [3.3 健康状态监控](#)

3.1. 七层流量管理

ADSG 支持对 HTTP 和 HTTPS 等七层流量进行管理，实现应用交付。要对七层流量进行管理，需要先创建虚拟服务器、虚拟资源路径、服务器组、静态/云服务器，然后关联服务器组和虚拟服务器的资源路径，并根据需要配置相应的应用交付功能。

本节介绍如何配置七层流量管理，包括：

- [3.1.1 配置基础框架](#)

包括创建虚拟服务器、资源路径、服务器组、静态服务器，关联服务器组和虚拟服务器的资源路径。
- 在虚拟服务器上配置：
 - [3.1.2 SSL 加密](#)
 - [3.1.3 URL 重写](#)
- 在资源路径上配置：
 - [3.1.4 内容缓存](#)
 - [3.1.5 内容压缩](#)
 - [3.1.6 反向代理](#)
- 在服务器组上配置：
 - [3.1.7 负载均衡](#)
 - [3.1.8 会话保持](#)
 - [3.1.9 持久连接](#)
 - [3.1.10 域名解析（容错）](#)
- 在静态服务器上配置：
 - [3.1.11 自动负载均衡](#)
 - [3.1.12 延迟停机](#)

ADSG 的后端服务器除了支持静态服务器，还支持云服务器：

- [3.1.13 云服务](#)

3.1.1. 配置基础框架

用户可以通过配置向导或手动方式完成七层流量管理的基础框架配置。关于如何使用配置向导完成基础框架配置，请参见 [9.1 配置向导](#)。

ADSG 产品源自 SEngine 开源软件，对于熟悉 SEngine/Nginx 的用户而言，直接编辑其配置文件也是一种常用的配置手段。为此，ADSG 在 WebUI 上增加了脚本配置功能，可以通过手工录入 SEngine/Nginx 命令的方式来编辑其配置文件。ADSG 的高级配置功能不仅允许用户对虚拟服务模块进行配置，也允许对其他模块进行配置。

要手动完成七层流量管理的基础框架配置，请执行以下操作：

1. 选择**公共对象>IP 地址集**，为虚拟服务器添加一个虚拟 IP 地址集。

基本配置

名称: *

地址集

类型	取值
IPv4地址	202.118.113.11
IPv4地址	58.240.113.11

类型: ▼

IPv4地址: *

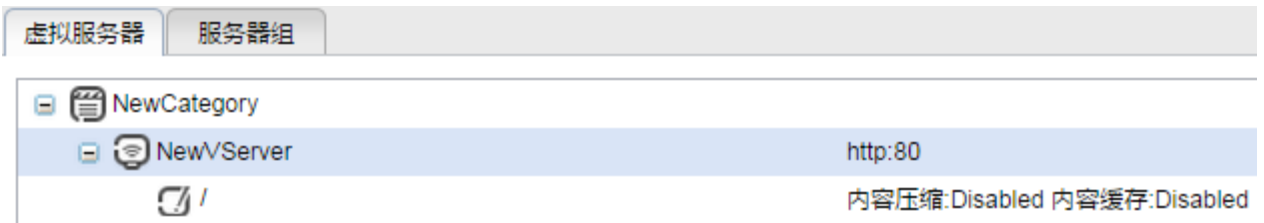
提示：虚拟服务器的IP地址集应包含单个IP地址或多个单IP（不能是IP地址段和子网IP），且必须与本地接口IP在同一网段。

2. 选择**虚拟服务>流量管理（七层）**。

3. 在视图区空白处点击右键，选择**添加虚拟服务器**。



此处也可以右键增加虚拟服务器的分类（Category），它类似于文件夹的功能，便于对多个虚拟服务器进行分类管理。可以通过拖拽的方式将创建的虚拟服务器拖入分类中。



提示：服务器组同样支持分类以及拖动操作，后续将不再赘述。

添加虚拟服务器条目后，可以在空白区域右键选择展开或收缩全部虚拟服务器条目。

右键选中虚拟服务器条目，可以选择添加资源路径、删除/启用/禁用虚拟服务器、展开/收缩虚拟服务器条目等操作。

4. 在下方配置区域，选择其中一种方式配置虚拟服务器的相关信息：


- 在**虚拟服务器基本配置**页签，根据需要设置虚拟服务器的配置参数。

参数	说明
服务器名称	虚拟服务器的名称，唯一标识一台虚拟服务器。
虚拟 IP 地址集	虚拟服务器对外提供服务的 IP 地址的集合。 虚拟 IP 地址要和设备的出口接口 IP 地址在同一网段。
缺省服务器	为同一端口上提供服务的多个虚拟服务器设置一个缺省服务器。 当匹配不到其他虚拟服务器时，ADSG 将转发客户端流量到缺省服务器。

- 透明代理** 可以以透明的方式访问后端真实服务器。此时，客户端直接访问后端服务器 IP，而不再访问虚拟服务器的地址，该虚拟服务器也不再承担负载均衡的功能。
这种配置多用于为后端的服务器提供透明模式的 Web 安全防护功能。
- 协议** 包括 HTTP 和 HTTPS。
启用 HTTPS 之前，需要先在 **SSL 证书** 页面导入或添加为该虚拟服务器签发的 SSL 证书。关于如何配置 SSL 加密，请参见 [3.1.2 SSL 加密](#)。
- 端口** 虚拟服务器对外提供服务的端口，提供不同服务的虚拟服务器通常配置不同的端口号。
通过 AD SG 访问虚拟服务器时，需要在浏览器中输入 AD SG 管理 IP 和端口号，例如 <http://192.168.1.100:8080> 和 <https://192.168.1.100:1443>。使用缺省端口号 80 时，则无需在 URL 地址最后加端口号。
- 域名** 虚拟服务器对外发布的域名或 IP 地址。
当不同的虚拟服务器使用相同的端口提供服务时，可以通过域名进行访问。
- 备用站点名称** 当更改服务器域名时，可将原有域名设置为备用站点名称。
可添加多个备用站点域名，多个域名之间用空格分隔。
允许输入附加主机名。对于 HTTPS，要求主机名与 SSL 证书名相匹配，所以对于启用 HTTPS 的虚拟服务器只能指定一个主机名。

- 点击**虚拟服务器高级配置**选项卡，可通过编辑 SEngine/Nginx 配置脚本文件配置新建虚拟服务器：



5. 新建虚拟服务器默认存在一个资源路径条目 ，用户可以修改缺省条目的配置后使用，也可以右键选中虚拟服务器后点击**添加资源路径**，添加新的资源路径。

点击资源路径条目，可在下方配置区域配置资源路径的相关信息：

- 在**资源路径基本配置**页面，可设置资源路径的名称、缺省访问路径、关联的服务器组、引用的安全策略等参数。



资源路径默认为根目录 (/)，可修改。

如果服务器地址发生迁移，又不想体现给用户，可以保持资源路径不变，在**转换后路径**文本框中输入新的服务器路径。

如果完成配置后想修改资源路径关联的服务器组，可在此处点击**关联到**，选择新的服务器组。

如果服务器重建，暂时不能提供服务，可选择**本地提示页面**。目前仅提供“建设中”一种提示页面。

在**安全策略**下拉框中可选择应用于此资源路径的安全策略。点击**管理安全策略**将跳转至安全策略配置界面（**Web 安全>安全策略**）。有关安全策略的配置请参见第4章，[Web 安全](#)。

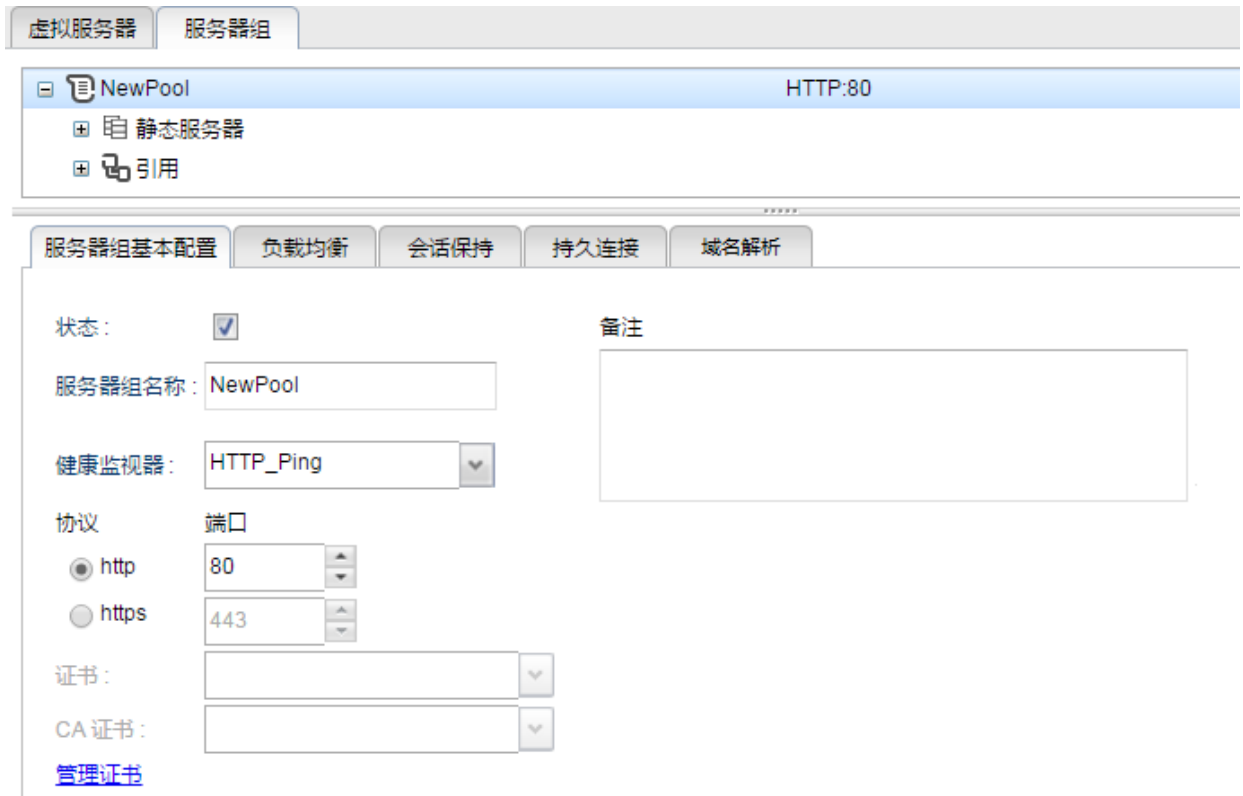
- 点击**资源路径高级配置**选项卡，可通过编辑 SEngine/Nginx 配置脚本文件配置资源路径：



提示：有关SEngine的配置命令集可以参考官网<http://www.sengine.org/cn/index.php/>。

右键选中资源路径条目，可以删除、启用/禁用资源路径，也可以选择资源路径要关联的服务器组和安全策略。

6. 点击**保存**。
7. 点击**服务器组**，在视图区空白处点击右键，选择**添加服务器组**：



设置服务器组的名称、协议和服务端口号。如果选择使用 HTTPS，还需要设置服务器组与后端服务器通信所使用的 SSL 证书。如果没有可选证书，需要到**虚拟服务>SSL 证书**页面添加证书。详细步骤请参见 [3.1.2 SSL 加密](#)。

选择一种健康监视器，监控服务器健康状态。服务器健康检测包括 TCP Ping、UDP Ping、ICMP Ping、HTTP Ping 和 HTTPS Ping 五种方式。

右键选中服务器组，可以选择删除、启用/禁用、展开/收缩、添加云服务器等操作。关于添加云服务器的操作，请参见 [3.1.13 云服务](#)。

8. 在**静态服务器**节点上点击右键，选择**添加静态服务器**：



选中**端口**复选框时，静态服务器将通过指定端口提供服务，否则使用服务器组端口。

点击**负载均衡配置**链接可跳转到所属服务器组的**负载均衡**配置页面选择算法。只有为静态服务器所属的服务器组选择了基于权重的负载均衡算法（**权重轮询算法**或**权重最少连接数算法**）时，才能为该静态服务器设置权重值。

新添加的静态服务器缺省处于 **down** 的状态，待后台探测器返回探测结果后，将变成最终的状态（包括 **up**、**down**）。如未开启健康检测，服务器状态将显示为 **unknown**。

右键选中添加的静态服务器条目，可以选择从服务器组中移除或启用/禁用该静态服务器等操作。当添加多个静态服务器时，可以右键选中**静态服务器**节点，选择展开/收缩其包含的静态服务器条目。

9. 使用相同的方法添加更多静态服务器。
10. 在服务器组的视图区右键点击**引用**，选择**添加资源路径**：



双击资源路径名称，将资源路径关联到服务器组：



当关联多个资源路径时，可以右键选中引用节点，选择展开/收缩该服务器组引用的资源路径条目。

11. 点击**保存**。

3.1.2. SSL 加密

SSL 加密功能使得客户端与 ADSG 之间以及 ADSG 与后端服务器之间可以使用 SSL 加密链路进行通信，避免信息明文传输带来的安全隐患。

ADSG 支持 SSL 卸载和 SSL 封装功能：

- SSL 卸载

配置在虚拟服务器上，面向客户端提供 SSL 解封装功能。此种情况下，ADSG 将与客户端建立 HTTPS 连接，并将客户端发来的数据解密，再进行后续处理。

- SSL 封装

配置在服务器组上，面向后端服务器提供 SSL 封装功能。此种情况下，ADSG 将于后端服务器建立 HTTPS 连接，并支持双向证书认证，将客户端的数据加密后发往后端服务器。

这里的“双向证书认证”是指 ADSG 可以上载后端服务器的 CA 证书，用以验证服务器证书的合法性；同理，在后端服务器上配置 ADSG 的 CA 证书，用以验证 ADSG 证书的合法性。ADSG 的 CA 证书通常和后端服务器是同一个 CA 颁发。

关于 SSL 证书：

- ADSG 支持上载证书以及内部生成自签名证书。
- 上传的证书格式支持两种：PEM 和 PKCS#12。
 - 当上传 PEM 格式证书时，证书文件的扩展名必须为.crt。
 - 当上传 PKCS#12 格式证书时，证书文件的扩展名必须为.pfx。
- 上传的密钥格式必须为 PEM 格式，且扩展名为.key。

要配置 SSL 加密功能，请执行以下操作：

1. 选择**虚拟服务>SSL 证书**，在视图区空白处点击右键，导入或生成证书：

- 如果选择**导入**菜单，需要在配置区域上传证书和密钥文件。

The image shows two side-by-side screenshots of the ADSG configuration interface for importing certificates. Both screenshots have tabs for '查看' (View), '生成' (Generate), and '导入' (Import).
 The left screenshot shows the '导入' tab selected. Under '导入证书方式' (Import Certificate Method), '公钥/私钥' (Public/Private Key) is selected. There are three input fields: '证书密钥文件' (Certificate Key File) with a '选择文件' (Select File) button and the text 'privkey_1.key'; '证书文件' (Certificate File) with a '选择文件' (Select File) button and the text 'cacert_1.crt'; and '私钥密码' (Private Key Password) with an empty text box.
 The right screenshot also shows the '导入' tab selected. Under '导入证书方式', 'PKCS12' is selected. There are two input fields: '证书文件' (Certificate File) with a '选择文件' (Select File) button and the text 'rootCA.pfx'; and 'PKCS12证书密码' (PKCS12 Certificate Password) with a text box containing several dots representing a password.

提示：如果选择导入私钥，需要输入私钥密码。

- 如果选择**生成**菜单，则需要在配置区域填入必要的证书信息后生成自签名证书。其中，**通用名**可以填 AD SG 的域名，也可以填 IP 地址。

点击生成按钮，将在查看区域显示新生成的证书。

SSL证书					
标题	签发者	签发日期	过期日期	密钥长度	引用者
CN=test, O=test123	CN=test, O=test123	2017-04-18	2022-04-17	2048	

2. 点击**保存**。
3. 选择**虚拟服务>流量管理（七层）>虚拟服务器>（虚拟服务器名称）**：

4. 点击**分配证书**链接或**SSL 加密**选项卡，在**证书**下拉菜单中选择之前导入或生成的证书，点击**保存**。

The screenshot shows the configuration page for a virtual server named 'NewVServer'. The 'SSL加密' (SSL Encryption) tab is selected. The '证书' (Certificate) dropdown menu is open, showing 'CN=www.aa.com, O=111, 2018'. Below it, there is a '管理证书' (Manage Certificate) link. The '会话超时' (Session Timeout) is set to 600 minutes. On the right, the '协议' (Protocol) section has checkboxes for 'SSLv2' (unchecked), 'SSLv3' (checked), and 'TLS' (checked).

5. 打开**虚拟服务器基本配置**选项卡，勾选 **https** 复选框，点击**保存**。

The screenshot shows the '虚拟服务器基本配置' (Virtual Server Basic Configuration) tab. The '状态' (Status) checkbox is checked. The '服务器名称' (Server Name) is 'NewVServer'. The '虚拟IP地址' (Virtual IP Address) is 'WebServer1'. The '默认服务器' (Default Server) checkbox is unchecked. The '透明代理' (Transparent Proxy) checkbox is unchecked. The '协议' (Protocol) section has checkboxes for 'http' (checked) and 'https' (checked). The '端口' (Port) for 'https' is '443', with a '分配证书' (Assign Certificate) link next to it. There are also fields for '域名' (Domain Name) and '备用站点名称' (Alternate Site Name), and a '备注' (Remarks) text area.

此时，客户端即可以通过使用 https 的方式访问 AD SG。

6. 如果要设置 AD SG 与后端服务器之间的 SSL 加密功能，则选择**服务器组**> (**服务器组名称**)>**服务器组基本配置**，点击 **https**，选择证书，点击**保存**。

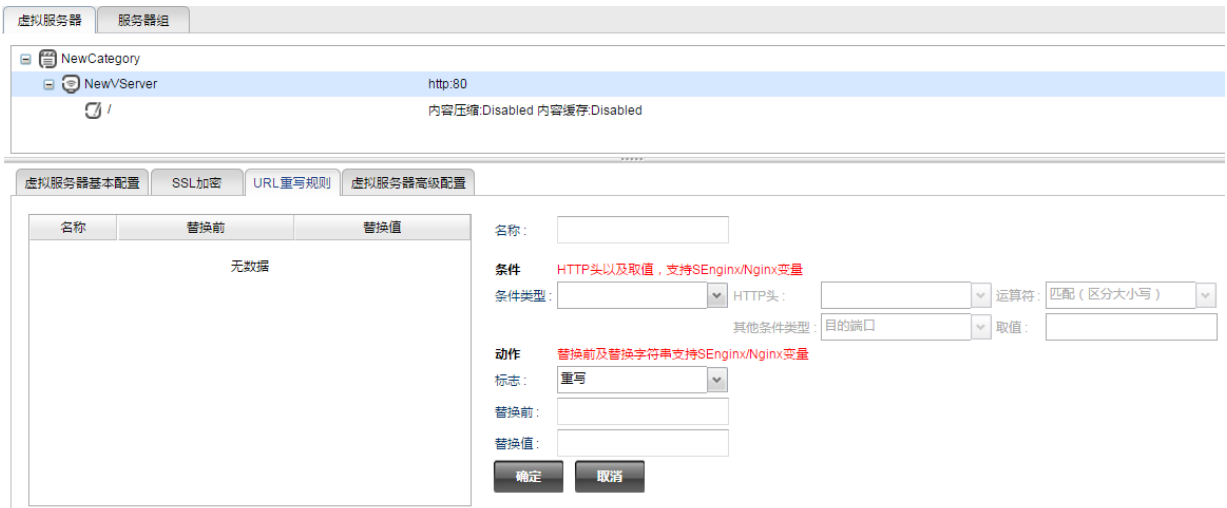
The screenshot shows the configuration page for a server group named 'NewPool'. The '服务器组基本配置' (Server Group Basic Configuration) tab is selected. The '状态' (Status) checkbox is checked. The '服务器组名称' (Server Group Name) is 'NewPool'. The '健康监视器' (Health Monitor) is 'HTTPS_Ping'. The '协议' (Protocol) section has radio buttons for 'http' (unselected) and 'https' (selected). The '端口' (Port) for 'https' is '443'. The '证书' (Certificate) dropdown menu is open, showing 'CN=www.aa.com, O=111, 2018'. Below it, the 'CA 证书' (CA Certificate) dropdown menu is also open, showing the same certificate. There is a '管理证书' (Manage Certificate) link. There is also a '备注' (Remarks) text area.

3.1.3. URL 重写

URL 重写规则用于修改 HTTP 请求中的 URL，并将包含修改后 URL 的请求转发给后端服务器，最终使客户端可以访问后端服务器组中的 Web 资源。

URL 重写规则配置在虚拟服务器上。要配置 URL 重写规则，请执行以下操作：

1. 选择**虚拟服务>流量管理(七层)>虚拟服务器>（虚拟服务器名称）>URL 重写规则**。



2. 设置相关参数，添加规则。

参数	说明
名称	为新建 URL 重写规则指定名称。
条件	<p>确定对什么样的 HTTP 请求进行 URL 重写。</p> <ul style="list-style-type: none"> ▪ 条件类型：包括 URL、HTTP 头 和其他，也可以为空。 <ul style="list-style-type: none"> • URL：匹配的条件为 URL，通常为 “/” 开头的 URL 片段。 • HTTP 头：匹配的条件为 HTTP 头中的参数，比如：User-Agent。支持自动补齐和用户自定义 HTTP 头。 • 其他：上述之外的其他匹配条件。（当前版本仅提供目的端口一种选择。） ▪ 运算符：指定 URL 重写规则的匹配方式，包括 匹配（区分大小写）、匹配（不区分大小写）、不匹配（区分大小写）、不匹配（不区分大小写） 和 等于（严格匹配） 指定的取值。 ▪ 取值：对 HTTP 请求进行过滤的关键字。

动作 定义如何重写 HTTP 请求中的 URL。

- **标志：**对匹配 URL 重写规则的 HTTP 请求的处理动作。
 - 重写：重写 URL，并按照已匹配的资源路径转发该 HTTP 请求。
 - 重写并重新匹配：重写 URL，并重新匹配资源路径，按照新匹配的资源路径转发该请求。
 - 临时重定向：向客户端（浏览器）发送 HTTP 重定向报文（状态码为 302），触发临时重定向。
 - 永久重定向：向客户端发送 HTTP 永久重定向报文（状态码为 301），触发永久重定向。
- **替换前：**替换前的 URL，支持正则表达式。
- **替换值：**替换后的 URL。

配置注意事项：

- 如果**条件类型**是 **URL**，则**运算符**和**取值**所指定的内容不能与替换前指定的内容冲突。例如，在**运算符**和**取值**中指定替换不匹配“aaa”的 URL，但是在 **URL** 中却指定替换“aaa”，这样的规则是不能生效的。
- **条件类型**选择**其他**时，**其他条件类型**可选**目的端口**，此时可在**取值**文本框中设置目的端口号。
- **条件类型**为空时，直接匹配**动作**中指定的替换前 URL。如果匹配，则直接替换为指定的替换值。
- 在**条件**和**动作**区域配置完参数后，点击**确定**，新建规则将添加到左边的列表中。

3. 以同样方式添加更多规则。

4. 点击**保存**。

配置案例 1

许多 Web 应用对外公布的 URL 对普通用户来说很难理解，如/dashboard.action。此时，ADSG 可以代替服务器对外发布一个新的、容易理解和记忆的 URL，如/confluence，然后在收到客户端请求时再将该 URL 改写为原来的 URL。

名称:

条件: HTTP头以及取值, 支持SEngine/Nginx变量

条件类型: HTTP头: 运算符:

其他条件类型: 取值:

动作: 替换前及替换字符串支持SEngine/Nginx变量

标志:

替换前:

替换值:

配置案例 2

由于业务需要，某网站后台服务器改用 PHP 技术实现。为了兼容以前的访问，ADSG 可以将原来的 URL 改写为新的 URL。同时，为了避免为每条 URL 都配置一条 URL 重写规则，此案例使用了正

则表达式。

名称:

条件: HTTP头以及取值, 支持SEngine/Nginx变量

条件类型: HTTP头: 运算符:

其他条件类型: 取值:

动作: 替换前及替换字符串支持SEngine/Nginx变量

标志:

替换前:

替换值:

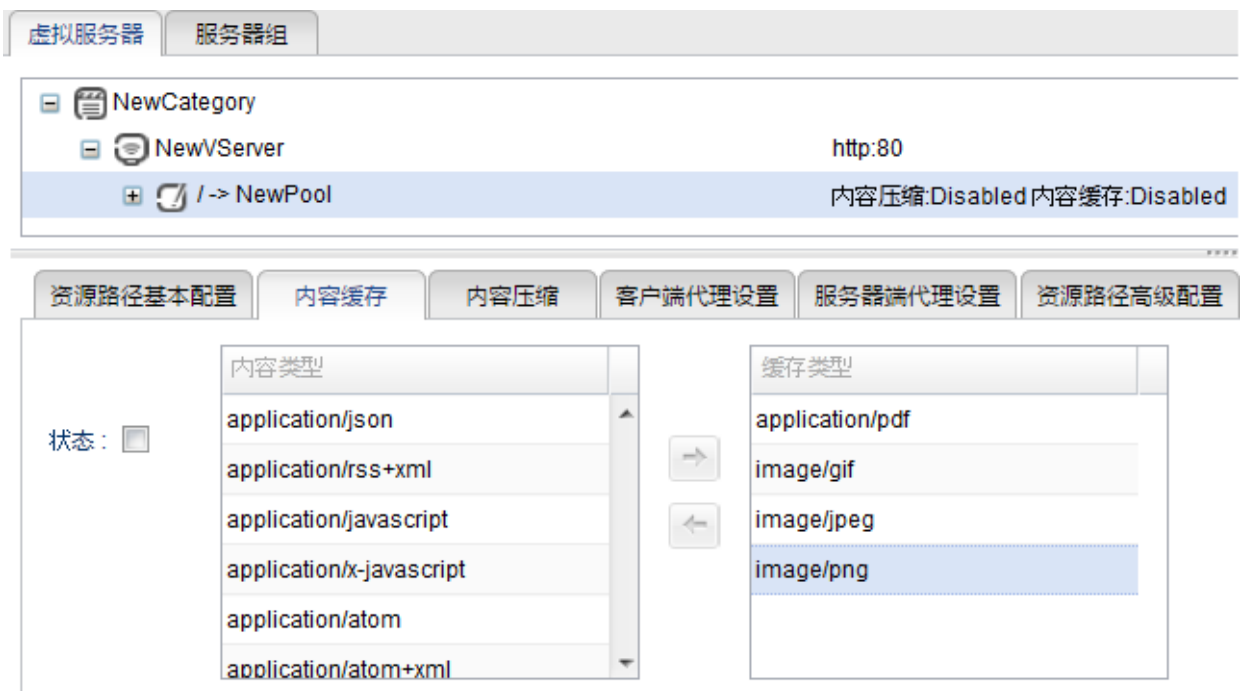
3.1.4. 内容缓存

开启内容缓存后, AD SG 可以缓存一些后端服务器的响应, 在下次相同请求到来时直接返回给客户

端。

内容缓存配置在资源路径上。要配置内容缓存, 请执行以下操作:

1. 选择**虚拟服务>流量管理 (七层)>虚拟服务器>(虚拟服务器名称)>(资源路径名称)>内容缓存**。



2. 内容缓存默认关闭; 勾选**状态**开启此功能。
3. 通过移动**内容类型**框中的条目到**缓存类型**框中, 选择允许缓存的内容类型。

提示: 按Ctrl键或Shift可同时多选。

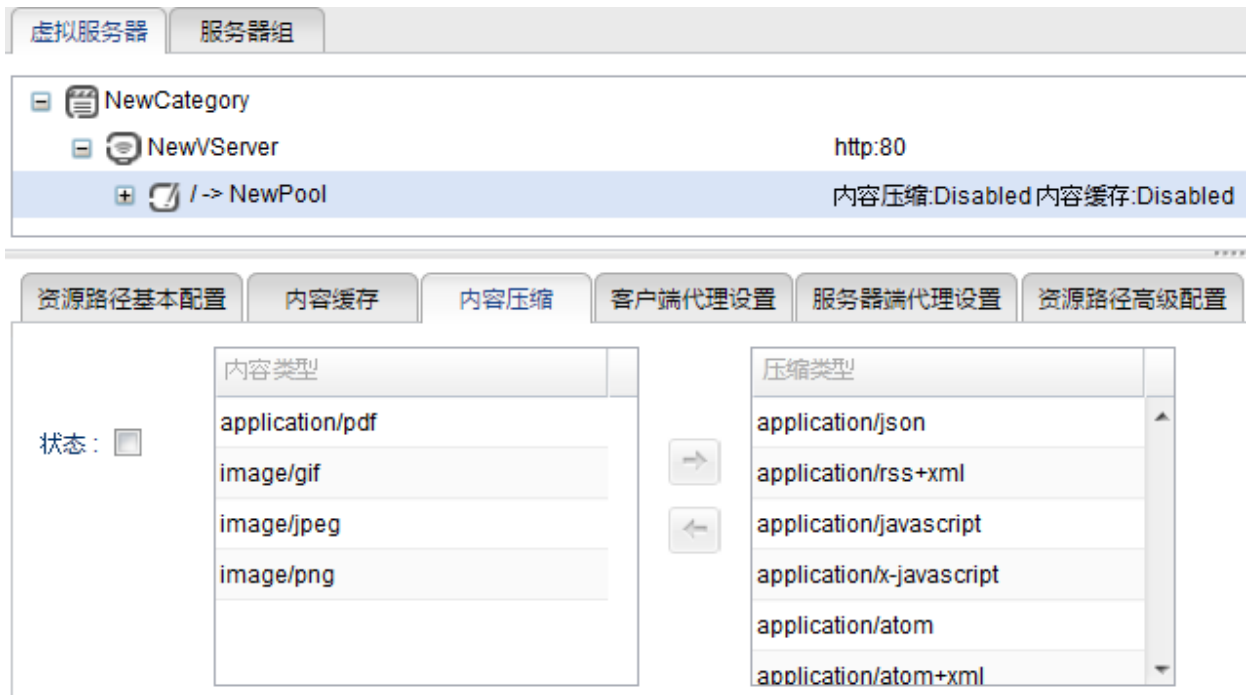
4. 点击**保存**。

3.1.5. 内容压缩

开启内容压缩后，ADSG 可以将服务器端响应的内容进行压缩，以减小 ADSG 与客户端的数据量，提升访问速度。目前 ADSG 仅支持 gzip 压缩算法。

内容压缩配置在资源路径上。要配置内容压缩，请执行以下操作：

1. 选择**虚拟服务>流量管理（七层）>虚拟服务器>（虚拟服务器名称）>（资源路径名称）>内容压缩**。



2. 内容压缩默认关闭；勾选**状态**开启此功能。
3. 通过移动**内容类型**框中的条目到**压缩类型**框中，选择要压缩的媒体类型。

提示：按Ctrl键或Shift可同时多选。

4. 点击**保存**。

3.1.6. 反向代理

反向代理（Reverse Proxy）是指 AD SG 代表内网服务器接收来自外网客户端的请求，然后将请求转发给内网服务器，并将从服务器接收到的应答返回给客户端。此时，AD SG 对外就表现为一个服务器。作为反向代理服务器的 AD SG 位于本地 Web 服务器和 Internet 之间，无论是客户端的请求还是服务器端的应答，都会通过 AD SG；AD SG 可以根据管理员的需求，自定义发送到真实服务器的请求内容，以及真实服务器发送给客户端的应答。

AD SG 面向客户端和服务器端分别提供反向代理功能。

反向代理配置在资源路径上。要配置反向代理功能，请执行以下操作：

1. 选择**虚拟服务>流量管理（七层）>虚拟服务器>（虚拟服务器名称）>（资源路径名称）>客户端代理设置**。



2. 设置客户端代理配置参数。

参数	说明
客户端请求头管理	<ul style="list-style-type: none"> ▪ HTTP 头：客户端发起的 HTTP 请求头。支持自动补齐和用户自定义 HTTP 头。 ▪ 取值：替换值。支持 NGINX 变量。
客户端超时设置	<ul style="list-style-type: none"> ▪ 请求体超时等级：设置为自定义时可继续设置下面三项。 ▪ 请求体读超时：读取客户端请求正文的超时时间。 ▪ 连接超时：客户端的长连接在服务器端保持的最长时间。 ▪ 传输响应超时：向客户端传输响应报文的超时时间。
客户端缓存设置	<ul style="list-style-type: none"> ▪ 请求体缓存等级：设置为自定义时可继续设置下面两项。 ▪ 请求体缓存大小：AD SG 读取客户端请求正文的缓冲容量。 ▪ 请求体最大值：AD SG 允许接收的客户端请求正文最大长度。

对于客户端请求头管理，AD SG 提供一条缺省策略：

将客户端请求头中的 **Connection** 字段替换为空，这样客户端收到 HTTP 应答后 HTTP 会话就不会自动关闭了，从而提高 HTTP 会话的复用率。

3. 点击**服务器端代理设置**选项卡，设置相关内容：



参数	说明
服务器端应答头管理	<ul style="list-style-type: none"> ▪ HTTP 头：从服务器返回的 HTTP 应答头。支持自动补齐和用户自定义 HTTP 头。 ▪ 取值：用于替换 HTTP 头的值。支持 NGINX 变量。 <p>单击列表头，可根据该列对规则条目进行排序（按首字母或数字排序）。</p>
服务器端应答体管理	<ul style="list-style-type: none"> ▪ 应答媒体类型：指定要替换的应答媒体类型。 <p>其中系统默认替换 text/html 媒体类型，但是 text/html 选项在界面上不可见。支持按 Ctrl 或 Shift 键多选。</p> <ul style="list-style-type: none"> ▪ 应答体替换规则： <ul style="list-style-type: none"> • 原始值：替换前的应答体内容，支持正则表达式。 • 替换值：用于替换应答体指定内容的字符串。 <p>单击列表头，可根据该列对规则条目进行排序（按首字母或数字排序）。</p>
服务器端应答重定向管理	<ul style="list-style-type: none"> ▪ 状态：勾选开启 HTTP 应答重定向功能。默认开启。 ▪ 原始值：替换前的 URL 片段，通常修改主机名。 ▪ 转换后：替换后的 URL 片段。 <p>例如，可以将 http://10.5.1.81/ 替换为 http://10.3.5.77:8888。</p> <p>单击列表头，可根据该列对规则条目进行排序（按首字母或数字排序）。</p>
服务器端应答错误识别	<p>勾选开启服务器端应答重定向识别功能。</p> <p>对于非 200 OK 的应答，将被替换为 ADSG 中定义的应答页面。</p>
服务器端超时设置	<ul style="list-style-type: none"> ▪ 服务器端超时等级：级别为自定义时可继续设置以下三项。 ▪ 连接超时：与后端服务器建立连接的超时时间。 ▪ 读超时：从后端服务器读取响应的超时时间。 ▪ 写超时：向后端服务器传输请求的超时时间。

- 服务器端缓存设置
- **服务器端缓存等级：**级别为自定义时可继续设置以下五项。
 - **应答缓存：**开启缓存应答功能。
 - **缓存数量：**每个连接缓冲区的数量。
 - **每块缓存大小：**每块缓冲区的大小。
 - **应答缓存大小：**应答缓存大小。
 - **缓存大小：**应答缓冲区大小，用于读取从后端服务器接收的响应的第一部分。

4. 点击保存。

▪ 配置案例 1

客户端发送的 HTTP 请求头中，User-Agent 为 Mozilla/5.0(Windows NT 6.1; rv:20.0) Gecko/20100101 Firefox/20.0。由于后端服务器运行时负载非常高，为了缓解后端服务器的负载，可以简化 User-Agent 请求头为 Firefox。这时，对于后端服务器而言，看到的 User-Agent 头就为 Firefox。

资源路径基本配置 内容缓存 内容压缩 客户端代理设置 服务器端代理设置 资源路径高级配置

客户端请求头管理

HTTP头	取值
Host	\$http_host
Connection	
User-Agent	Firefox

HTTP头: User-Agent

取值: Firefox 取值支持SEngineX/Nginx变量

确定 取消

▪ 配置案例 2

真实服务器发送的 HTTP 应答头中，Server 为 Apache-Coyote/1.1。管理员如果想隐藏真实服务器的信息，可以将 Server 头设置为 AC，这时客户端看到的 Server 头就为 AC。

资源路径基本配置 内容缓存 内容压缩 客户端代理设置 服务器端代理设置 资源路径高级配置

服务器端应答头管理

HTTP头	取值
Server	AC

HTTP头: Server

取值: AC 取值支持SEngineX/Nginx变量

确定 取消

3.1.7. 负载均衡

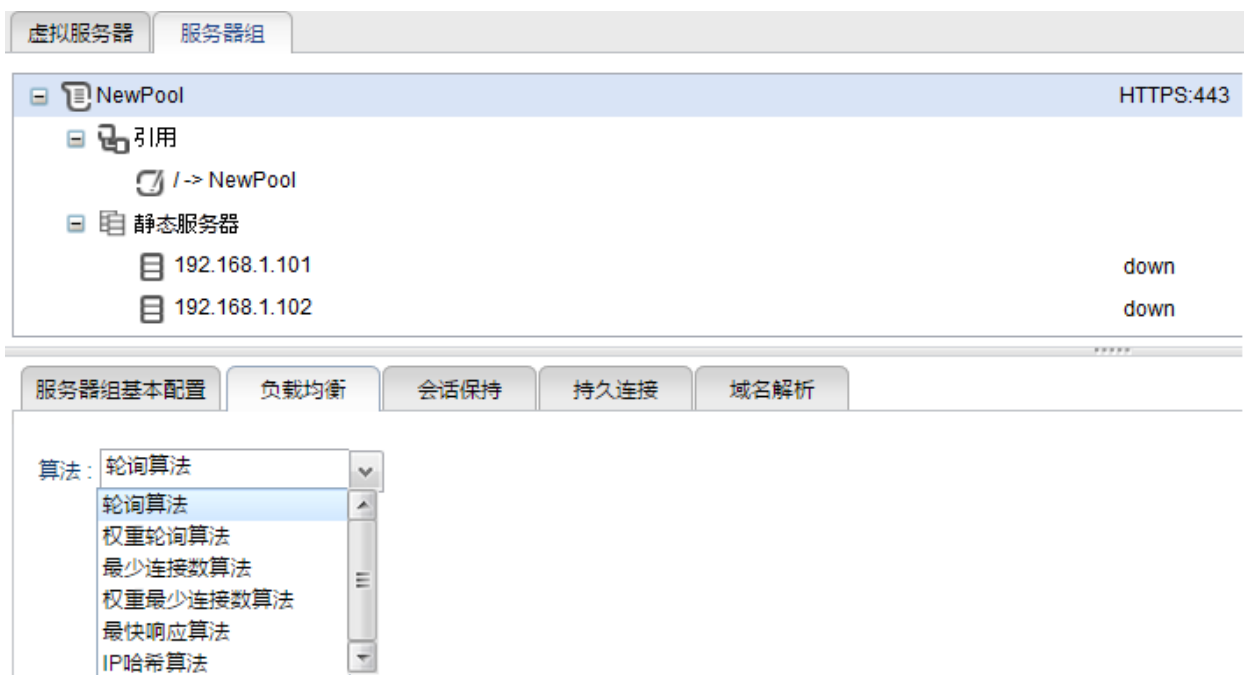
通过负载均衡，ADSG 可以根据服务器的可用性和服务能力将客户端请求发送到最合适后端服务器。

ADSG 支持以下几种负载均衡算法：

- **轮询算法：**将请求依次转发给不同的服务器。
- **权重轮询算法：**根据权重将请求依次转发给不同的服务器，权重越大的服务器收到请求的次数就越多。
- **最少连接数算法：**将请求转发给并发连接数最少的服务器。
- **权重最少连接数算法：**根据权重将请求转发给并发连接数最少的服务器，权重越大的服务器收到请求的概率越大。
- **最快响应算法：**将请求转发给响应最快的服务器。
- **IP 哈希算法：**根据源 IP 的哈希值将请求转发给固定的服务器。

负载均衡配置在服务器组上。要配置负载均衡功能，请执行以下操作：

1. 选择**虚拟服务>流量管理（七层）>服务器组>（服务器组名称）>负载均衡**：



2. 选择一种负载均衡算法，点击**保存**。链路探测完成（大约需要 15 秒）后，页面将更新静态服务器的状态。
3. 如果静态服务器的状态变成“up”，则表示用户可以通过 ADSG 访问静态服务器。即，在浏览器中输入：**http://ADSG-IP:Port/**。

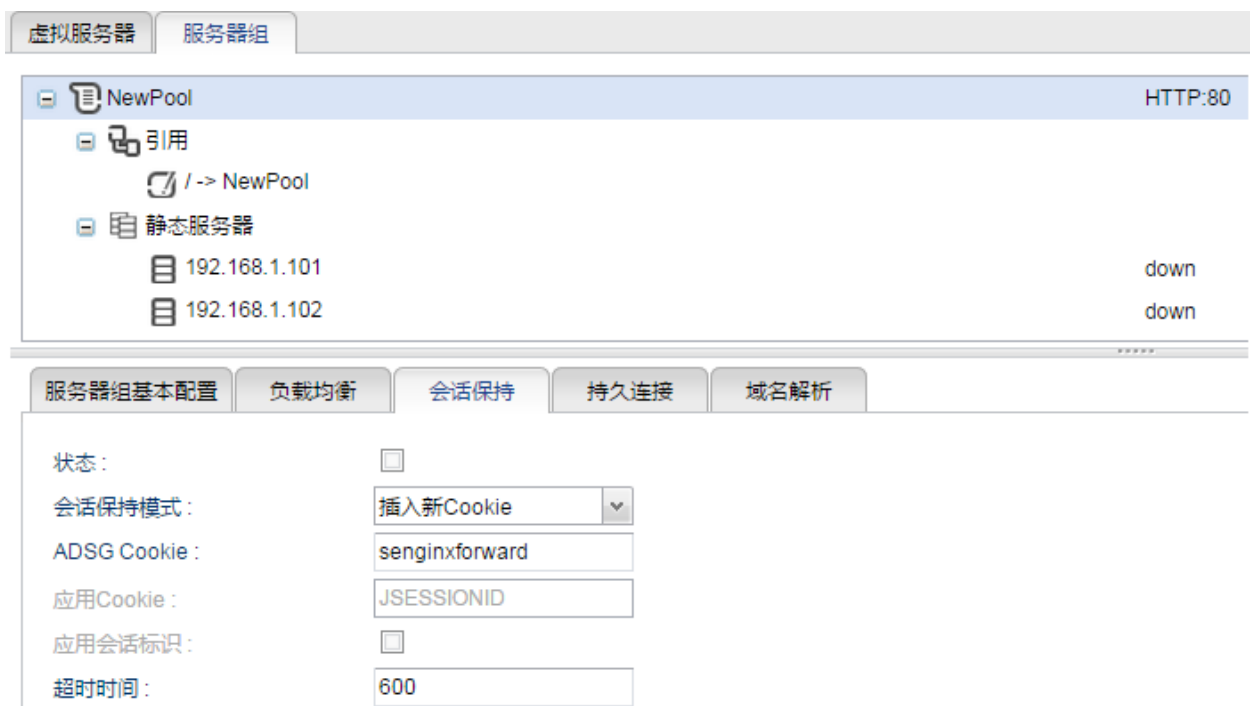
3.1.8. 会话保持

会话保持功能是指在一个 HTTP 会话建立后，当基于这条会话的请求到达 ADSG 时，ADSG 会将其转发给参与建立该会话的服务器。

会话保持功能可以与任意负载均衡算法配合使用。当一个新的请求到来时，ADSG 先根据负载均衡算法将其转发到后端服务器，从而建立会话；当基于这个会话的请求再次到来时，ADSG 会根据会话保持算法直接将请求转发给系统的服务器。

会话保持配置在服务器组上。要配置会话保持功能，请执行以下操作：

1. 选择**虚拟服务>流量管理（七层）>服务器组>（服务器组名称）>会话保持**。



2. 设置相关参数。

参数	说明
状态	勾选启用会话保持功能。
会话保持模式	ADSG 支持以下三种会话保持模式： <ul style="list-style-type: none"> ▪ 插入新 Cookie: 通过插入新 Cookie 的方式对所有的会话实现保持功能。 ▪ 监控应用 Session 标识: 对出现指定 QueryString 或应用 Cookie 的会话实现保持功能。如选此模式，需配置应用会话标识或应用 Cookie 项。 ▪ IP 哈希算法: 根据源 IP 的哈希值实现会话保持功能。
ADSG Cookie	要插入 HTTP 报文的 ADSG Cookie。
应用 Cookie	要监控的应用 Cookie，比如 JSESSIONID。

应用会话标识 勾选此项后，系统将依据 HTTP 请求中的 QueryString 进行会话识别。

超时时间 会话保持的超时时间。

3. 点击**保存**。

3.1.9. 持久连接

ADSG 和后端服务器建立的 HTTP 连接缺省使用 HTTPv1.1 协议，这使得 ADSG 可以复用现有的 TCP 连接直接将 HTTP 请求转发给服务器，提高服务器的响应速度。管理员可以设置 ADSG 与后端服务器之间的最大持久连接数。

持久连接功能配置在服务器组上。要配置持久连接功能，请执行以下操作：

1. 选择**虚拟服务>流量管理（七层）>服务器组>（服务器组名称）>持久连接**：



2. 开启持久连接，可以设置最大持久连接数。

如果与客户端通信的接口同时与后端服务器进行通信，最大持久连接数过大会影响客户端与后端服务器的并发连接，所以最大持久连接数不宜设置过大，建议不要超过 1024。

3. 点击**保存**。

3.1.10. 域名解析（容错）

当后端服务器使用动态 IP 地址时，则只能使用域名来识别服务器。这时需要配置 DNS 服务器用于域名解析。针对静态服务器域名解析失败的情况，用户可以设置 ADSG 的处理机制。

域名解析功能配置在服务器组上。要配置域名解析失败处理机制，请执行以下操作：

1. 选择**虚拟服务>流量管理（七层）>服务器组>（服务器组名称）>域名解析**：



2. 开启域名解析，设置相关参数。

参数	说明
状态	勾选该复选框，开启域名解析失败处理机制。
结果缓存时间	ADSG 获取域名解析结果后的有效时间，超过这个时间后需要重新发起域名解析请求。
失败动作	当域名解析失败时，ADSG 的处理动作，包括： <ul style="list-style-type: none"> ▪ 使用获取的旧地址：使用缓存的旧地址，即上次解析结果； ▪ 选择下一个静态服务器：将负载分配给下一个静态服务器； ▪ 结束当前请求：即丢弃当前负载，不再分配给其他静态服务器。
失败超时时间	为避免频繁请求域名解析导致系统资源浪费，可以设置 ADSG 在域名解析失败后多长时间再发起域名解析请求。

3. 点击**保存**。

3.1.11. 自动负载均衡

ADSG 支持通过 SNMP 获取后端服务器的状态信息，用于辅助判断服务器的负载权重。需要先为服务器组选择一种基于权重的负载均衡算法，然后才能为静态服务器设置 SNMP 相关信息。

自动负载均衡功能配置在静态服务器上。要配置自动负载均衡，请执行以下操作：

1. 选择**虚拟服务>流量管理（七层）>服务器组>（服务器组名称）>负载均衡**，选择一种基于权重的负载均衡算法。
2. 选择**虚拟服务>流量管理（七层）>服务器组>（服务器组名称）>静态服务器>（静态服务器名称）>自动负载均衡配置**：

The screenshot shows the configuration page for a static server. The top navigation bar includes '虚拟服务器' and '服务器组'. The main content area shows a tree view with 'NewPool' and 'NewStaticServer' selected. Below the tree view, there are three tabs: '静态服务器基本配置', '自动负载均衡配置', and '延迟停机'. The '自动负载均衡配置' tab is active, showing the following configuration options:

- 状态:
- 监控资源类型: 空闲CPU百分比 (dropdown)
- 监控资源OID: .1.3.6.1.4.1.2021.11.11.0 (text input)
- SNMP版本: v3 (dropdown)
- SNMP团体字符串: (text input)
- SNMP安全级别: 不认证不加密 (dropdown)
- SNMP安全用户: (text input)
- SNMP验证协议: MD5 (dropdown)
- SNMP验证字符串: (text input)
- SNMP加密协议: DES (dropdown)
- SNMP加密字符串: (text input)

3. 开启自动负载均衡，设置相关参数。

参数	说明
状态	勾选开启自动负载均衡功能。
监控资源类型	获取后端服务器何种系统资源状态信息，包括空闲 CPU 百分比和实体空闲内存。
监控资源 OID	要监控的系统资源在系统中的对象标识符。
SNMP 版本	获取后端服务器状态信息所使用的 SNMP 协议版本，ADSG 支持 v1、v2c 和 v3。
SNMP 团体字符串	当选择 v1 或 v2c 版本时，需要设置团体字符串，用于验证后端服务器的身份。

SNMP 安全级别	ADSG 与后端服务器之间 SNMP 通信的安全级别，包括不认证不加密、认证不加密和认证并加密三种。
SNMP 安全用户	当选择 v3 版本时，需要设置 SNMP 用户，用于验证后端服务器的身份。
SNMP 验证协议	ADSG 与后端服务器之间 SNMP 通信的认证算法和认证密码。
SNMP 加密协议	ADSG 与后端服务器之间 SNMP 通信的加密算法和密钥。

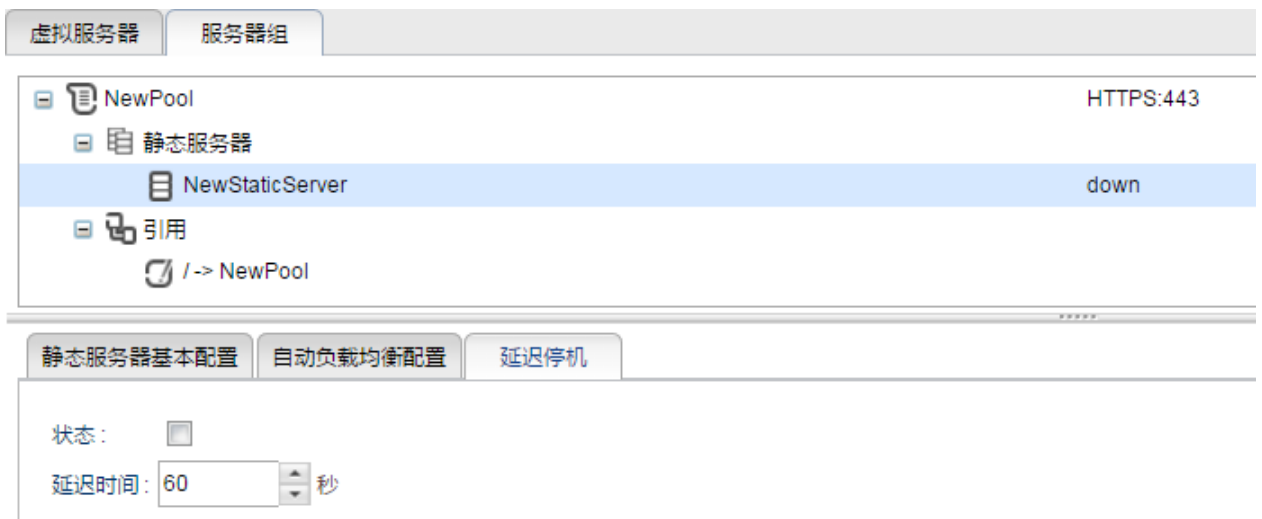
4. 点击**保存**。

3.1.12. 延迟停机

当开启会话保持功能时，用户可以设置后端服务器的延迟停机时间，保证服务器平滑退出。

延迟停机功能配置在静态服务器上。要配置延迟停机功能，请执行以下操作：

1. 选择**虚拟服务>流量管理（七层）>服务器组>（服务器组名称）>会话保持**，开启会话保持功能。
2. 选择**虚拟服务>流量管理（七层）>服务器组>（服务器组名称）>静态服务器>（静态服务器名称）>延迟停机**：



3. 开启延迟停机功能，设置延迟停机时间。
4. 点击**保存**。

3.1.13. 云服务

ADSG 可以使用 Amazon EC2 平台的 Instance 实例作为后端服务器，并且可以按照用户设定的策略基于时间进行自动缩放。

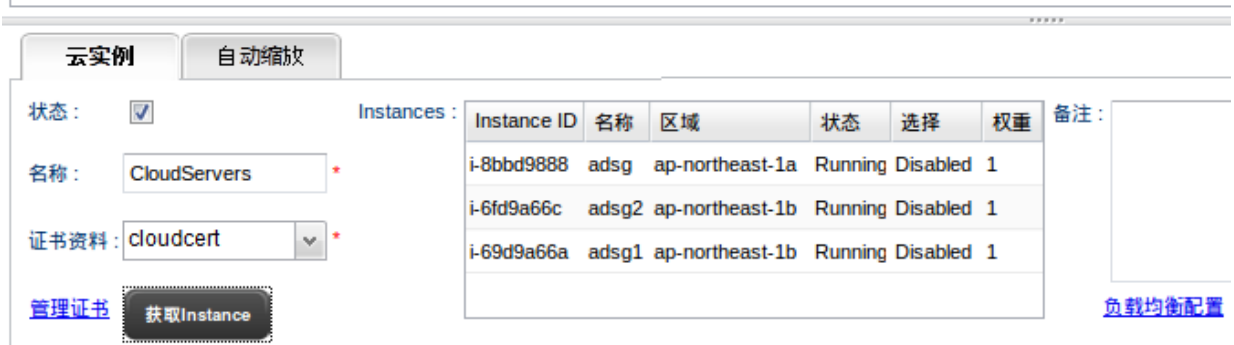
要为云服务器配置七层流量管理，请执行以下操作：

1. 选择**虚拟服务>云证书**，在云证书列表空白处点击右键，点击**创建**，填入相关信息后点击**保存**，生成证书：

提示：生成的证书将在后面的步骤3中引用。

2. 选择**虚拟服务>流量管理（七层）>服务器组**，右键点击服务器组名称，选择**添加云服务器**：

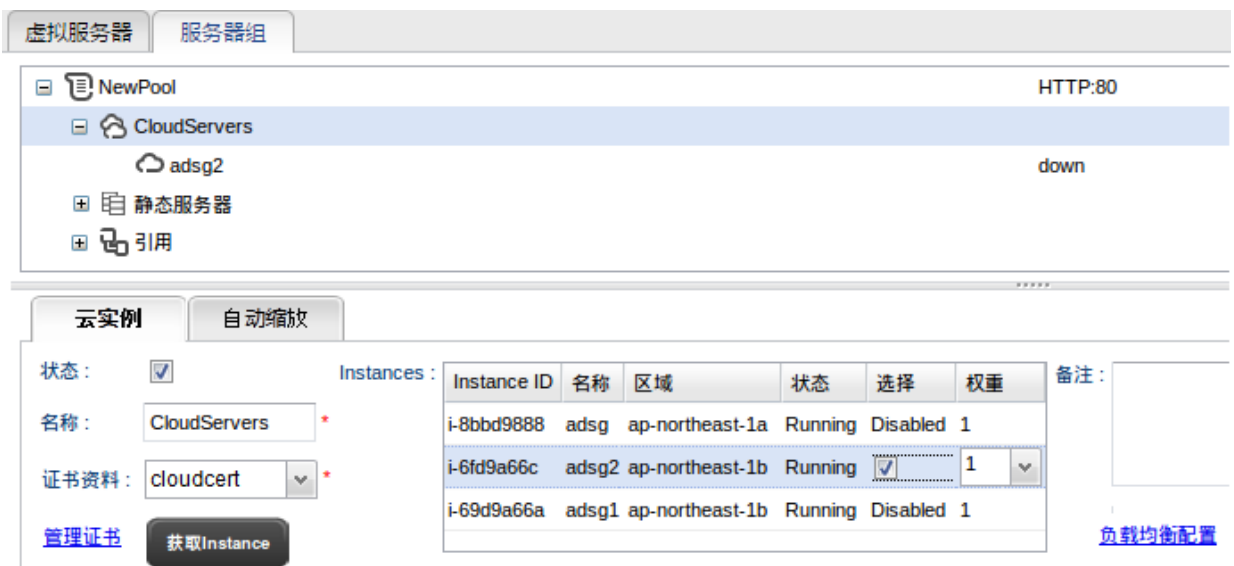
3. 从**证书资料**下拉框中选择之前创建的云证书，点击**获取 Instance**。过一段时间后，如果连接成功，右面列表中将显示获取到的云实例。



4. 点击实例对应的**选择**列 **Disabled**，勾选复选框，将云服务器添加到服务器组：



5. 在视图区的 **CloudServers** 下面可以看到已选择的 Instance 已经加入到服务器组中。



6. 以同样方式将更多的实例添加到服务器组中：

7. 点击**保存**，等实例的状态由 **down** 变为 **up** 后就可以通过 AD SG 访问实例了。
8. 如果需要使用自动缩放功能，则点击**自动缩放**，勾选**状态**，启用此功能。此功能默认关闭。**服务器组**中的 **Instances** 框中只显示之前选中并启用的 Instance；如果要指定 Instance 加入自动缩放，可以通过点击其对应的**资源伸展/资源收缩**下面的 **Disabled**，然后勾选复选框：

自动缩放 (Auto Scaling) 是虚拟化及云计算数据中心的一个概念，是指服务器组中的 Instance (实例，服务器节点) 可以由云计算控制器以及负载均衡器依据某些条件自动进行增加或者减少的过程。目前 AD SG 支持依据设定时间段进行自动缩放。

9. 可以勾选**每日缩放**，也可以手动设置具体的自动缩放时间。如果资源伸展与收缩设置在同一天，则其时间间隔不能小于 30 分钟。

3.2. 四层流量管理

ADSG 四层流量管理功能相对于七层 HTTP/HTTPS 流量管理而言，主要定位于承载自 TCP/UDP 协议的应用流量。这是一种四层负载均衡功能，根据报文的目的 IP 地址及应用层协议端口，再结合系统提供的负载均衡算法，对流量进行分发。

本节内容包括：

- [3.2.1 配置四层流量管理基础框架](#)

在虚拟服务器上配置：

- [3.2.2 会话保持](#)

在服务器组上配置：

- [3.2.3 负载均衡](#)

在静态服务器上配置：

- [3.2.4 自动负载均衡](#)
- [3.2.5 延迟停机](#)

3.2.1. 配置四层流量管理基础框架

要配置四层流量管理的基础框架，请执行以下操作：

1. 选择公共对象>IP 地址集，为虚拟服务器添加一个 IP 地址集。

基本配置

名称：VServer_IPset *

地址集

类型	取值
IPv4地址	202.118.108.11
IPv4地址	58.18.10.11

类型：IPv4地址

IPv4地址：*

确定 取消

提示：虚拟服务器的IP地址集应包含单个的IP地址。

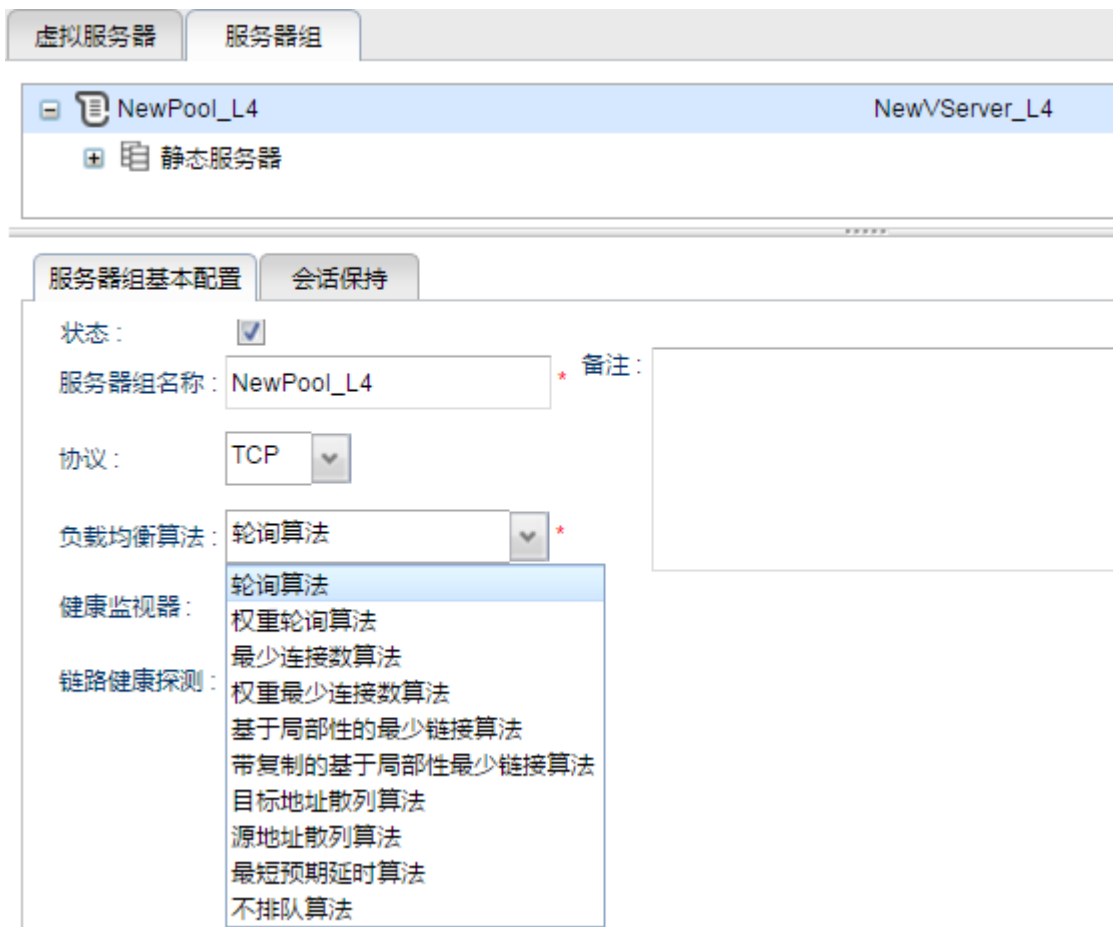
2. 选择**虚拟服务>流量管理（四层）**。在**虚拟服务器**区域空白处点击右键，选择**添加虚拟服务器**。



3. 在**虚拟服务器基本配置**区域配置相关参数。

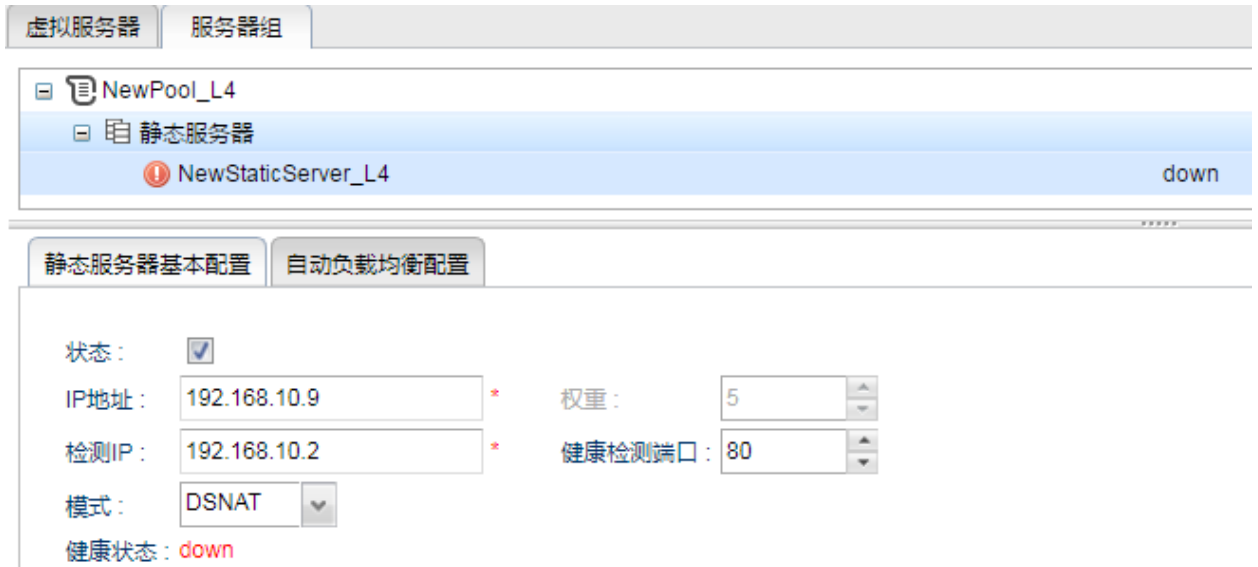
参数	说明
服务器名称	虚拟服务器的名称。
保持时间	会话保持的超时时间。超过此时间，会话保持关系将被取消。
本地 IP	与关联的静态服务器能够通信的接口 IP 地址。 HA 部署时，本地 IP 需要配置为浮动 IP。
虚拟 IP 地址地址集	虚拟服务器对外提供服务的 IP 地址的集合。 虚拟 IP 地址需和本地接口的 IP 地址在同一网段。
协议	虚拟服务器提供服务使用的协议。

4. 点击**服务器组**页签，在空白处点击右键，选择**添加服务器组**。在**服务器组基本配置**区域配置相关参数。



参数	说明
服务器组名称	添加服务器组的名称。
协议	通信所用协议。服务器组协议需与虚拟服务器的协议保持一致，才能对二者进行关联。
负载均衡算法	当虚拟服务器所对应的的服务器组中有多台静态服务器时，ADSG 转发流量所采取的负载均衡算法。 关于负载均衡算法的解释，请参见 3.2.3 负载均衡 。
健康监视器	探测后端服务器健康状态的方式，包括 TCP Ping、UDP Ping、ICMP Ping、HTTP Ping 和 HTTPS Ping 五种。

5. 右键点击所选服务器组的**静态服务器**项，选择**添加静态服务器**。在**静态服务器基本配置**区域进行相关配置。



参数	说明
IP 地址	提供服务的静态服务器的 IP 地址。
权重	ADSG 作为负载均衡器转发流量时，为静态服务器分配的权重比。 只有选择基于权重的负载均衡算法时，权重值才生效。
检测 IP	用于检测服务器健康状态的 IP 地址。
健康检测 端口	静态服务器提供服务的端口。
模式	静态服务器的工作模式。有三种模式可选分别为 DSNAT、DNAT 和 DR。三种模式对请求处理速度由慢到快为 DSNAT、DNAT 和 DR。三种模式对网络及静态服务器的要求如下： <ul style="list-style-type: none"> ▪ DSNAT：DSNAT 对网络拓扑没有要求。由 ADSG 接收客户端请求，替换源、目的 IP 地址并转发给后端服务器，后端静态服务器的应答发送给 ADSG，由 ADSG 转发给客户端。 ▪ DNAT：DNAT 模式要求后端服务器的网关都要配置为 ADSG 的接口 IP 地址。由 ADSG 接收客户端请求，替换目的 IP 地址为后端服务器真实 IP 地址，并转发给后台静态服务器，后端静态服务器将应答报文发送给 ADSG，由 ADSG 转发给客户端。 ▪ DR：要求 ADSG 和静态服务器在同一网段内；每台静态服务器都需要在 loopback 接口上配置虚拟服务器的虚拟 IP 地址；loopback 接口的 ARP 应答需关闭。由 ADSG 接收客户端请求，替换 MAC 地址为后端服务器网卡 MAC 地址并转发，后端服务器直接发送相应报文到客户端。

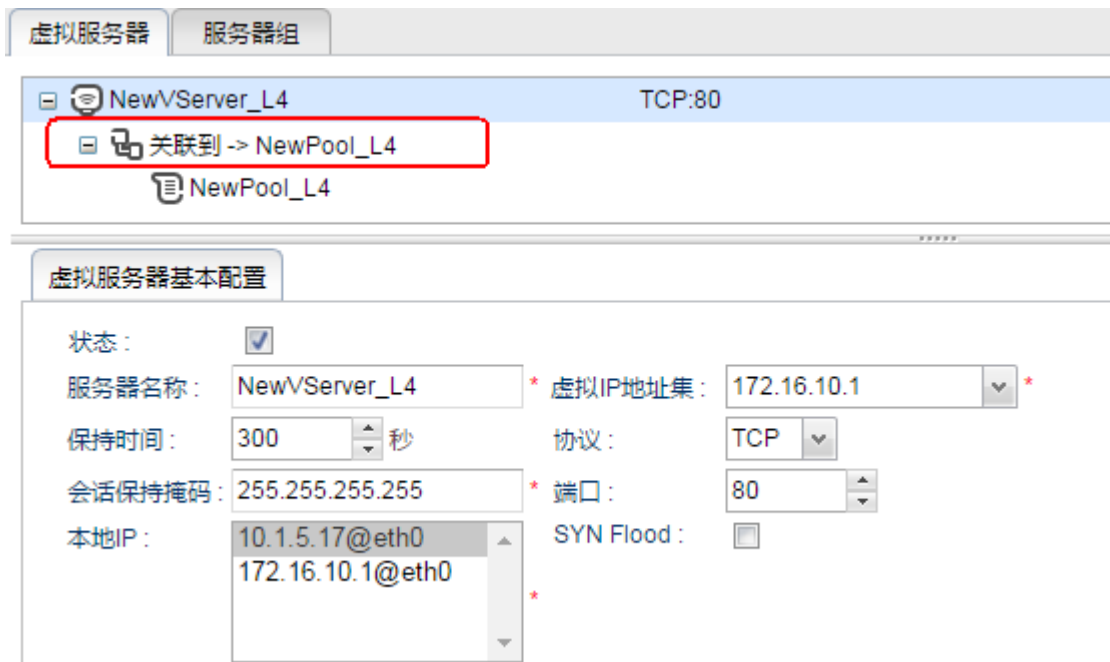
健康状态 静态服务器的通信状态，分别为：up、down 和 unknown。

- up 表示与后端服务器通信正常；
- down 表示与后端服务器通信异常；
- unknown 表示系统未开启健康检测功能。

6. 点击**保存**。

如启用健康状态监控功能，在连通正常的情况下，一段时间后，健康状态变为 up。

7. 点击**虚拟服务器**页签，右键点击对应的关联到项，点击**修改服务器组**，双击需要关联的服务器组，关联虚拟服务器和服务器组。



8. 点击**保存**。

3.2.2. 会话保持

会话保持功能是指在一个 HTTP 会话建立后，当基于这条会话的请求到达 AD SG 时，AD SG 会将其转发给参与建立该会话的服务器。

会话保持功能可以与任意负载均衡算法配合使用。当一个新的请求到来时，AD SG 先根据负载均衡算法将其转发到后端服务器，从而建立会话；当基于这个会话的请求再次到来时，AD SG 会根据会话保持算法直接将请求转发给系统的服务器。

会话保持配置在虚拟服务器上，AD SG 默认开启四层流量的会话保持功能。要配置会话保持功能，请执行以下操作：

1. 选择**虚拟服务>流量管理（四层）>虚拟服务器>（虚拟服务器名称）**。



2. 在**虚拟服务器基本配置**区域配置会话保持的时间、本地 IP。

参数	说明
保持时间	会话保持的超时时间。超过此时间，会话保持关系将被取消。
本地 IP	与关联的静态服务器能够通信的 IP 地址。

3. 点击**保存**。

3.2.3. 负载均衡

通过负载均衡，ADSG 可以根据服务器的可用性和服务能力将客户端请求发送到最合适后端服务器。

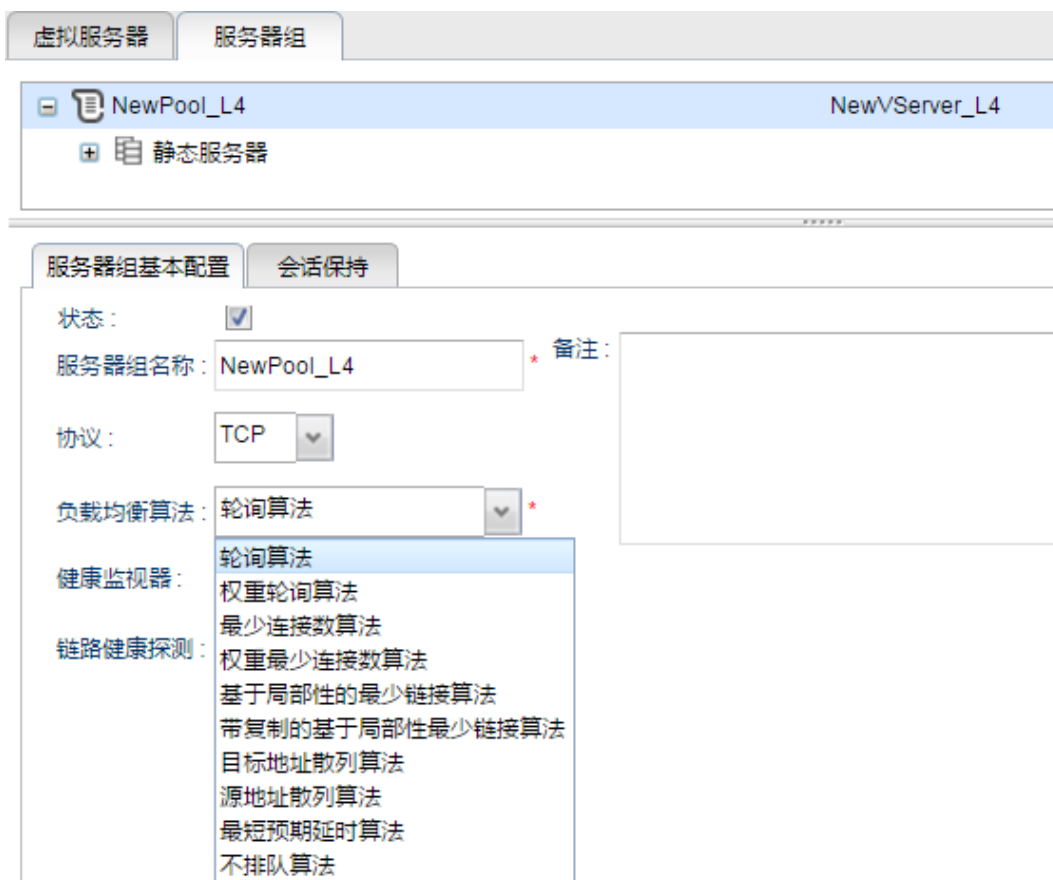
ADSG 支持以下几种负载均衡算法：

- **轮询算法：** Round Robin（简称 RR），将请求依次转发给不同的服务器，而不管服务器实际的连接数和系统负载。
- **权重轮询算法：** Weighted Round Robin（简称 WRR），根据权重将请求依次转发给不同的服务器，权重越大的服务器收到请求的次数就越多。这样可以保证处理能力强的服务器处理更多的访问流量。权重根据服务器的处理能力和负载情况设定，ADSG 可以自动问询真实服务器的负载情况，并动态地调整其权重值。
- **最少连接数算法：** Least Connections（简称 LC），将请求转发给并发连接数最少的服务器。如果集群中的真实服务器具有相近的系统性能，采用此种算法可以较好地均衡负载。
- **权重最少连接数算法：** Weighted Least Connections（简称 WLC），根据权重将请求转发给并发连接数最少的服务器，权重越大的服务器收到请求的概率越大。如果集群中的服务器性能差异较大，采用此种算法可以优化负载均衡性能，具有较高权值的服务器将承受较大比例的活动连接负载。ADSG 可以自动问询真实服务器的负载情况，并动态地调整其权重值。
- **基于局部性的最少连接算法：** Locality-Based Least Connections（简称 LBLC），根据请求的目标 IP 地址找出该目标 IP 地址最近使用的服务器，若该服务器是可用的且没有超载，将请求发送到该服务器；若服务器不存在，或者该服务器超载且有服务器处于一半的工作负载，则根据"最少连接"的原则选出一个可用的服务器，将请求发送到该服务器。此种算法主要用于 Cache 集群系统。
- **带复制的基于局部性最少链接算法：** Locality-Based Least Connections with Replication（简称 LBLCR），同 LBLC 算法相似，不同之处是它要维护从一个目标 IP 地址到一组服务器的映射，而 LBLC 算法维护从一个目标 IP 地址到一台服务器的映射。该算法根据请求的目标 IP 地址找出该目标 IP 地址对应的服务器组，按"最少连接"原则从服务器组中选出一台服务器：若服务器没有超载，将请求发送到该服务器；若服务器超载，则按"最少连接"原则从这个集群中选出一台服务器，将该服务器加入到服务器组中，并将请求发送到该服务器。同时，当该服务器组有一段时间没有被修改，则将最忙的服务器从服务器组中删除，以降低复制的程度。

- **目标地址散列算法：** Destination Hashing（简称 DH），根据请求的目标 IP 地址，作为散列键 (HashKey) 从静态分配的散列表找出对应的服务器，若该服务器是可用的且未超载，将请求发送到该服务器，否则继续查询下一台服务器。
- **源地址散列算法：** Source Hashing（简称 SH），根据请求的源 IP 地址，作为散列键 (HashKey) 从静态分配的散列表找出对应的服务器，若该服务器是可用的且未超载，将请求发送到该服务器，否则继续查询下一台服务器。
- **最短预期延时算法：** Shortest Expected Delay（简称 SED），基于 WLC 算法。按以下公式计算服务器当前负载情况： $active * 256 + inactive = overhead$ ，从中选出负载最小的一台服务器转发请求。
- **不排队算法：** Never Queue（简称 NQ），将请求转发给一台空闲的服务器，此服务器不一定是最快的那台；如果所有服务器都是繁忙的，则采取最短预期延时算法分配请求。

四层流量负载均衡配置在服务器组上。要配置四层流量负载均衡，请执行以下操作：

1. 选择**虚拟服务>流量管理（四层）>虚拟服务器>（虚拟服务器名称）>服务器组>（服务器组名称）>服务器组基本配置**。
2. 在**负载均衡算法**下拉框中，选择一种负载均衡算法。



3. 点击**保存**。

3.2.4. 自动负载均衡

ADSG 支持通过 SNMP 获取后端服务器的状态信息，用于辅助判断服务器的负载权重。需要先为服务器组选择一种基于权重的负载均衡算法，然后为静态服务器设置 SNMP 相关信息。

自动负载均衡功能配置在静态服务器上。要配置自动负载均衡，请执行以下操作：

1. 选择**虚拟服务>流量管理（四层）>服务器组>（服务器组名称）>服务器组基本配置**，选择一种基于权重的负载均衡算法。
2. 选择**虚拟服务>流量管理（四层）>服务器组>（服务器组名称）>静态服务器>（静态服务器名称）>自动负载均衡配置**：

3. 开启自动负载均衡，设置相关参数。

参数	说明
状态	勾选开启自动负载均衡功能。
监控资源类型	获取后端服务器何种系统资源状态信息，包括空闲 CPU 百分比和实体空闲内存。
监控资源 OID	要监控的系统资源在系统中的对象标识符。
SNMP 版本	获取后端服务器状态信息所使用的 SNMP 协议版本，ADSG 支持 v1、v2c 和 v3。
SNMP 团体字符串	当选择 v1 或 v2c 版本时，需要设置团体字符串，用于验证后端服务器的身份。

SNMP 安全级别	ADSG 与后端服务器之间 SNMP 通信的安全级别，包括不认证不加密、认证不加密和认证并加密三种。
SNMP 安全用户	当选择 v3 版本时，需要设置 SNMP 用户，用于验证后端服务器的身份。
SNMP 验证协议	ADSG 与后端服务器之间 SNMP 通信的认证算法和认证密码。
SNMP 加密协议	ADSG 与后端服务器之间 SNMP 通信的加密算法和密钥。

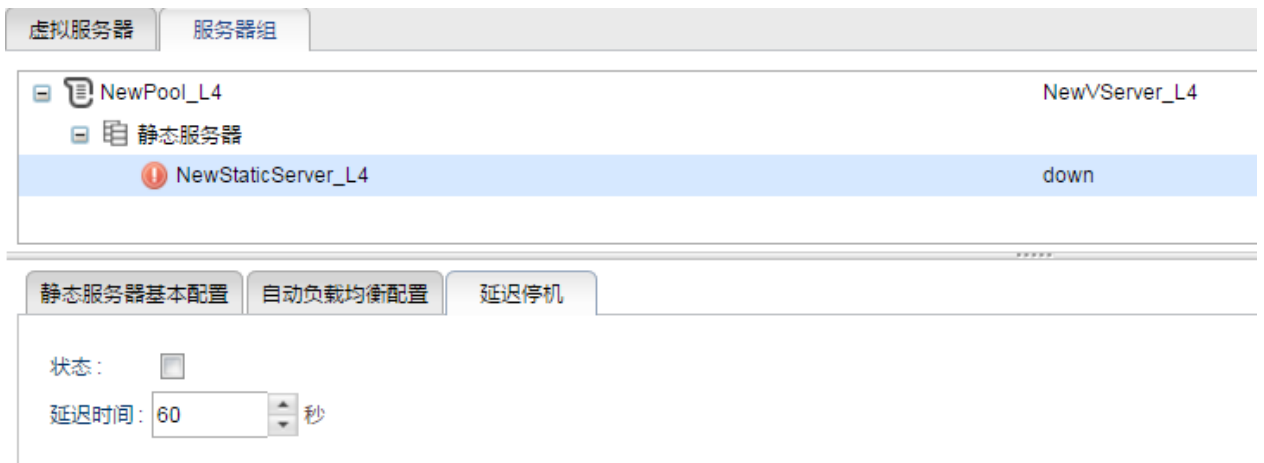
4. 点击**保存**。

3.2.5. 延迟停机

用户可以设置后端服务器的延迟停机时间，保证服务器平滑退出。

延迟停机功能配置在静态服务器上。要配置延迟停机功能，请执行以下操作：

1. 选择**虚拟服务>流量管理（四层）>服务器组>（服务器组名称）>静态服务器>（静态服务器名称）>延迟停机**：



2. 开启延迟停机功能，设置延迟停机时间。
3. 点击**保存**。

3.3. 健康状态监控

开启健康状态监控后，ADSG 可以实时监控与后端服务器的链路状态：当一台服务器出现故障或被移除时，ADSG 不会将客户端流量继续转发到该服务器上，而是根据负载均衡算法将流量分发给其他服务器；当故障服务器恢复工作时，ADSG 还能继续向其转发流量。此功能使 ADSG 具有高容错性。

ADSG 支持以下探测方式：

- **ARP Ping**：以发送 ARP Ping 请求的方式进行探测，可探测服务器是否开机。
- **HTTP Ping**：以发送 HTTP 请求的方式进行探测，可探测具体的 HTTP 应用是否可用。
- **HTTPS Ping**：以发送 HTTPS 请求的方式探测，可探测具体的 HTTPS 应用是否可用。
- **ICMP Ping**：以发送 ICMP 报文的方式进行探测，可探测服务器是否开机。
- **TCP Ping**：以发送 TCP 报文的方式进行探测，可探测服务器端口是否开启。
- **UDP Ping**：以发送 UDP 报文的方式进行探测，可探测服务器端口是否开启。

提示：全局配置健康状态监控后，还需要在服务器组中引用才能生效。

要配置服务器健康状态监控功能，请执行以下操作：

1. 选择**虚拟服务>健康监视器**。
2. 查看缺省的探测方式。

健康监视器

动作

名称	方式	状态
ARP_Ping	ARP	✓
HTTP_Ping	HTTP Ping	✓
HTTPS_Ping	HTTPS Ping	✓
ICMP_Ping	ICMP Ping	✓
TCP_Ping	TCP Ping	✓
UDP_Ping	UDP Ping	✓

基本配置

状态：

名称： *

方式： ▼

访问的资源：

期望的应答：

请求超时： *秒

失败阈值： *次

成功阈值： *次

请求间隔： *秒

3. 点击**动作**，选择**添加健康监视器**，根据需要设置服务器健康检测方式。

基本配置

状态：

名称：

方式：

访问的资源：

期望的应答：

请求超时： *秒

失败阈值： *次

成功阈值： *次

请求间隔： *秒

参数	说明
状态	勾选复选框，启用新建健康监视器。
名称	新建健康监视器名称。
方式	探测方式，包括 ARP Ping、TCP Ping、UDP Ping、ICMP Ping、HTTP Ping 和 HTTPS Ping。 当选择 HTTP Ping 或 HTTPS Ping 探测方式时，还需要指定： <ul style="list-style-type: none"> ▪ 访问的资源：探测后端服务器状态时访问的资源路径，默认为服务器根路径“/”。 根路径下包含的资源较多，应答响应时间较长。为了提高探测效率，可指定访问资源为具体路径下的某个静态文件。例如：/index.html、/status.php 或 /imgae/favorico。 此处仅需输入一个资源路径。 ▪ 期望的应答：期望收到的第一个 HTTP 应答报文。只有收到期望应答时，才认为被探测应用为可用状态。 例如：200 OK、301 或 Success。缺省为 200 OK。 可以为空，表示服务器返回任意内容的 body，系统都认为被探测应用可用。 此处仅需输入一个期望应答值。支持正则表达式。
请求超时	发送的探测报文在这个时间内得不到应答就会认为探测失败。
失败阈值	探测连续失败的次数超过这个阈值就会认为被探测服务器或应用不可访问。
成功阈值	探测连续成功的次数超过这个阈值就会认为被探测服务器或应用可以访问。
请求间隔	发送探测报文的时间间隔，这个数值必须大于请求超时时间。

4. 点击**保存**。

5. 选择**虚拟服务>流量管理（七层/四层）>服务器组>（服务器组名称）>服务器组基本配置**，从健康监视器下拉列表选择一个健康监视器。

提示：健康监视器还可以在**网络>接口>WAN**页面引用，用于监控链路状态。

6. 在上方查看区域可以查看对静态服务器的探测结果：

- **up:** 服务器工作正常。
- **down:** 服务器出现故障，工作异常。
- **unknown:** 当关闭监控状态监控时，服务器健康状态未知。系统默认会向服务器转发流量，如果没有收到服务器应答，则停止转发流量。

第4章 Web 安全

Web 相关服务已经成为互联网上的主流业务，同时也成了网络攻击的首选目标。近年来，Web 服务器频繁遭受网络攻击的事件时有发生，如 SQL 注入、网页被篡改、信息失窃，甚至被用作传播木马的“肉鸡”，Web 安全形势日趋严峻。

攻击者首选 Web 服务器的原因有二：

- Web 服务器自身存在技术上的安全漏洞和安全隐患；
- 相关的防护设备和防护手段有欠缺。

ADSG 基于东软在安全领域的多年积淀，提供被动防御和主动防御的全方位防护手段，不仅能够防范 SQL 注入、XSS（跨站脚本）等常见攻击，而且能防范未知攻击的威胁。

本章介绍如下内容：

- [4.1 安全策略](#)
- [4.2 主动防御](#)
- [4.3 DDoS 防御](#)
- [4.4 漏洞扫描](#)

4.1. 安全策略

要应用 Web 安全防护功能，首先需要创建安全策略，然后在七层虚拟服务器的资源路径上引用。每条资源路径可引用一条安全策略，每条安全策略可被多条资源路径所引用。

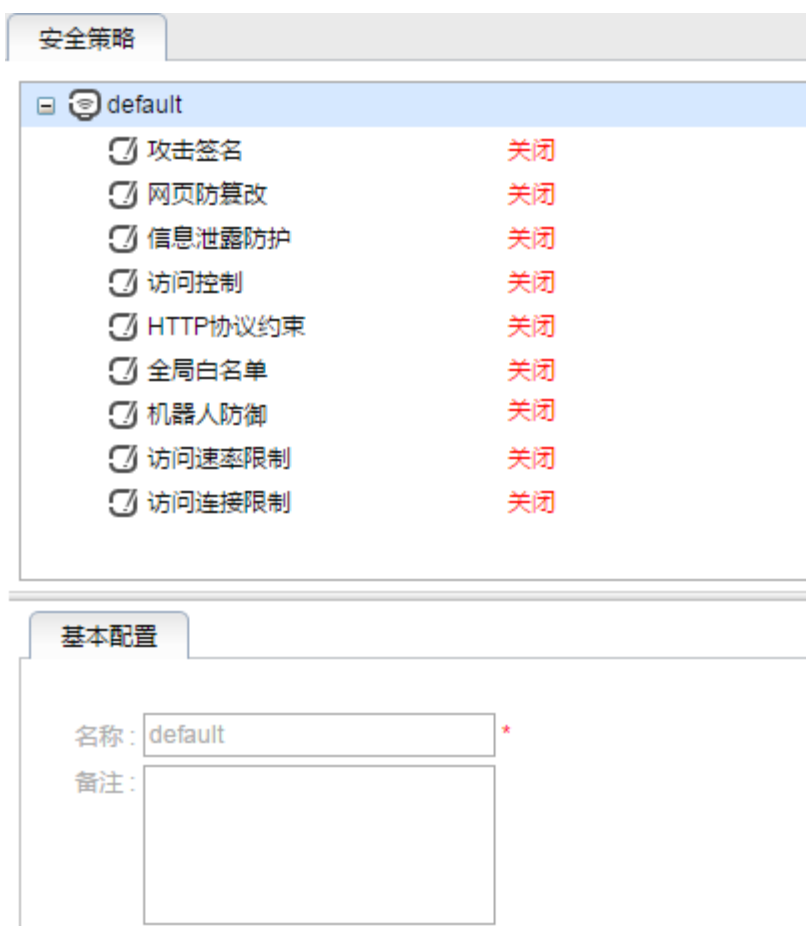
本节介绍如下内容：

- [4.1.1 添加和引用安全策略](#)
- [4.1.2 编辑安全策略](#)

4.1.1. 添加和引用安全策略

要添加和引用安全策略，请执行以下操作：

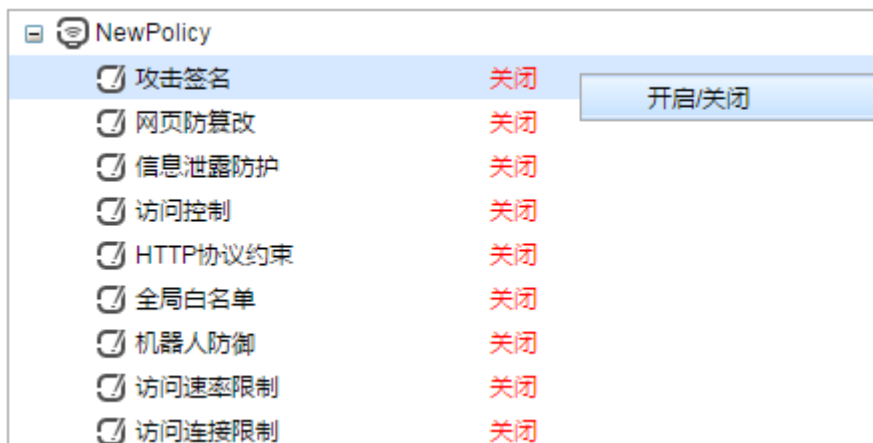
1. 选择 **Web 安全>安全策略**。
2. 缺省情况下，系统自带一条 default 安全策略。该条策略可编辑，不可删除。



3. 在查看区域的空白处点击右键，选择**添加安全策略**，设置新建策略的名称和备注。



- 缺省情况下，新建安全策略中的各项功能均为关闭状态，可右键点击对应功能项，然后点击**开启/关闭**，开启对应功能。



- 点击策略中的任意一项功能，可在下方进行编辑。详细步骤请参见下一节。

4. 选择**虚拟服务>流量管理（七层）>虚拟服务器>（虚拟服务器名称）>（虚拟资源路径名称）**，在下方资源路径基本配置区域的安全策略下拉框中，选取所需安全策略。

资源路径基本配置 | 内容缓存 | 内容压缩 | 客户端代理设置 | 服务器端代理设置 | 资源路径高级配置

状态：

资源名称：

资源路径：

转换后路径：

关联到

本地提示页面

安全策略：

备注：

default
NewPolicy

5. 点击**保存**。

4.1.2. 编辑安全策略

本节介绍如何编辑安全策略中的如下功能：

- [4.1.2.1 攻击签名](#)
- [4.1.2.2 网页防篡改](#)
- [4.1.2.3 信息泄露防护](#)
- [4.1.2.4 访问控制](#)
- [4.1.2.5 HTTP 协议约束](#)
- [4.1.2.6 全局白名单](#)
- [4.1.2.7 机器人防御](#)
- [4.1.2.8 访问速率限制](#)
- [4.1.2.9 访问连接限制](#)

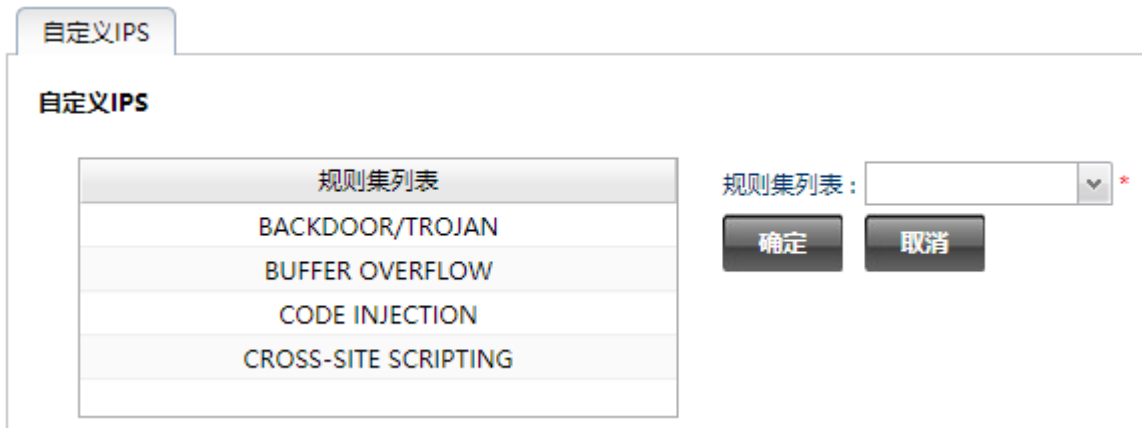
4.1.2.1. 攻击签名

此功能可以解析 HTTP 报文并将其与已知攻击的特征进行匹配，从而发现攻击并采取相应动作。

要配置攻击签名检测，请执行以下操作：

1. 选择 **Web 安全>安全策略**。
2. 在查看区域右键点击对应策略的**攻击签名**，点击**开启/关闭**，开启攻击签名功能。

3. 在自定义 IPS 配置区域进行相关配置。



在规则集列表中通过选择相应的 IPS 规则，将其加入到左侧的列表中。系统将根据加入列表中的规则对进入系统的 HTTP 报文进行安全检查，具体可参见 [5.5 自定义 IPS 规则](#)。

4. 点击保存。

4.1.2.2. 网页防篡改

本功能用于监控后端服务器的网页是否被异常更改，ADSG 能够在检测到网页被异常更改后记录日志。

ADSG 的“网页防篡改”功能通过预先生成网站资源指纹，并在访问请求到达时检测待访问网页的指纹是否发生变化，据此判断网页是否被异常更改。当检测到网页被异常更改后，ADSG 将根据预先的配置终止本次访问或者给客户端返回事先备份的网页，从而防止被篡改网页的内容外泄。

要配置网页防篡改功能，请执行以下操作：

1. 选择 **Web 安全>安全策略**。
2. 在查看区域右键点击策略对应的**网页防篡改**，点击**开启/关闭**，开启网页防篡改功能。
3. 在**基本配置**区域进行相关配置。



网页防篡改的配置参数

配置参数	说明
默认文件名	Web 应用首页对应的文件名称，比如：index.html。
服务器根路径	Web 服务器的根目录。比如：Linux 下，Apache 服务器的根路径缺省为/var/www/html。 Windows 操作系统的 Web 服务器不需要配置此参数。
资源文件路径	指 Web 应用的资源文件在服务器中所处的文件路径名称。这个是相对于“服务器根路径”而言的相对路径。比如：对于工作在 Apache 服务器下的 phpbb 应用，其完整的 Web 资源路径为/var/www/html/phpbb，此处填写资源文件的文件夹名称“phpbb”即可。
备份文件路径	Web 资源备份文件所在的路径。资源文件备份在 Web 服务器上。此路径也是相对于“服务器根路径”而言的相对路径。 当动作选择“恢复”或“恢复并记录日志”时，备份文件路径为必填项。
主机名/IP 地址	指 Web 服务器的域名或者 IP 地址。 配置域名时，需要配置 AD SG 的域名服务器，以便能够成功解析服务器的域名。
主机系统	主机的操作系统，包括 Linux 和 Windows。
用户名	指访问 Web 服务器时使用的用户名称，这个参数仅对 Windows 服务器有效。
密码	指访问 Web 服务器时使用的用户口令，这个参数仅对 Windows 服务器有效。
动作	指检测到网页被篡改时，AD SG 系统采取的动作，包括： <ul style="list-style-type: none"> ▪ 恢复：仅恢复 Web 资源文件，不记录日志。 ▪ 恢复并记录日志：读取之前备份的 Web 资源文件并返回给客户端，同时记录日志。 ▪ 阻断并返回提示信息：阻断当前访问，并返回 403 错误。 ▪ 阻断并记录日志：阻断当前访问，返回 403 错误，并记录日志。

4. 点击**保存**，提交配置。

5. 点击**应用**，使网页防篡改的配置生效。点击**应用**按钮时，系统将完成如下交互过程：

a. 挂载 Web 服务器上的 Web 资源文件到 AD SG。

a. 生成 Web 资源文件的指纹数据。

提示： 点击该按钮仅使当前策略的网页防篡改配置生效。

6. 点击**取消应用**，可取消上一次应用的网页防篡改配置。

4.1.2.3.信息泄露防护

本功能通过对后台敏感信息进行替换或者对包含敏感信息的应答进行阻断，来防止后端服务器中的敏感信息泄露。

要配置信息泄露防护功能，请执行以下操作：

1. 选择 **Web 安全>安全策略**。
2. 在查看区域右键点击策略对应的**信息泄露防护**，点击**开启/关闭**，开启信息泄露防护功能。
3. 在**基本配置**页面修改预定义防护规则，设置其他相关配置。

基本配置
高级配置

预定义防护列表

<input type="checkbox"/>	类型
<input checked="" type="checkbox"/>	身份证
<input type="checkbox"/>	电话号码
<input checked="" type="checkbox"/>	信用卡
<input checked="" type="checkbox"/>	储蓄卡

其他配置

日志：

解压应答体：

媒体类型：

动作：

最后修改时间标记：

信息泄露防护的配置参数（基本配置）

参数	说明
预定义防护列表	需要被防护的信息，有身份证、电话号码、信用卡、储蓄卡四项可选。
日志	是否产生信息泄露防护日志。可在 查看>日志>攻击日志 页面查看产生的日志。
解压应答体	勾选后可以阻止服务器对 HTTP 应答进行压缩处理，以便系统对应答中的敏感信息进行过滤。如 HTTP 应答被服务器压缩，系统将不能进行敏感信息检测，所以推荐勾选该选项。
媒体类型	设置需要进行敏感信息过滤的媒体类型。
动作	包括替换和阻断。替换表示替换检测到的敏感信息，阻断表示阻断本次 HTTP 应答。
最后修改时间标记	选择是否清空或者保持应答头中的 Last-Modified 标记。

4. （可选）在**高级配置**页面添加替换规则。



信息泄露防护的配置参数（高级配置）

参数	说明
忽略大小写	匹配规则时，是否忽略大小写。
原始值	被替换的值或其正则表达式。
替换值	替换后的值或其正则表达式。

5. 点击**保存**。

4.1.2.4. 访问控制

访问控制是指根据访问者的特征（如 IP 地址、用户名等）来控制其可以访问的网络资源或禁止其访问网络资源的一种技术手段，通常通过访问控制规则的形式来体现。同时，它也是系统管理员在管理网络中最常用的工具之一。

ADSG 根据请求头、URL、IP 地址和请求方法对 HTTP 请求进行访问控制。

要配置访问控制功能，请执行以下操作：

1. 选择 **Web 安全>安全策略**。
2. 在查看区域右键点击策略对应的**访问控制**，点击**开启/关闭**，开启访问控制功能。

3. 在下方**请求头配置**页面配置请求头过滤条件。

请求头配置 | URL配置 | 允许的请求方法

请求头条件设置

全局动作: 允许

动作: 禁止

日志:

HTTP头	运算符	取值
If-Match	~*	ASD

HTTP头: If-Match *

运算符: 匹配(不区分大小写) *

取值: ASD * 取值支持SEnginx/Nginx变量

确定 取消

请求头配置参数

参数	说明
全局动作	对于所有 HTTP 请求的缺省处理动作。
动作	对匹配访问控制规则的 HTTP 请求所采取的动作。
日志	允许或拒绝匹配的 HTTP 请求时是否产生日志。
HTTP 头	指定对 HTTP 头中的什么内容进行过滤。支持自动补齐和用户自定义 HTTP 头。
运算符	指定如何过滤 HTTP 请求头。
取值	HTTP 头要进行比对的值。

提示: 具体规则的动作应不同于全局缺省动作。

4. 点击 **URL 配置** 页签，配置 URL 相关信息。

请求头配置 | URL配置 | 允许的请求方法

HTTP路径设置

URL	运算符	动作	日志
abc	~*	Deny	Enabled

URL: abc *

运算符: 匹配(不区分大小写) *

动作: 禁止

日志:

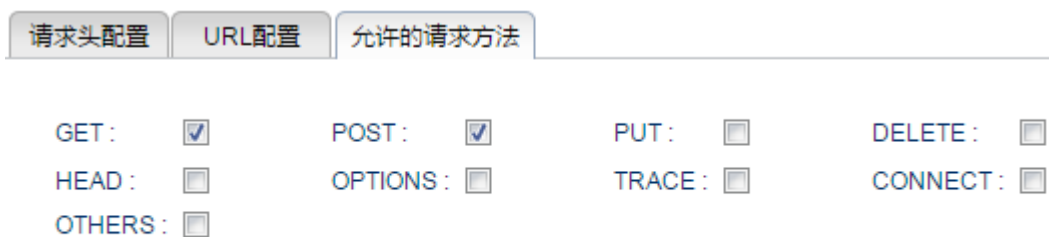
确定 取消

URL 配置参数

参数	说明
URL	指定对 HTTP 头中的 URL 进行过滤时要匹配的字符串。
运算符	指定如何过滤 HTTP 请求头。
动作	对匹配访问控制规则的 HTTP 请求所采取的动作。
日志	允许或拒绝匹配的 HTTP 请求时是否产生日志。

提示：具体规则的动作应不同于**请求头配置**中的全局缺省动作。

5. 点击允许的请求方法页签，配置允许的请求方法。



请求头配置 URL配置 允许的请求方法

GET: POST: PUT: DELETE:

HEAD: OPTIONS: TRACE: CONNECT:

OTHERS:

注意：选择的方法是被允许的

ADSG 针对 HTTP 请求的“方法”进行访问控制，使用所勾选方法的 HTTP 请求将被允许通过。

6. 点击**保存**。

4.1.2.5.HTTP 协议约束

HTTP 协议约束主要是根据 HTTP 协议自身的属性（如报文头、报文体长度等）去分析客户端请求内容，并根据分析的结果对客户端请求采取下一步处理动作。

要配置 HTTP 协议约束，请执行以下操作：

1. 选择 **Web 安全>安全策略**。
2. 在查看区域右键点击策略对应的 **HTTP 协议约束**，点击**开启/关闭**，开启 HTTP 协议约束功能。
3. 在下方**基本配置**页面，通过拖动滑块设置相关功能的阈值，并设置相应的处理动作。

配置项	滑块	单位	动作
HTTP请求长度	小	自定义 16777216 Bytes	放行
HTTP请求头长度	小	自定义 4096 Bytes	放行
HTTP请求头中最大行长度	小	自定义 2048 Bytes	放行
URL长度	小	自定义 4096 Bytes	放行
HTTP请求头行数	小	自定义 16	放行
URL参数个数	小	自定义 16	放行
请求中Cookies的个数	小	自定义 16	放行
Range头域请求实体的范围	小	自定义 5	放行
检测主机名的合法性	关	开	放行
检测HTTP版本	关	开	放行

4. (可选)点击**高级配置**选项卡，添加高级规则，限制请求头字段的最大长度和动作。

HTTP头	大小	动作
User-Agent	48	丢弃, 记录日志
Host	32	丢弃, 记录日志

HTTP头: Host *
 大小: 32 *字节
 动作: 丢弃, 记录日志

5. 点击**保存**。

4.1.2.6.全局白名单

全局白名单可允许符合条件的 HTTP 请求跳过指定的安全检查模块，提高系统性能和数据包处理速度。

要配置全局白名单，请执行以下操作：

1. 选择 **Web 安全>全局白名单**。
2. 在查看区域右键点击策略对应的**全局白名单**，点击**开启/关闭**，开启全局白名单功能。
3. 在**基本配置**区域添加白名单条目。

基本配置

白名单列表

状态	名称	IP地址	用户代理	跳过	用户代理忽略大小写
✓	whitelist1	2.2.2.0/24	msie	攻击签名,主动防御,机器人缓解	Enabled
✓	whitelist2	3.3.3.0		HTTP协议约束,网页防篡改,信息泄...	Enabled

详细配置

状态：

名称： *

跳过：

攻击签名
 主动防御
 机器人缓解
 IP访问控制
 访问速率限制
 HTTP协议约束

 *

用户代理忽略大小写：

IP地址

IP地址
2.2.2.0/24

IP地址：

用户代理

用户代理
msie

用户代理： 支持正则表达式

- a. 在**详细配置**区域，设置白名单状态、名称、跳过的检测模块、匹配用户代理条件时是否忽略大小写。
- b. 在**IP地址**区域添加 IP 匹配条件，支持 IP 地址或地址段；在**用户代理**区域添加用户代理匹配条件，可以是浏览器名称或正则表达式。IP 和代理至少设置一项。

c. 点击**确定**，在上方**白名单列表**中将出现新添加的白名单条目。

4. 点击**保存**。

4.1.2.7. 机器人防御

很多黑客通过工具发送少量特定的应用层请求到指定网站，使服务器执行一系列杂乱、耗时的操作，最终导致服务器不堪重负，无法响应正常的请求。这种类型的攻击称之为机器人攻击（又称“应用层 DDoS 攻击”）。

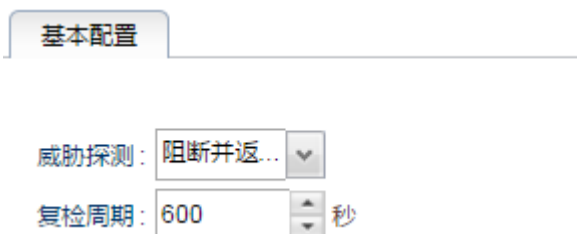
由于其攻击报文发送速率低，使得传统的基于网络层和传输层的 DDoS 防御模块很难检测到。ADSG 通过校验请求发送端是否为正常浏览器，可以使服务器免受机器人攻击的困扰。

ADSG 防御机器人攻击的具体过程如下：

1. 在收到请求后先不转发给服务器，而是返回一个带 javascript 的响应；
2. 如果客户端能够成功解析 javascript，再转发其请求；如果不能解析，则认为其可能是机器人攻击。

要配置机器人攻击防御功能，请执行以下操作：

1. 选择 **Web 安全 > 安全策略**。
2. 在查看区域右键点击策略对应的**机器人防御**，点击**开启/关闭**，开启机器人攻击防御功能。
3. 在下方**基本配置**区域配置防御动作和检测周期。



机器人防御配置参数

参数	说明
威胁探测	探测到机器人攻击威胁时 ADSG 采取的处理动作，目前仅可以选择 阻断并返回提示页面 。 阻断是指丢弃含有威胁的请求报文。
复检周期	指两次探测之间的时间间隔。

4. 点击**保存**。

4.1.2.8.访问速率限制

DDoS 攻击发生时，攻击者通常会利用有限的 TCP 连接发起数量庞大的 HTTP 请求，通过这种方式造成 Web 服务器长时间忙于响应 HTTP 请求，进而影响到正常业务的处理。

ADSG 通过限制客户端与 ADSG 建立的 TCP 连接数以及每条连接上传送 HTTP 应答的速率，来减缓攻击者对服务器的影响。访问速率限制并不影响用户对服务器的访问，只是降低服务器发送应答的速率。访问速率限制主要是基于控制 ADSG 接收客户端请求的速率实现的，超过当前速率的请求会被搁置到延迟队列中。如果延迟队列已满，ADSG 则丢弃该客户端后续的 HTTP 请求。

要配置访问速率限制，请执行以下操作：

1. 选择 **Web 安全 > 安全策略**。
2. 在查看区域右键点击策略对应的**访问速率限制**，点击**开启/关闭**，开启访问速率限制功能。
3. 在下方的**基本配置**区域，设置是否记录日志，添加访问速率限制规则。

The screenshot shows the 'Basic Configuration' section of the ADSG interface. It includes a 'Log Status' checkbox which is checked. Below it is a table with columns: Name, Type, Condition, Queue Length, Rate, and Remark. Two rules are listed: one for 'User-Agent-MSIE' with a queue length of 23 and a rate of 23, and another for '2.2.2.2' with a queue length of 3 and a rate of 3. To the right of the table is a form for adding a new rule, with fields for Name (control01), Queue Length (23), Rate (23/sec), Type (HTTP头), Parameter (User-Agent), Operator (匹配 (区分大小写)), and Value (MSIE). There are '确定' (OK) and '取消' (Cancel) buttons at the bottom.

访问速率限制参数

参数	说明
名称	访问速率限制规则的名称。
类型	速率限制检查的类型，有 HTTP 头、源 IP 和虚拟 IP 三种方式。
参数	指定根据什么条件来匹配访问速率限制规则。只有在类型选择 HTTP 头时才可以配置。 假定客户端所发的 HTTP 请求头中包含自定义参数 <code>Priority</code> ，则可以根据此参数的取值来检查是否对其进行速率限制。
运算符	指定 HTTP 请求如何匹配访问速率限制规则。只有在类型选择 HTTP 头时才可以配置。
取值	要匹配的值。
队列长度	对于要进行速率限制的请求，允许的访问队列的最大长度。

速率	每秒处理的最大请求数。与队列长度共同决定访问速率的限制效果。 当发包速度超出这里指定的处理速率时，系统将 HTTP 请求放入缓存队列；当队列满后，系统将丢弃后续的请求，直至队列中有空闲空间。
备注	访问速率限制规则的备注信息。

ADSG 仅对匹配过滤条件的流量按照配置的速率和队列长度进行速率限制。

4. 点击**保存**。

4.1.2.9.访问连接限制

ADSG 可控制客户端与服务器端建立的连接数，进而防止恶意连接消耗服务器资源。

要配置访问连接限制功能，请执行以下操作：

1. 选择 **Web 安全 > 安全策略**。
2. 在查看区域右键点击策略对应的**访问连接限制**，点击**开启/关闭**，开启访问连接限制功能。
3. 在下方的**基本配置**区域，添加访问连接限制规则。

基本配置

名称	条件	最大连接数	备注
control001	User-Agent~*MSIE	5	
control002	2.2.2.2	6	

名称:	control002	* 最大连接数:	6	(1 ~ 65536)	
条件:	源IP	备注:			
类型:					
参数:					
运算符:					
取值:	2.2.2.2				
<input type="button" value="确定"/> <input type="button" value="取消"/>					

访问连接限制参数

参数	说明
名称	访问连接限制规则的名称。
最大连接数	允许的最大连接数。
类型	连接限制检查的类型，有 HTTP 头和源 IP 两种方式。
参数	指定根据什么参数来匹配连接限制规则。只有在类型选择 HTTP 头时才可以配置。 假定客户端所发的 HTTP 请求头中包含自定义参数 Priority ，则可以根据此参数的取值来检查是否对其进行连接数限制。
运算符	指定 HTTP 请求如何匹配连接数限制规则。只有在类型选择 HTTP 头时才可以配置。
取值	要匹配的值。
备注	访问连接数限制规则的备注信息。

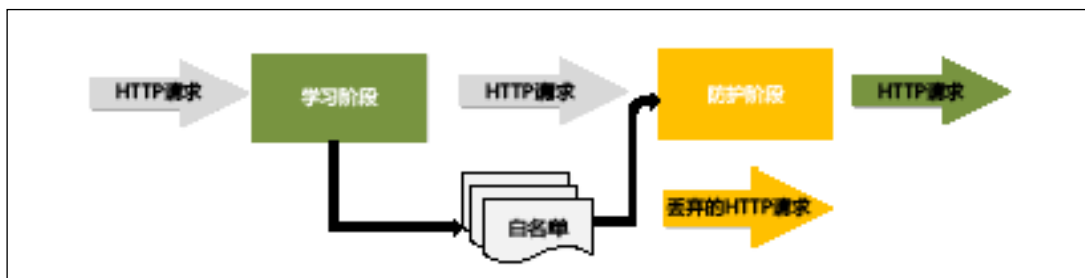
ADSG 仅对匹配过滤条件的流量按照配置的速率和队列长度进行访问连接数限制。

4. 点击**保存**。

4.2. 主动防御

ADSG 的主动防御功能基于主动学习模式，分为学习阶段和防御阶段：在学习阶段基于白名单的方式建立安全访问模型；在进入防御阶段后，系统将针对不符合安全模型的访问进行打分，当分值达到设定阈值后，该访问将作为恶意请求处理。

系统的安全访问模型基于东软在安全领域多年积累形成的核心威胁库构建而成，不仅能够防御诸如 SQL 注入、跨站脚本等知名攻击手段，而且基于宽泛的安全规则集合，可以防范未知攻击。



要配置主动防御功能，请执行以下操作：

1. 选择**虚拟服务>流量管理（七层）**，添加虚拟服务器。
2. 选择 **Web 安全>主动防御**，在**查看区域**点击对应的虚拟服务器资源。

3. 在下方**基本配置**区域进行相关配置。

基本配置

学习信息

基本设置

状态：

日志状态：

动作：阻断

URI共享内存： MB*

学习次数：

IP白名单
1.1.1.1

IP白名单：

确定 取消

URI白名单	类型
/abc	普通字符串

类型：
 普通字符串
 正则表达式

URI白名单：

确定 取消

阈值设置

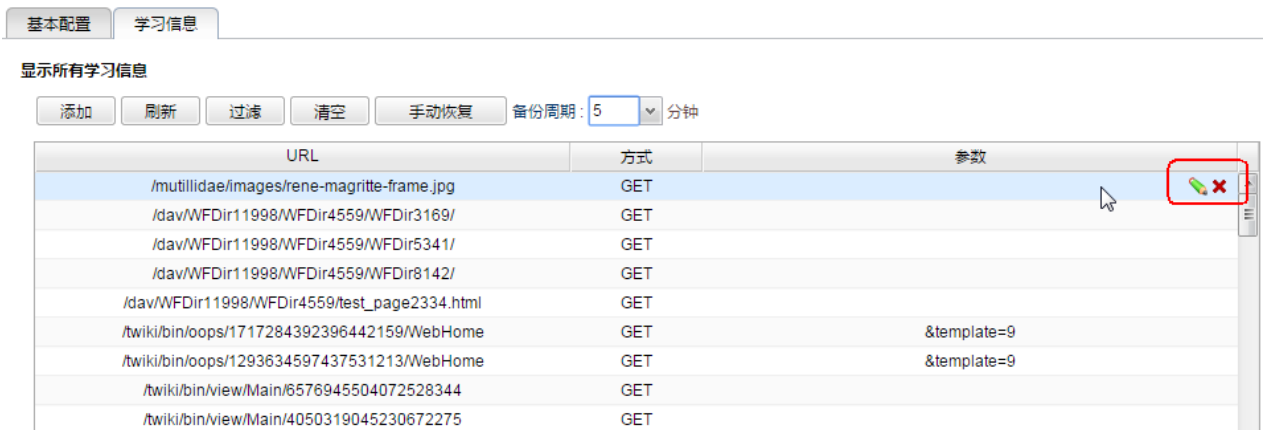
	小	中	大	自定义
SQL注入：	<input type="range" value="24"/>			<input style="width: 50px;" type="text" value="24"/>
远程文件包含：	<input type="range" value="24"/>			<input style="width: 50px;" type="text" value="24"/>
路径遍历：	<input type="range" value="12"/>			<input style="width: 50px;" type="text" value="12"/>
跨站脚本攻击：	<input type="range" value="12"/>			<input style="width: 50px;" type="text" value="12"/>
Evading Tricks：	<input type="range" value="24"/>			<input style="width: 50px;" type="text" value="24"/>
ASP/PHP文件上传：	<input type="range" value="24"/>			<input style="width: 50px;" type="text" value="24"/>

主动防御基本设置参数

参数	说明
状态	控制主动防御的开启或者关闭。勾选表示开启。
日志状态	是否生成主动防御日志。勾选表示生成日志。
动作	主动防御模块检测到攻击时 AD SG 的处理动作，包括阻断和放行。
URI 共享内存	为自学习防御系统分配的记录资源特征的共享内存。推荐配置为 30M。
学习次数	某个资源由学习状态变为可信状态的学习次数。默认为 3 次。

- IP 白名单** IP 地址白名单，含有这些 IP 地址的请求包直接放行。
- URI 白名单** URI 白名单，支持普通字符串和正则表达式两种添加方式。
访问这些 URI 的请求包直接放行。
- 阈值设置** 拖拽滑块可以设置各种攻击的检测阈值，拖拽到最右侧可以输入自定义阈值。
阈值的高低代表了判断攻击的严格程度：阈值越小则越严格，越大则越宽松。

4. 点击**学习信息**页签，能够在此处看到学习记录，并能够对学习记录进行添加、编辑、删除等操作。



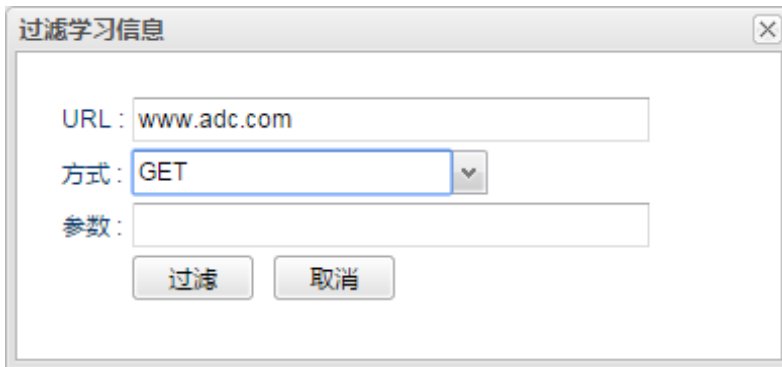
- 点击学习条目后的 图标，可以编辑已有学习记录，编辑后点击**保存**。



- 点击 可删除该条学习记录。
- 点击**添加**，可手动添加一条学习记录，点击**保存**。



- 点击**过滤**，输入过滤条件，点击**过滤**，学习记录中将显示过滤后的内容。



- 点击**清空**，显示的所有学习记录将被清空（只是清空显示框，并未删除）。
- 点击**手动恢复**，可恢复显示之前的学习记录。

当主动防御功能被关闭再开启时，将不会立即显示之前的学习记录，需要先点击**手动恢复**按钮，再点击**刷新**按钮，才能显示之前的学习记录内容。

- **备份周期**是指两次备份学习记录之间的时间间隔。备份周期可选择 5 分钟、15 分钟、30 分钟。

4.3.DDoS 防御

在 Internet 中，当黑客通过控制多个系统对单个目标进行攻击，从而引起目标系统用户的服务遭到拒绝时，即发生了分布式拒绝服务（Distributed Denial of Service，DDoS）攻击。

ADSG 可防范 SYN Flood、UDP Flood 和 ICMP Flood 等多种 DDoS 攻击。

要使用 DDoS 防御功能，请执行以下操作：

1. 选择 **Web 安全>DDoS 防御**。
2. 勾选**状态**复选框，开启 DDoS 防御功能。
3. 通过选择接口，指定要保护的**网络**。

接口配置



4. 开启防护功能，并设置阈值和动作。

防护配置

SYN Flood防护：
 阈值： 包/秒
 动作： ▼
 UDP Flood防护：
 阈值： 包/秒
 动作： ▼
 ICMP Flood防护：
 阈值： 包/秒
 动作： ▼

攻击类型 攻击含义和 AD SG 防护措施

SYN Flood 在短时间内向受害主机发送带有虚假源 IP 地址的 TCP SYN 数据包，使受害主机系统中堆积大量的半连接，直至资源耗尽。

ADSG 可通过限制每秒钟允许通过的 TCP SYN 请求数据包数防御 SYN Flood 攻击。

UDP Flood 在短时间内向受害主机发送大量 UDP 数据包，耗尽主机资源。

ADSG 可通过限制每秒钟允许通过的 UDP 数据包个数防御 UDP Flood 攻击。

ICMP Flood 在短时间内向受害主机发送大量 ICMP 包，耗尽主机资源。

ADSG 可通过限制每秒钟允许通过的 ICMP 数据包个数防御 ICMP Flood 攻击。

5. 添加不进行 DDoS 检测的白名单地址。

白名单配置

源IP地址
192.168.1.11
192.168.2.10-192.168.2.100
10.1.2.0/24

IP类型： ▼
 IPv4地址： *

6. 点击**保存**。

4.4. 漏洞扫描

本功能可以扫描内部服务器的系统漏洞，并且将扫描结果进行文档记录以供下载，便于管理员了解内部服务器存在的漏洞。同时，系统能够自动生成安全策略用来应对内部服务器的漏洞。

要配置漏洞扫描功能，请执行以下操作：

1. 选择 **Web 安全>漏洞扫描**。
2. 配置需要扫描的虚拟服务器、URI 路径及扫描验证信息：

漏洞扫描参数

参数	说明
虚拟服务器	待扫描的虚拟服务器。只有 up 状态的虚拟服务器才支持进行漏洞扫描。
URI	需要扫描的 URI。缺省为根目录。
验证 URL 扫描	是否开启认证扫描。勾选表开启。 <ul style="list-style-type: none"> • 登录 URI：登录 Web 的 URL。 • 用户名域：登录页面表单中用户名的 name。 • 密码域：登录页面表单中密码的 name。 • 用户名：登录用的用户名。 • 密码：登录用的密码。 • 参数：登录时的参数。 • 登录响应信息：登录成功后的关键字标记。 • 退出响应信息：退出登录后的关键字标记。

3. 点击扫描，等待一段时间后系统将生成扫描结果和对应的安全策略。

扫描成功

[点击这里](#) 下载扫描报告  生成的安全策略：[NewVServer](#)

ADSG扫描报告

告警概览

告警级别	告警数量
高	14
中	104
低	352
提示	167

第5章 公共对象

公共对象用于配置服务器负载均衡和链路负载均衡中调用的一些常用地址对象，包括 IP 地址集、ISP 地址集和用户地域。通过配置常用地址对象，可避免用户在配置过程中重复配置相同的 IP 地址。

- [5.1 IP 地址集](#)
- [5.2 ISP 地址集](#)
- [5.3 用户地域](#)
- [5.4 自定义错误页面](#)
- [5.5 自定义 IPS 规则](#)

5.1.IP 地址集

IP 地址集是一组常用的 IP 地址或地址段的集合。IP 地址集主要用于虚拟服务、DNS 代理配、智能路由和 ACL 规则配置。

添加自定义 IP 地址集，请执行以下操作：

1. 选择**公共对象>IP 地址集**。
2. 点击**动作**，选择**添加 IP 地址集**。
3. 在**基本配置**区域，设置 IP 地址集名称，并添加包含的 IP 地址。

基本配置

名称： *

地址集

类型	取值
IPv4地址	10.1.1.1
IPv4地址范围	10.1.2.100-10.1.2.200
IPv4地址/掩码	10.1.3.0/24

类型：

IPv4地址：

确定
取消

提示：为虚拟服务器添加的虚拟IP地址集只能包含单个IP或多个单IP，不能是IP地址段和子网IP；为DNS透明代理添加的虚拟IP地址集只能包含子网IP地址。

4. 点击**保存**。
5. 在虚拟服务、智能路由、ACL 规则或 DNS 透明代理中引用已添加的 IP 地址集。详细信息请参见[第 3 章，虚拟服务](#)，[6.2 透明代理](#)，[8.4 智能路由](#)和 [8.8 ACL 配置](#)。

5.2.ISP 地址集

ISP 地址集用于自定义运营商的 IP 地址段，帮助 AD SG 判断用户链路所属运营商。ISP 地址集主要用于智能 DNS 配置。AD SG 默认提供中国电信、中国移动、中国联通和中国教育网的 IP 地址库，支持自定义。

要查看缺省 ISP 地址集和添加自定义 ISP 地址段，请执行以下操作：

1. 选择**公共对象>ISP 地址集**。
2. 在列表中查看缺省的运营商地址集。

ISP地址集		自动更新
动作		
名称	地址集	
中国教育网	202.192.0.0-202.199.255.255,58.200.0.0-58.207.255.255,210.40.0.0-210.47.255.255,183.172.0.0-183.17...	
中国电信	183.0.0.0-183.63.255.255,36.96.0.0-36.127.255.255,49.64.0.0-49.95.255.255,113.64.0.0-113.95.255.255,...	
中国移动	36.128.0.0-36.191.255.255,183.192.0.0-183.255.255.255,120.192.0.0-120.255.255.255,117.128.0.0-117.1...	
中国联通	27.192.0.0-27.223.255.255,39.64.0.0-39.95.255.255,112.224.0.0-112.255.255.255,120.0.0.0-120.15.255.2...	

3. 点击**动作**，选择**添加 ISP 地址集**，在**基本配置**区域设置新建 ISP 地址集名称和所包含的 IP 地址。

基本配置

名称： *

地址集

地址
1.1.1.1-1.1.1.100
1.1.1.120-1.1.1.150

起始地址： *

终止地址： *

确定
取消

4. 点击**保存**。

5. 打开**自动更新**页签，开启 ISP 自动更新，设置更新间隔和更新时间。

WHOIS 是一个用来查询域名是否已经被注册以及注册域名的详细信息的数据库。ADSG 的 ISP 自动更新服务器地址固定为 `whois.apnic.net`。开启 ISP 自动更新后，ADSG 定期向 `whois.apnic.net` 查询域名注册信息，获取最新的 ISP 地址库。

6. 在 LDNS 集合中引用已添加的 ISP 地址集，详细信息请参见 [7.3 LDNS 集合](#)。

5.3. 用户地域

ADSG 支持根据用户地域判断用户链路，用户地域主要用于智能 DNS。系统默认提供全国 34 个省级行政区域的 IP 地址库，支持自定义。

要添加自定义用户地域，请执行以下操作：

1. 选择**公共对象**>**用户地域**。
2. 在列表中查看缺省的用户地域地址集。

名称	地址集
北京市	110.96.0.0-110.127.255.255,123.64.0.0-123.95.255.255,110.192.0.0-110.223.255.255,36.192.0.0-36.223.2...
天津市	117.8.0.0-117.15.255.255,60.24.0.0-60.27.255.255,125.36.0.0-125.39.255.255,123.150.0.0-123.151.255.2...
河北省	120.0.0.0-120.15.255.255,110.240.0.0-110.255.255.255,27.184.0.0-27.191.255.255,60.0.0.0-60.7.255.255...
山西省	223.8.0.0-223.15.255.255,183.184.0.0-183.191.255.255,171.120.0.0-171.127.255.255,110.176.0.0-110.183...
内蒙古自治区	1.24.0.0-1.31.255.255,1.180.0.0-1.183.255.255,116.112.0.0-116.115.255.255,110.16.0.0-110.19.255.255,...
辽宁省	175.160.0.0-175.175.255.255,113.224.0.0-113.239.255.255,42.248.0.0-42.255.255.255,60.16.0.0-60.23.25...
吉林省	122.136.0.0-122.143.255.255,119.48.0.0-119.55.255.255,175.16.0.0-175.23.255.255,123.172.0.0-123.173....
黑龙江省	1.56.0.0-1.63.255.255,113.0.0.0-113.7.255.255,112.100.0.0-112.103.255.255,122.156.0.0-122.159.255.25...
上海市	180.160.0.0-180.175.255.255,101.80.0.0-101.95.255.255,114.80.0.0-114.95.255.255,116.224.0.0-116.239...

3. 点击**动作**，选择**添加用户地域**，在**基本配置**区域设置用户地域的名称和起始终止 IP 地址。

基本配置

名称： *

地址集

地址
192.168.1.10-192.168.1.100

起始地址： *

终止地址： *

4. 点击**保存**。

5. 在 LDNS 集合中引用已添加的 ISP 地址集，详细信息请参见 [7.3 LDNS 集合](#)。

5.4. 自定义错误页面

ADSG 支持将后台应用服务器返回的错误码以及页面替换为系统自带的页面。系统默认提供从错误码 400 到 505 的错误页面，支持自定义。

要添加自定义错误页面，请执行以下操作：

1. 选择**公共对象>自定义错误页面**。
2. 在列表中查看缺省的系统自带错误定义页面。

名称	页面标题	页面内容
400	Error	400 Bad Request
401	Error	401 Unauthorized
403	Error	403 Forbidden
404	Error	404 Not Found
405	Error	405 Method Not Allowed
406	Error	406 Not Acceptable
407	Error	407 Authentication Required
408	Error	408 Request Timeout

3. 点击**动作**，选择**添加页面**，在**基本配置**区域设置用户地域的名称和起始终止 IP 地址。

基本配置

名称： *

页面标题： *

页面内容： *

4. 点击**保存**。
5. 在 **Web 安全>安全策略>访问控制>响应码转换**中引用已添加的错误页面，详细信息请参见 [4.1.2.4 访问控制](#)。

5.5. 自定义 IPS 规则

ADSG 支持自定义 IPS 规则集，以方便用户根据系统实际情况灵活定义所需要的防护策略。系统默认提供 6 条内置规则集，以应对常见的漏洞攻击，并支持自定义。

要添加自定义 IPS 规则，请执行以下操作：

1. 选择**公共对象>自定义 IPS 规则**。
2. 在列表中查看缺省的系统自带 IPS 规则页面。

规则集	备注	漏洞编号	动作	日志
BACKDOOR/TROJAN	后门和木马防护	37113,37729,35536,35535	Deny	Enabled
BUFFER OVERFLOW	缓冲溢出防护	7443,15949,20814,28393,25044,7268,37578,25395,36611,37525,21,931,1052,1356,1828,183...	Deny	Enabled
CODE INJECTION	代码注入防护	8348,19939,19958,19980,19997,19999,20023,20183,20300,20529,20568,20591,20773,21558,...	Deny	Enabled
CROSS-SITE SCRIPTING	跨站脚本攻击防护	36116,36188,36196,8350,15961,17176,23353,35803,35847,35857,35858,35860,35865,36894,...	Deny	Enabled
OS COMMAND INJECTION	命令注入防护	4430,19944,37517,37594,13068,13888,26186,35592,35662	Deny	Enabled
SQL INJECTION	SQL注入防护	36224,20230,20390,20813,23765,23852,23854,24096,24160,24197,24199,24342,36194,3694...	Deny	Enabled

3. 点击**动作**，选择**添加 IPS 规则**，在**基本配置**区域设置 IPS 规则的名称、备注、动作和日志信息，并在漏洞防护规则列表中根据漏洞和攻击类型选取漏洞防护规则，构成 IPS 规则的具体防护配置组合。

自定义IPS

动作

规则集	备注	漏洞编号	动作	日志
BACKDOOR/TROJAN	后门和木马防护	37113,37729,35536,35535	Deny	Enabled
BUFFER OVERFLOW	缓冲溢出防护	7443,15949,20814,28393,25044,7268,37578,25395,36611,37525,21,931,1052,1356,1828,183...	Deny	Enabled
CODE INJECTION	代码注入防护	8348,19939,19958,19980,19997,19999,20023,20183,20300,20529,20568,20591,20773,21558,...	Deny	Enabled
CROSS-SITE SCRIPTING	跨站脚本攻击防护	36116,36188,36196,8350,15961,17176,23353,35803,35847,35857,35858,35860,35865,36894,...	Deny	Enabled
OS COMMAND INJECTION	命令注入防护	4430,19944,37517,37594,13068,13888,26186,35592,35662	Deny	Enabled
SQL INJECTION	SQL注入防护	36224,20230,20390,20813,23765,23852,23854,24096,24160,24197,24199,24342,36194,3694...	Deny	Enabled

基本配置

名称： *

备注：

动作：允许 *

日志：

漏洞编号	规则编号	CVE	漏洞名称	攻击类型	选择
36711	10806	CVE-2...	2daybiz Matrimonial Scri...	SQL INJECTION	<input checked="" type="checkbox"/>
36707	10805	CVE-2...	2daybiz Multi Level Mark...	SQL INJECTION	<input checked="" type="checkbox"/>
36705	10799	CVE-2...	2daybiz Video Communi...	CODE INJECTION	<input checked="" type="checkbox"/>
36712	10807	CVE-2...	2daybiz Video Communi...	SQL INJECTION	<input type="checkbox"/>
36706	10804	CVE-2...	2daybiz Web Template S...	SQL INJECTION	<input type="checkbox"/>
9914	4857	CVE-2...	3Com 3CRADSL72 ADSL	LINPROPERLY A	<input type="checkbox"/>

对于“动作”、“日志”，有如下组合配置：

- **允许**：将报文转发，此外没有其它任何动作。
- **允许、记录日志**：将报文转发，并将此次攻击记录在日志中。

- **禁止：** 丢弃报文，此外没有其它任何动作。
 - **禁止、记录日志：** 丢弃报文，并将此次攻击记录在日志中。
4. 点击**保存**。
 5. 在 **Web 安全>安全策略>攻击签名>**中引用已添加的自定义规则，详细信息请参见 [4.1.2.1 攻击签名](#)。

第6章 DNS 代理

当内网没有 DNS 服务器且出口存在 2 条或 2 条以上链路时，为达到出站链路负载均衡和优化带宽利用的目的，通常会使用 DNS 代理功能。ADSG 可以作为 DNS 代理，代理内网 PC 去找相应的 DNS 服务器完成域名解析，以优化 DNS 解析过程。

本章介绍 ADSG 的 DNS 代理功能，内容包括：

- [6.1 网关 DNS](#)
- [6.2 透明代理](#)
- [6.3 前置调度](#)
- [6.4 内网记录](#)

ADSG DNS 代理功能的配置逻辑如下所示：



DNS 代理配置步骤

配置项	操作路径	备注
1.配置网络接口。	网络>接口>WAN	可同时配置链路繁忙比例和链路健康监控。
	网络>接口>LAN	
2.配置出站链路负载均衡。	网络>智能路由	添加内网用户访问外网时，通往不同链路的出站路由。
	网络>源地址转换	
3.配置 DNS 代理。	DNS 代理>网关 DNS	添加外网 DNS 服务器，用于解析内网 DNS 请求。

DNS 代理>透明代理

启用 DNS 透明代理，指定 DNS 代理范围以及调度策略。

如果需要对内网 PC 的 DNS 请求统一管理，需要配置 DNS 透明代理的监听地址为 AD SG 的 LAN 口地址，并将内网 PC 的 DNS 服务器设置为该 LAN 口地址。

DNS 代理>前置调度

如有特殊域名需要通过指定 DNS 服务器进行解析，请添加前置调度策略。

DNS 代理>内网记录

4.配置内网 PC 的 DNS 服务器。

- 如果配置透明代理的监听地址为 AD SG 的 LAN 口 IP，则内网 PC 的 DNS 服务器也指定为该 LAN 口 IP。
- 如果未配置透明代理的监听地址，则内网 PC 的 DNS 服务器地址指定为本地运营商的公网 DNS 服务器地址。

6.1.网关 DNS

要使用 AD SG 的 DNS 代理功能，需指定公网 DNS 服务器，用于解析内网 DNS 请求。

要配置网关 DNS 服务器，请执行以下操作：

1. 选择 **DNS 代理>网关 DNS**。
2. 点击**动作**，选择**添加 DNS 服务器**。
3. 在下方**基本配置**区域，填写相关信息。

网关 DNS 配置参数

参数	说明
IP 地址	用于解析内网 DNS 请求的外网 DNS 服务器的 IP 地址。
WAN 口	连接外网 DNS 服务器的 WAN 口。
权重	DNS 服务器所在链路的权重。 用于为内网 DNS 请求选择 DNS 服务器时选路使用。

4. 点击**保存**。

5. 同样方式添加更多 DNS 服务器。
6. 查看已添加的 DNS 服务器。

ip地址	WAN口	权重
202.118.2.11	WAN1	1
58.16.2.12	WAN2	2

6.2.透明代理

ADSG 的 DNS 透明代理功能默认关闭。开启后，需指定调度策略和调度范围。

要配置 DNS 透明代理，请执行以下操作：

1. 选择 **DNS 代理>透明代理**。
2. 启用 DNS 透明代理，并设置相关参数。

状态：

 监听地址：

 监听端口：

 内容缓存：

 调度策略：

 代理目标范围：

 用户：

 探测域名： *

前置调度策略：

 繁忙保护：

透明代理配置参数

参数	说明
状态	勾选启用 DNS 透明代理。
监听地址	指定要监听的内网接口 IP 地址。 当需要对内网用户的 DNS 请求做统一管理时，需要设置监听地址。监听地址需要设置为 ADSG 的 LAN 口 IP 地址，内网 PC 的 DNS 服务器地址也需要设置为该 IP 地址。
监听端口	指定要监听来自哪个端口的内网 DNS 请求。
内容缓存	是否启用 DNS 透明代理的缓存功能。 启用内容缓存后，DNS 服务器返回的域名解析结果将被缓存在 ADSG 本地，下一次再有内网用户请求相同域名的解析，将直接返回本地缓存结果。

调度策略	<p>如何将内网的 DNS 请求调度到 DNS 服务器，包括：</p> <ul style="list-style-type: none"> ▪ 加权轮询：根据权重选择 DNS 服务器列表中的 DNS 服务器。 ▪ 最少连接：根据 ADSG 出口上的连接数选择 DNS 服务器。 ▪ IP 哈希：根据哈希值选择 DNS 服务器。 ▪ 权重优先：优先选择权重值最大的 DNS 服务器。
代理目标范围	<p>代理内网 DNS 请求的范围，包括：</p> <ul style="list-style-type: none"> ▪ 全部请求：代理全部内网 DNS 请求。只能代理部分用户的全部请求，即代理的用户范围需指定为部分用户，且需指定代理的内网用户 IP 范围。 ▪ 指定服务器：代理目的地址为网关 DNS 服务器列表中服务器地址的 DNS 请求。 ▪ 指定域名：代理对前置调度策略和内网 DNS 记录中指定的域名的 DNS 请求。
用户	<p>代理内网 DNS 请求的用户范围，包括：</p> <ul style="list-style-type: none"> ▪ 全部用户：代理全部内网用户的 DNS 请求。 ▪ 部分用户：代理部分内网用户的 DNS 请求，需指定用户的 IP 地址集。需事先在公共对象>IP 地址集页面添加 IPv4 地址/掩码类型的 IP 地址集。
探测域名	通过向 DNS 服务器列表中的 IP 地址发送此域名的解析请求，来判断 DNS 服务器是否可用。
前置调度策略	是否开启前置调度策略。
繁忙保护	是否开启链路繁忙保护。需要设置 WAN 口的带宽繁忙比例。

提示：一旦内网PC将DNS设为监听地址，无论其是否在代理目标或代理用户范围内，ADSG都会对其DNS请求进行代理。

3. 点击**保存**。

6.3.前置调度

当内网用户访问特殊域名必须通过指定的 DNS 服务器解析时，需要在配置 DNS 透明代理时启用前置调度，并添加相应的调度策略。前置调度策略的优先级高于透明代理的调度策略。

要配置前置调度策略，请执行以下操作：

1. 选择 **DNS 代理>透明代理**，启用前置调度。
2. 选择 **DNS 代理>前置调度**。点击**添加**，选择**添加前置策略**。

3. 在下方的**基本配置**区域，设置相关参数。

The screenshot shows the 'Basic Configuration' (基本配置) section of a web interface. It contains the following fields and options:

- 状态:**
- 名称:** PreS1 *
- 用户:** 全部用户
- 域名:** www.baidu.com *
- 繁忙保护:**
- 失败动作:** 匹配下一条

Below the fields are two lists of DNS servers:

- 已选DNS服务器:** 202.96.64.86:WAN:3
- 待选DNS服务器:** 8.8.8.8:WAN:2

There are two arrows between the lists: a right-pointing arrow (→) and a left-pointing arrow (←).

前置调度策略配置参数

参数	说明
状态	是否启用新添加的前置调度策略。
名称	输入新添加的前置调度策略的名称。
用户	选择调度用户范围，包括： <ul style="list-style-type: none"> ▪ 全部用户: 对全部内网用户的 DNS 请求执行当前调度策略。 ▪ 部分用户: 对部分内网用户的 DNS 请求执行当前调度策略，需指定用户的 IP 地址集。需事先在公共对象>IP 地址集页面添加 IPv4 地址/掩码类型的 IP 地址集。
域名	指定对什么域名的 DNS 请求执行当前调度策略。
繁忙保护	是否开启链路繁忙保护。 当指定 DNS 服务器所属链路过于繁忙，则不会将 DNS 请求调度到该服务器上。
失败动作	调度失败时，ADSG 执行的动作，包括 匹配下一条 和 强制调度 。
已选/待选 DNS 服务器	选择要将特定 DNS 请求调度到哪些 DNS 服务器上。

4. 点击**保存**。

6.4. 内网记录

用户可以通过配置内网 DNS 记录实现内部域名解析。对于请求解析记录中域名的 DNS 请求，直接返回记录中指定的值。

要配置内网 DNS 记录，请执行以下操作：

1. 选择 **DNS 代理>内网记录**。
2. 点击**添加**，选择**添加内网记录**。
3. 在下方的**基本配置**区域，设置相关参数。

内网 DNS 记录配置参数

参数	说明
状态	是否启用新添加的内网 DNS 记录。
域名	内网 DNS 记录对应的域名。
记录类型	内网 DNS 记录类型，包括： <ul style="list-style-type: none"> ▪ A 记录：用于指定主机名（或域名）对应的 IP 地址。 对于请求解析 A 记录中域名的 DNS 请求，直接返回记录中指定的 IP 地址。 ▪ CNAME 记录：用于指定域名对应的别名。 对于请求解析 CNAME 记录中域名的 DNS 请求，直接返回记录中指定的域名别名。 ▪ NS 记录：用于指定域名由哪个 DNS 服务器进行解析。 对于请求解析 NS 记录中域名的 DNS 请求，直接返回下一跳 DNS 服务器的域名。
TTL	内网 DNS 记录的缓存时间。

- 资源信息 针对该记录中域名的请求返回的值。
- **A 记录：** 针对请求域名返回的 IP 地址。
 - **CNAME 记录：** 针对请求域名返回的域名别名。
 - **NS 记录：** 针对请求域名返回的下一跳 DNS 服务器域名。
-

4. 点击**保存**。

第7章 智能 DNS

当用户网络存在多条运营商链路时，可以通过智能 DNS 提供入站链路负载均衡服务，提升网络访问速度和用户访问体验。

本章介绍 AD SG 的智能 DNS 功能，内容包括：

- [7.1 DNS 服务器](#)
- [7.2 站点集合](#)
- [7.3 LDNS 集合](#)
- [7.4 虚拟 IP 池](#)
- [7.5 DNS 映射](#)
- [7.6 静态就近性](#)
- [7.7 全局配置同步](#)

提示：使用智能DNS功能之前，需要先在域名注册服务提供商处修改域名NS记录，使ADSG获得域名解析权；另外，需配置好虚拟服务，以确定智能DNS解析后要调度的虚拟IP地址。

ADSG 智能 DNS 支持本地单站点负载均衡和多地站点全局负载均衡，配置逻辑如下：

本地单站点负载均衡	多地站点全局负载均衡
1.配置 WAN 接口并为其指定健康监视器，用于指定 AD SG 监听来自哪些 WAN 口的 DNS 请求。 2.配置虚拟服务，将内网服务器节点的 IP 地址池映射到对外公布的虚拟服务 IP 地址。 3.获得域名解析权，在域名注册服务商处修改 NS 记录，将域名指向本地站点的虚拟服务 IP 地址。	4.开启智能 DNS 服务器功能，指定监听请求范围。 5.配置虚拟 IP 池，添加可被调度的虚拟服务 IP 并指定调度策略。 6.配置 DNS 映射，添加域名与虚拟 IP 池的映射关系，并指定调度策略。 7.配置 LDNS 集合，添加 ISP 地址段，用于判断用户所属运营商链路。 8.配置虚拟 IP 池级别的静态就近性策略，根据所属运营商链路为指定用户选取池内虚拟 IP 返回。
4.开启智能 DNS 服务器功能，指定监听请求范围。 5.配置虚拟 IP 池，添加可被调度的虚拟服务 IP 并指定调度策略。 6.配置 DNS 映射，添加域名与虚拟 IP 池的映射关系，并指定调度策略。 7.配置 LDNS 集合，添加用户地域和 ISP 地址段，用于判断用户所属地域和所属运营商链路。 8.配置静态就近性策略： 一级调度：DNS 映射级别，根据 DNS 映射关系以及 LDNS 集合（地域）判断用户访问的虚拟 IP 池。	4.开启智能 DNS 服务器功能，指定监听请求范围，开启全局负载均衡模式。 5.配置虚拟 IP 池，添加可被调度的虚拟服务 IP 并指定调度策略。 6.配置 DNS 映射，添加域名与虚拟 IP 池的映射关系，并指定调度策略。 7.配置 LDNS 集合，添加用户地域和 ISP 地址段，用于判断用户所属地域和所属运营商链路。 8.配置静态就近性策略： 一级调度：DNS 映射级别，根据 DNS 映射关系以及 LDNS 集合（地域）判断用户访问的虚拟 IP 池。

	<p>二级调度：虚拟 IP 池级别，根据 LDNS 集合（运营商）为用户选取池内虚拟 IP。</p> <p>9.配置站点集合，添加本地站点和其他各地站点，指定站点间用于通讯的 IP/端口以及站点角色。</p> <p>10.登录 None 或其他 Master 角色的 AD SG，配置本地站点信息，同步 Master 的配置到本地。</p>
--	--

7.1.DNS 服务器

要实现入站链路负载均衡，用户首先需要开启智能 DNS 功能，并设置要监听 DNS 请求的接口 IP 和端口。对于请求域名不存在的情况，还可以设置 AD SG 的处理动作。

要配置 DNS 服务器，请执行以下操作：

1. 选择**智能 DNS>DNS 服务器**。
2. 启用智能 DNS 功能，指定监听接口和端口，设置请求域名不存在时 AD SG 的处理动作。

DNS服务器

状态：

监听地址

已选地址		待选地址
10.1.3.111@wan1	→	10.1.5.24@test2
10.1.5.28@wan1	←	10.1.5.71@wan1

监听端口： *(1-65535)

域名不存在动作： ▼

工作模式： 本地模式 全局模式

参数	说明
状态	勾选复选框，开启智能 DNS 服务。
监听地址	指定要监听 DNS 请求的接口 IP 地址。 从右侧列表中选择要监听的接口 IP 地址，点击左箭头，添加到左侧列表。
监听端口	指定要监听 DNS 请求的端口，默认 53。
域名不存在动作	设置请求域名不存在时 AD SG 的处理动作： <ul style="list-style-type: none"> ▪ 不回应：丢弃请求包，不作回应。

- 工作模式
- **拒绝**：返回解析结果为空，拒绝访问。
- ADSG 开启智能 DNS 服务器功能时提供负载均衡的工作模式，包括：
- **本地模式**：用于单一站点入站链路负载均衡；
 - **全局模式**：用于多站点入站链路负载均衡。

提示：需要在网络>接口>WAN页面添加WAN接口，此处才会出现可选接口和地址。

3. 点击**保存**。

7.2. 站点集合

ADSG 在开启智能 DNS 功能时，可实现多地站点间的全局负载均衡。配置全局负载均衡之前，需要在各地站点网络出口的 ADSG 设备上配置站点集合，确定各站点 ADSG 设备的角色，包括 Master 和 None。

- **Master 站点 ADSG**
 - 负责接收用户的 DNS 请求并进行全局调度，为用户选取一个最佳访问路径；
 - 需配置所有智能 DNS 信息，任何修改都要同步到其他 Master；
 - 需配置所有站点信息，收到 None 站点同步请求时，将站点信息同步到 None。
- **None 站点 ADSG**
 - 不接收用户 DNS 请求，只负责接收 Master 转发的用户访问请求；
 - 不参与 DNS 请求调度，无需配置站点信息之外的其他智能 DNS 信息；
 - 只需配置本地站点信息，从 Master 同步其他站点信息。

提示：在域名注册服务商处申请获取域名解析权时，要将域名指向 Master 站点 ADSG 上配置的虚拟 IP，这样所有用户的 DNS 请求都将发往 Master 站点的 ADSG 进行解析。

1. 选择**智能 DNS>DNS 服务器**，开启全局负载均衡工作模式。
2. 选择**智能 DNS>站点集合**。
3. 点击**动作**，选择**添加站点**，在**基本配置**区域进行相关配置，点击**保存**。

参数	说明
站点名称	新建站点的唯一标识。
站点类型	新建站点的类型，包括本地站点和其他站点。 集合中仅能有一个本地站点。
通讯地址	用于与其他站点进行通讯的 IP 地址。 新建本地站点时可以直接选取本地的接口 IP 地址作为通讯地址，新建其他站点时则需要手动输入对端站点的通讯 IP 地址。
通讯端口	用于与其他站点进行通讯的端口。
通讯角色	新建站点的角色，包括 Master 和 None。 Master 用于解析用户 DNS 请求，None 用于接收用户收到 DNS 应答后的访问请求。 集合中允许存在多个 Master，但需要将多个 Master 的虚拟 IP 都在域名服务商处进行注册，适用于一个域名映射到多个公网 IP 的情况。
通讯密钥	输入本地站点 AD SG 用于解密通讯数据的密钥。
确认密钥	再次输入本地站点 AD SG 用于解密通讯数据的密钥。
备注	新建站点的备注信息。

- 如果是 Master 站点 AD SG，需要配置本地站点和其他所有站点信息；
- 如果是 None 站点 AD SG，只需配置本地站点信息，其他站点信息可通过配置同步从 Master 站点 AD SG 获取；
- 如果集群中有多个 Master，配置完一个 Master 后，其他 Master 也只需配置本地站点，然后从已配置的 Master 站点同步所有站点信息。

4. 点击保存。

7.3.LDNS 集合

LDNS（Local DNS）集合是用户链路的地址全集，用于判断用户所属链路。如果收到的 DNS 请求对应的 DNS 服务器地址在某个链路地址集内，则认为用户属于该链路。

用户链路缺省按运营商或地域划分，如果系统提供的 ISP 或地域地址集不全，可通过自定义 IP 地址集进行补充。用户如有特殊链路地址，也可通过添加自定义 IP 地址集进行链路判断。

要配置 LDNS 集合，请执行以下操作：

1. 选择**智能 DNS>LDNS 集合**。
2. 点击**动作**，选择**添加 LDNS**，在**基本配置**区域进行相关配置，点击**保存**。
 - **ISP 地址段**：根据各大运营商的 IP 地址库判断用户所属链路。

名称： *

地址集

地址
36.128.0.0-36.191.255.255
183.192.0.0-183.255.255.255
120.192.0.0-120.255.255.255
117.128.0.0-117.191.255.255

23条记录

地址类型：

地址段：

中国电信
中国联通
中国教育网

提示：如需自定义ISP地址段，请到公共对象> ISP地址集页面添加。

- **用户地域**：根据用户所在地域判断用户所属链路。

名称： *

地址集

地址
110.96.0.0-110.127.255.255
123.64.0.0-123.95.255.255
110.192.0.0-110.223.255.255
36.192.0.0-36.223.255.255

346条记录

地址类型：

地址段：

提示：如需自定义用户地域地址集，请到公共对象> 用户地域页面添加。

- （自定义）IP 地址段：根据用户自定义的 IP 地址段判断用户所属链路。

名称： *

地址集

地址
1.1.1.1-2.2.2.2

1条记录

地址类型：

起始地址： *

终止地址： *

提示：当获取的ISP地址库不全时，可以通过自定义IP地址段的方式加以补充。

- 选中地址库条目，点击**动作**，选择**删除 LDNS**，删除选中的 LDNS 集合，点击**保存**。

提示：正在被静态就近性策略引用的LDNS集合，需先解除引用关系，才能删除。

7.4. 虚拟 IP 池

用户可能在运营商那里租了不止一条链路。此时，可通过智能 DNS 的二级调度，实现更精细的进站链路负载均衡：

- 一级调度（DNS 映射）：在域名和虚拟 IP 池之间建立映射关系，根据调度策略选择虚拟 IP 池；
- 二级调度（虚拟 IP 池）：按不同运营商或地域添加不同的虚拟 IP 池，并为每个 IP 池指定所包含的虚拟 IP 和调度策略，根据调度策略选择虚拟 IP。

虚拟 IP 池的作用是根据负载均衡策略，从多个虚拟 IP 地址中选出一条最佳路径，实现二级调度。

ADSG 的虚拟 IP 池支持以下调度策略：

轮询	依次返回虚拟 IP 池中的 IP。 适用场景：用户想要将进站流量均匀分配到每条链路上。
加权轮询	根据加权计算结果返回虚拟 IP 池中的某个 IP。 适用场景：用户想要将进站流量按比例分配到每条链路上。
加权最小连接	根据权重和当前该 IP 所在链路连接数的加权计算结果，返回某个虚拟 IP。 适用场景：用户想要根据链路的连接状态，动态选择最优进站链路。
加权最小流量	根据权重和当前该 IP 所在链路流量的加权计算结果，返回某个 IP。 适用场景：用户想要根据链路的流量（客户端业务请求流量，非 DNS），动态选择最优进站链路。

静态就近性	<p>将客户端本地 DNS 的 IP 地址与各大网络运营商的 IP 地址库进行对比，确定客户端运营商，并将该运营商对应的 VIP 作为 DNS 解析结果返回；作为此功能的扩展，在选择静态就近性调度策略时，用户可以自定义地址库，并建立地址库与链路的映射关系，当客户端本地 DNS 的 IP 地址匹配到地址库时，返回对应的链路 IP 地址。</p> <p>适用场景：用户想要根据客户端所属运营商，为其分配同一运营商的链路作为进站链路。</p>
动态就近性	<p>通过 PING 方式对客户端本地 DNS 进行动态探测，选择时延最短的链路，将相应 IP 作为 DNS 解析结果返回。</p> <p>适用场景：用户想要通过探测每条链路到客户端的时延，动态选择针对每个客户端的最优进站链路。</p>
IP Hash	<p>通过哈希算法对 DNS 请求的源 IP 进行运算，由此确定返回的链路 IP。</p> <p>适用场景：用户想要将进站流量分配到多条链路上，并且将同一用户的流量分配到同一条链路上。</p>
首个可用	<p>将虚拟 IP 池中第一个可用的链路 IP 作为 DNS 解析结果返回。</p> <p>适用场景：用户想要尽快响应客户端，对业务访问的响应时延比较敏感。</p>
返回全部	<p>不对 IP 进行任何筛选，将虚拟 IP 池中的所有链路 IP 返回给客户端。</p> <p>适用场景：不对链路 IP 进行筛选，返回所有可用 IP。</p>

要配置虚拟 IP 池，请执行以下操作：

1. 选择**智能 DNS>虚拟 IP 池**。
2. 点击**动作**，选择**添加虚拟 IP 池**。
3. 在**基本配置**区域进行相关配置。

基本配置

状态:
 繁忙保护:
 名称: *
 策略: 加权轮询

虚拟IP列表

虚拟IP	权重
10.1.10.11	1
10.1.10.12	2

虚拟IP:
 权重:

确定
取消

策略: 动态就近性 ▾
 探测超时时间: *秒
 探测结果缓存时间: *秒
 探测方法: PING方式 ▾

参数	说明
状态	勾选复选框，启用新建虚拟 IP 池。
繁忙保护	勾选复选框，启用链路繁忙保护。 当某条链路处于繁忙状态时，对应的虚拟 IP 不参与入站调度。
名称	新建虚拟 IP 池的名称。
策略	为新建虚拟 IP 池选择一种调度策略。 <ul style="list-style-type: none"> ▪ 如果选择静态就近性策略，需要在智能 DNS >静态就近性>虚拟 IP 池级别中进行具体调度策略的配置。 ▪ 如果选择动态就近性策略，需要指定服务器探测方法、超时时间和探测结果缓存时间。
虚拟 IP 列表	为新建虚拟 IP 池添加所包含的虚拟 IP 及权重。 此处添加的虚拟 IP 即虚拟服务器的虚拟 IP 地址。

4. 点击**保存**。

7.5.DNS 映射

DNS 映射用于智能 DNS 的一级调度，其作用是在域名和虚拟 IP 池之间建立映射关系，实现 AD SG 根据域名选择虚拟 IP 池的一级调度。一个域名可以映射到多个虚拟 IP 池，用户可以为 DNS 映射规则指定虚拟 IP 池的调度策略。

AD SG 的 DNS 映射支持以下调度策略：

轮询	依次调度到不同的虚拟 IP 池。 适用场景：多运营商链路接入，用户想要将入站流量均匀分配到每个运营商的链路上。
加权轮询	根据权值，加权计算调度到的虚拟 IP 池。 适用场景：多运营商链路接入，用户想要将入站流量按比例分配到每个运营商的链路上。
静态就近性	根据客户链路所属运营商调度虚拟 IP 池。 适用场景：用户想要根据客户端本地 DNS 所属运营商，为其分配同一运营商的链路作为入站链路。

要配置 DNS 映射，需事先配置好要引用的虚拟 IP 池，然后执行以下操作：

1. 选择**智能 DNS>DNS 映射**。
2. 点击**动作**，选择**添加 DNS 映射**。
3. 在**基本配置**区域进行相关配置。

基本配置

状态：

名称：

策略：静态就近性

会话保持：

会话超时： 秒

TTL： 秒

域名列表

域名
www.example.com

域名：

虚拟IP池列表

虚拟IP池	权重
VIP_pool1	1
VIP_pool2	2

虚拟IP池：虚拟IP池

权重：

参数

说明

状态	勾选复选框，启用新建 DNS 映射规则。
名称	新建 DNS 映射规则的名称。
策略	为新建 DNS 映射规则选择一种调度策略，即指定如何为匹配的域名选择一个虚拟 IP 池。 DNS 映射规则支持轮询、加权轮询和静态就近性三种调度策略。 如果选择静态就近性算法，需要在 智能 DNS >静态就近性>DNS 映射级别 中进行具体调度策略的配置。
会话保持	为新建 DNS 映射规则启用会话保持功能。 启用会话保持功能后，来自相同源的多次 DNS 请求将调度到相同虚拟 IP 池。
会话超时	DNS 请求会话的超时时间。
TTL	DNS 解析结果在客户端本地 DNS 的缓存时间。
域名列表	为新建 DNS 映射规则添加需要解析的域名地址。 此处添加的域名即虚拟服务器的域名。
虚拟 IP 池列表	为新建 DNS 映射规则添加可调度的虚拟 IP 池。 此处添加的虚拟 IP 池中包含的虚拟 IP 即虚拟服务器的虚拟 IP 地址。

4. 点击**保存**。

7.6.静态就近性

当用户网络连接多条不同运营商链路，且内网有多台服务器通过多个运营商的多个地址提供服务时，可以使用智能 DNS 的静态就近性解析策略，将与 DNS 请求客户端所属运营商相同的服务器地址通过 DNS 返回给客户端，使得客户可以通过对应的运营商链路进行访问，提高网络的使用体验。

ADSG 提供 DNS 映射级别和虚拟 IP 池级别的静态就近性策略：

DNS 映射级别	规定 DNS 映射规则、LDNS 地址库以及虚拟 IP 池之间的对应关系，即当客户端请求的域名命中 DNS 映射规则中的域名，并且客户端的本地 DNS 地址命中静态就近性策略中指定的 LDNS 地址集，则返回指定虚拟 IP 池中的虚拟 IP。
虚拟 IP 池级别	规定虚拟 IP 池、LDNS 地址库以及虚拟 IP 之间的对应关系，即当客户端请求同时匹配指定的虚拟 IP 池以及 LDNS 地址库时，根据静态就近性原则返回指定的虚拟 IP。

要配置静态就近性策略，需事先配置好要引用的 LDNS 集合、虚拟 IP 池和 DNS 映射规则，然后执行以下操作：

1. 选择**智能 DNS>静态就近性**。
2. 在**DNS 映射级别**页签添加 DNS 映射级别就近性策略：

- a. 点击**动作**，选择**新建规则**。
- b. 在**基本配置**区域选择要映射的 DNS 映射规则、LDNS 集合和虚拟 IP 池。

基本配置

DNS映射: DNS_map1

LDNS集合: 地址库1

虚拟IP池: VIP_pool1

- c. 点击**保存**。
3. 点击**虚拟 IP 池级别**页签，添加虚拟 IP 池级别静态就近性策略：

- a. 点击**动作**，选择**新建规则**。
- b. 在**基本配置**区域选择要映射的虚拟 IP 池和 LDNS 集合，添加可调度的虚拟 IP。

基本配置

虚拟IP池: VIP_pool2

LDNS集合: 电信

池内IP

已选IP	待选IP
20.2.20.2	20.2.20.3
202.2.20.22	

- c. 点击**保存**。

7.7.全局配置同步

要实现多个站点间的全局负载均衡，必须正确配置站点集合信息。只有正确区分 Master 和 None 站点，全局负载均衡才能生效。

为了方便用户配置，ADSG 提供了配置同步功能，可将 Master 站点 ADSG 上的站点集合配置信息同步到其他站点 ADSG，保证各站点 ADSG 上的站点集合配置一致。

- 当站点集合中仅有一个 Master 时，可通过配置同步将 Master 站点 ADSG 上的站点集合配置信息同步到所有 None 站点 ADSG 上；
- 当站点集合中有多个 Master 时，可以将先配置的 Master 站点 ADSG 上的站点集合信息连同所有其他智能 DNS 配置一起同步到其他 Master 站点的 ADSG 上。

1. 选择**智能 DNS>全局配置同步**。
2. 输入对端 Master 站点 ADSG 的通讯 IP 地址和端口，点击**更新**：

配置同步

同步内容

如果本端为None，仅同步对端站点集合信息。
如果本端为Master，则同步站点集合信息和所有智能DNS配置。

对端设置

对端站点通讯地址： *

对端站点通讯端口： *(1-65535)

更新

提示：需要先到站点集合界面添加本地站点并正确配置通讯地址和角色等信息。

3. 点击**保存**。

第8章 网络配置

本章介绍 ADSG 网络相关功能，内容包括：

- [8.1 接口](#)
- [8.2 VLAN](#)
- [8.3 静态路由](#)
- [8.4 智能路由](#)
- [8.5 DNS](#)
- [8.6 端口映射](#)
- [8.7 源地址转换](#)
- [8.8 ACL 配置](#)

8.1. 接口

ADSG 允许用户对以太网接口进行配置，包括为以太网接口配置 IP 和 MAC 地址、通过划分以太网接口创建外网口（WAN）和内网口（LAN）。

- [8.1.1 以太网接口](#)
- [8.1.2 WAN](#)
- [8.1.3 LAN](#)

提示： WAN和LAN用于出站链路负载均衡，可以在智能路由配置中引用。

8.1.1. 以太网接口

要使 ADSG 接入网络，需正确配置以太网接口的 IP 地址：

1. 选择网络 > 接口 > 接口。

接口						
WAN						
LAN						
状态	名称	IP地址	MAC地址	速率	双工	备注
	eth0	192.168.1.100/24	00:90:fb:51:46:8b	100Mb/s	Full	
	eth-s1p1		08:35:71:07:e2:fc	auto	auto	
	eth-s1p2		08:35:71:07:e2:fd	auto	auto	

表示接口处于启用状态， 表示接口处于禁用状态。接口速率和双工模式由接口和对端设备自动协商。

2. 在**基本配置**区域进行相关配置，如启用/禁用接口、添加 IP、修改 MAC 和设置备注。

基本配置

状态:

名称: eth1

IP设置

IP地址	掩码长度
11.11.12.13	24
11.11.12.12	24

IP地址:

掩码长度:

MAC地址:

备注:

接口可设置多个 IP 地址，所设置 IP 地址可为相同网段或者不同网段。

3. 点击**保存**。

8.1.2. WAN

WAN 口即 ADSG 连接外网的接口，它指定了内网用户请求发往外网的出口接口和下一跳网关，或 ADSG 接收外网用户请求的入口接口。用户还可以为 WAN 口设置上下行带宽和带宽繁忙比例，用于入站链路负载均衡的链路繁忙保护。ADSG 还支持对 WAN 口链路的健康状态进行监控。

提示：只有配置了 WAN 口，用户在配置智能路由、智能 DNS 和 HA 故障切换检测时才有可选出/入站链路。

要配置 WAN 口，请执行以下操作：

1. 选择**网络>接口>WAN**，点击**动作**按钮，选择**添加 WAN**。
2. 在**基本配置**区域，勾选复选框启用新建 WAN 口，指定新建 WAN 口名称以及出口接口和下一跳网关，设置 WAN 口的上下行带宽和带宽繁忙比例。

基本配置
健康状态监控

状态:

名称:

接口: 网关:

上行带宽: Kbps %

下行带宽: Kbps %

3. 点击**健康状态监控**页签，选择健康监视器。

- ARP Ping:

- HTTP Ping/HTTPS Ping/TCP Ping/UDP Ping:

- TCP Ping:

提示： TCP Ping通过探测WAN口的网关地址监控其链路状态。管理员可到**虚拟服务>健康监视器**页面添加自定义健康监视器。

4. 点击**保存**。

8.1.3. LAN

LAN 口即 ADSG 连接内网的接口，它指定了 ADSG 接收内网用户请求的入口接口和将外网请求发往内网服务器的出口接口。

要配置 LAN 口，请执行以下操作：

1. 选择**网络>接口>LAN**，点击**动作**按钮，选择**添加 LAN**。
2. 在**基本配置**区域，指定 LAN 口的入口接口，即 ADSG 连接内网的接口。

3. 点击**保存**。

8.2.VLAN

ADSG 支持 VLAN 功能，可根据需要将以太网接口划分到不同的 VLAN 之中。通过 VLAN 功能，用户能够实现 AD SG 进行透明模式部署。

注意：为防止通信中断，请不要将ADSG管理IP地址所在的接口划入任何VLAN。

要配置 VLAN，请执行以下操作：

1. 选择**网络 > VLAN**，点击**动作**按钮，选择**添加 VLAN**。

VLAN							
动作							
状态	名称	VLAN ID	未标记接口	标记接口	IP地址	MAC地址	备注
🔴	vlan1	1				46:ab:07:ae:f1:81	

系统默认存在一个名称为vlan1的本征VLAN，ID为1，缺省禁用，配置为空。

🟢 表示 VLAN 处于启用状态，🔴 表示 VLAN 处于禁用状态。

2. 在基本配置区域对 VLAN 进行配置。

基本配置

状态：

VLAN ID： * (1 ~ 4094)

名称：

接口配置：

未标记接口

eth1

←

→

可用接口

eth0

→

←

标记接口

eth2

IP设置

IP地址	掩码长度
2.2.2.2	24
2.2.3.3	24

IP地址：

掩码长度：

确定

取消

MAC地址：

备注：

VLAN ID 是 VLAN 的唯一标识，配置后不能更改。取值范围 1-4094。

如果一个接口被设置为未标记接口，则从此接口转发出去的数据包上都不打标记。一个未标记接口只能划入一个 VLAN。

如果一个接口被设置为标记接口，则从此接口转发出去的数据包上都会有 VLAN 标记（根据对端设备的 Trunk 口配置决定）。一个标记接口可以划入多个 VLAN。

VLAN 支持配置多个 IP 地址。

3. 点击**保存**。

8.3. 静态路由

ADSG 的静态路由页面显示所有直连路由、缺省路由和用户自定义静态路由的信息。直连路由由系统自动生成，缺省路由和用户自定义静态路由由用户手动添加。只有手动添加的路由可编辑。

要配置静态路由，请执行以下操作：

1. 选择**网络 > 静态路由**。
2. 点击**动作**下拉框，选择**增加路由**，在**基本配置**选项卡中配置相关内容。

The screenshot shows the 'Basic Configuration' tab for adding a static route. The fields are as follows:

- 目的地址: 192.168.1.0 *
- 掩码: 255.255.255.0 *
- 网关: 192.168.1.1 *
- Metric: 3
- 接口: eth1

静态路由配置参数

参数	说明
目的地址	路由的目的 IP 地址或 IP 地址段。
掩码	目的 IP 地址的掩码。
网关	路由下一跳网关的 IP 地址。
Metric	路由的度量值。
接口	数据包的出口接口。

3. 点击**保存**。

8.4. 智能路由

智能路由本质上是一种增强型的静态路由。基于策略的智能路由比传统路由控制能力更强，使用更灵活。它使网络管理者不仅能够根据目的地址来选择转发路径，而且能够根据协议类型、报文大小、应用、源地址或者其它策略条件选择要转发的数据包。

当数据包经过 ADSG 转发时，ADSG 根据预先设定的策略对数据包进行匹配：

- 如果匹配到一条策略，就根据该条策略指定的智能路由进行转发。
- 如果没有匹配到任何策略，就使用静态路由表根据目的地址对报文进行路由。

当用户网络有多个运营商出口链路时，可以通过智能路由提供出站链路负载均衡服务，提升内网用户访问互联网资源的速度。

严格来说，ADSG 通过智能路由和源地址转换功能实现出站链路负载均衡。出站链路的选择主要通过智能路由来实现，选定链路后，再采用 SNAT 将源地址转换为链路出口的 IP 地址。出站负载均衡策略主要根据内网主机访问请求的源 IP 地址、目的 IP 地址、协议、端口等来决定出口链路。其中，每条策略的出口链路可以为多个并根据预先设置好的负载均衡算法来决定最终的链路出口。

要实现出站链路负载均衡：

- 在配置智能路由之前，需要事先配置内外网口（**网络>接口>LAN/WAN**）。
- 在配置智能路由之后，还需要配置源地址转换规则（**网络>源地址转换**）。

要配置智能路由，请执行以下操作：

1. 选择**网络 > 智能路由**。
2. 点击**动作**下拉框，选择**添加智能路由**，在**基本配置**区域配置相关参数。

基本配置

序号：

名称： *

源IP地址： ▼

IPv4地址： *

掩码长度： *

目的IP地址： ▼

TOS： *

协议： ▼ *

使用链路：

链路	权重
WAN1	1
WAN2	2

链路： ▼

权重：

链路策略： ▼ *

生效时间： ▼ *

链路繁忙保护： 开启 关闭

调度失败动作： ▼

智能路由配置参数

参数	说明
序号	智能路由的策略优先级。编号越小，优先级越高。可通过修改编号修改策略优先级。
名称	智能路由的策略名称。
源 IP 地址	数据包的源 IP 地址。 源 IP 地址支持 IP 地址集，可到 公共对象 > IP 地址集 页面添加自定义 IP 地址集。
目的 IP 地址	数据包的目的 IP 地址，也是路由转发的依据。 目的 IP 地址支持 ISP 地址段和域名，可到 公共对象 > ISP 地址集 页面添加 ISP 地址集。

TOS	用于定义数据包中的交付服务（吞吐量、延迟、可靠性及经济成本）。取值范围 0 ~ 15： <ul style="list-style-type: none"> 0 表示不要求任何服务。 1 表示要求最低的时延。 2 表示要求最高的吞吐量。 4 表示要求最高的可靠性。 8 表示要求最小的代价。
协议	数据包传输所使用的协议。
使用链路	匹配智能路由策略的数据包对应的出站链路（即 WAN 口）。 如无可选链路，可到 网络>接口>WAN 页面添加 WAN 口。
链路策略	当有两条或两条以上出站链路时所使用的链路调度策略。目前支持三种策略： <ul style="list-style-type: none"> 轮询：依次选取出站链路。 带宽比例：按出口链路最大带宽比例选择出站链路。 加权最小流量：基于当前流量与链路权重的比值计算，选择比值最小的出站链路。
生效时间	智能路由的生效时间，包括全天、指定星期、指定日期和自定义四种方式。
链路繁忙保护	开启或关闭链路繁忙保护。如果开启，当链路处于繁忙状态时，不参与出站调度。
调度失败动作	出站链路调度失败时的处理动作，包括匹配下一条和丢弃。

3. 点击**高级配置**页签，启用会话保持功能并设置会话保持掩码和保持时间，或禁用会话保持功能。

The screenshot shows the configuration interface for session persistence. It includes the following fields:

- 智能路由** (Smart Routing) and **高级配置** (Advanced Configuration) tabs.
- 会话保持** (Session Persistence) section header.
- 状态** (Status):
- 会话保持掩码** (Session Persistence Mask): *
- 保持时间** (Persistence Time): *秒

ADSG 基于用户访问的目的地址提供会话保持功能。会话保持掩码用于指定会话保持的应用范围。例如，会话保持掩码为 255.255.255.0，内网用户首次访问的目的地址为 1.1.1.1。根据出站链路负载均衡算法，该请求由 WAN1 接口转发出去。那么内网用户再次访问 1.1.1.0/24 网段的 IP 地址，将仍由 WAN1 接口转发出去。

4. 点击**保存**。

8.5.DNS

ADSG 可以作为 DNS 客户端，从 DNS 服务器地址请求域名解析。

要配置 DNS，请执行以下操作：

1. 选择**网络 > DNS**。
2. 设置首选和备选 DNS 服务器地址。

DNS

IPv4 DNS服务器

首选DNS：

备选DNS1：

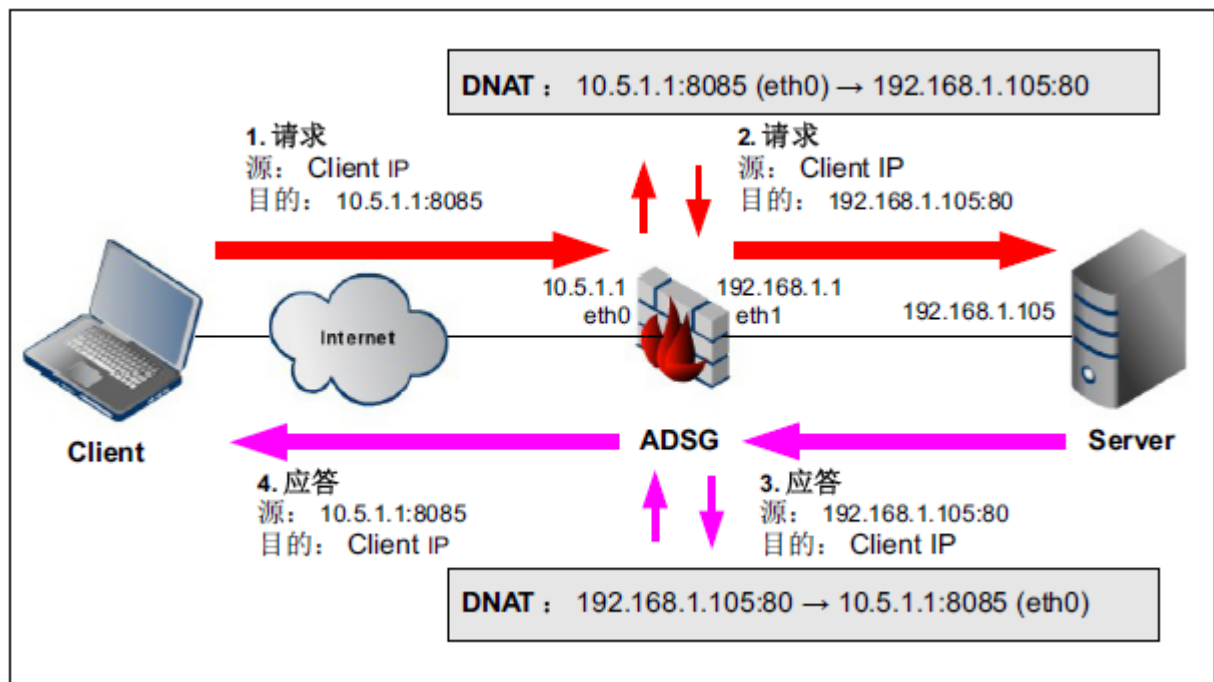
备选DNS2：

3. 点击**保存**。

8.6.端口映射

当 ADSG 作为网关（而非负载均衡器）使用时，需要开启端口映射功能。通过设置 ADSG 的目的地址转换（DNAT）规则，使得外网用户可以访问内网服务器特定端口的服务。

目的地址转换使得外网客户端可以访问内网服务器，同时可以保护内网服务器不受外部攻击。使用场景示例如下：



提示：此功能单独使用，不需要配合负载均衡功能使用。此外，服务器网关需指向ADSG。

要配置端口映射，请执行以下操作：

1. 点击网络>端口映射，点击动作，选择新建规则：



提示：如果端口映射的目的端口与流量管理规则中的端口冲突，系统将优先匹配端口映射功能。此时，流量管理中对应的虚拟服务器将获取不到流量，不能正常工作。

2. 在下方配置区域，设置端口映射规则：

协议选项包括 TCP、UDP、ICMP、GRE 和 Others。当选择 Others 时，右边的输入框激活，可输入相应的 TCP/IP 协议族的传输层协议号，比如：50（ESP 协议）。

如果想让外网 Client 访问 IP 为内网私有 IP 地址的 Server 的 80 端口，可以配置如下 NAT 规则：

- a. 目的 IP 只能选择 ADSG 本地接口的 IP；
 - b. 转换后 IP 必需能够被 ADSG 正确路由。
3. 点击保存。

8.7.源地址转换

内网用户访问互联网资源时，需要将内网的源 IP 地址转换为外网 IP 地址，才能接收到返回的数据包。ADSG 支持一对一、多对一和多对多源地址转换。

要配置源地址转换，请执行以下操作：

1. 选择**网络>源地址转换**，点击**动作**，选择**新建规则**。
2. 在下方**基本配置**区域，为新建源地址转换规则设置相关参数：

基本配置

序号：

名称：*

协议：

出口接口：

源IP地址

任意IPv4地址

下列IPv4地址

类型	取值
IPv4地址/掩码	192.168.1.0/24

类型：

IPv4地址：*

转换后IP地址/接口

使用网口地址

下列IPv4地址

IP类型：

IPv4地址：*

目的IP地址

任意IPv4地址

下列IPv4地址

类型	取值
	无数据

IP类型：

IPv4地址：*

源地址转换规则配置参数

参数	说明
序号	源地址转换规则的优先级，取值范围 1~80000。序号越小，优先级越高。
名称	源地址转换规则的名称。
协议	匹配此协议的请求数据包，才能进行源地址转换。 协议选项包括 TCP、UDP 和 ICMP，也可以为 Any。
出口接口	ADSG 转发内网请求数据包的出站接口。
源 IP 地址	请求数据包的源 IP 地址，即转换前的内网 IP 地址。
转换后 IP 地址/接口	转换后的公网 IP 地址，也可以指定为出口接口的 IP 地址。
目的 IP 地址	请求数据包的目的 IP 地址。 只有匹配该目的 IP 地址的数据包，才进行源地址转换。

3. 点击**保存**。

8.8.ACL 配置

ADSG 默认允许所有访问流量通过，访问控制列表（Access Control List，简称 ACL）主要用于限制外网用户对内网服务器的访问。

ADSG 提供基本 ACL 控制，可以根据包协议、源 IP 地址、目的 IP 地址、入口接口对请求数据包进行过滤。

要配置 ACL 功能，请执行以下操作：

1. 选择**网络>ACL 配置>基本 ACL 控制**。
2. 在**基本 ACL 控制**页签点击**动作**，选择**新建规则**，在下方**基本配置**区域设置基本 ACL 规则的相关参数。

基本配置

序号：	<input style="width: 80%;" type="text" value="1"/>
名称：	<input style="border: 1px solid #ccc; border-bottom: none; border-right: none; border-left: none;" type="text" value="basic_ACL1"/> *
协议：	<input style="border: 1px solid #ccc; border-bottom: none; border-right: none; border-left: none;" type="text" value="所有协议"/> ▼
协议号：	<input style="border: 1px solid #ccc; border-bottom: none; border-right: none; border-left: none;" type="text" value="0"/> *
入口接口：	<input style="border: 1px solid #ccc; border-bottom: none; border-right: none; border-left: none;" type="text" value="全部"/> ▼
源IP地址：	<input style="border: 1px solid #ccc; border-bottom: none; border-right: none; border-left: none;" type="text" value="所有IP"/> ▼
目的IP地址：	<input style="border: 1px solid #ccc; border-bottom: none; border-right: none; border-left: none;" type="text" value="所有IP"/> ▼
动作：	<input style="border: 1px solid #ccc; border-bottom: none; border-right: none; border-left: none;" type="text" value="禁止"/> ▼

基本 ACL 规则配置参数

参数	说明
序号	基本 ACL 规则的优先级，取值范围 1~80000。序号越小，优先级越高。
名称	基本 ACL 规则的名称。
协议	匹配此协议的请求数据包，才进行 ACL 控制。协议选项包括： <ul style="list-style-type: none"> ▪ TCP：需要指定源端口和目的端口。 ▪ UDP：需要指定源端口和目的端口。 ▪ ICMP：需要指定 ICMP 类型，包括 13 种自定义 ICMP 类型。 ▪ 所有协议：表示对任意协议的数据包都进行 ACL 控制。 ▪ 自定义：需手动输入自定义协议号。
协议号	协议与协议号的对应关系： <ul style="list-style-type: none"> ▪ TCP：6； ▪ UDP：17； ▪ ICMP：1； ▪ 所有协议：0； ▪ 自定义：0-255。
入口接口	ADSG 接收请求数据包的外网接口。
源 IP 地址	请求数据包的源 IP 地址，即发起访问请求的外网客户端的公网 IP 地址。 源 IP 地址支持 IP 地址集，可到 公共对象>IP 地址集 页面添加自定义 IP 地址集。
目的 IP 地址	请求数据包的目的 IP 地址，即外网用户要访问的虚拟服务器的 VIP 地址。 目的 IP 地址支持 IP 地址集，可到 公共对象>IP 地址集 页面添加自定义 IP 地址集。
动作	对匹配基本 ACL 规则的请求数据包的处理动作，包括允许和禁止。

- 选择 TCP 或 UCP 时，需要指定源和目的端口：

基本配置

序号：

名称：*

协议：*

协议号：*

入口接口：

源IP地址：

IPv4地址：*

源端口：*~*

目的IP地址：

IPv4地址：*

目的端口：*~*

动作：

- 选择 ICMP 协议时，需要配置 ICMP 协议类型：

基本配置

序号：

名称：*

协议：

协议号：*

入口接口：

源IP地址：

IPv4地址：*

目的IP地址：

IPv4地址：*

动作：

ICMP类型：

类型	取值
	无数据

类型：

确定

- 回送应答
- 目的不可达
- 源抑制
- 重定向
- 回送请求
- 路由通告
- 路由询问
- 超时时间
- 参数问题
- 时间戳请求
- 时间戳应答
- 掩码请求
- 掩码应答

ICMP 自定义类型

参数	说明
目的不可达	路由器不能路由分组时向发送源发送的差错报告报文，告知目的不可达。
超时时间	分组在传输过程中因超时被丢弃时，丢弃该分组的路由器向源主机发送一个超时报文。
参数问题	路由器或目的主机发现 IP 分组协议头有模糊不清之处时，丢弃该分组并发送参数问题报文给源主机。

源抑制	发生网络拥塞时，目的主机向源主机发送一个差错报告报文，告诉源主机减少数据发送量。
重定向	路由器的路由表可以随着网络拓扑结构的变化动态更新，而主机的路由表是静态的，路由器通过 ICMP 重定向报文修改主机的路由表，告知主机发送分组的最佳路径。
回送请求和应答	用来测试两个系统是否有通信能力的查询报文。请求方发送 IP 分组给应答方，如果在规定时间内收到应答方的回复，证明两者之间通信正常；否则，说明两个系统之间不能通信。
时间戳请求和应答	请求方和应答方发送和接收分组/报文时分别打上时间戳，可用于测试分组在两个机器之间传输花费的时间。
掩码请求和应答	主机可以向路由器发送掩码请求报文，获取其掩码信息。
路由询问和通告	主机可以用广播方式发送路由器询问报文，获取路由器的工作状态和路由信息。有时路由器即使没收到询问报文，也可以定期发送路由器通告报文，通告其自身以及其他路由器的路由信息。

- 选择自定义时，需要指定自定义协议号。

基本配置

序号：	<input style="width: 80%;" type="text" value="1"/>
名称：	<input style="width: 80%;" type="text" value="basic_ACL1"/> *
协议：	自定义 ▼
协议号：	<input style="width: 80%;" type="text"/> *
入口接口：	全部 ▼
源IP地址：	所有IP ▼
目的IP地址：	IPv4地址/掩码 ▼
IPv4地址：	<input style="width: 80%;" type="text" value="192.168.0.0"/> *
掩码长度：	<input style="width: 80%;" type="text" value="16"/> *
动作：	允许 ▼

3. 点击**保存**。

第9章 系统配置

系统设置功能使得用户能够方便地通过 WebUI 来管理 ADSG 系统。本章结构如下：

- [9.1 配置向导](#)
- [9.2 系统维护](#)
- [9.3 管理设置 \(Web 和 SSH\)](#)
- [9.4 管理用户](#)
- [9.5 日志设置](#)
- [9.6 报警设置](#)
- [9.7 升级设置](#)
- [9.8 报表设置](#)
- [9.9 高可用性](#)
- [9.10 系统参数](#)
- [9.11 SNMP](#)
- [9.12 日期/时间设置](#)

9.1.配置向导

本向导可以引导用户完成“流量管理(七层)”的基础拓扑配置。配置结束后，系统将生成如下配置项：

- 一个虚拟服务器
- 一个资源路径
- 一个服务器组
- 一个静态服务器

同时，ADSG 将自动关联虚拟服务器的资源路径到服务器组。

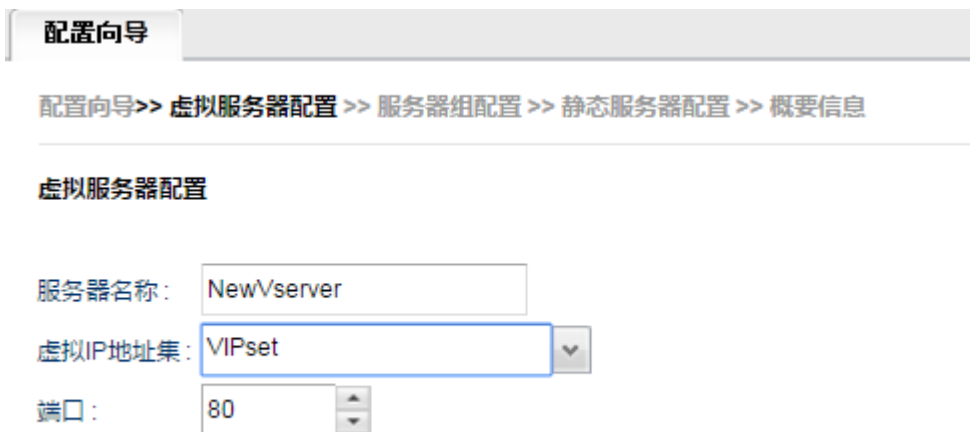
通过配置向导完成基础拓扑后，用户可以通过[虚拟服务>流量管理\(七层\)](#)页面完成详细配置。详细配置请参见 [3.1 七层流量管理](#)。

要使用配置向导，请执行以下操作：

1. 选择**系统>配置向导**。首页给出配置向导的配置步骤及基本功能说明。点击**下一步**。



2. 配置虚拟服务器。填写虚拟服务器的名称,指定虚拟IP地址集及端口,点击**下一步**。



提示: 到**公共对象>IP地址集**添加IP地址集。添加多个虚拟服务器时,端口不能重复。

3. 配置服务器组。填写服务器组的名称,指定服务器健康监视器及端口,点击**下一步**。



4. 配置静态服务器。配置静态服务器的域名或者 IP 地址（必配）、端口，点击下一步。

配置向导

配置向导 >> 虚拟服务器配置 >> 服务器组配置 >> 静态服务器配置 >> 概要信息

静态服务器配置

域名/IP地址:

端口:

提示：必须填写有效的域名或IP地址，否则保存时会提示配置错误。

5. 确认配置信息。概要信息页面显示之前步骤的全部配置信息。此时，可以选择保存或者回退到某一步骤对配置进行修改，然后再保存。

配置向导

配置向导 >> 虚拟服务器配置 >> 服务器组配置 >> 静态服务器配置 >> 概要信息

虚拟服务器配置

服务器名称:

虚拟IP地址集:

端口:

资源路径配置

资源名称:

资源路径:

关联到:

系统自动关联缺省资源路径到服务器组

服务器组配置

服务器组名称:

健康监视器:

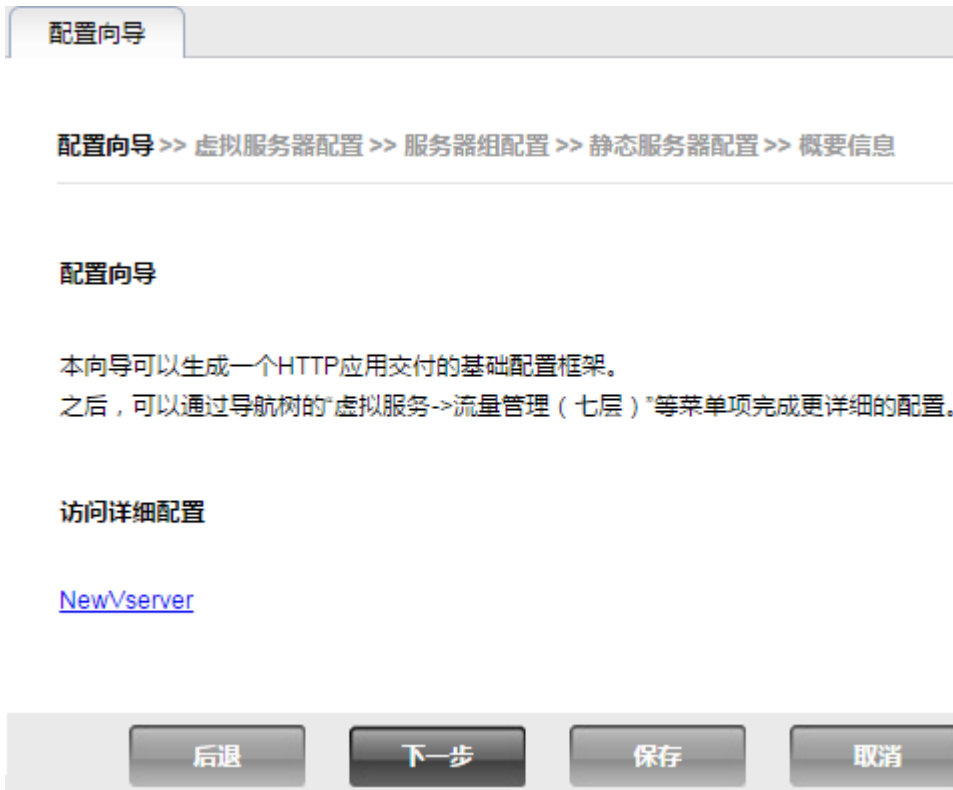
端口:

静态服务器配置

域名/IP地址:

端口:

6. 保存成功后，返回配置向导首页。



这时，可以点击新建虚拟服务器链接跳转到**虚拟服务>流量管理（七层）**页面对虚拟服务器和服务组进行详细配置，也可以点击下一步，继续通过向导添加更多虚拟服务器和服务组。

9.2. 系统维护

系统维护功能包括：

- [9.2.1 备份恢复](#)
- [9.2.2 许可](#)
- [9.2.3 重启和关闭](#)
- [9.2.4 诊断工具](#)
- [9.2.5 技术支持](#)

9.2.1. 备份恢复

备份是将 AD SG 系统内部的各种配置信息（除系统日志、诊断文件和 License 外）打包成文件，并通过 WebUI 下载到管理终端的过程。

备份恢复有三种操作：

- 备份系统配置

对应 WebUI 上的“导出”操作，将系统当前的配置导出并备份到本地管理终端。

- 恢复系统配置

对应 WebUI 上的“导入”操作，将之前备份的文件包重新导入到系统中，系统的配置将替换为导入的文件包中备份的设置。

- 恢复出厂设置

对应 WebUI 上的“恢复出厂设置”操作，系统将恢复到出厂默认状态。此时，除网络配置（IP、路由、DNS）外，其他配置均恢复到产品第一次启动后的状态。

提示：不要人为修改备份文件中的内容，否则使用该文件恢复系统配置会导致系统工作异常。

1. 选择系统>维护>备份/恢复。



2. 点击**导出**按钮，系统将生成当前配置文件包，同时浏览器将自动下载生成的文件包。

3. 选择之前导出的备份文件包，点击**导入**按钮，则系统将恢复到备份包中的配置状态。

4. 点击**恢复出厂设置**，则系统将恢复到出厂时的配置状态。

9.2.2. 许可

许可（License）限制 ADSG 最大虚拟服务器的数量及相关功能的可用性。

许可限制说明

功能	说明
虚拟服务器数量	限制四层和七层的最大虚拟服务器个数。 如未上载许可，则四层和七层各限制使用两个虚拟服务器；如上载许可，则虚拟服务器数量没有限制。

许可到期后，如果四层或七层的虚拟服务器数量大于两个，则保留当前配置，但不能进行创建和修改等操作，只能执行删除操作。上载新的许可之后，可恢复正常操作。

攻击签名	控制攻击签名功能是否可用。
攻击签名升级	控制攻击签名规则升级功能是否可用。
主动防御	控制主动防御功能是否可用。
网页防篡改	控制网页防篡改功能是否可用。
漏洞扫描	控制漏洞扫描功能是否可用。
系统升级	控制系统升级功能是否可用。

如需加载许可，请执行以下操作：

1. 选择**系统>维护>许可**。

备份/恢复
许可
重启/关闭
诊断工具
技术支持

系统主机ID

03000200-0400-0500-0006-000700080009

系统许可信息


功能	状态	有效值	到期时间
虚拟服务器数量	✘	2	-
攻击签名	✘		-
攻击签名升级	✘		-
主动防御	✘		-
网页防篡改	✘		-
漏洞扫描	✘		-
系统升级	✘		-

安装许可

输入License 导入License文件

许可:

- 查看系统主机 ID 号。将系统主机 ID 号发送给技术支持工程师，获取许可文件。
- 将许可字符串输入到**许可**栏中，或者选择导入许可文件，点击**提交**。

4. 上传成功后，系统许可信息栏中，激活功能的状态会显示为，并显示相应的到期时间和有效值。

系统许可信息

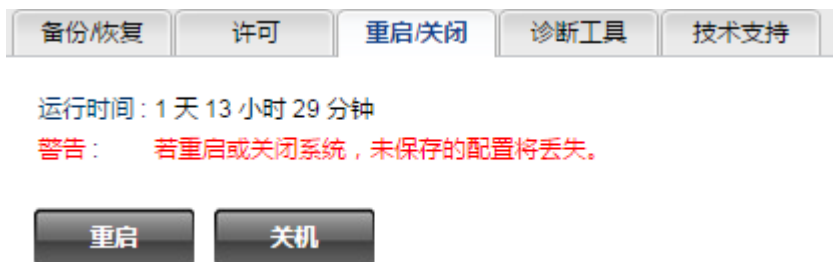
功能	状态	有效值	到期时间
虚拟服务器数量		unlimited	2099-12-31
攻击签名			2099-12-31
攻击签名升级			2019-3-15
主动防御			2099-12-31
网页防篡改			2099-12-31
漏洞扫描			2099-12-31
系统升级			2019-3-15

9.2.3. 重启和关闭

ADSG 可以显示连续运行的时间，并支持用户通过 WebUI 重启或关闭 ADSG 系统。

要重启和关闭系统，请执行以下操作：

1. 选择系统>维护>重启/关闭。



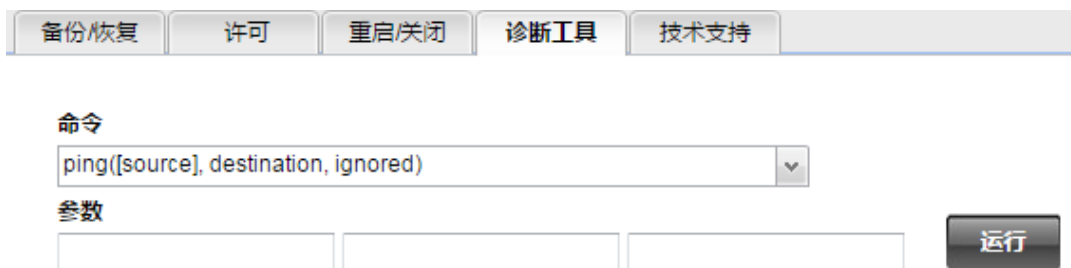
2. 点击重启会重启 ADSG 系统，点击关闭会关闭 ADSG 系统。

9.2.4. 诊断工具

ADSG 支持 ping、tcpdump、tcp scan、capture、show 等诊断命令。

要使用诊断工具，请执行以下操作：

1. 选择系统>维护>诊断工具。



一个诊断工具由一个命令加 0-3 个参数组成。[*]表示可选参数；ignored 表示无需指定参数。

2. 选择命令并输入相关参数，点击**运行**查看诊断结果信息。例如：

命令

ping([source], destination, ignored)

参数

```
# ping -n -c 4 10.1.1.1
PING 10.1.1.1 (10.1.1.1) 56(84) bytes of data:
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=3.87 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=64 time=2.71 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=64 time=7.19 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=64 time=2.62 ms

--- 10.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3011ms
rtt min/avg/max/mdev = 2.629/4.103/7.190/1.850 ms
```

9.2.5. 技术支持

ADSG 支持一键技术支持。管理员可以通过一键式操作，方便地将诊断文件发送给 ADSG 的技术支持中心，尽快地解决问题。诊断信息的内容包括配置文件、系统状态、事件日志等信息。

诊断文件保存在 ADSG 上，可以下载到本地。当生成新的诊断文件时，旧文件会被覆盖。

要使用技术支持功能，请执行以下操作：

1. 选择**系统>维护>技术支持**。
2. 点击**生成**按钮，生成技术支持文件。

技术支持文件

文件名:	tech_support.tar.gz
生成日期:	2018-03-15 15:27:48
大小:	3793142 bytes

3. 点击**下载**，可以将技术支持文件下载到本地管理主机。

9.3.管理设置（Web 和 SSH）

ADSG 默认存在一个系统管理员 admin 和一个根管理员 root，默认允许所有 IP 地址的管理访问，包括 Web 和 SSH 方式。用户可以 admin 身份登录 WebUI，设置 admin 的 Web 访问权限和 root 的 SSH 访问权限。

要设置 Web 和 SSH 访问权限，请执行以下操作：

1. 选择系统>管理设置：

The screenshot shows the 'Global Settings' (全局设置) configuration page. It is divided into three main sections:

- Web管理端口 (Web Management Port):** The 'HTTPS' port is set to 9000. A red warning note states: '注意：请不要配置系统保留端口：22,873,10000...，包括虚拟服务器监听的端口。' (Note: Do not configure system reserved ports: 22, 873, 10000..., including ports listened by virtual servers).
- Web管理访问控制 (Web Management Access Control):**
 - '监听IP地址' (Listen IP Address) is set to '全部IP' (All IP).
 - Below it is a table for 'IP地址' (IP Address) which currently contains '无数据' (No data).
 - '允许访问的源IP地址' (Allow access source IP address) is also set to '全部IP'.
- SSH管理访问控制 (SSH Management Access Control):**
 - '状态' (Status) is checked.
 - '允许访问的源IP地址' (Allow access source IP address) is set to '全部IP'.
 - A yellow tooltip indicates the format: '格式形如：10.1.1.1, 10.2.1.0/24,...' (Format like: 10.1.1.1, 10.2.1.0/24,...).

2. 在 **Web 管理端口**区域，可以修改 ADSG 管理端口号，但注意修改后的管理端口不能与系统中正在使用的端口重复。缺省为 9000。

用户可通过 HTTPS 连接对 ADSG 进行 Web 管理访问。

3. 在 **Web 管理访问控制**区域，可以修改 ADSG 管理口所监听的 IP 地址；也可以设置允许访问 ADSG 管理页面的源 IP 地址，可以设置多个 IP，也可以设置为某个网段的 IP。

4. 在 **SSH 管理访问控制**子项中，可以开启或关闭 SSH 访问功能，设置允许 SSH 管理的源 IP 地址；如果开启，用户可以使用 SSH 以 root 用户身份登录 ADSG 控制台，进行故障诊断或调试。

9.4. 管理用户

ADSG 出厂默认存在两个管理用户：

- 根系统管理员 admin，密码为 neteye。以 admin 身份登录 WebUI，可以修改自身密码、添加根系统审计员、配置根系统所有功能。
- 根管理员 root，密码为 neteye。以根管理员 root 身份登录 WebUI，可以修改自身密码、添加根系统管理员，此外还可以通过 SSH 方式登录 CLI 进行系统调试。

各管理用户角色的关系如下图所示：



本节介绍以下内容：

- [9.4.1 修改 admin/root 密码](#)
- [9.4.2 添加根系统管理员](#)
- [9.4.3 添加根系统审计员](#)

关于如何开启 SSH 访问方式，请参考[错误!未找到引用源。](#)。

9.4.1. 修改 admin/root 密码


要修改 admin/root 的密码，请执行以下操作：

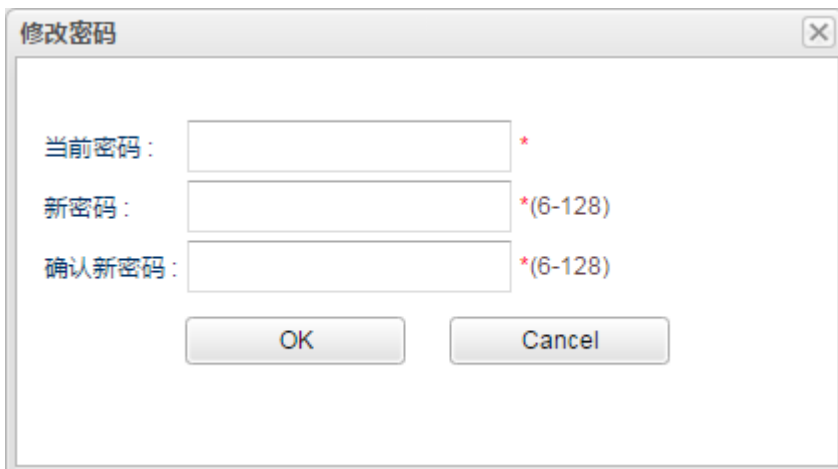
1. 以 admin/root 身份登录 WebUI。
 - 以 admin 身份登录并选择系统>管理用户：



- 以 root 身份登录：



2. 点击界面右上角的快捷菜单，打开**修改密码**对话框。



3. 分别输入新旧密码，点击 **OK**。

9.4.2. 添加根系统管理员

要添加新的根系统管理员，请执行以下操作：

1. 以 root 身份登录 WebUI。
2. 选择**系统>管理用户**。点击**动作**下拉按钮，选择**添加用户**。
3. 在**基本配置**区域的**用户类型**下拉框中，选择 **Administrator**，设置新建根系统管理员的名称、密码和备注信息。



4. 点击**保存**。

9.4.3. 添加根系统审计员

要创建根系统审计员，请执行以下操作：

1. 以 admin 身份登录 WebUI。
2. 选择**系统>管理用户**。点击**动作**下拉按钮，选择**添加用户**。

3. 在**基本配置**区域，设置新建审计员的名称、密码和备注信息。

基本配置

名称： *

密码： *(6-128)

确认密码： *(6-128)

用户类型： ▼

备注：

4. 点击**保存**。

5. 以审计员 **auditor** 身份登录：

东软应用交付安全网关
Neusoft Application Delivery Security Gateway

2017-08-24 23:19:10

auditor

查看

首页 版权信息

系统信息

产品名称:	东软应用交付安全网关
软件版本:	1.3.19.5.14
内存 (KB):	总计: 1876320 已使用: 887728 空闲: 988592
存储 (MB):	总计: 21843 已使用: 3624 空闲: 17303
发布时间:	2018-03-05 09:40:59
系统运行时间:	1 天 9 小时 25 分钟

虚拟服务

域名/IP地址
NewV Server
NewPool
192.168.2.12

事件日志

日期	时间	消息
2018-03-15	23:17:31	User auditor login successfully from WebUI(10.1.4.149)
2018-03-15	23:17:26	User admin logout successfully from WebUI(10.1.4.149)
2018-03-15	23:17:24	User admin add User: auditor successfully
2018-03-15	23:09:59	User admin generate technical support file successfully

系统监控

9.5. 日志设置

ADSG 将各种事件按照分类记录到流量日志、攻击日志和事件日志中。本节介绍如何设置 ADSG 的日志策略。关于如何查看日志信息，请参考 11.5 日志。

要配置 ADSG 的日志功能，请执行以下操作：

1. 选择**系统>日志设置**。
2. 在**基本日志设置**中，可以设置是否生成七层/四层流量日志、攻击日志和事件日志，以及设置日志的保留时间。

3. 点击**高级日志设置**：

- 设置日志占用的最大磁盘空间，最大不能超过 ADSG 系统的磁盘大小；通过下拉菜单设置磁盘空间达到上限时的动作，包括**覆盖最早日志**和**不记录**两种。
- 设置是否记录七层流量和四层流量日志。对性能要求高的用户建议关闭流量日志记录功能。
系统默认记录攻击和事件日志，无需开启。

- 要删除日志，可以勾选不同日志类型对应的复选框，点击**删除**。

4. 点击**保存**。

9.6.报警设置

ADSG 支持邮件报警，可以在发生攻击或事件时通过邮件方式及时通知系统管理员。

要使用邮件报警功能，请执行以下操作：

1. 选择**系统>报警设置**。

SMTP服务器设置

状态：	<input checked="" type="checkbox"/>
语言设置：	简体中文
服务器地址：	10.1.5.56 *
端口：	25
发送间隔：	5 分钟
	<input checked="" type="checkbox"/> SSL安全连接
发件人地址：	adsg@neusoft.com *
收件人：	admin@neusoft.com,infosec@ne... *
	<input checked="" type="checkbox"/> 身份认证
用户名：	adsg *
密码：	***** *

类型设置

攻击日志 事件日志

2. 在 **SMTP 服务器设置**区域，进行如下配置：

- 勾选**状态**，启用邮件报警功能。
- 设置邮件报警的显示语言。
- 设置用于发送报警邮件的服务器地址、端口号、发送间隔、发件人地址、收件人地址，以及是否启用 SSL 安全连接和身份认证。如果启用身份认证，还需要设置发件人的用户名和密码。
收件人允许填写多个收件人地址，多个收件人地址之间用英文逗号隔开。

3. 在**类型设置**区域，选择要发送的日志类型，包括攻击日志和事件日志。

4. 点击**保存**。

9.7. 升级设置

为识别互联网上出现的新型攻击，ADSG 需要及时更新攻击签名规则；ADSG 本身的功能也需要不断完善，所以 ADSG 需要不断的升级以便能更好地为客户提供服务。ADSG 提供在线和本地两种升级方式。其中，在线升级功能有手动和自动两种。缺省情况下，升级功能为关闭状态。

注意：升级过程中，经过ADSG的流量会中断，需要谨慎选择升级时间。当未激活许可时，“攻击签名升级”功能不可用。

请按照以下步骤配置系统升级功能：

1. 选择系统 > 升级设置。

升级设置

状态：

在线升级

攻击签名规则升级：可用

升级方式： 自动 手动

每日升级：0 时 0 分

升级 []

本地升级

升级文件： 未选择任何文件

安装

警告：升级过程中将不能进行系统配置。

软件包列表

名称
adsg-common-tools-1.0-1803
adsg-license-0.11-1741
adsg-administration-ui-0.1-10550
adsg-smartdns-1.0-1762
adsg-nginx-1.11.04-20
adsg-splash-0.0.1-1595
adsg-snmpd-0.11-1438
adsg-isp-spider-1.0-1722
adsg-diagnostic-tool-0.11-1065
adsg-svslog-ng-3.7.3-16

2. 开启升级功能，配置升级类型和条件：

■ 在线升级

选择自动升级时，需配置每天升级的时间，时间采用二十四小时制。

选择手动升级时，需点击**升级**按钮开始系统升级。

■ 本地升级

点击**选择文件**按钮，选择升级文件（从技术支持人员处获取），点击**安装**。

9.8. 报表设置

ADSG 的日志信息可以通过报表功能展现，报表中使用了表格、图表等丰富的表现手段，使得用户能够直观、方便地浏览各种信息。

此外，报表功能还能提供如下功能：

- 定时生成报表；
- 手动生成报表；
- 自定义报表的标题、页眉、页脚和标识；
- 根据时间范围或流量类型选取日志；
- 设置输出的报表文件格式。

要使用报表功能，请执行以下操作：

1. 选择**系统>报表设置**，点击**查看**区域的**动作**，点击**新建报表计划**：

The screenshot shows the 'Report Plan List' interface. At the top, there is a tab labeled '报表计划列表' and a dropdown menu for '动作'. Below this is a table with three columns: '报表计划名称', '报表标题', and '报表生成策略'. The table is currently empty, displaying '无数据'. Below the table, there are five tabs: '基本设置', '范围设置', '生成策略设置', '统计类型设置', and '输出格式设置'. The '基本设置' tab is active, showing a form with the following fields and options:

- 报表计划名称: [Text Input] *
- 报表标题: [Text Input]
- 报表标题标识: 无标识, 自定义 [选择文件] 未选择任何文件 [上传]
- 页眉: [Text Input]
- 页脚: [Text Input]
- 备注: [Text Area]

2. 在**基本配置**区域，可以设置报表计划名称、标题、页眉、页脚、备注信息。**报表标题标识**可以自定义。

3. 点击**范围设置**，设置报表的日志时间范围和数据范围：

4. 点击**生成策略设置**：

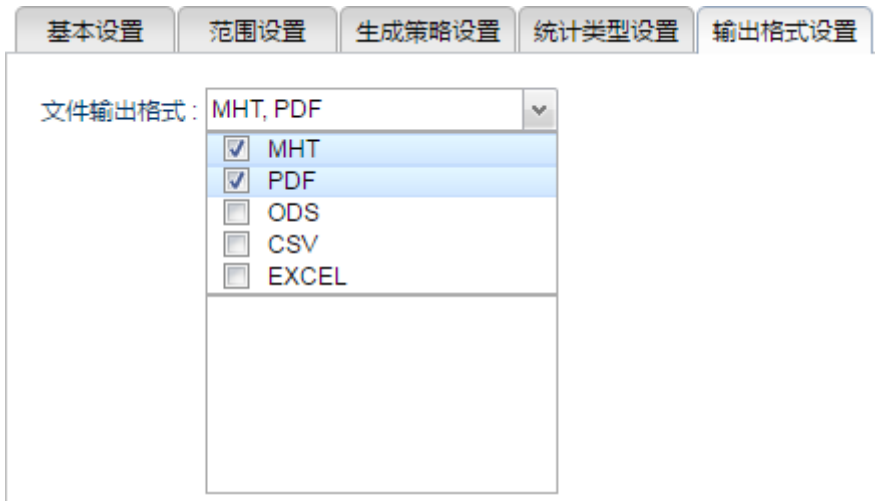
报表生成方式默认为**手动**，用户还可以点击**每天**、**星期**或**日期**，设定生成报表的具体时间。

5. 点击**统计类型设置**：

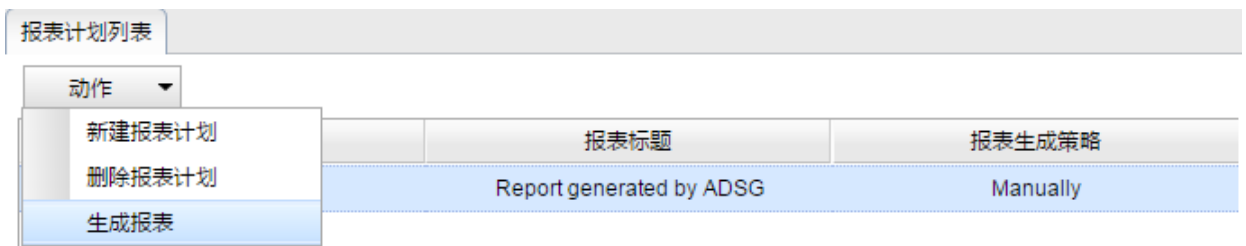
- **Top 数量**：设置 AD SG 显示的各个统计类型中出现次数最多的日志条目数量，取值范围 3-10，默认 5。
- **统计类型**：分为**流量**、**攻击**和**事件**三大类，具体类型分别显示在列表框中。

提示：支持按Ctrl或Shift键多选。

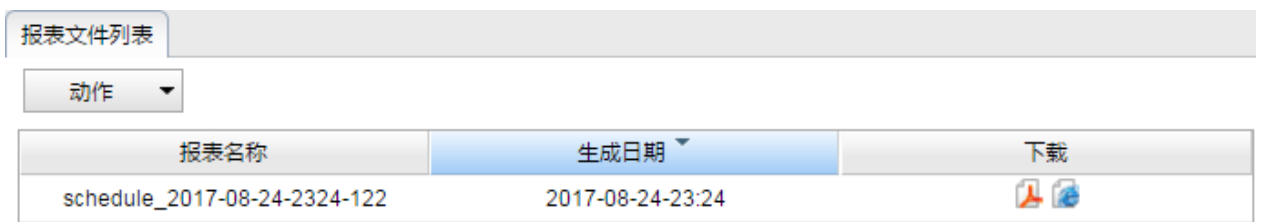
6. 点击**输出格式设置**，使用下拉菜单选择输出的文件格式：



7. 点击**保存**。
8. 选中报表计划，点击**动作**，选择**生成报表**。



9. 报表生成完毕后点击**保存**。
10. 选择**查看>报表**，查看生成的报表：



11. 点击**下载**下方的图标即可下载报表。

9.9.高可用性

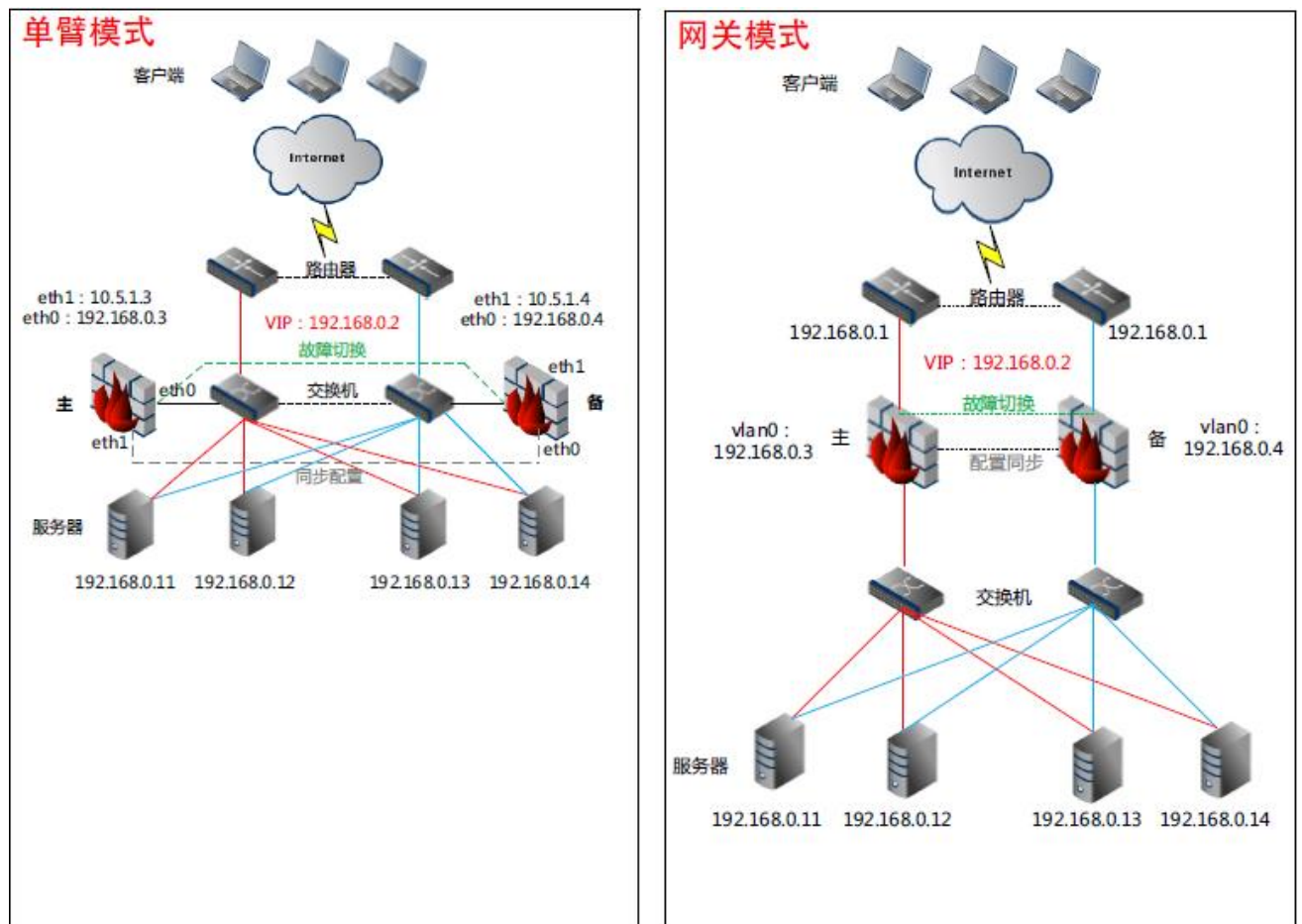
HA（High Availability）即“高可用性”，是指一台 ADSG 在发生故障导致不可用的情况下，其流量自动由另外一台配置相同的 ADSG 接管，从而不间断地为客户提供服务。

ADSG 支持标准的 VRRP（Virtual Router Redundancy Protocol）协议，使用虚拟路由器（VR，Virtual Router）的概念。配置了相同 VRID 的 ADSG 设备构成一个 VR 对，不同 ADSG 上的 VR 选举接口必须处于网络连通状态。

ADSG 支持主备双机热备：主机负责处理业务流量，备机用于在主机不可用时接管主机的流量并继续提供服务。目前 ADSG 仅支持两台 ADSG 设备进行 HA 选举和主备切换。

ADSG 支持手动批量同步配置功能，可手动将本端设备的配置同步到对端设备。同步信息不包括 IP 地址（浮动 IP 除外）和报表文件数据。

ADSG 支持以下高可用性部署场景：



要为 AD SG 配置 HA 功能，请执行以下操作：

1. 选择**系统>高可用性**。
2. 配置全局设置：勾选**状态**按钮，开启 HA 功能，并进行相关配置。

高可用性

全局设置

状态：

MAC同步：

角色：Master *

虚拟路由器ID：10 *

注意：Master和Backup的ID必须相同

心跳口：eth1 *

运行状态：

HA 全局设置参数

参数	说明
状态	是否开启高可用性。
MAC 同步	是否将浮动 IP 的网卡 MAC 修改为自定义的 MAC 地址，即指定浮动 IP 时指定的 MAC 地址。 这样在浮动 IP 漂到备机时，可以保证浮动 IP 对应的接口 MAC 不变，防止上游交换机 ARP 识别错误。
虚拟路由器 ID	虚拟路由器的唯一标识。
角色	当前 AD SG 在虚拟路由器对中所扮演的角色，包括 Master 和 Backup。 如果一台 AD SG 设备的角色设置为 Master，则该 AD SG 上所有虚拟路由器接口在其各自的 VR 对中都为 Master。当 AD SG 上的一个 VR 发生故障切换时，该设备将发生整体切换，即该设备上的所有 VR 都会切换到备状态。
心跳口	监控对端设备状态的接口。建议设为出口浮动 IP 接口。
运行状态	AD SG 作为主/备设备的运行状态，包括 Master 和 Backup。

3. 配置浮动 IP/接口设置：

浮动IP地址/接口设置

接口	浮动IP/掩码	MAC地址
eth2	10.6.226.6/24	2c:41:38:90:91:06

接口： *

浮动IP/掩码： *

MAC地址： *

确定
取消

浮动 IP/接口设置参数

参数	说明
接口	虚拟路由器的选举接口。
浮动 IP/掩码	虚拟路由器选举接口的 IP 地址和掩码。 单臂模式仅需配置一个浮动 IP，网关模式需要配置出入口两个浮动 IP。 添加的浮动 IP 地址将显示在接口列表中，但在接口界面不可修改，只能在此处修改。
MAC 地址	为虚拟路由器的选举接口指定一个自定义的 MAC 地址。

4. 配置同步设置：

同步设置

自动同步配置： 开启 关闭

同步口： *

本地IP： *

远端IP： *

同步设置参数

参数	说明
自动同步配置	是否开启自动同步。
同步口	用于同步配置信息的接口。建议设为管理接口。
本地 IP	本端设备用于同步配置信息的接口 IP 地址。
远端 IP	对端设备用于同步配置信息的接口 IP 地址。
同步	点击该按钮将本端配置同步到对端。 备设备的虚拟服务、安全防护等功能通常不用手动配置，通常通过主设备同步： 1) 配置主设备，包括虚拟服务、安全防护、高可用性等。 2) 登录备设备，配置接口、网关和高可用性。 3) 登录主设备，点击同步按钮，同步配置到备设备。

5. 配置故障切换：

故障切换

关键检测列表：

类型	参数
IP地址检测	任意IP地址;10.176.24.30
掉线检测	eth1
掉线检测	eth2
健康检测	wan1

切换条件：至少 3 条 检测失败

一般检测列表：

类型	参数
掉线检测	eth3
健康检测	wan1
服务进程检测	七层负载均衡
服务进程检测	智能DNS

切换条件：至少 6 条 检测失败

检测类型：IP地址检测 *

检测方式： 任意IP地址 全部IP地址

目的IP：*

确定 取消

检测类型：IP地址检测 *

检测方式： 任意IP地址 全部IP地址

目的IP：*

确定 取消

故障切换设置参数

参数	说明
检测列表	分为关键条件检测列表和一般条件检测列表。
检测类型	<p>包括以下几种：</p> <ul style="list-style-type: none"> IP地址检测：通过 Ping 指定的 IP 地址判断检测结果。 检测方式包括任意 IP 和全部 IP 两种。当添加多个目的 IP 地址时： 任意 IP 地址：只要有一个目的 IP 不可达，即认为检测失败。 全部 IP 地址：只有当全部目的 IP 都不可达，才认为检测失败。 掉线检测：通过探测指定接口的状态判断检测结果。 接口为 Up 时认为检测成功；接口为 Down 时认为检测失败。 接口可以是任意以太网接口。 健康检测：通过探测指定链路的状态判断检测结果。 链路状态为正常或繁忙时，认为检测成功；链路状态为断开时，认为检测失败。 只有链路处于正常或繁忙状态时，才可以选择该链路用于健康检测。 服务进程检测：通过探测指定服务进程的状态判断检测结果。 服务进程正常时，认为检测成功；检测不到服务进程时，认为检测失败。 目前支持对七层负载均衡和智能 DNS 两种服务进程的检测。
切换条件	<p>触发故障切换需要满足的条件。</p> <p>关键检测列表的切换条件建议设置小一些，一般检测列表的切换条件可以放宽一些。</p>

6. 点击**保存**按钮。
7. 配置对端接口和 HA 后，在本端点击**同步**按钮，可将本端设备上的配置信息同步到对端。

9.10. 系统参数

SYN Cookie 是防御 TCP Flood 攻击的主要手段之一，但是其对系统性能有一定影响。ADSG 支持关闭 TCP Flood 防御，还支持多种系统加速技术，可以优化系统内核处理 TCP 流量的性能。

系统有一套缺省配置，请不要随意更改配置内容，如需调整参数以便获取更佳性能，请联系技术支持工程师。

要开启 TCP Flood 防御或系统加速功能，请执行以下操作：

1. 选择**系统>系统参数**。
2. 查看默认配置：

TCP Flood 防御

SYN Cookie :

系统加速

拥塞避免 :	<input checked="" type="checkbox"/>	慢启动 :	<input checked="" type="checkbox"/>
快速重传 :	<input checked="" type="checkbox"/>	接收数据缓冲 :	16777216 字节
快速恢复 :	<input checked="" type="checkbox"/>	发送数据缓冲 :	16777216 字节
慢启动阈值缓存 :	<input type="checkbox"/>		

3. 根据需要修改默认配置，点击**保存**。

9.11.SNMP

ADSG 支持网络中的管理站通过 SNMP 协议获取 ADSG 的一些状态信息，如主机名、CPU 占用率、内存占用率和接口状态等。

ADSG 支持 SNMP v1、v2 和 v3：

- 在 SNMP v1 和 SNMP v2 中，管理站和被管 ADSG 之间通过团体字符串进行认证，数据通过明文传输。
- 在 SNMP v3 中，管理站和被管 ADSG 之间通过 SNMP 用户信息进行认证，数据传输支持加密。

为保证管理数据安全，建议使用 SNMP v3 进行管理。

要使用 SNMP 服务，请执行以下操作：

- 选择**系统>SNMP**。
- 在**SNMP 基本配置**区域，开启 SNMP 服务，设置 SNMP 管理端口号和团体字符串。



SNMP设置

SNMP基本配置

启用SNMP：

SNMP版本：**v1/v2/v3**

端口： *

团体字符串： *

提示：ADSG上设置的团体字符串必须与管理站保持一致。

- 当 SNMP 管理站使用 SNMP v3 通信时，需要在**SNMP 用户列表**区域添加 SNMP 用户。

SNMP用户列表

名称	权限	安全级别
SNMPuser1	只读	认证并加密
SNMPuser2	读写	认证但不加密

名称： *

权限：

安全级别：

认证： * 认证算法 MD5

密钥： * 加密算法 DES

ADSG 支持添加只读和读写两种 SNMP 用户，SNMP 用户支持采用认证并加密、认证但不加密两种认证方式。SNMP 用户具有何种读写权限、采用何种认证方式，必须和 SNMP 管理站保持一致。认证算法和加密密钥必须为 8 到 16 位的字符。

- 点击**保存**。

9.12. 日期/时间设置

ADSG 允许用户修改系统时间和时区，支持手动更新系统时间和使用 NTP 服务器自动同步两种方式，而使用 NTP 服务器又分为手动和自动两种方式。

要更新系统时间，请执行以下操作：

1. 选择**系统>日期/时间设置**：

2. 点击系统当前时间后面的 图标，手动修改系统时间：

3. 在**时区设置**区域，点击**时区**的下拉菜单选择时区。
4. 在**NTP 服务器设置**区域，设置 NTP 服务器地址并选择 NTP 同步方式：
 - 选择**手动**，点击**同步**按钮，立即使用 NTP 服务器进行时间同步。
当正在**连接服务器**的提示框消失后，即表示时间同步完成，此时不需要保存。
 - 选择**自动**，使 ADSG 以自动的方式实现 NTP 时间同步。
5. 点击**保存**。

第10章 虚拟系统

一个 ADSG 系统可以在逻辑上划分为多个虚拟系统，每个虚拟系统可以被看成一个独立的 ADSG 系统，拥有独立的管理 IP、负载均衡策略和安全策略。只有根管理员 root 才有权限创建虚拟系统和添加虚拟系统管理员。

提示： 由于虚拟系统对系统资源有较高要求，仅高端机型才支持虚拟系统功能。

本章介绍以下内容：

- [10.1. 创建虚拟系统](#)
- [10.2. 添加虚拟系统管理员](#)
- [10.3. 管理虚拟系统](#)

10.1. 创建虚拟系统

要创建虚拟系统，请执行以下操作：

1. 以根管理员 root 身份登录 WebUI。
2. 选择**系统>虚拟系统**。点击**动作**下拉按钮，选择**添加虚拟系统**。
3. 在**基本配置**区域，设置新建虚拟系统的相关信息。

基本配置

状态：

虚拟系统： *(1-255)

CPU数量： *

内存： *

备注：

接口列表

可用接口	已选接口
eth-s1p1	eth-s1p3
eth-s1p2	eth-s1p4
eth-s1p6	eth-s1p5
eth-s1p7	
eth-s1p8	

管理IP地址



接口：

管理IP地址：

掩码长度：

提示： 必须为虚拟系统选择接口并配置管理IP地址，才能创建成功。

4. 点击**保存**。
5. 查看已创建的虚拟系统。

虚拟系统	CPU数量	内存 (G...	接口	状态	Web管理	备注
vsys1	2	2	eth-s3p7,eth-s3p8,eth-s3p6	✓		
vsys2	2	2	eth-s3p1,eth-s3p4,eth-s3p5	✓		

6. 点击 Web 管理列的图标，可跳转到指定虚拟系统的登录页面。

10.2. 添加虚拟系统管理员

要添加虚拟系统管理员，请执行以下操作：

1. 以 root 身份登录 WebUI。
2. 选择**系统>管理用户**。点击**动作**下拉按钮，选择**添加用户**。
3. 在**基本配置**区域的用户类型下拉框中，选择 **Vsys Administrator**，设置新建系统管理员的名称、密码、备注信息和被管理虚拟系统。

基本配置

名称： *

密码： *(6-128)

确认密码： *(6-128)

用户类型： ▼

备注：

虚拟系统列表

<div style="background-color: #f0f0f0; padding: 2px; text-align: center;">备选虚拟系统</div> <div style="padding: 5px; text-align: center;">vsys2</div>	<input type="button" value="→"/> <input type="button" value="←"/>	<div style="background-color: #f0f0f0; padding: 2px; text-align: center;">已选虚拟系统</div> <div style="padding: 5px; text-align: center;">vsys1</div>
---	--	---

提示：需要事先创建虚拟系统，才能为新建虚拟系统管理员指定被管理的虚拟系统。一个虚拟系统管理员可以管理多个虚拟系统。

4. 点击**保存**。

10.3.管理虚拟系统

虚拟系统不支持重启、关机、修改系统时间、上载 License、配置出站链路负载均衡等全局性操作。

提示：管理客户端需要和虚拟系统管理接口在同一网段才能访问和管理虚拟系统。

要管理虚拟系统，请执行以下操作：

1. 在浏览器中输入虚拟系统的管理地址：https://Vsys_Mgt_IP:9000。
2. 以虚拟系统管理员身份登录。
3. 参考其他章节，配置网络、虚拟服务、Web 安全等相关功能。

推荐配置顺序：路由->网络接口->虚拟服务->Web 安全。

第11章 监控

通过 ADSG 提供的状态监控功能用户可以直观地了解 ADSG 的系统运行状态以及日志、报表信息。本章节结构如下所示：

- [11.1 首页](#)
- [11.2 版权信息](#)
- [11.3 监控](#)
- [11.4 统计](#)
- [11.5 日志](#)
- [11.6 报表](#)

11.1. 首页

ADSG 监控首页可以方便用户实时查看系统活动状态、最新的事件日志、资源使用情况和虚拟服务器状态，从而根据需要调整系统配置信息。

用户登录 ADSG 后，默认进入系统首页，首页显示内容如下：

- 系统信息：

系统信息

产品名称:	东软应用交付安全网关
软件版本:	1.3.19.5.17
语言:	简体中文
内存 (KB):	总计: 1876320 已使用: 941696 空闲: 934624
存储 (MB):	总计: 21660 已使用: 3247 空闲: 17497
发布时间:	2018-03-22 17:04:41
系统运行时间:	3 天 19 小时 11 分钟

- 事件日志：

事件日志

日期	时间	消息
2018-03-26	10:42:20	用户(admin)修改IP地址集【VserverIPset】成功
2018-03-26	10:42:20	用户(admin)修改七层静态服务器【192.168.10.9】成功
2018-03-26	10:42:20	用户(admin)修改七层静态服务器【192.168.10.8】成功
2018-03-26	10:42:20	用户(admin)修改七层静态服务器【192.168.10.7】成功

虚拟服务：

虚拟服务

域名/IP地址	端口	服务器组	健康状态
[-] NewVServer			
[-] NewPool			
10.1.3.166	80	NewPool	up
[-] NewVServer_L4			
[-] NewPool_L4			
10.1.3.166	80	NewPool_L4	down

系统监控（包括 CPU、内存和磁盘使用率）：

系统监控



11.2. 版权信息

1. 选择查看>首页>版权信息。
2. 查看 AD SG 的版权信息：

首页 版权信息

[开放源码信息](#)

版权所有 (c) 2012-2017 沈阳东软系统集成工程有限公司

软件受以下版权约束：

- Copyright (c) 2009, Valery Kholodkov. All rights reserved.
- Copyright (c) 2013, NBS System. All rights reserved.
- Copyright (c) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
- Copyright (c) 1997-2011, PostgreSQL Global Development Group All rights reserved.
- Copyright (c) 2007 Free Software Foundation, Inc. <<http://fsf.org/>>
- Copyright (c) 1999-2013, The Apache Software Foundation Apache Tomcat, Tomcat, Apache, the Apache feather, and the Apache Tomcat project logo are trademarks of the Apache Software Foundation.

11.3. 监控

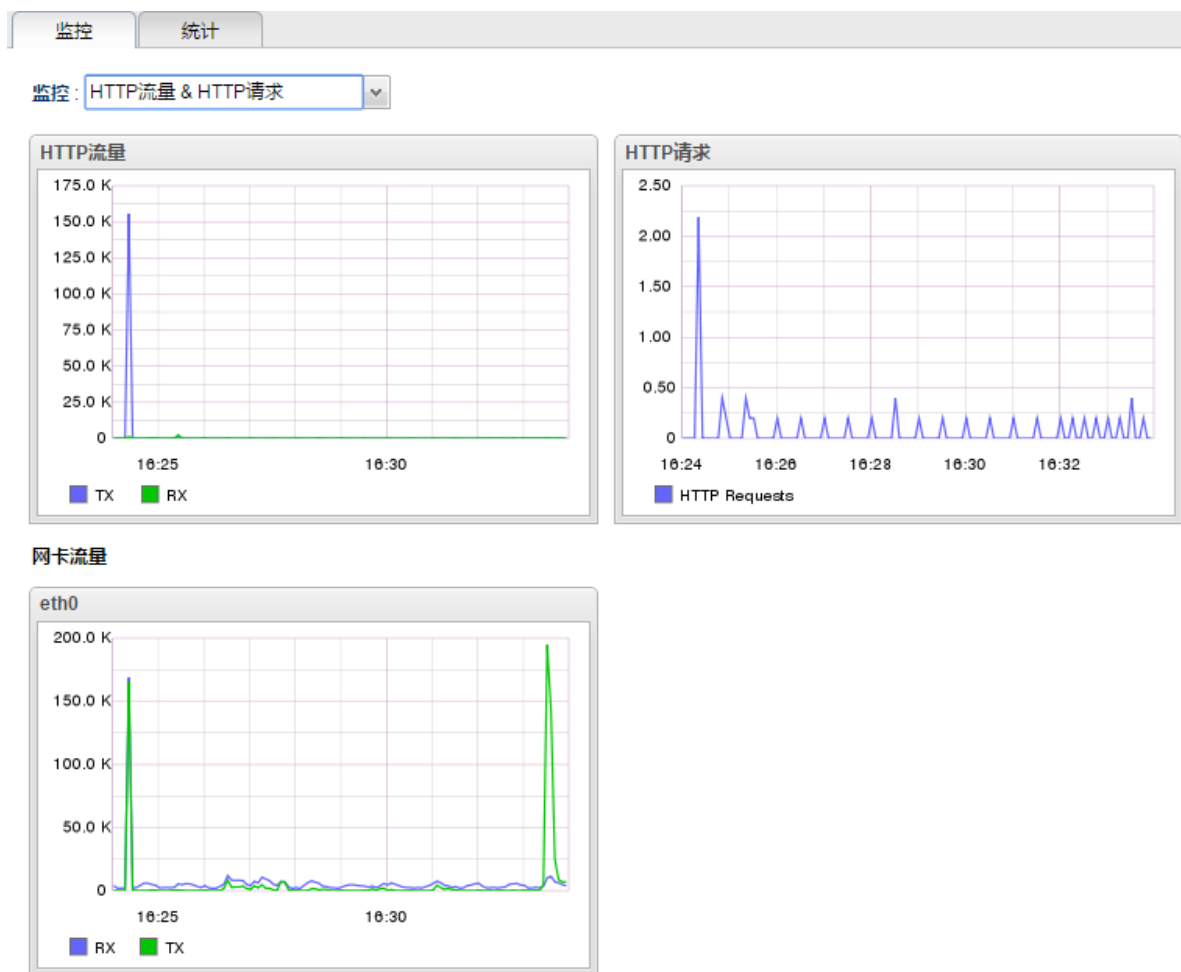
通过监控页面，用户可实时查看 HTTP 流量、各虚拟服务器/静态服务器流量以及网卡流量。

1. 选择查看>监控>监控。
2. 在监控下拉框中选择监控对象，包括 HTTP 流量&HTTP 请求、虚拟服务器、静态服务器。

提示：需配置七层虚拟服务器并关联服务器组，才能查看虚拟服务器、静态服务器的流量信息。无论选择哪种监控对象，页面下方始终显示各网卡进出流量。

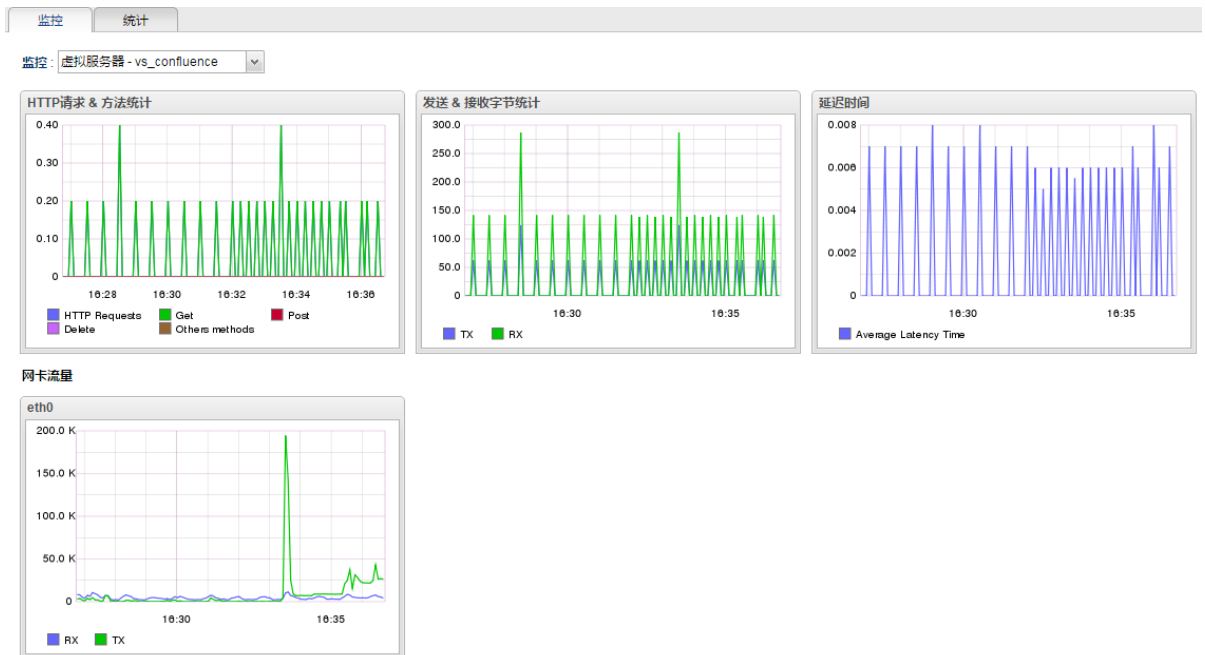
3. 查看流量信息：

- 当选择 HTTP 流量&HTTP 请求时，显示如下信息：



- HTTP 流量和网卡流量的坐标图中，横轴表示时间，纵轴表示流量大小，纵轴单位根据现网实际流量的大小进行自适应调节。缺省情况下单位为字节（B），当达到 KB 时则显示 K，以此类推。
- HTTP 请求的坐标图中，横轴表示时间，纵轴表示一段时间内 HTTP 请求数量与时间段的比值。
- TX 表示发送的流量，RX 表示接收的流量。

- 当选择虚拟服务器或静态服务器时，显示如下信息：



- 在 **HTTP 请求&方法统计**坐标图中，横轴表示时间，纵轴表示请求次数，线条颜色表示请求种类。
- 在**发送&接收字节数**坐标图中，横轴表示时间，纵轴表示流量大小，纵轴单位根据现网实际流量的大小进行自适应调节。缺省情况下单位为字节（B），当达到 KB 时则显示 K，以此类推。TX 表示发送的流量大小，RX 表示接收的流量大小。
- 在**延迟时间**坐标图中，横轴表示时间，纵轴表示虚拟服务器的延迟时间（单位为秒）。

提示： 此处监控的流量信息受**虚拟服务>流量管理(七层)**配置的影响。

11.4. 统计

统计页面可显示一段时间内的 HTTP 流量/请求信息、各虚拟服务器/静态服务器流量信息、系统资源使用情况以及网卡流量信息。

1. 选择**查看>监控>统计**。
2. 在**统计**下拉框中选择统计时间段，包括**最近 30 分钟**、**最近 1 小时**、**最近 3 小时**、**最近 1 天**、**最近 7 天**和**最近 30 天**。
3. 在**监控**下拉框中选择监控对象，包括**系统资源**、**HTTP 流量&HTTP 请求**、**虚拟服务器**、**静态服务器**。

提示：需配置七层虚拟服务器并关联服务器组，才能查看虚拟服务器、静态服务器的流量统计信息。无论选择哪种监控对象，页面下方始终显示各网卡进出流量。

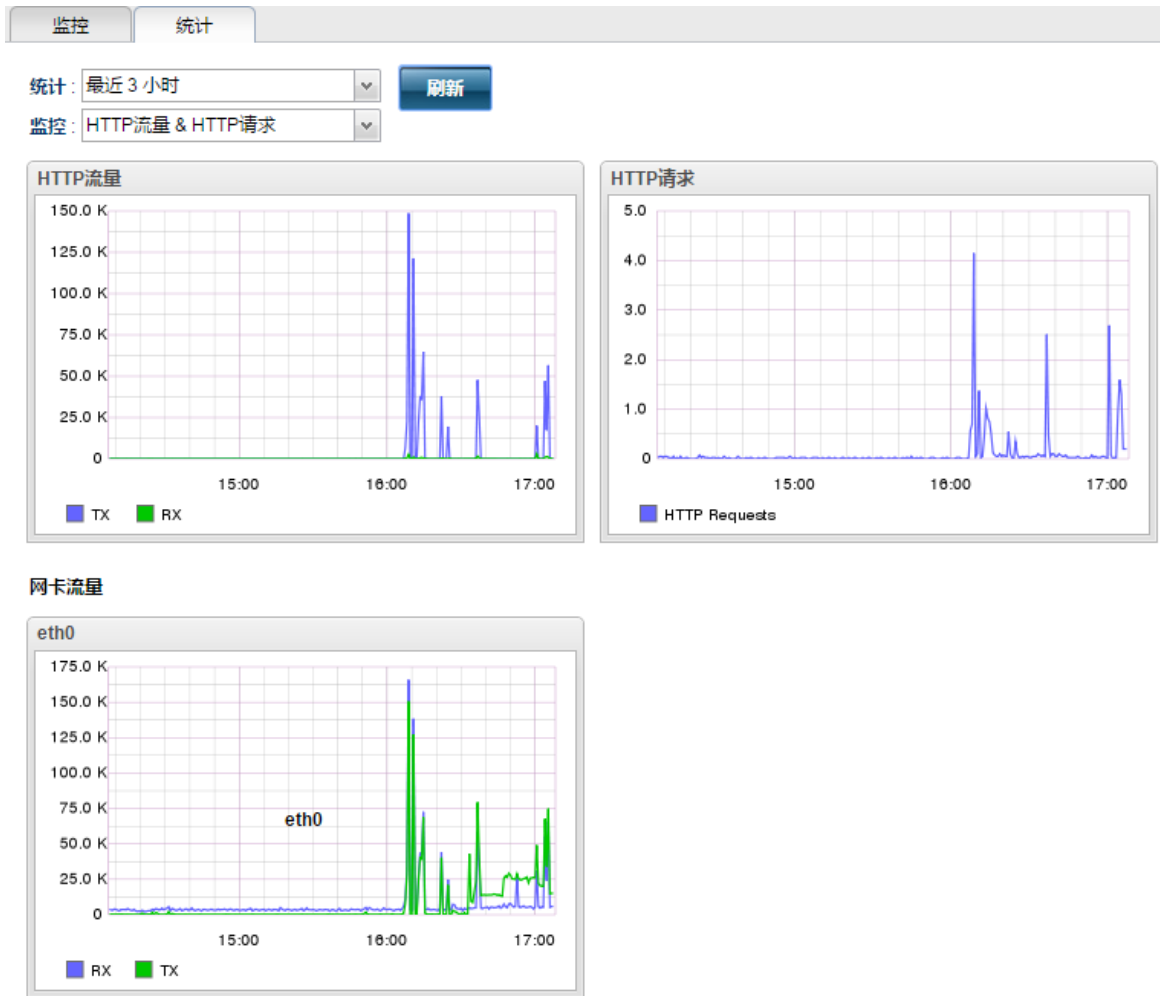
4. 点击**刷新**。查看统计信息：

- 当选择监控系统资源时，显示如下信息：



- CPU 使用率图表中，横轴表示时间，纵轴表示使用率。不同 CPU 通过不同颜色加以区分。
- 内存使用图表中，横轴表示时间，纵轴表示内存使用大小。不同内存使用类型用不同的颜色区分。
- 磁盘使用图表中，横轴表示时间，纵轴表示磁盘容量使用大小。

- 当选择监控 HTTP 流量&HTTP 请求时，显示如下信息：



- 当选择监控虚拟服务器或静态服务器时，显示如下信息：



相关参数解释请参考 [11.3 监控](#)。

11.5. 日志

ADSG 支持本地查看系统日志信息，包括流量日志、攻击日志、事件日志和访问统计。ADSG 支持通过一些过滤条件过滤日志、以 csv 文件的格式下载日志。关于日志的详细信息，请参见[附录 B，日志信息](#)。

本节介绍以下内容：

- [11.5.1 七层流量日志](#)
- [11.5.2 四层流量日志](#)
- [11.5.3 攻击日志](#)
- [11.5.4 事件日志](#)
- [11.5.5 访问统计](#)
- [11.5.6 自定义显示的日志信息](#)


11.5.1. 七层流量日志

要查看或过滤七层流量日志信息，请执行以下操作：

1. 选择查看>日志>七层流量日志。
2. 在查看区域查看七层流量日志，在配置区域设置日志过滤条件：

The screenshot displays the ADSG interface for viewing Layer 7 traffic logs. At the top, there are tabs for '七层流量日志', '四层流量日志', '攻击日志', '事件日志', and '访问统计'. Below the tabs is a navigation bar with '首页', '上一页', '1/2', '下一页', and '尾页'. The main area contains a table with the following columns: 编号, 日期, 时间, 源IP, 目的IP, 主机, 用户代理, URL, 虚拟服务器, 服务器组, 节点, HTTP请求, 应答码, 字节, and 响应时间. The table lists 11 log entries. Below the table is a '过滤' (Filter) panel with input fields for '起始日期时间', '终止日期时间', '源IP', '目的IP', '虚拟服务器', '服务器组', and 'URL'. There are also '重置' (Reset), '过滤' (Filter), and '下载' (Download) buttons.

编号	日期	时间	源IP	目的IP	主机	用户代理	URL	虚拟服务器	服务器组	节点	HTTP请求	应答码	字节	响应时间
1	2018-03-...	10:52:08	10.9.208...	10.176.2...	10.176.2...	Mozilla/5...	/rest/pop...	NewVServer...	-		GET	425	1439	0.0
2	2018-03-...	10:52:08	10.9.208...	10.176.2...	10.176.2...	Mozilla/5...	/rest/pro...	NewVServer...	-		GET	425	1439	0.0
3	2018-03-17	10:52:08	10.9.208...	10.176.24...	10.176.24...	Mozilla/5...	/dashboar...	NewVServer	NewPool	10.9.211.1...	GET	200	7672	1.068
4	2018-03-17	10:52:07	10.9.208...	10.176.24...	10.176.24...	Mozilla/5...	/favicon.i...	NewVServer	NewPool	10.9.211.1...	GET	200	370317	0.594
5	2018-03-...	10:52:07	10.9.208...	10.176.2...	10.176.2...	Mozilla/5...	/rest/pop...	NewVServer...	-		GET	425	1439	0.0
6	2018-03-...	10:52:07	10.9.208...	10.176.2...	10.176.2...	Mozilla/5...	/rest/pro...	NewVServer...	-		GET	425	1439	0.0
7	2018-03-17	10:52:07	10.9.208...	10.176.24...	10.176.24...	Mozilla/5...	/dashboar...	NewVServer	NewPool	10.9.211.1...	GET	200	7671	0.096
8	2018-03-...	10:51:44	10.9.208...	10.176.2...	10.176.2...	Mozilla/5...	/favicon.i...	NewVServer...	-		GET	421	1446	0.0
9	2018-03-...	10:51:44	10.9.208...	10.176.2...	10.176.2...	Mozilla/5...	/favicon.i...	NewVServer...	-		GET	421	1446	0.0
10	2018-03-...	10:51:44	10.9.208...	10.176.2...	10.176.2...	Mozilla/5...	/dashboa...	NewVServer...	-		GET	421	1446	0.0
11	2018-03-...	10:51:44	10.9.208...	10.176.2...	10.176.2...	Mozilla/5...	/dashboa...	NewVServer...	-		GET	421	1446	0.0

- 过滤条件中，日期可以通过点击 来选择。
- 点击右下方的**过滤**，则上方只显示符合条件的日志。
- 点击**下载**，则会将显示的信息以 csv 文件的格式保存到本地。

11.5.2. 四层流量日志

要查看或过滤四层流量日志信息，请执行以下操作：

1. 选择查看>日志>四层流量日志。
2. 在查看区域查看四层流量日志，在配置区域设置日志过滤条件。

编号	日期	时间	源IP	源端口	目的IP	目的端口	本地IP	本地端口	动作
1	2018-03-17	09:39:47	10.9.208.133	52536	10.176.24.39	80	10.176.24.36	5022	DELETE
2	2018-03-17	09:39:47	10.9.208.133	52535	10.176.24.39	80	10.176.24.36	5021	DELETE
3	2018-03-17	09:39:47	10.9.208.133	52541	10.176.24.39	80	10.176.24.36	5026	DELETE
4	2018-03-17	09:39:47	10.9.208.133	52539	10.176.24.39	80	10.176.24.36	5025	DELETE
5	2018-03-17	09:39:47	10.9.208.133	52538	10.176.24.39	80	10.176.24.36	5024	DELETE
6	2018-03-17	09:39:47	10.9.208.133	52537	10.176.24.39	80	10.176.24.36	5023	DELETE
7	2018-03-17	09:36:41	10.9.208.133	52541	10.176.24.39	80	10.176.24.36	5026	NEW
8	2018-03-17	09:36:41	10.9.208.133	52539	10.176.24.39	80	10.176.24.36	5025	NEW
9	2018-03-17	09:36:41	10.9.208.133	52538	10.176.24.39	80	10.176.24.36	5024	NEW
10	2018-03-17	09:36:41	10.9.208.133	52537	10.176.24.39	80	10.176.24.36	5023	NEW

11.5.3. 攻击日志

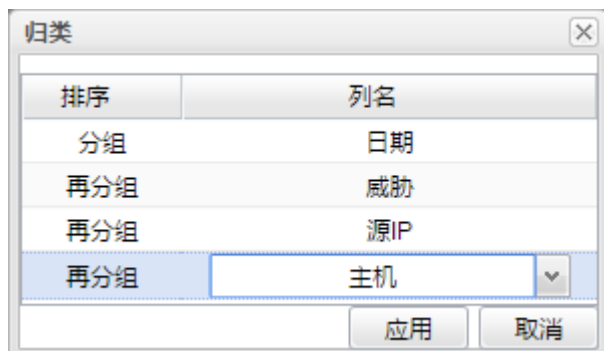
要查看或过滤攻击日志信息，请执行以下操作：

1. 选择查看>日志>攻击日志。
2. 查看或过滤攻击日志：

编号	日期	时间	源IP	主机	用户代理	URL	虚拟服务器	威胁	动作	规则	消息
1	2018-03-17	10:52:08	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /rest/popula...	NewVServer	Unknown Th...	Block	Number of ...	命中Number o...	
2	2018-03-17	10:52:08	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /rest/protot...	NewVServer	Unknown Th...	Block	Number of ...	命中Number o...	
3	2018-03-17	10:52:07	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /rest/popula...	NewVServer	Unknown Th...	Block	Number of ...	命中Number o...	
4	2018-03-17	10:52:07	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /rest/protot...	NewVServer	Unknown Th...	Block	Number of ...	命中Number o...	
5	2018-03-17	10:51:44	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /favicon.ico	NewVServer	Unknown Th...	Block	HTTP Reque...	命中HTTP Req...	
6	2018-03-17	10:51:44	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /favicon.ico	NewVServer	Unknown Th...	Block	HTTP Reque...	命中HTTP Req...	
7	2018-03-17	10:51:44	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /dashboard...	NewVServer	Unknown Th...	Block	HTTP Reque...	命中HTTP Req...	
8	2018-03-17	10:51:44	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /dashboard...	NewVServer	Unknown Th...	Block	HTTP Reque...	命中HTTP Req...	
9	2018-03-17	10:51:44	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /favicon.ico	NewVServer	Unknown Th...	Block	HTTP Reque...	命中HTTP Req...	
10	2018-03-17	10:51:44	10.9.208.133	10.176.24.39	Mozilla/5.0 (... /favicon.ico	NewVServer	Unknown Th...	Block	HTTP Reque...	命中HTTP Req...	

3. 当攻击日志条目数量较多时，可以通过归类功能查看具有相同特点的日志信息，以便快速定位问题。

a. 点击**日志归类**，弹出**归类**对话框。



b. 双击列名列表的条目，选择分组依据的列名，点击**应用**。

攻击日志支持最多四种类型的分组，分别是威胁、日期、源 IP 和主机。系统根据列名列从上到下依次做为分组依据。

4. 攻击日志和事件日志针对日志级别进行条目底色区分，方便用户查看。具体颜色表达级别含义如下所示：

红	LOG_EMERG 0
橙	LOG_ALERT 1
黄	LOG_CRIT 2
青	LOG_ERR 3

提示：具体日志级别划分请参见[附录B，日志信息](#)。

11.5.4. 事件日志

要查看或过滤事件日志信息，请执行以下操作：

1. 选择查看>日志>事件日志。
2. 查看或过滤事件日志：

The screenshot shows the '事件日志' (Event Log) tab selected. The log entries are as follows:

编号	日期	时间	等级	模块	消息
1	2018-03-17	09:41:15	notice	WebUI	用户:admin 通过WebUI(10.9.208.133)登录成功
2	2018-03-17	09:41:10	error	WebUI	用户:admin 通过WebUI(10.9.208.133)登录失败
3	2018-03-17	09:41:07	notice	WebUI	用户:root 通过WebUI(10.9.208.133)退出成功
4	2018-03-17	09:38:44	notice	WebUI	用户:root 通过WebUI(10.9.208.133)登录成功
5	2018-03-17	09:38:41	error	WebUI	用户:root 通过WebUI(10.9.208.133)登录失败
6	2018-03-17	09:38:39	notice	WebUI	用户:admin 通过WebUI(10.9.208.133)退出成功
7	2018-03-17	09:30:11	notice	WebUI	用户(admin)修改四层静态服务器【10.9.211.120】成功
8	2018-03-17	09:30:11	notice	WebUI	用户(admin)修改健康监视器【TCP_Ping】成功
9	2018-03-17	09:30:11	notice	WebUI	用户(admin)新建四层虚拟服务器【NewVServer_L4】成功
10	2018-03-17	09:30:11	notice	WebUI	用户(admin)修改IP地址集【10.176.24.39】成功

Below the log list is a '过滤' (Filter) section with the following fields:

- 起始日期时间: [Date Picker] 0 : 0 : 0
- 终止日期时间: [Date Picker] 0 : 0 : 0
- 模块: [Dropdown]
- 日志ID: [Text Input]
- [重置] button

3. 可通过日志条目底色快速定位特定级别的日志信息。颜色对应的级别同攻击日志。

11.5.5. 访问统计

要查看或过滤访问统计信息，请执行以下操作：

1. 选择查看>日志>访问统计。
2. 查看或过滤访问统计信息：

The screenshot shows the '访问统计' (Access Statistics) tab selected. The statistics table is as follows:


虚拟服务器	服务器组	静态服务器	访问数量
NewVServer	NewPool	223.1.1.2:80	16
NewVServer	NewPool	223.1.1.5:80	147

Below the table is a '过滤' (Filter) section with the following fields:

- 虚拟服务器: [Dropdown]
- 服务器组: [Dropdown]
- [重置] button

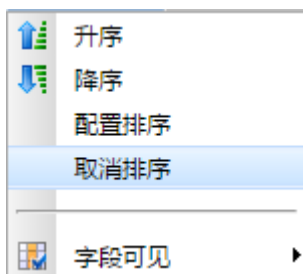
At the bottom right of the interface are buttons for '过滤' (Filter) and '下载' (Download).

11.5.6. 自定义显示的日志信息

1. 移动鼠标到日志列表表头，会出现一个  按钮。
2. 点击该按钮，可以：
 - 1) 对显示的日志信息排序（升序/降序）；
 - 2) 设置排序条件；
 - 3) 设置要显示的日志信息列。



您也可以根据需要清空排序条件。

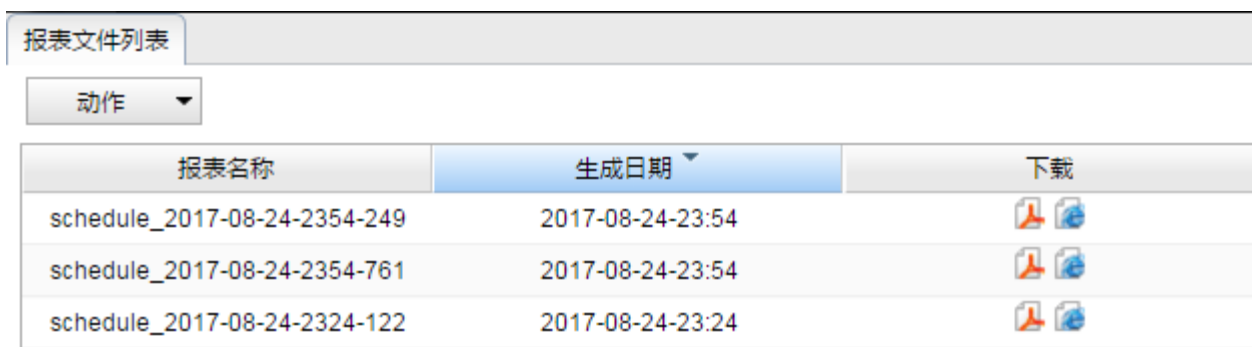


11.6. 报表







显示已经生成的报表。可到**系统>报表设置**页面设置报表生成计划，详细信息请参见 9.8 报表设置。

请按照以下步骤查看报表信息：

1. 选择**系统>报表设置**，添加报表生成计划或手动生成报表。
2. 选择**查看>报表**，查看生成的报表结果。



The screenshot shows a web interface titled '报表文件列表' (Report File List). Below the title is a '动作' (Action) dropdown menu. The main content is a table with three columns: '报表名称' (Report Name), '生成日期' (Generation Date), and '下载' (Download). The table contains three rows of data, each with a report name, a generation date, and two download icons (PDF and image).

报表名称	生成日期	下载
schedule_2017-08-24-2354-249	2017-08-24-23:54	 
schedule_2017-08-24-2354-761	2017-08-24-23:54	 
schedule_2017-08-24-2324-122	2017-08-24-23:24	 

3. 点击**下载**下方的图标可以下载报表到本地查看。
4. 选中报表后点击右下方的**删除**能够删除报表，也可以点击左上方的**动作**，再点击**删除**来删除选中的报表。删除报表后点击**保存**生效，也可以点击**恢复**取消删除。

第12章 范例

本章提供 ADSG 的应用实例，包括：

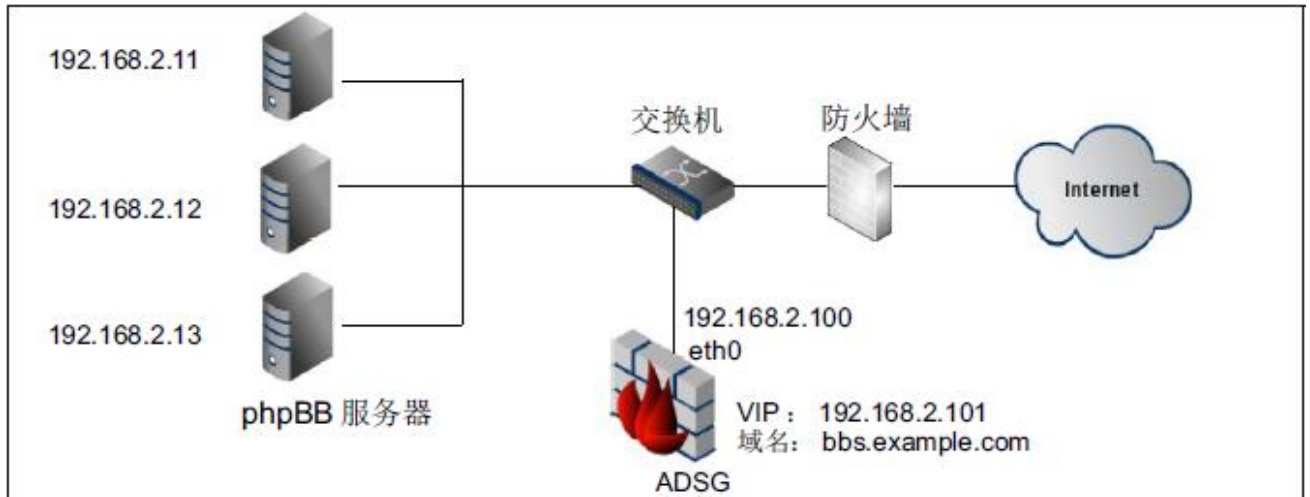
- [12.1 服务器负载均衡](#)
- [12.2 Web 安全防护](#)
- [12.3 主动防御](#)
- [12.4 进站链路负载均衡（单数据中心）](#)
- [12.5 全局负载均衡（多数据中心）](#)
- [12.6 出站链路负载均衡](#)
- [12.7 出站链路负载均衡（启用 DNS 透明代理）](#)
- [12.8 某城市轨道交通用户配置实例](#)
- [12.9 电力网正反向虚拟隔离（虚拟系统）](#)

12.1. 服务器负载均衡

背景：

某公司处有多台论坛服务器（内部采用 phpBB 实现），ADSG 部署在其前面作为负载均衡器使用。管理员不希望改变现有的网络拓扑，所以我们推荐使用 ADSG 的单臂模式。

拓扑：



配置指南：

1. 在防火墙上配置 DNAT 规则，将访问 80 端口的流量转发到 ADSG 上。
2. 在 ADSG 上配置虚拟服务器 VServer_phpBB，监听 80 端口，并设置相应的域名，比如：
bbs.example.com。
3. 在 ADSG 上配置服务器组 Pool_phpBB，添加三个静态服务器节点，开启 80 端口。
4. 在 Pool_phpBB 上启用会话保持，并设置工作模式为插入新 Cookie 方式。

配置步骤：

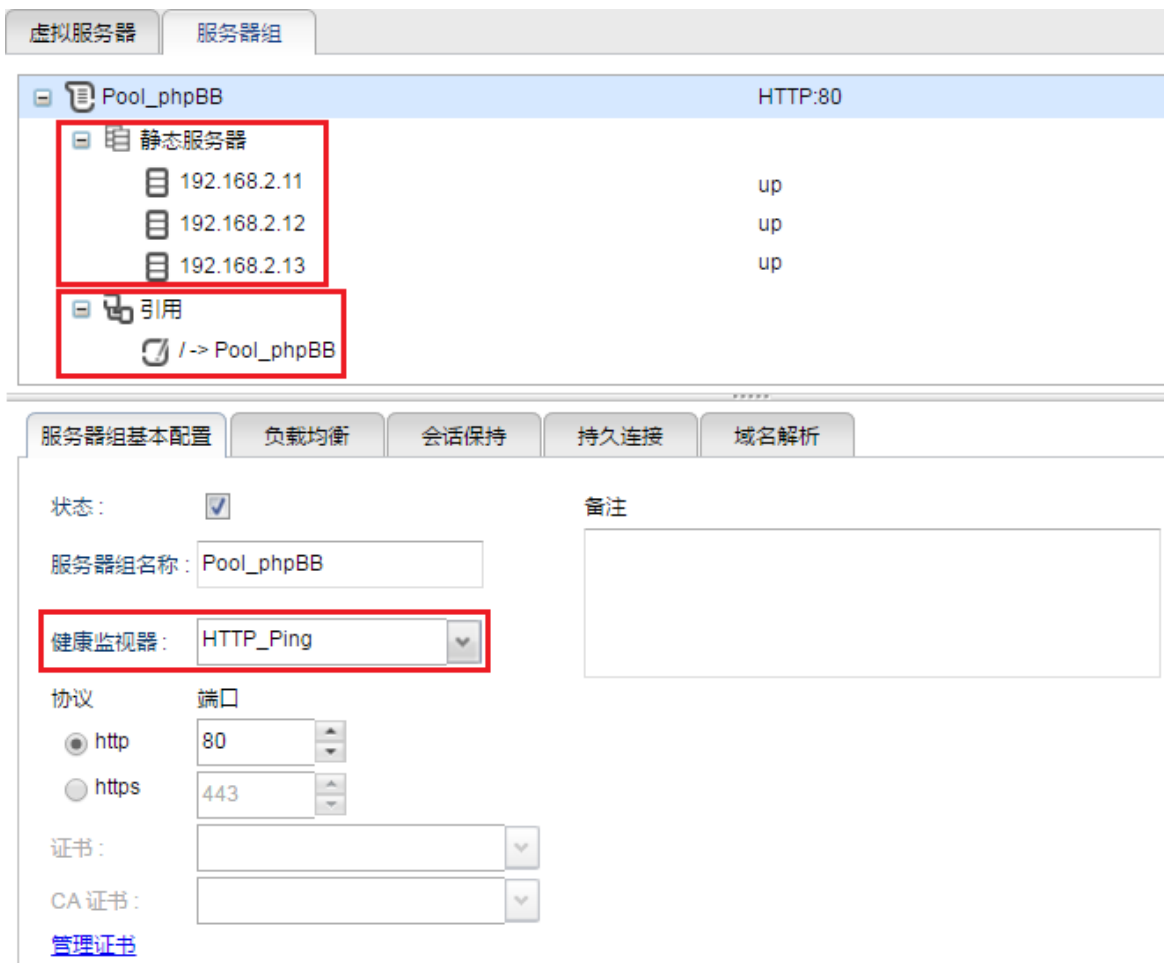
1. 选择公共对象>IP 地址集，为虚拟服务器添加虚拟 IP 地址集 VServer_IPset，包含虚拟服务器的虚拟 IP 地址 192.168.2.101。

IP地址集	
动作	
名称	地址集
VServer_IPset	192.168.2.101

2. 选择**虚拟服务>流量管理（七层）>虚拟服务器**，新建虚拟服务器 VServer_phpBB，虚拟 IP 地址选择新建的 IP 地址集 VServer_IPset，域名设置为 bbs.example.com。



3. 选择**虚拟服务>流量管理（七层）>服务器组**，新建服务器组 Pool_phpBB，关联虚拟服务器 VServer_phpBB 资源，开启会话保持功能。



服务器组基本配置 负载均衡 会话保持 持久连接 域名解析

算法： ▼

服务器组基本配置 负载均衡 会话保持 持久连接 域名解析

状态：

会话保持模式： ▼

ADSG Cookie：

应用Cookie：

应用会话标识：

超时时间：

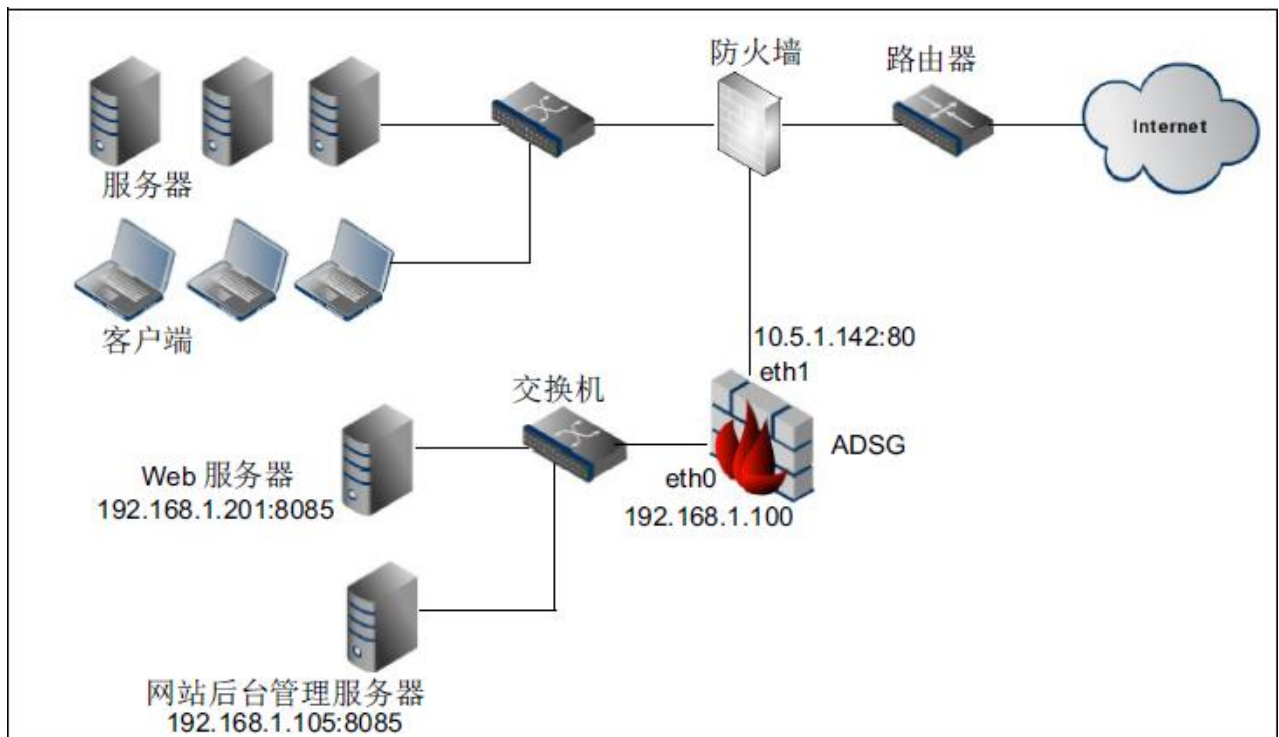
12.2.Web 安全防护

背景：

下图为某政府部门的网络拓扑。其现有 Web 服务器承载了整个行政区域该部门所负责的业务数据的管理，日均访问量大约 100000HTTP 请求/天。

为保证 Web 服务器的应用交付可以正常进行，该部门管理员在 Web 服务器前面部署了一台 ADSG，作为 Web 应用防火墙（WAF）使用。该部门 Web 服务器通过一台直连的后台管理服务器进行管理，委托一家托管公司代为管理，所以还需要在 ADSG 上配置相应的 NAT 规则（端口映射），允许来自代理公司的管理流量通过。

拓扑：



拓扑说明：

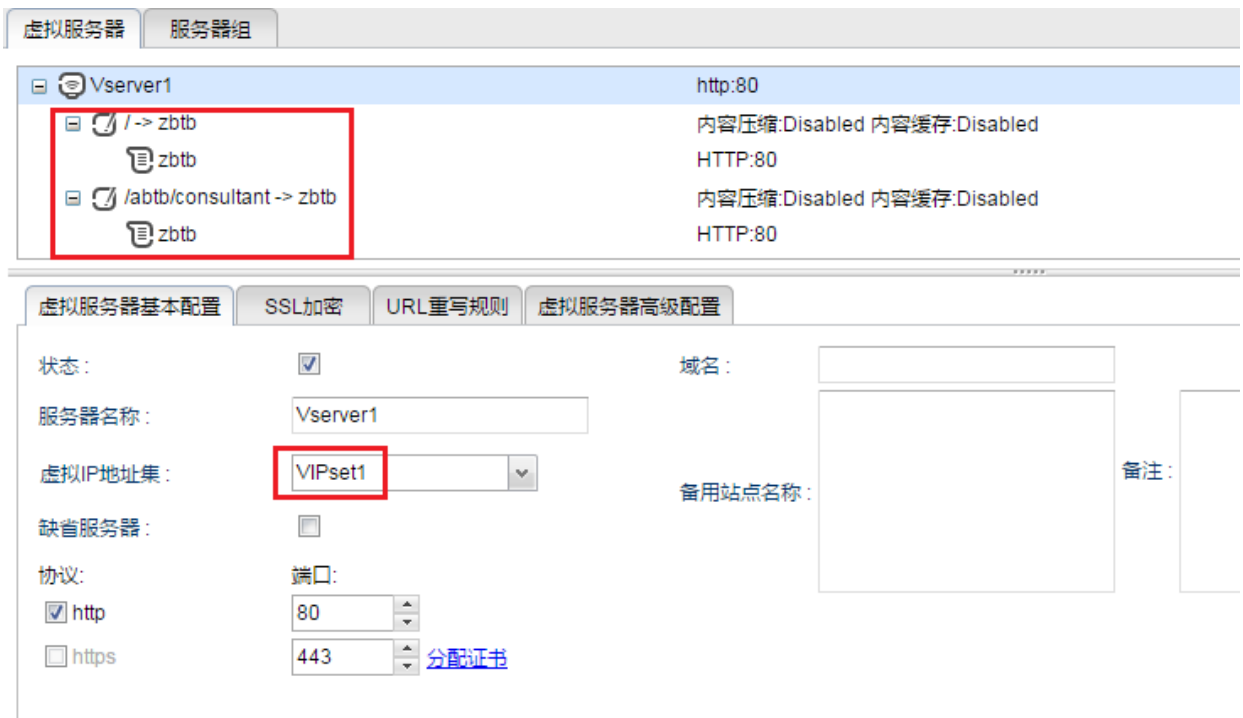
- 外部用户通过 10.5.1.142 访问 Web 服务器，内部工作人员仍然通过 192.168.1.201 访问。
- 对于“网站后台管理服务器”（192.168.1.105），需要从外部访问来对其进行维护，通过在 ADSG 上配置“端口映射”规则实现了这一需求。
- 该服务器的业务包括新闻发布、订单生成、单据上传、视频播放等。不同业务有不同的安全需求，有的需要开启 IPS。

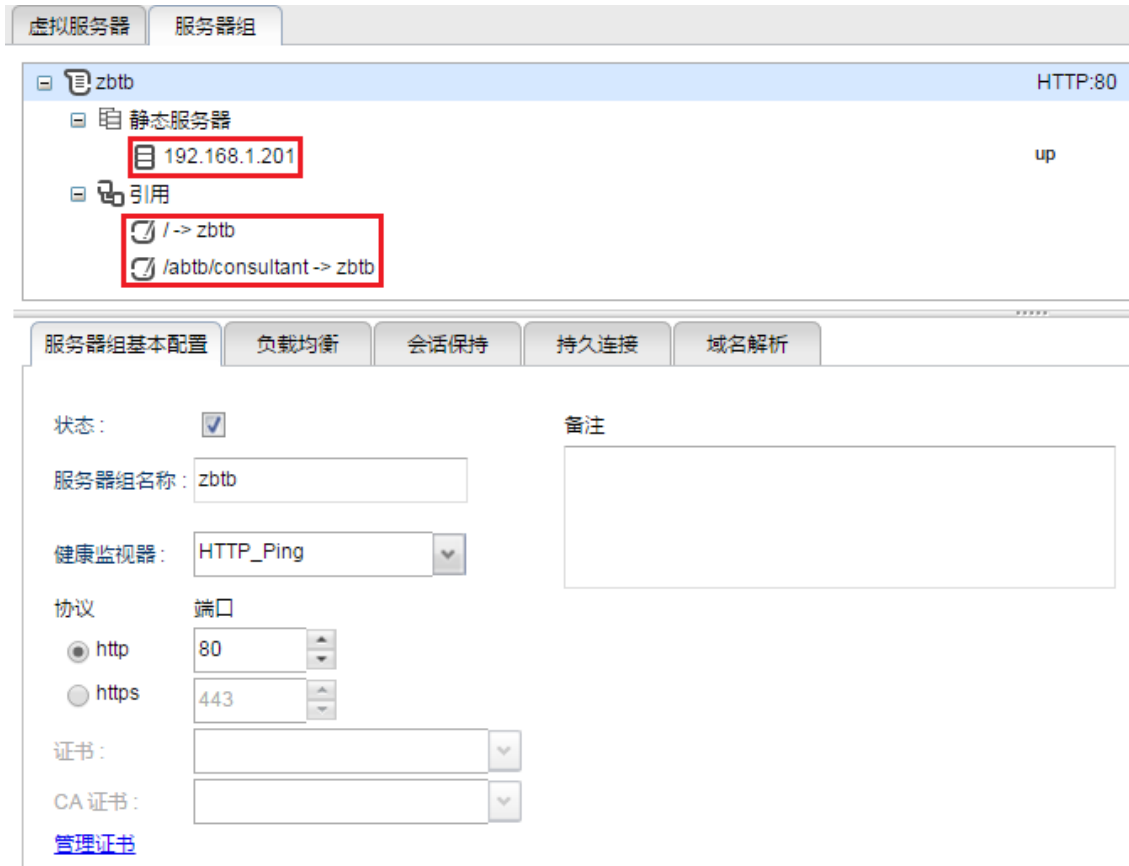
配置思路：

- 新建一个虚拟服务器 Vserver1，在其下面建立多个资源路径对应不同的 Web 应用。
 - 新建资源路径/zbtb/consultant/，用于工作人员从内部访问。在此资源路径上开启全部攻击签名检测。
 - 缺省资源路径/，用于处理除上述之外的应用。
- 在端口映射部分设置一条端口映射规则，使得托管公司可以通过网站后台管理服务器维护网站。

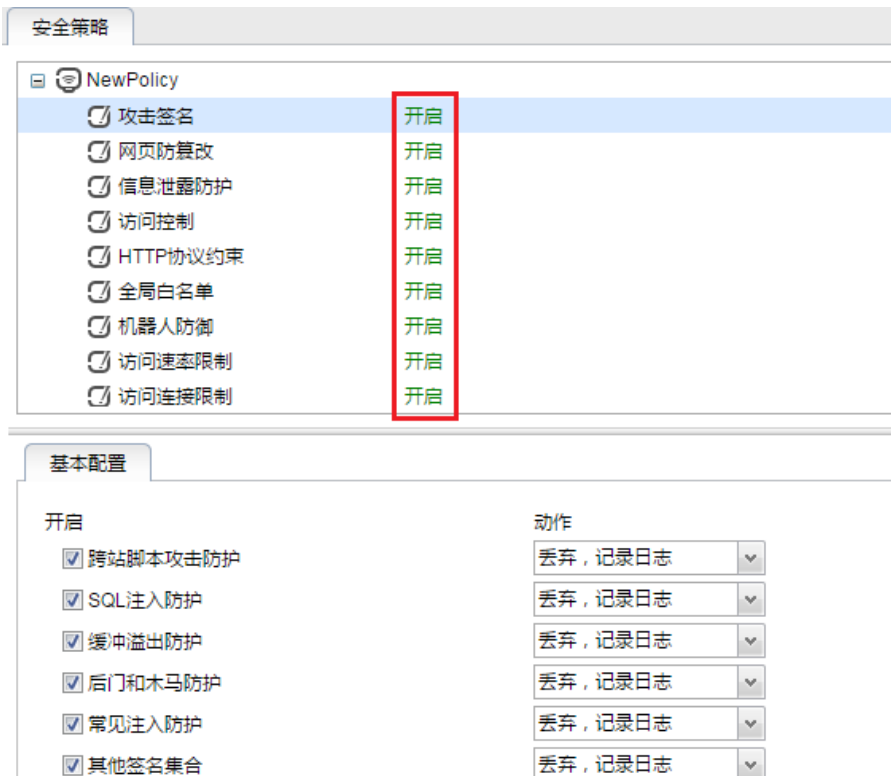
配置步骤：

- 选择公共对象>IP 地址集，为虚拟服务器添加虚拟 IP 地址集。
- 选择虚拟服务>流量管理（七层），创建虚拟服务器、服务器组以及对应不同 Web 应用的资源路径，并关联虚拟服务器与服务器组：





3. 点击**保存**。
4. 选择 **Web 安全>安全策略**，右键点击空白处，选择**添加安全策略**。
5. 右键点击**攻击签名**，选择**开启/关闭**，开启攻击签名，并在下方配置所需安全策略：



6. 点击**保存**。
7. 选择**虚拟服务>流量管理（七层）**，选择相应资源路径，引用创建的安全策略。

资源路径基本配置 | 内容缓存 | 内容压缩 | 客户端代理设置 | 服务器端代理设置 | 资源路径高级配置

状态：

资源名称： 关联到 本地提示页面

资源路径： 安全策略：

转换后路径： [管理安全策略](#)

8. 点击**保存**。
9. 选择**网络>端口映射**，开启端口映射并设置 NAT 规则：

端口映射

动作 ▼

名称	规则	状态
maintenance	10.1.5.142:8085 -> 192.168.1.105:8085	Enabled

端口映射

状态：

名称：

协议：

目的地址转换

目的IP： 目的端口：

转换后目的IP： 转换后目的端口：

10. 点击**保存**。

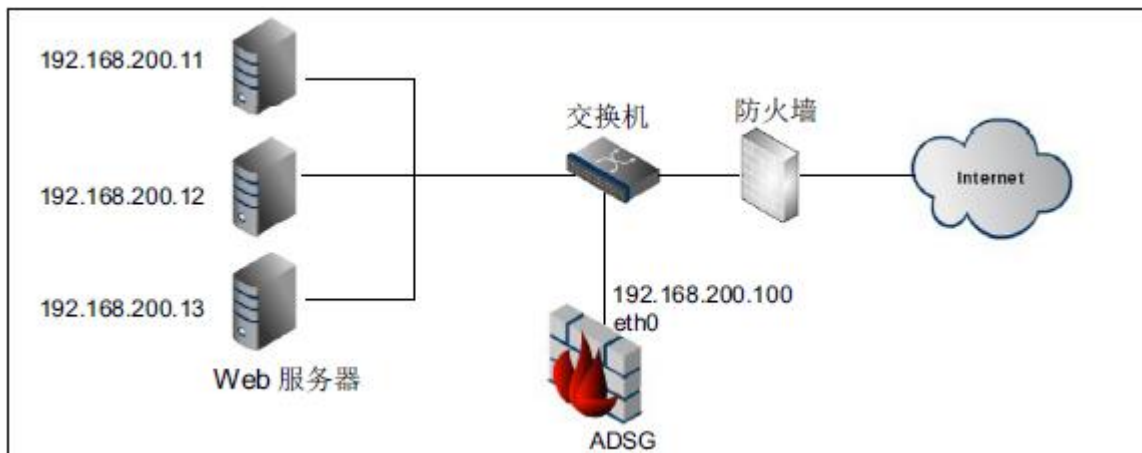
12.3. 主动防御

背景：

用户处有多台项目管理服务器，ADSG 部署在其前面作为 WAF 使用。

项目管理类应用属于一种 workflow 管理类软件，其流程相对固定，这种情况比较适合使用主动防御功能。

拓扑：

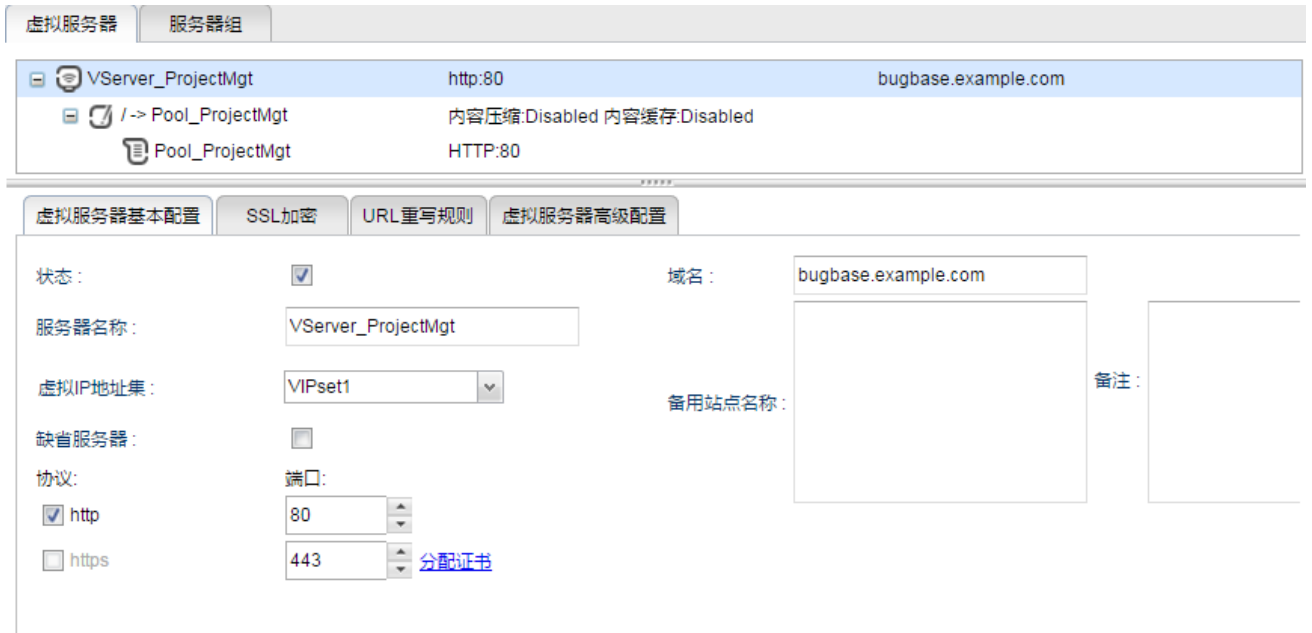


配置思路：

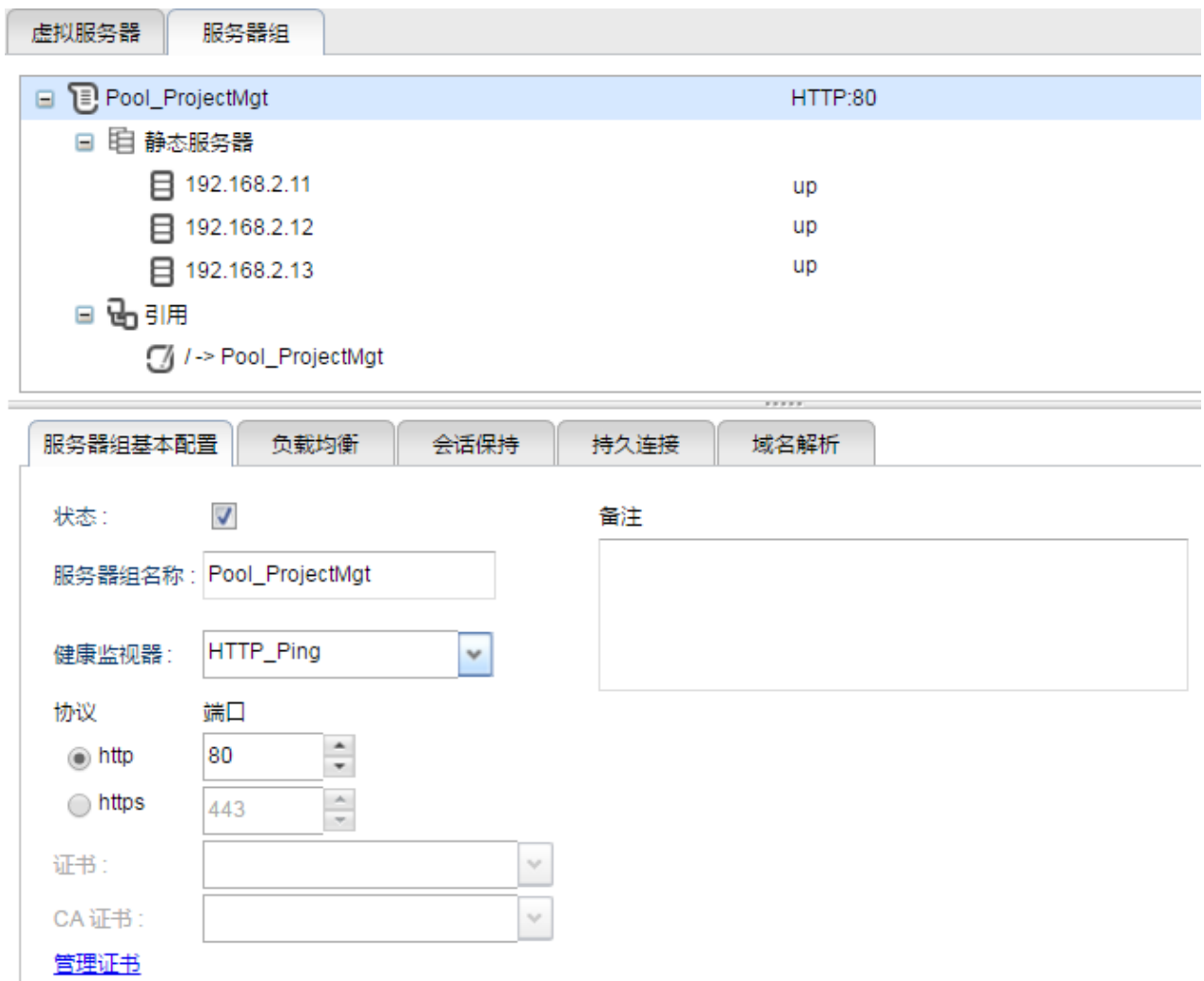
1. 在防火墙上配置 DNAT 规则，将访问 80 端口的流量转发到 ADSG 上。
2. 在 ADSG 上配置 VServer_ProjectMgt，监听 80 端口，并配置相应域名，如：
bugbase.example.com。
3. 在 ADSG 上配置 Pool_ProjectMgt，开启 80 端口。
4. 在 Pool_ProjectMgt 上启用会话保持，并设置工作模式为插入新 Cookie 方式。
5. 转到 Web 安全，配置主动防御功能。

配置步骤：

1. 在防火墙上配置 DNAT 规则。
2. 选择公共对象>IP 地址集，为虚拟服务器添加虚拟 IP 地址集。
3. 选择虚拟服务>流量管理（七层）>虚拟服务器，新建虚拟服务器 VServer_ProjectMgt。



4. 选择**虚拟服务>流量管理（七层）>服务器组**，新建服务器组 Pool_ProjectMgt，关联虚拟服务器 VServer_ProjectMgt，开启会话保持功能，并设置工作模式为**插入新 Cookie** 方式。



服务器组基本配置 负载均衡 会话保持 持久连接 域名解析

状态：

会话保持模式：

ADSG Cookie：

应用Cookie：

应用会话标识：

超时时间：

5. 选择 **Web 安全>主动防御**，配置主动防御功能。

基本配置 学习信息

基本设置

状态：

日志状态：

动作：

URI共享内存： MB*

学习次数：

IP白名单	
192.168.200.11	
192.168.200.12	
192.168.200.13	

IP白名单：

URI白名单	类型
bugbase.example.com	普通字符串

类型：
 普通字符串
 正则表达式

URI白名单：

阈值设置

小 中 大 自定义

SQL注入：

远程文件包含：

路径遍历：

跨站脚本攻击：

Evading Tricks：

ASP/PHP文件上传：

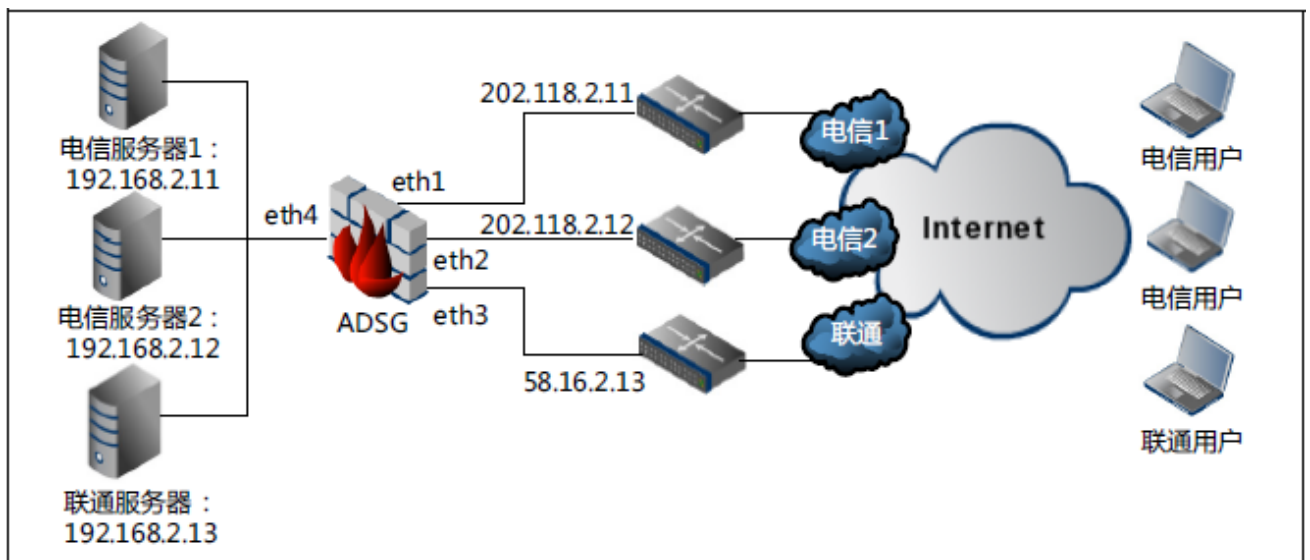
12.4. 入站链路负载均衡（智能 DNS，单数据中心）

背景：

某公司网络有三条运营商线路接入，两条带宽一样的电信链路和一条带宽较高的联通链路。公司内网部署三台服务器，两台通过电信线路提供服务，一台通过联通线路提供服务。网络出口部署了 ADSG 作为负载均衡器，使外网用户访问内网服务的入站流量合理分配到内网服务器。

为了充分利用链路带宽资源并提升用户访问体验，客户想让电信用户访问电信服务器，联通用户访问联通服务器，同时电信用户的入站流量可以均匀分配到两台电信服务器。

拓扑：



配置指南：

1. 在公网域名服务商处申请 DNS 解析权。
2. 配置网络接口和虚拟服务。
3. 配置本地智能 DNS，使电信用户解析到电信服务器的 IP 地址，联通用户解析到联通服务器的 IP 地址。

配置步骤：

1. 在公网域名服务商处申请 DNS 解析权，生成两条 DNS 记录：
 - NS 记录：www.example.com->abc.example.com
 - A 记录：abc.example.com->202.118.2.1,202.118.2.2（或 58.16.2.3）
2. 选择**网络>接口>接口**，根据网络拓扑配置网络接口的 IP 地址。
3. 选择**网络>接口>WAN**，划分以太网接口，设置入站流量的入口接口。

接口		WAN	LAN			
动作 ▾						
状态	名称	接口	网关	上行带宽	下行带宽	
✓	WAN1	eth1	202.118.2.11	100000	100000	
✓	WAN2	eth2	202.118.2.12	100000	100000	
✓	WAN3	eth3	58.16.2.13	100000	100000	

4. 选择**网络>接口>LAN**，划分以太网接口，设置入站流量的出口接口。

接口		WAN	LAN			
动作 ▾						
状态	名称	接口				
✓	LAN	eth4				

5. 选择**虚拟服务>流量管理（七层/四层）**，配置虚拟服务，对外提供服务的虚拟 IP 为：
202.118.2.1、202.118.2.2 或 58.16.2.3。

关于如何配置虚拟服务，请参见 [12.1 服务器负载均衡](#)。

6. 配置智能 DNS：

- a. 选择**智能 DNS>DNS 服务器**，配置智能 DNS 基本信息。

开启智能 DNS 功能，指定监听接口和端口，设置请求域名不存在时 AD SG 的处理动作，工作模式选择本地模式。

DNS服务器

状态：

监听地址

<div style="border-bottom: 1px solid #ccc; padding: 2px 5px; text-align: center;">已选地址</div> <div style="padding: 5px;"> <p>202.118.2.1@WAN1</p> <p>202.118.2.2@WAN2</p> <p>58.16.2.3@WAN3</p> </div>	<div style="border: 1px solid #ccc; width: 20px; height: 20px; margin: 5px auto; display: flex; align-items: center; justify-content: center;">→</div> <div style="border: 1px solid #ccc; width: 20px; height: 20px; margin: 5px auto; display: flex; align-items: center; justify-content: center;">←</div>	<div style="border-bottom: 1px solid #ccc; padding: 2px 5px; text-align: center;">待选地址</div> <div style="padding: 5px; text-align: center;">无数据</div>
---	---	---

监听端口： *(1-65535)

域名不存在动作： ▾

工作模式： 本地模式 全局模式

- b. 选择**智能 DNS>LDNS 集合**，添加电信和联通地址集，用于判断用户所属链路。

LDNS集合	
动作	
名称	地址集
电信	183.0.0.0-183.63.255.255,36.96.0.0-36.127.255.255,49.64.0.0-49.95.255.255,113.64.0.0-113.95.255.255,115.192.0.0...
联通	27.192.0.0-27.223.255.255,39.64.0.0-39.95.255.255,112.224.0.0-112.255.255.255,120.0.0.0-120.15.255.255,113.224...

- c. 选择**智能 DNS>虚拟 IP 池**，分别为电信和联通链路添加可分配的虚拟 IP 池。

虚拟IP池			
动作			
名称	策略	虚拟IP池	状态
VIPool2	静态就近性	58.16.2.3	✓
VIPool1	静态就近性	202.118.2.1,202.118.2.2	✓

- d. 选择**智能 DNS>DNS 映射**，添加域名与虚拟 IP 池的映射关系。

DNS映射			
动作			
名称	域名	虚拟IP池	状态
DNSmap1	abc.example.com	VIPool1,VIPool2	✓

- e. 选择**智能 DNS>静态就近性>DNS 映射级别**，添加 DNS 映射级别的静态就近性策略，使电信用户的访问匹配到电信的虚拟 IP 池，联通用户的访问匹配到联通的虚拟 IP 池。

DNS映射级别			虚拟IP池级别
动作			
DNS映射	LDNS集合	虚拟IP池	
DNSmap1	LDNS1	VIPool1	
DNSmap1	LDNS2	VIPool2	

- f. 选择**智能 DNS>静态就近性>虚拟 IP 池级别**，添加虚拟 IP 池级别的静态就近性策略，根据匹配到的虚拟 IP 池的调度策略，为电信用户选取电信链路的虚拟 IP，为联通用户选取联通链路的虚拟 IP。

DNS映射级别			虚拟IP池级别
动作			
虚拟IP池	LDNS集合	IP列表	
VIPool1	联通	202.118.2.2,202.118.2.1	
VIPool2	电信	58.16.2.3	

7. 点击**保存**。

12.5.全局负载均衡（多数据中心）

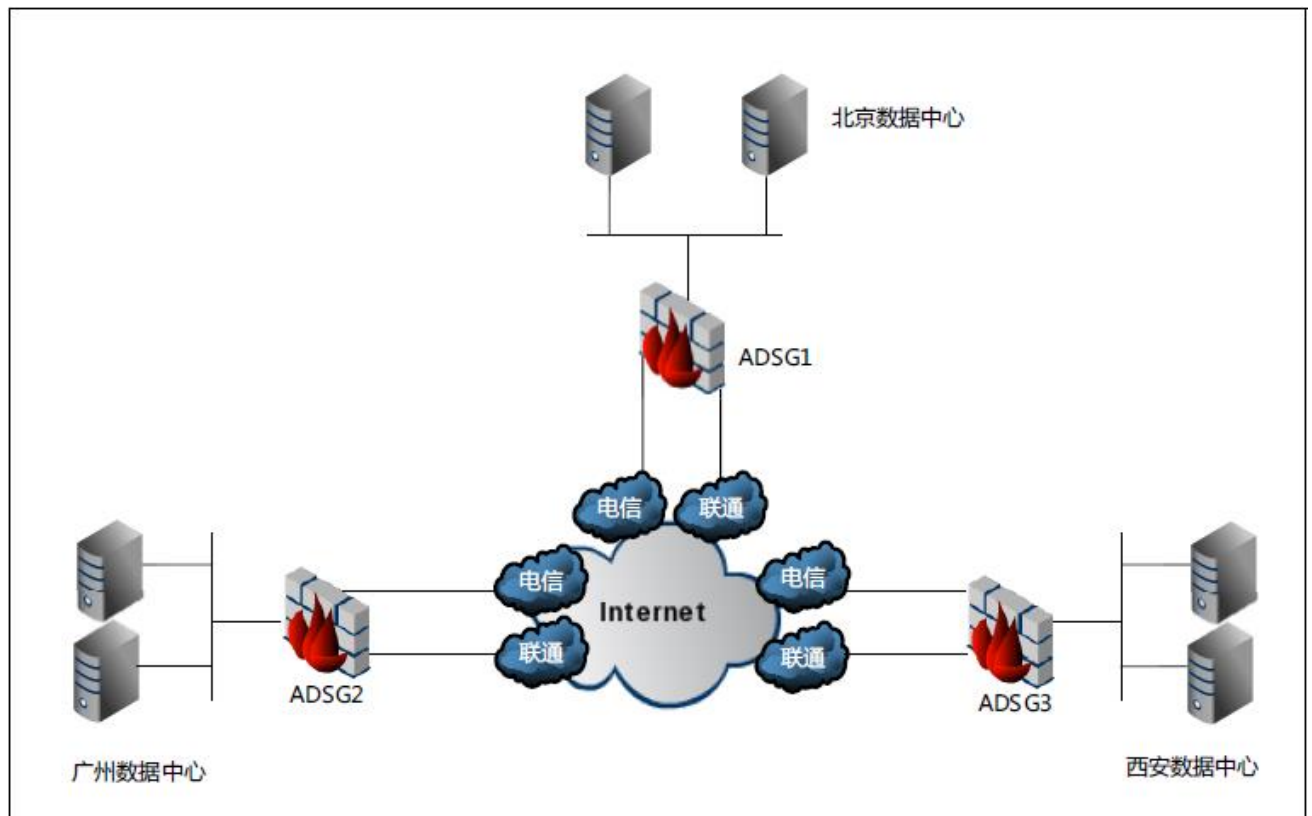
背景：

某公司门户网站域名为 www.example.com。为了提升用户访问速度，该公司在北京、广州、西安三地分别设有数据中心，网络出口部署 ADSG 作为负载均衡器，且外网都是电信、联通双链路。

为了充分利用链路带宽资源并提升用户访问体验，需要实现如下需求：

- 华北、东北的用户请求调度到北京数据中心，并通过相同运营商的链路访问服务器，其他运营商的用户请求则通过轮询算法选择路线接入；
- 西北、西南的用户请求调度到广州数据中心，并通过相同运营商的链路访问服务器，其他运营商的用户请求则通过轮询算法选择路线接入；
- 华中、华南的用户请求调度到西安数据中心，并通过相同运营商的链路访问服务器，其他运营商的用户请求则通过轮询算法选择路线接入；
- 其他地区的用户请求调度到北京数据中心，并通过相同运营商的链路访问服务器，其他运营商的用户请求则通过轮询算法选择路线接入。

拓扑：



配置指南：

1. 在公网域名服务商处申请 DNS 解析权。
2. 配置网络接口和虚拟服务。
3. 配置全局智能 DNS，使不同地域的用户就近访问公司站点。

配置步骤：

以北京 ADSG 为例：

1. 在公网域名服务商处申请 DNS 解析权，生成两条 DNS 记录：
 - NS 记录：www.example.com->abc.example.com
 - A 记录：abc.example.com->202.108.2.2（或 58.58.2.2）
2. 选择**网络>接口>接口**，根据网络拓扑配置网络接口的 IP 地址。
3. 选择**网络>接口>WAN**，划分 WAN 接口，设置入站流量的入口接口。

接口					
WAN					
LAN					
动作					
状态	名称	接口	网关	上行带宽	下行带宽
✓	WAN1	eth1	202.108.2.1	100000	100000
✓	WAN2	eth2	58.58.2.1	100000	100000

提示：为了随时监控入站链路的健康状态，可为WAN口指定健康监视器。

4. 选择**网络>接口>LAN**，划分以太网接口，设置入站流量的出口接口。

接口		
WAN		
LAN		
动作		
状态	名称	接口
✓	LAN	eth3

5. 选择**虚拟服务>流量管理（七层/四层）**，配置虚拟服务，对外提供服务的虚拟 IP 为 202.108.2.2 或 58.58.2.2。

关于如何配置虚拟服务，请参见[第 3 章，虚拟服务](#)。

6. 配置智能 DNS:

- a. 选择**智能 DNS>DNS 服务器**，开启智能 DNS 功能，指定监听接口和端口，设置请求域名不存在时 AD SG 的处理动作，选择全局工作模式。

DNS服务器

状态:

监听地址

已选地址	待选地址
202.108.2.2@WAN1	无数据
58.58.2.2@WAN2	

监听端口: *(1-65535)

域名不存在动作:

工作模式: 本地模式 全局模式

- b. 选择**智能 DNS>虚拟 IP 池**，分别为北京、西安和广州站点添加可分配的虚拟 IP 池。

虚拟IP池

动作 ▼

名称	策略	虚拟IP池	状态
北京ADSG	静态就近性	202.108.2.2,58.58.2.2	✓
广州ADSG	静态就近性	202.108.3.2,58.58.3.2	✓
西安ADSG	静态就近性	202.108.4.2,58.58.4.2	✓

- c. 选择**智能 DNS>DNS 映射**，添加域名与虚拟 IP 池的映射关系。

DNS映射

动作 ▼

名称	域名	虚拟IP池	状态
abc	abc.example.com	北京ADSG,西安ADSG,广州ADSG	✓

- d. 选择**智能 DNS>LDNS 集合**，添加地址集，用于判断用户所属地域和运营商链路。

LDNS集合	
动作	
名称	地址集
北京	110.96.0.0-110.127.255.255,123.64.0.0-123.95.255.255,110.192.0.0-110.223.255.255,36.192.0.0-36.223.25...
广州	183.0.0.0-183.63.255.255,113.64.0.0-113.95.255.255,116.16.0.0-116.31.255.255,219.128.0.0-219.143.255.2...
其他地域	0.0.0.0-255.255.255.255
电信	183.0.0.0-183.63.255.255,36.96.0.0-36.127.255.255,49.64.0.0-49.95.255.255,113.64.0.0-113.95.255.255,11...
联通	27.192.0.0-27.223.255.255,39.64.0.0-39.95.255.255,112.224.0.0-112.255.255.255,120.0.0.0-120.15.255.255...
西安	223.8.0.0-223.15.255.255,183.184.0.0-183.191.255.255,171.120.0.0-171.127.255.255,110.176.0.0-110.183....

- e. 选择**智能 DNS>静态就近性>DNS 映射级别**，添加 DNS 映射级别的静态就近性策略，为不同地域的用户请求就近调度虚拟 IP 池。

DNS映射级别		
虚拟IP池级别		
动作		
DNS映射	LDNS集合	虚拟IP池
abc	北京	北京ADSG
abc	西安	西安ADSG
abc	广州	广州ADSG
abc	其他地域	北京ADSG

- f. 选择**智能 DNS>静态就近性>虚拟 IP 池级别**，添加虚拟 IP 池级别的静态就近性策略，使电信用户访问电信虚拟 IP，联通用户访问联通虚拟 IP。

DNS映射级别		
虚拟IP池级别		
动作		
虚拟IP池	LDNS集合	IP列表
北京ADSG	电信	58.58.2.2
北京ADSG	联通	202.108.2.2
广州ADSG	电信	58.58.3.2
广州ADSG	联通	202.108.3.2
西安ADSG	电信	58.58.4.2
西安ADSG	联通	202.108.4.2

- g. 选择**智能 DNS>站点集合**，添加本地站点和其他站点，用于 ADSG 对 DNS 请求进行全局调度时区分本地站点和其他站点。

站点集合						
动作						
状态	站点名称	站点类型	通讯地址	通讯端口	通讯角色	备注
↑	北京	本地站点	202.108.2.2 58.58.2.2	588	Master	
↑	广州	其他站点	202.108.3.2 58.58.3.2	588	None	
↑	西安	其他站点	202.108.4.2 58.58.4.2	588	None	

7. 点击**保存**。

登录其他站点 AD SG:

1. 配置接口和虚拟服务。
2. 选择**智能 DNS>站点集合**，添加本地站点和其他站点，用于同步站点配置信息。

站点集合						
动作						
状态	站点名称	站点类型	通讯地址	通讯端口	通讯角色	备注
+	西安	本地站点	202.108.4.2 58.58.4.2	588	None	

站点集合						
动作						
状态	站点名称	站点类型	通讯地址	通讯端口	通讯角色	备注
+	广州	本地站点	202.108.3.2 58.58.3.2	588	None	

3. 选择**智能 DNS>全局配置同步**，输入北京站点 AD SG 的通讯 IP 和端口，点击同步。

配置同步	
同步内容	
如果本端为None，仅同步对端站点集合信息。	
如果本端为Master，则同步站点集合信息和所有智能DNS配置。	
对端设置	
对端站点通讯地址：	<input type="text" value="202.108.2.2"/> *
对端站点通讯端口：	<input type="text" value="588"/> *(1-65535)
<input type="button" value="更新"/>	

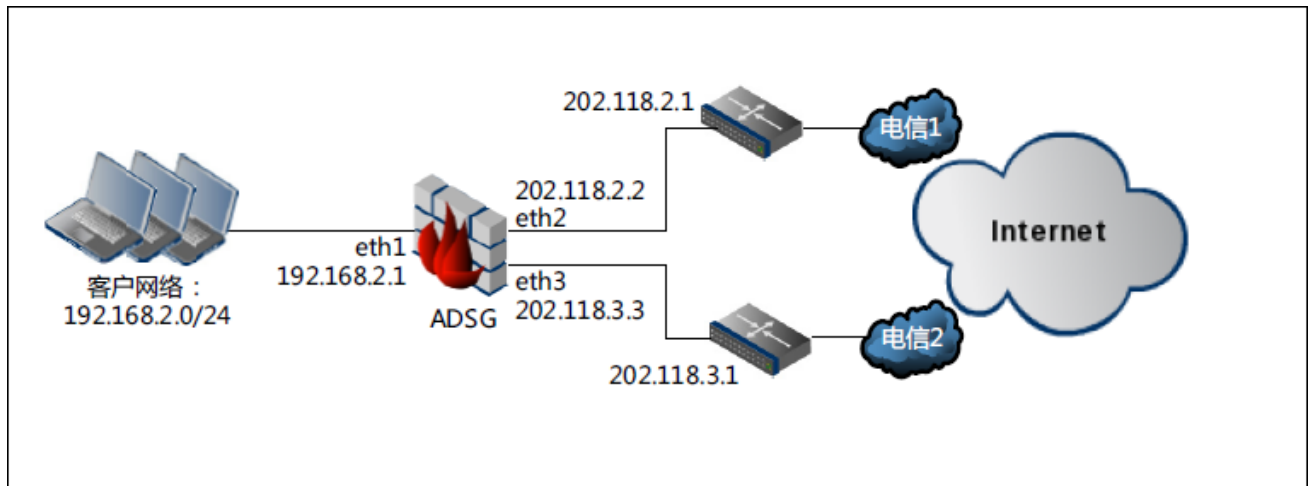
4. 点击**保存**。

12.6. 出站链路负载均衡

背景：

某公司网络出口部署了 ADSG 作为网关代理内网用户访问互联网。该公司有两条电信线路，且两条电信线路带宽相同。客户希望将内网用户访问互联网的出站流量均匀分配到两条电信线路。

拓扑：



配置步骤：

1. 选择**网络>接口>接口**，设置网络接口的 IP 地址。

接口		WAN	LAN			
状态	名称	IP地址	MAC地址	速率	双工	备注
↑	eth0	10.1.3.108/21	00:0c:29:64:a2:74	1000Mb/s	Full	
↑	eth1	192.168.2.1/24	00:0c:29:64:a2:88	1000Mb/s	Full	
↑	eth2	202.118.2.2/24	00:0c:29:64:a2:92	1000Mb/s	Full	
↑	eth3	202.118.3.3/24	00:0c:29:64:a2:9c	1000Mb/s	Full	

2. 选择**网络>接口>LAN**，划分以太网接口，设置出站流量的入口接口。

接口		WAN	LAN			
状态	名称	接口				
✓	LAN	eth1				

3. 选择**网络>接口>WAN**，划分以太网接口，设置出站流量的出口接口。

接口		WAN	LAN			
动作						
状态	名称	接口	网关	上行带宽	下行带宽	
✓	WAN1	eth2	202.118.2.1	100000	100000	
✓	WAN2	eth3	58.16.2.13	50000	50000	

4. 选择**网络>智能路由**，添加内网用户访问外网所需的智能路由。

智能路由		高级配置					
动作							
编号	名称	源IP地址	目的IP地址	协议	使用链路	链路策略	生效时间
1	ISProute1	192.168.2.0/24	任意IPv4地址	Any	WAN1,WAN2	轮询	全天

基本配置							
名称:	ISProute1 *						
源IP地址:	IPv4地址/掩码						
IPv4地址:	192.168.2.0 *						
掩码长度:	24 *						
目的IP地址:	任意IPv4地址						
TOS:	0 *						
协议:	Any *						
使用链路:	<table border="1"> <thead> <tr> <th>链路</th> <th>权重</th> </tr> </thead> <tbody> <tr> <td>WAN1</td> <td>1</td> </tr> <tr> <td>WAN2</td> <td>2</td> </tr> </tbody> </table>	链路	权重	WAN1	1	WAN2	2
链路	权重						
WAN1	1						
WAN2	2						
链路策略:	轮询 *						
生效时间:	全天 *						
链路繁忙保护:	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭						
调度失败动作:	匹配下一条						

链路:	
权重:	1
<input type="button" value="确定"/> <input type="button" value="取消"/>	

5. 选择**网络>源地址转换**，设置源地址转换规则，将内网的源 IP 地址转换为出口接口的公网 IP 地址。

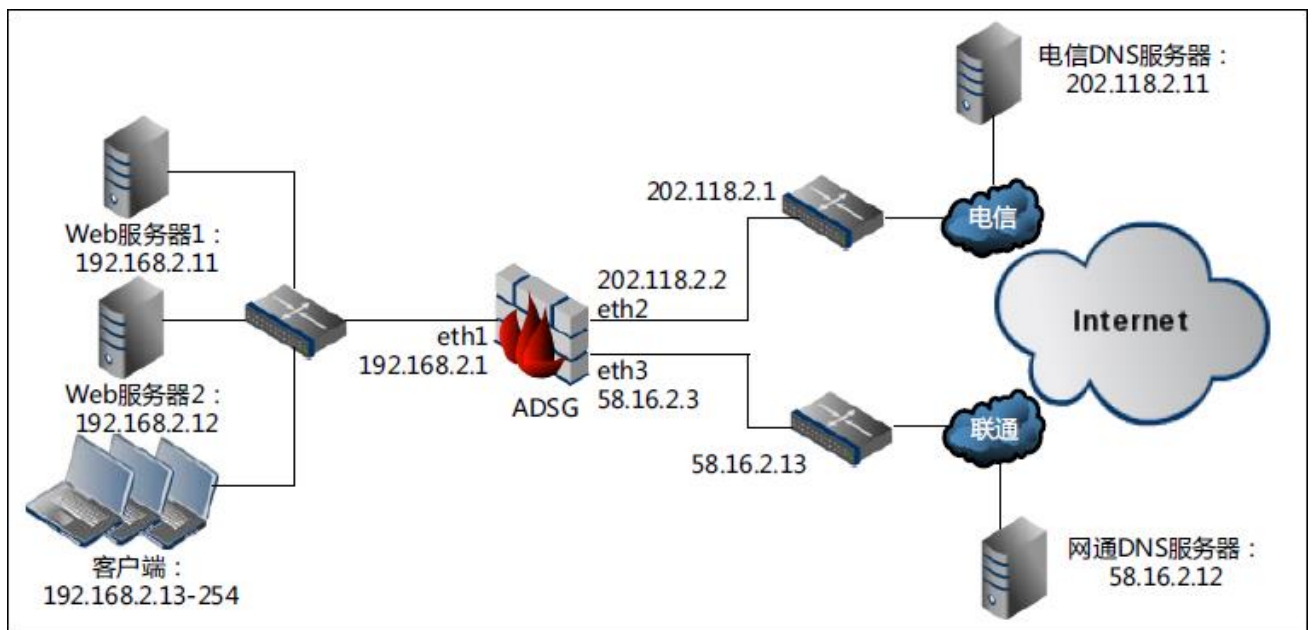
源地址转换						
动作						
编号	名称	源IP地址	转换后IP地址/接口	目的IP地址	协议	出口接口
1	SNAT1	192.168.2.0/24	使用网口地址	任意IPv4地址	Any	eth2
2	SNAT2	192.168.2.0/24	使用网口地址	任意IPv4地址	Any	eth3

12.7. 出站链路负载均衡（启用 DNS 透明代理）

背景：

某公司网络出口部署了 ADSG 作为网关代理内网用户访问互联网。出口有两条线路，一条电信线路和一条联通线路。内网有两台服务器提供相同的 WEB 服务，使用同一域名。客户希望 ADSG 实现出站链路负载均衡的同时，可以代理内网 PC 进行域名解析。同时，内网用户只能通过电信线路解析域名 www.sina.com.cn。

拓扑：



配置步骤：

1. 选择**网络>接口>接口**，设置网络接口的 IP 地址。

接口	WAN	LAN				
状态	名称	IP地址	MAC地址	速率	双工	备注
↑	eth0	10.1.3.108/21	00:0c:29:64:a2:74	1000Mb/s	Full	
↑	eth1	192.168.2.1/24	00:0c:29:64:a2:88	1000Mb/s	Full	
↑	eth2	202.118.2.2/24	00:0c:29:64:a2:92	1000Mb/s	Full	
↑	eth3	58.16.2.3/24	00:0c:29:64:a2:9c	1000Mb/s	Full	

2. 选择**网络>接口>LAN**，划分以太网接口，设置出站流量的入口接口。

接口	WAN	LAN				
状态	名称	接口				
✓	LAN	eth1				

3. 选择**网络>接口>WAN**，划分以太网接口，设置出站流量的出口接口。

接口						
WAN						
LAN						
动作						
状态	名称	接口	网关	上行带宽	下行带宽	
✓	WAN1	eth2	202.118.2.1	100000	100000	
✓	WAN2	eth3	58.16.2.13	50000	50000	

4. 选择**网络>智能路由**，添加内网用户访问外网所需的智能路由。

智能路由							
高级配置							
动作							
编号	名称	源IP地址	目的IP地址	协议	使用链路	链路策略	生效时间
1	ISProute1	192.168.2.0/24	任意IPv4地址	Any	WAN1,WAN2	轮询	全天

基本配置

名称： *

源IP地址：

IPv4地址： *

掩码长度： *

目的IP地址：

TOS： *

协议： *

使用链路：

链路	权重
WAN1	1
WAN2	2

链路： *

权重：

链路策略： *

生效时间： *

链路繁忙保护： 开启 关闭

调度失败动作：

5. 选择**网络>源地址转换**，设置源地址转换规则，将内网的源 IP 地址转换为出口接口的公网 IP 地址。

源地址转换						
动作						
编号	名称	源IP地址	转换后IP地址/接口	目的IP地址	协议	出口接口
1	SNAT1	192.168.2.0/24	使用网口地址	任意IPv4地址	Any	eth2
2	SNAT2	192.168.2.0/24	使用网口地址	任意IPv4地址	Any	eth3

6. 选择 **DNS 代理>网关 DNS**，添加电信和联通的 DNS 服务器。

ip地址	WAN口	权重
202.118.2.11	WAN1	1
58.16.2.12	WAN2	2

7. 选择 **DNS 代理>透明代理**，启用并配置 DNS 透明代理。

状态：

 监听地址：

 监听端口：

 内容缓存：

 调度策略：

 代理目标范围：

 用户：

 探测域名： *

前置调度策略：

 繁忙保护：

8. 选择 **DNS 代理>前置调度**，添加前置调度策略，使内网用户通过电信 DNS 服务器解析 www.sina.com.cn。

状态：

 名称： *

 用户：

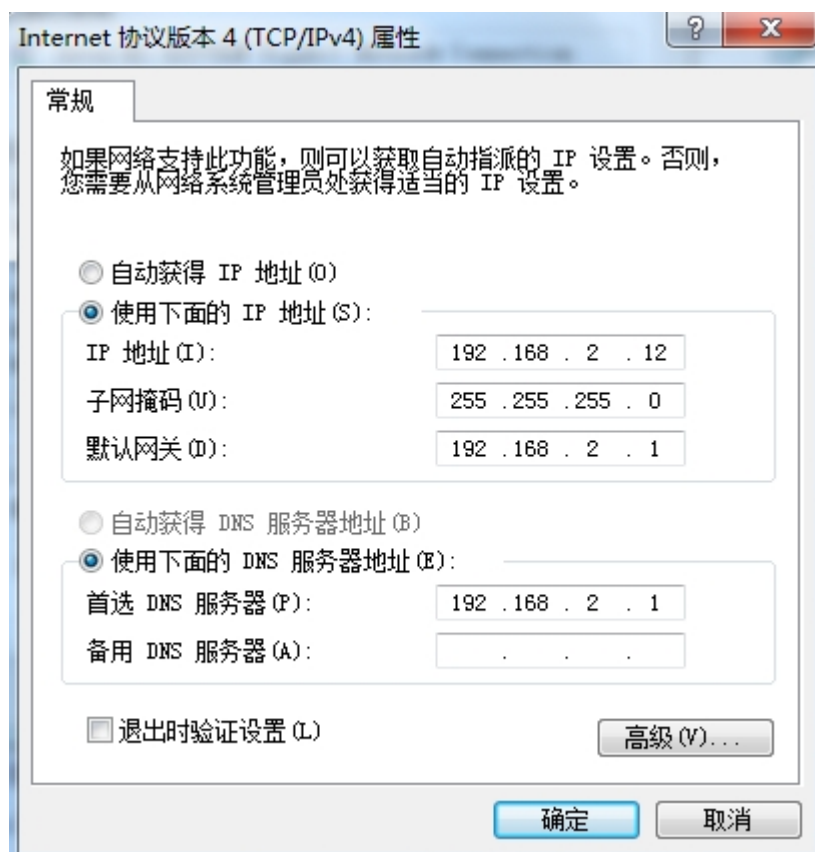
 域名： *

 繁忙保护：

 失败动作：

已选DNS服务器	待选DNS服务器
202.118.2.11:WAN1:1	58.16.2.12:WAN2:2

9. 配置内网 PC 的 DNS 服务器地址为 192.168.2.1。



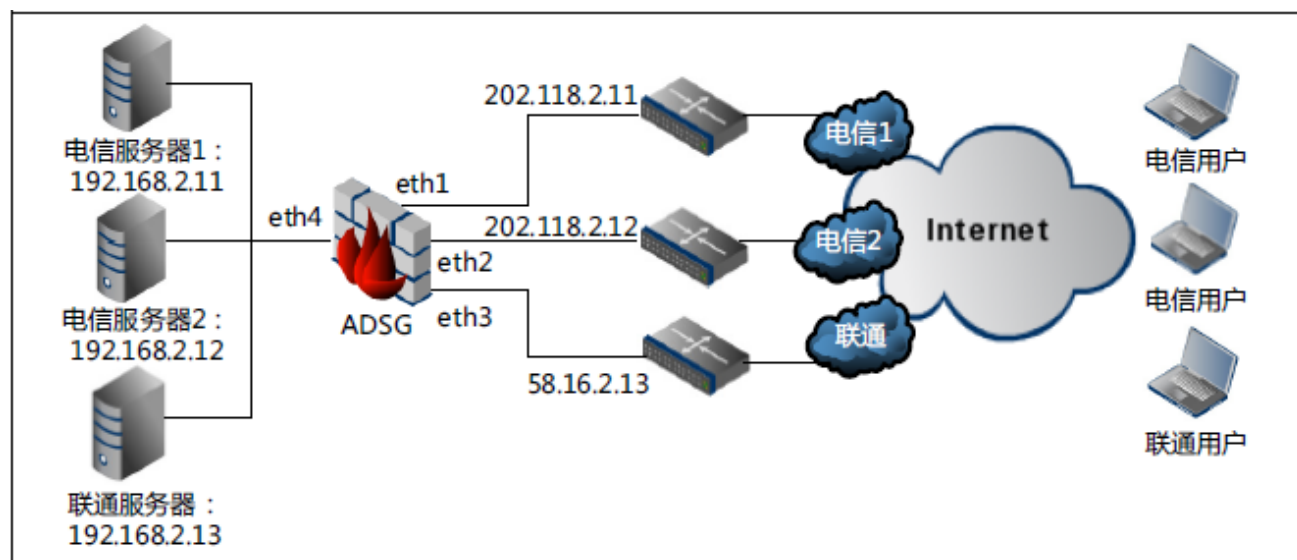
12.8. 出站、入站复合链路负载均衡（地址映射，出站负载）

背景：

某公司网络有多条运营商线路接入，公司内网服务器在对外提供服务（地址映射）的同时还要访问外网。网络出口部署了 ADSG 作为负载均衡器，对出入站流量做负载分担。

此外，不同于前面的基于智能 DNS 方式的入站访问。本例中，系统通过地址映射对外提供服务，用户直接访问公网 IP 地址，此时要保证来自外网用户访问的应答流量能够正常返回给用户。因为不同运营商的网络间存在限制，可能导致来自一个 ISP 的请求无法通过其它 ISP 进行应答。这就要求外网的入站流量的请求和应答均由同一链路处理，也就是要保证流量“哪来哪回”的特性。

拓扑：



配置指南：

1. 按照常规配置出站负载均衡，参见 12.6 出站负载均衡。
2. 针对入站请求的应答流量，需要在后台针对用户具体拓扑进行专门配置。
3. 具体实施时，可由厂商技术支持来完成。

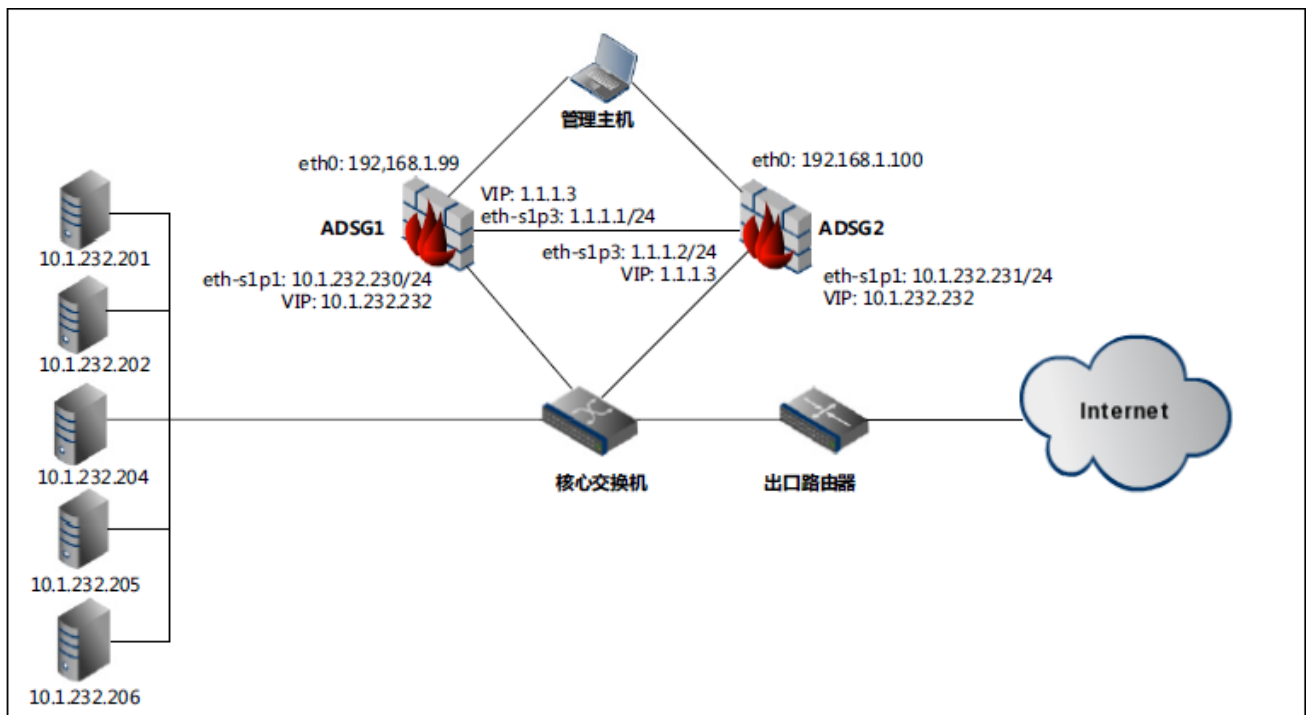
12.9.某城市轨道交通用户配置实例

背景：

某市轨道交通客户有多台银联服务器对外提供服务，要求部署两台 ADSG 在其前面作为负载均衡器使用。

管理员不希望改变现有的网络拓扑，所以我们推荐使用 ADSG 的单臂模式。

拓扑：



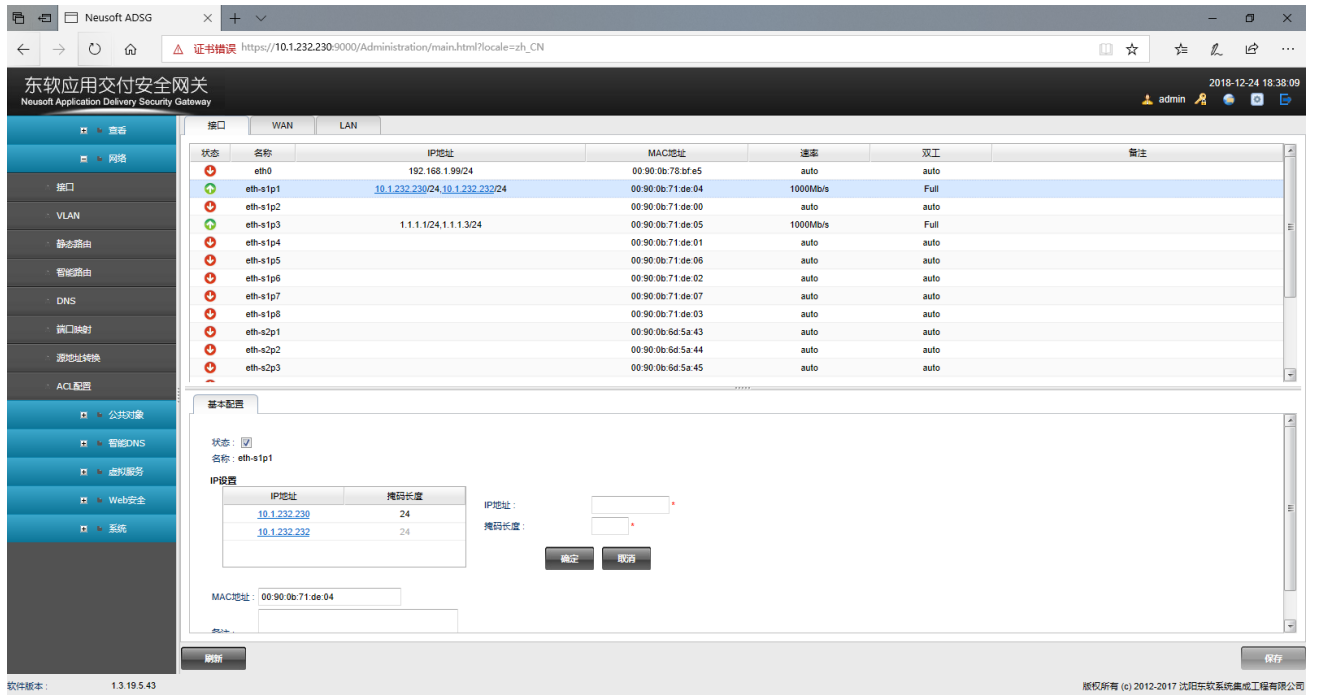
配置指南：

1. 配置接口 IP 地址和静态路由。
2. 配置高可用性。
3. 添加虚拟 IP 地址集。
4. 添加虚拟服务器、服务器组并进行关联。
5. 查看监控统计信息和日志。
6. 配置完主设备之后配置备设备。

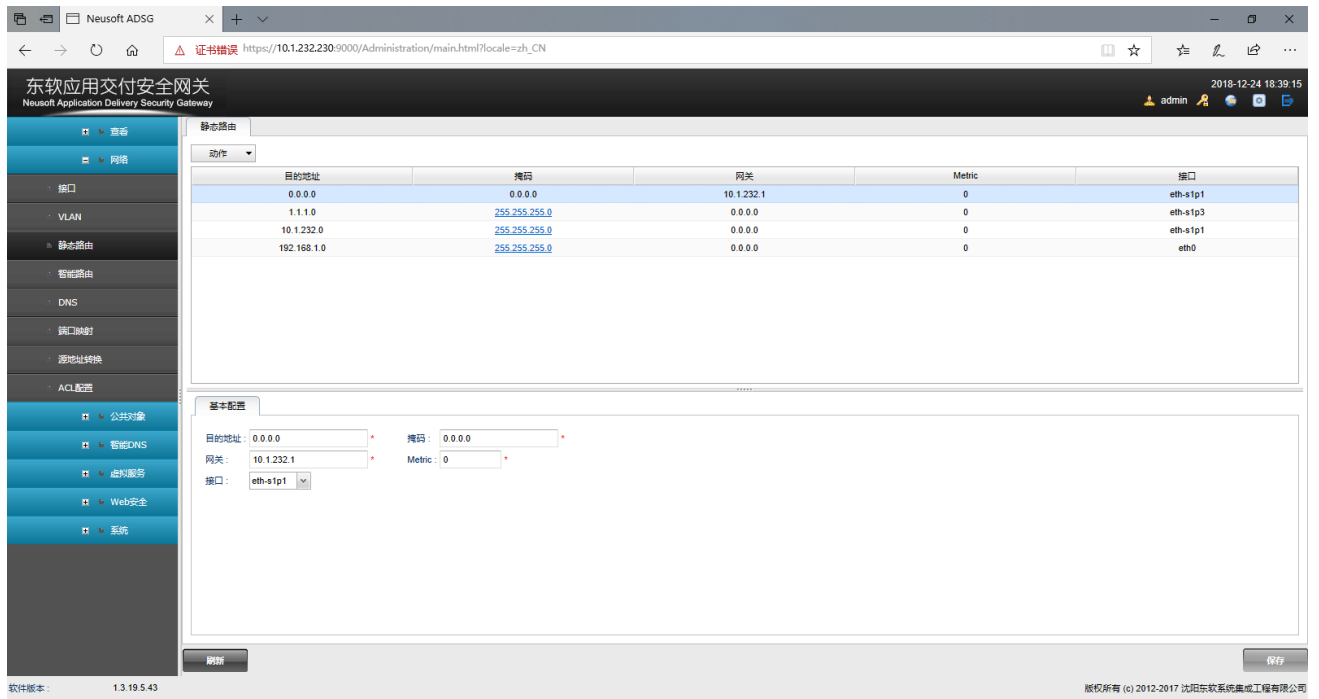
配置步骤：

配置主设备：

1. 选择**网络>接口>接口**，根据网络拓扑配置主设备网络接口的 IP 地址。
 - 业务口：eth-s1p1，IP=10.1.232.230/24
 - 心跳口：eth-s1p3，IP=1.1.1.1/24

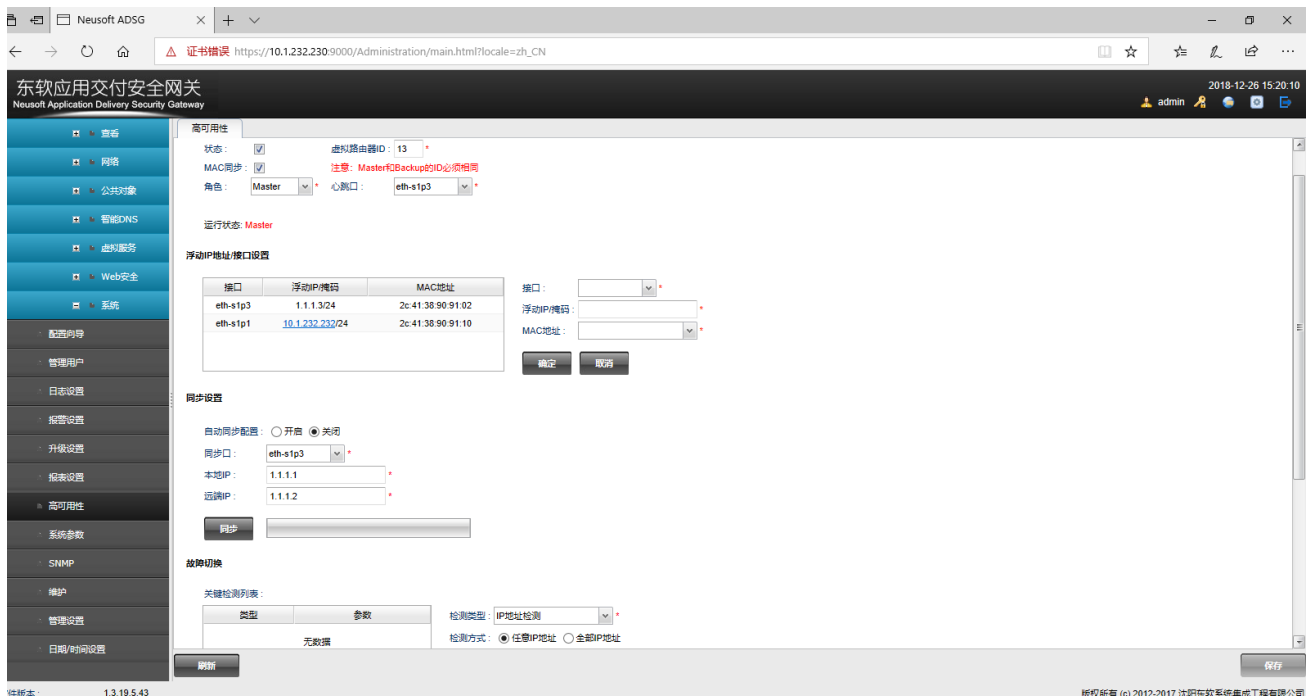


2. 选择**网络>静态路由**。点击**动作**下拉框，选择**增加路由**，配置静态路由。

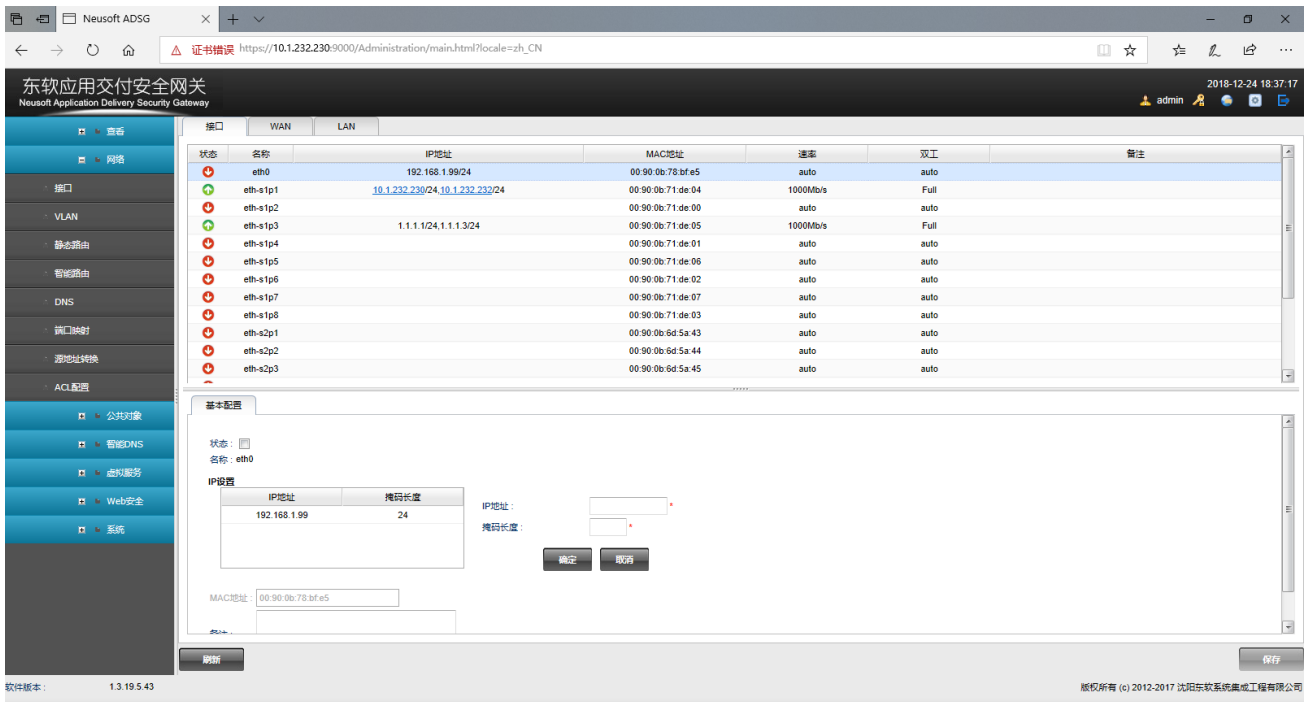


3. 选择系统>高可用性，配置高可用性。

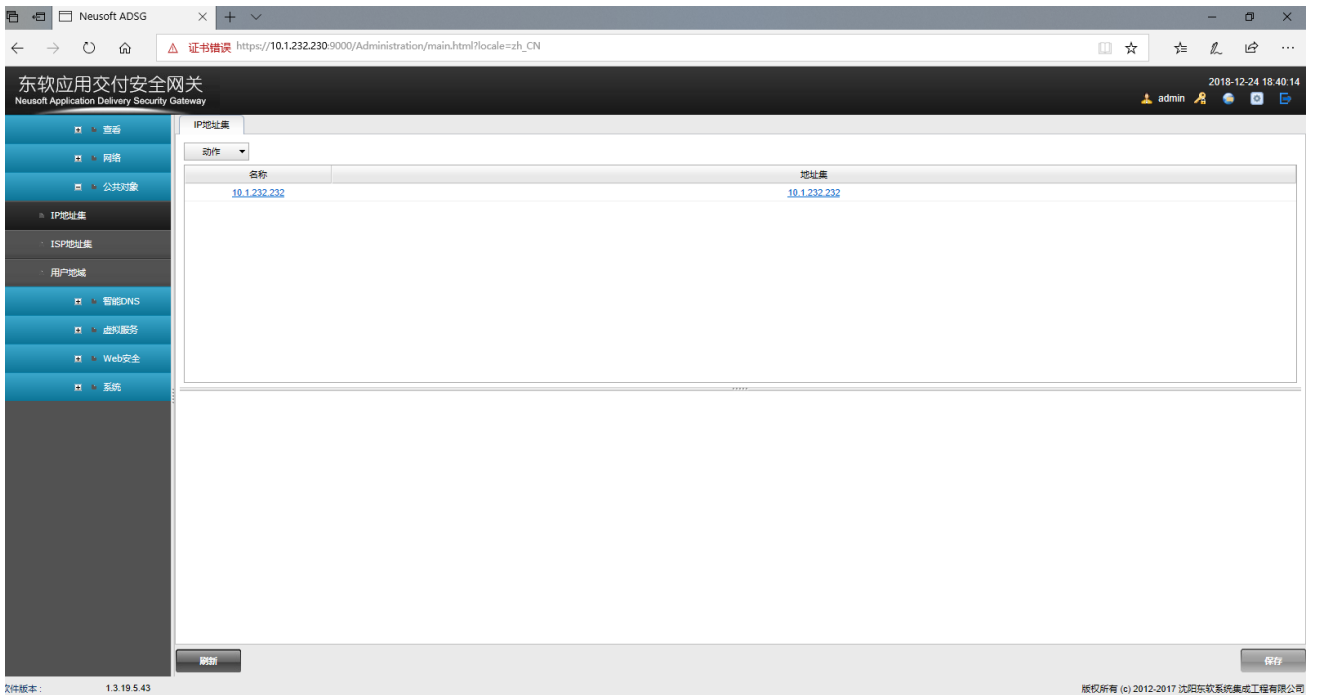
- 状态：勾选（开启 HA 功能）
- 虚拟路由器 ID：13（主备机的虚拟路由器 ID 必须相同）
- MAC 同步：勾选
- 角色：Master
- 心跳口：eth-s1p3
- 配置浮动 IP 和接口：eth-s1p1=10.1.232.232/24，eth-s1p3=1.1.1.3/24。
- 配置同步设置：本地 IP 选择 1.1.1.1@eth-1p3，远程 IP 填写备机 IP1.1.1.2。
- 自动同步配置：关闭。

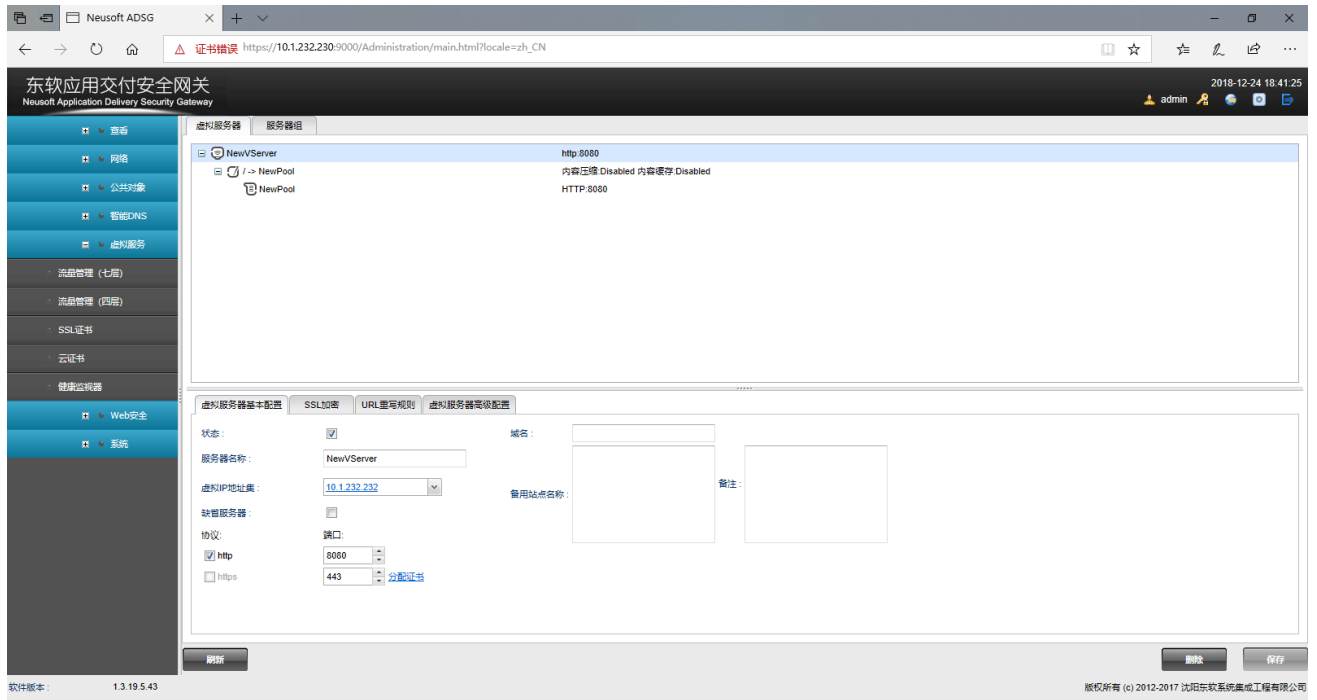
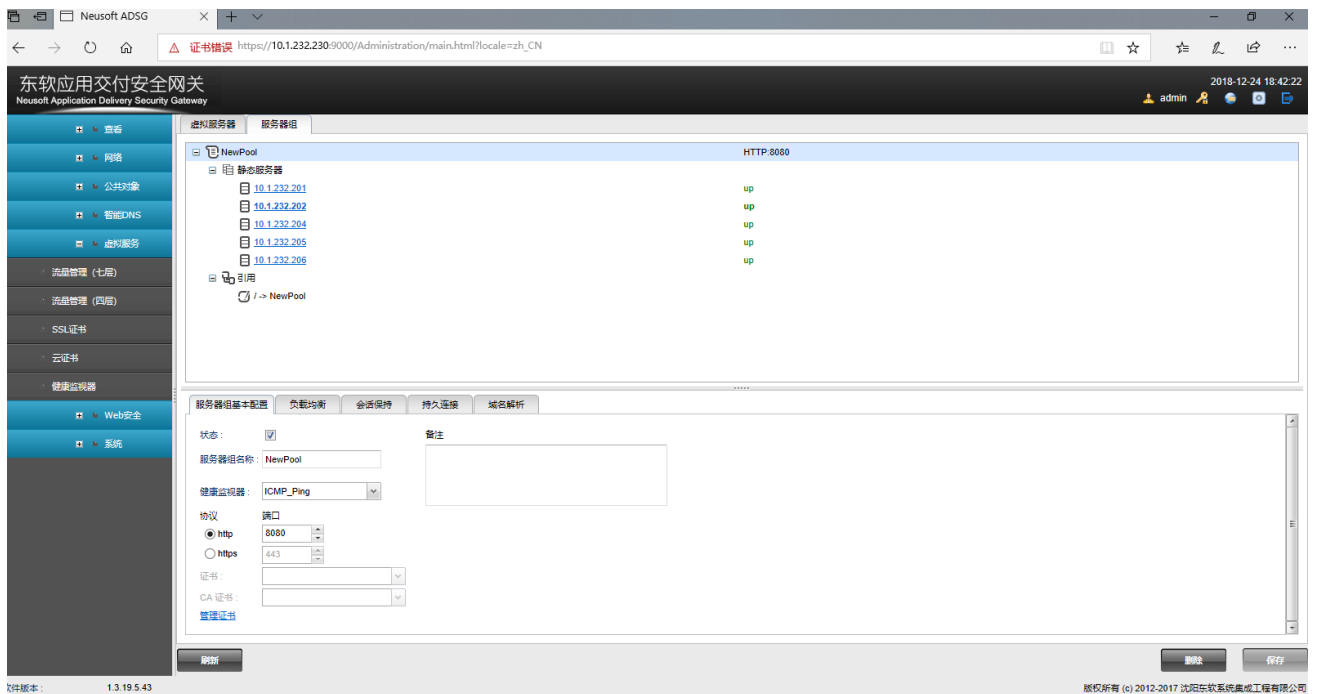


之后查看接口状态：



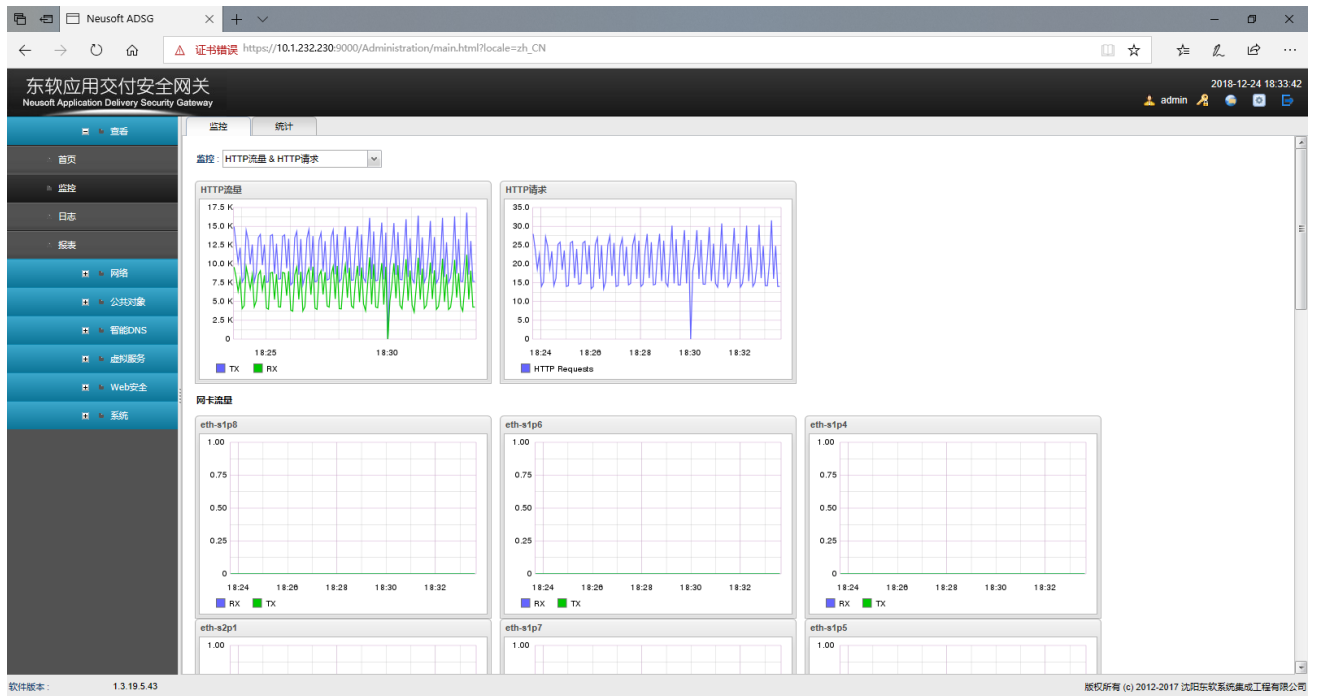
4. 选择公共对象>IP地址集，为虚拟服务器添加虚拟IP地址集10.1.232.232。



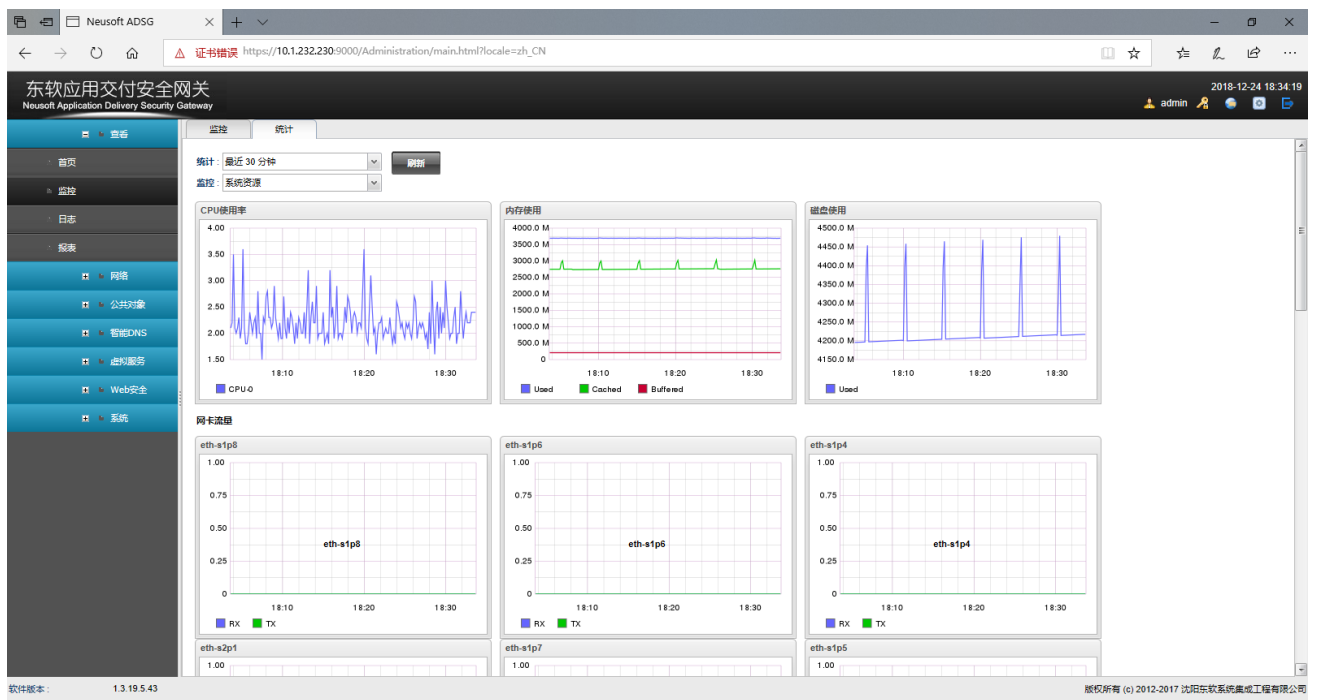
5. 选择**虚拟服务>流量管理（七层）**。a. 在视图区空白处点击右键，选择**添加虚拟服务器**。b. 右键点击**静态服务器**，选择**添加静态服务器**，添加静态服务器。c. 点击**服务器组**，在视图区空白处点击右键，选择**添加服务器组**。d. 在服务器组的视图区右键点击引用，选择**添加资源路径**，双击资源路径名称，将虚拟服务器关联到虚拟服务器组。

6. 配置完以上步骤后，流量通过。

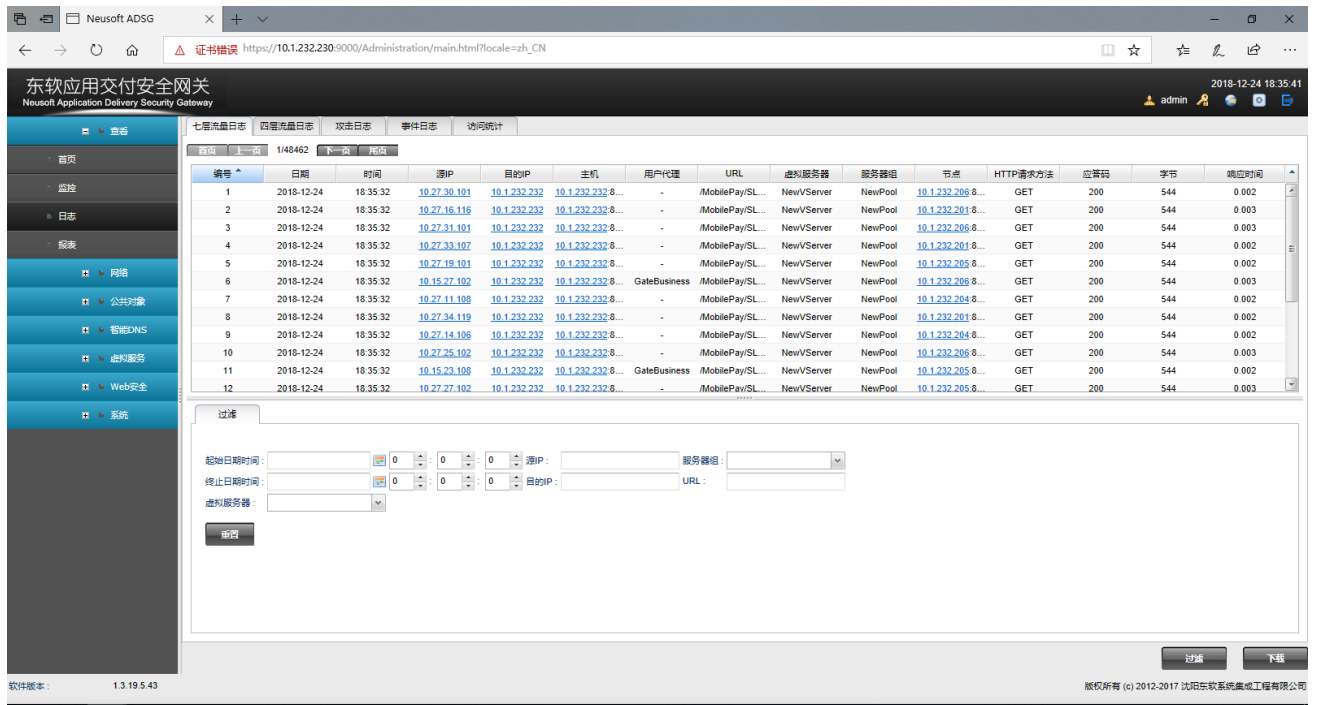
7. 选择查看>监控>监控。在监控下拉框中选择监控对象，查看流量信息。



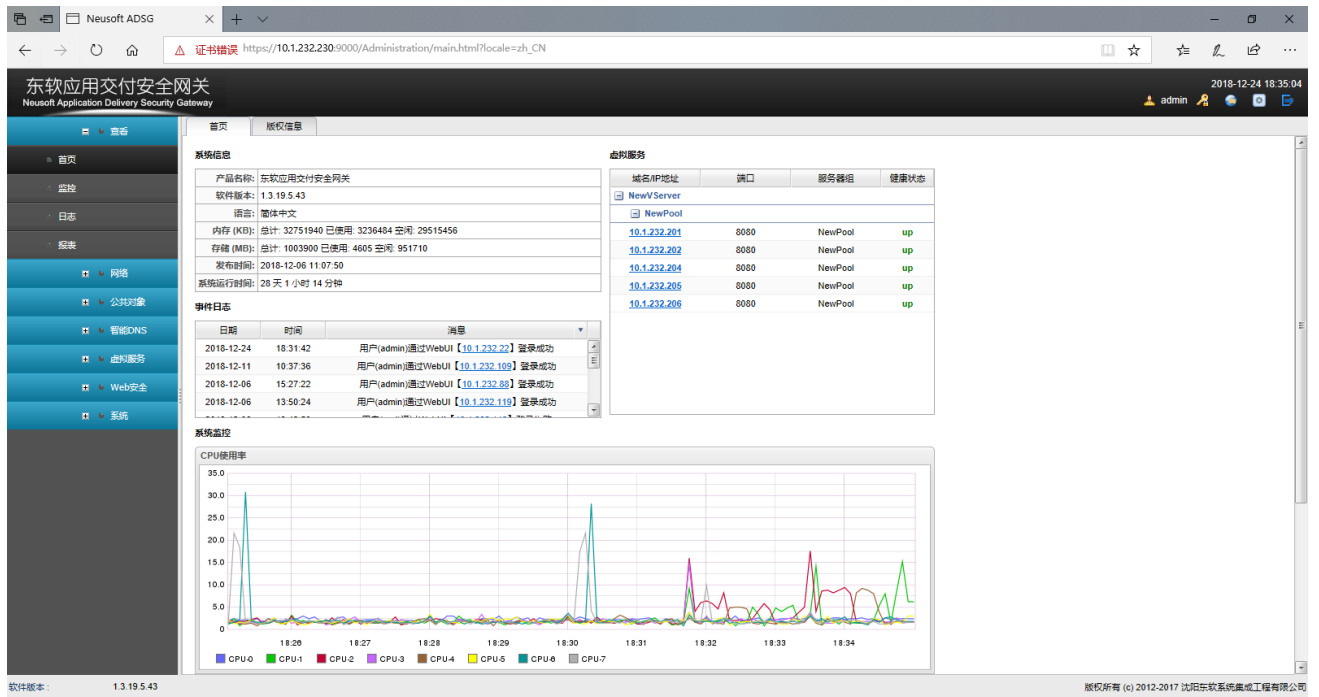
8. 选择查看>监控>统计。在统计下拉框中选择统计时间段，在监控下拉框中选择监控对象，点击刷新，查看统计信息。



9. 选择查看>日志查看日志。



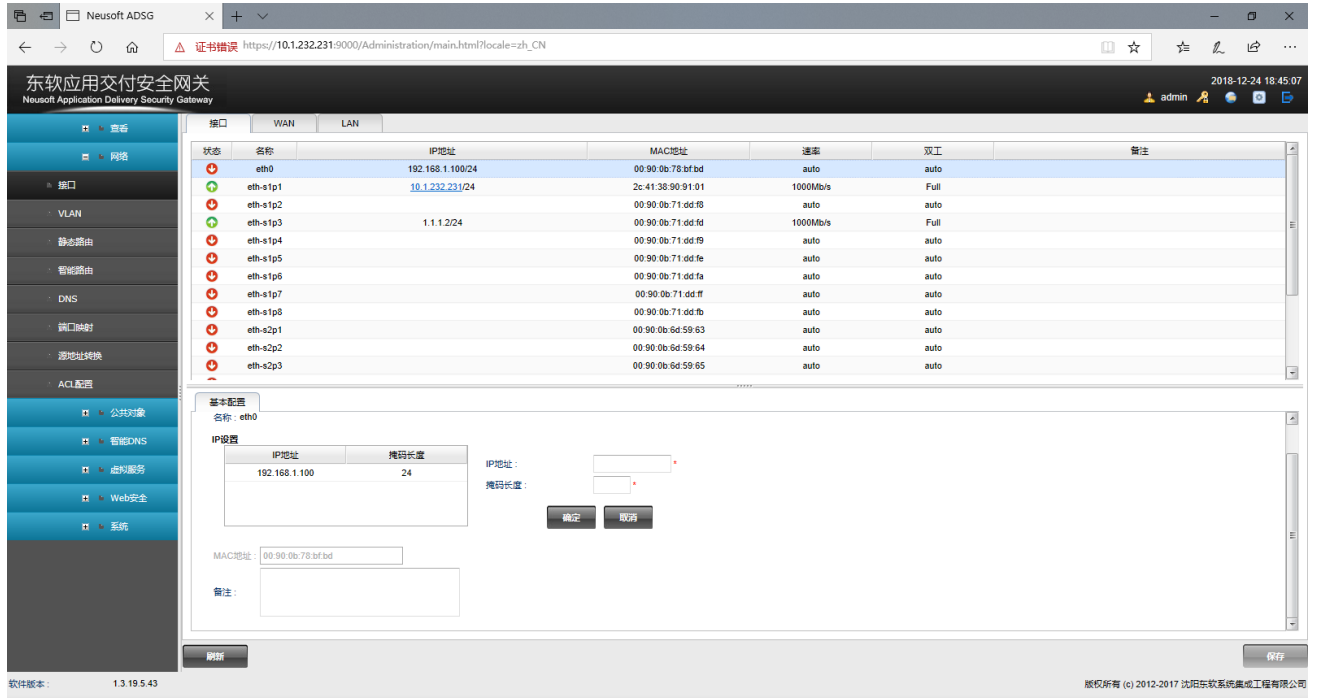
10. 进入首页，查看虚拟服务和系统运行状态。



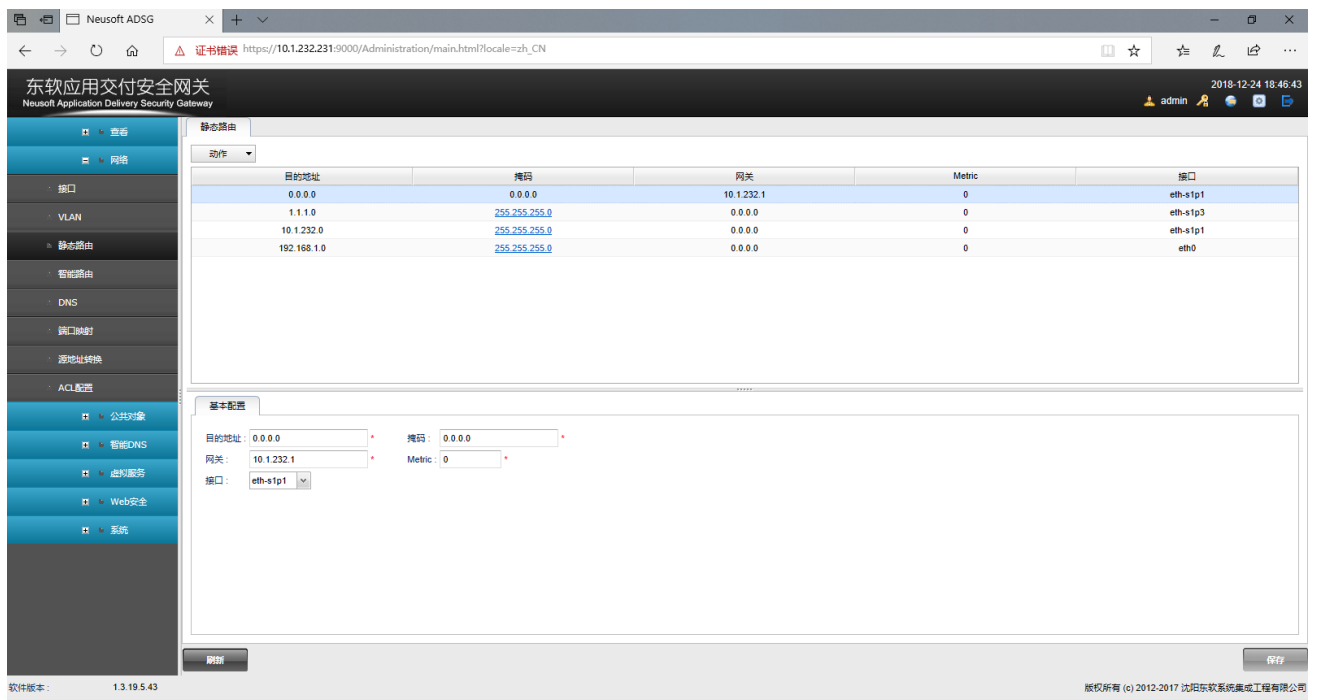
配置设备：

1. 选择**网络>接口>接口**，根据网络拓扑配置设备网络接口的 IP 地址。

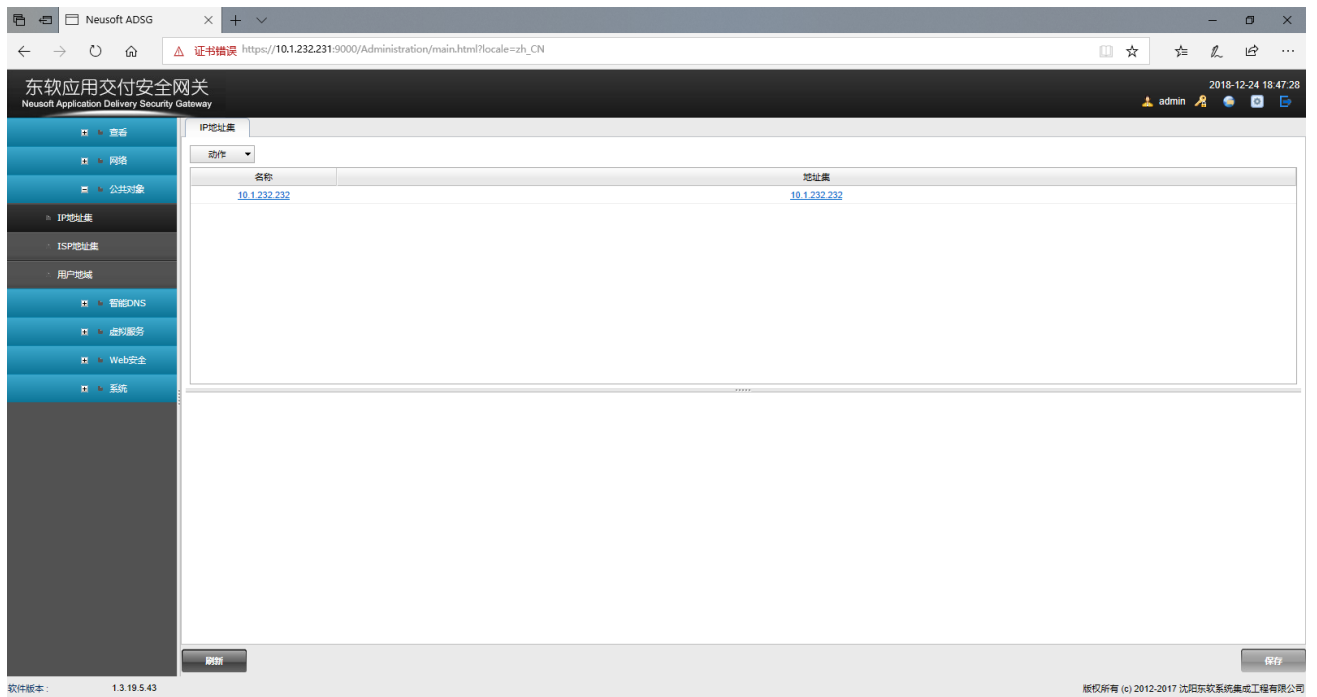
- 管理接口：eth0，IP=192.168.1.100/24
- 业务口：eth-s1p1，IP=10.1.232.231/24
- 心跳口：eth-s1p3，IP=1.1.1.2/24



2. 选择**网络>静态路由**。点击**动作**下拉框，选择**增加路由**，配置静态路由。

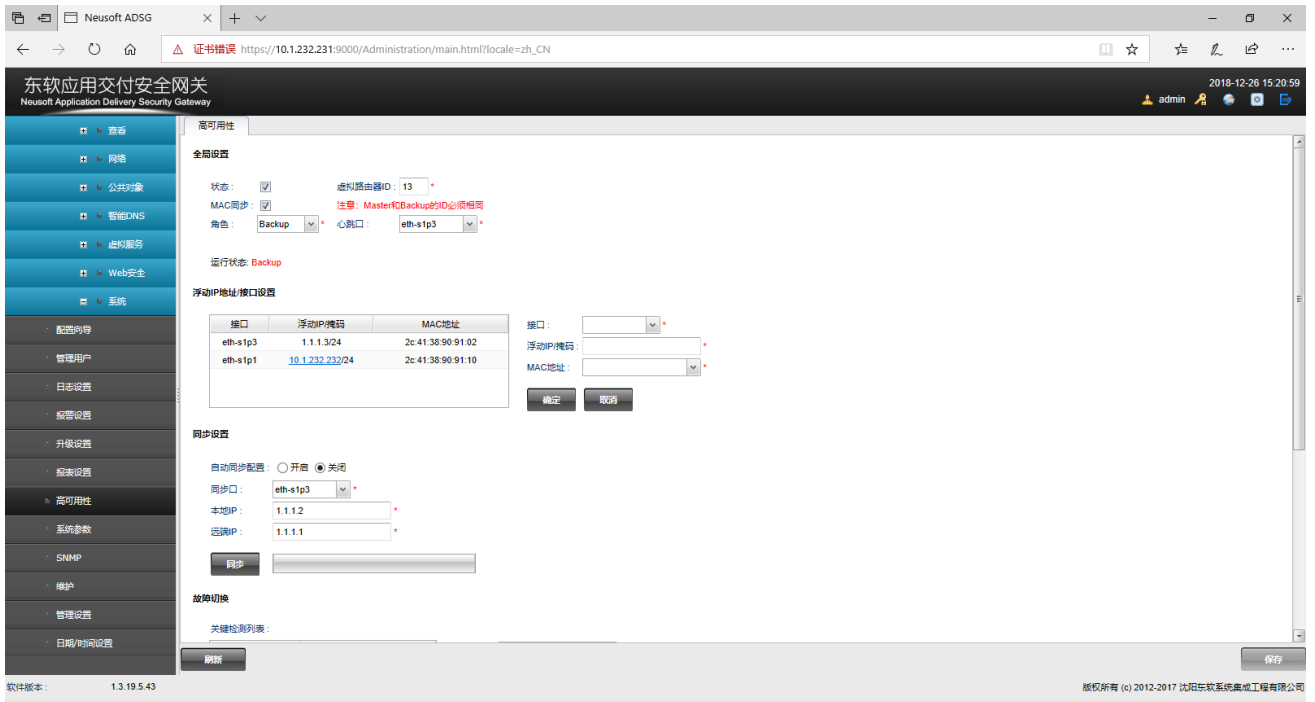


3. 选择**公共对象>IP地址集**，为虚拟服务器添加虚拟 IP 地址集 10.1.232.232。



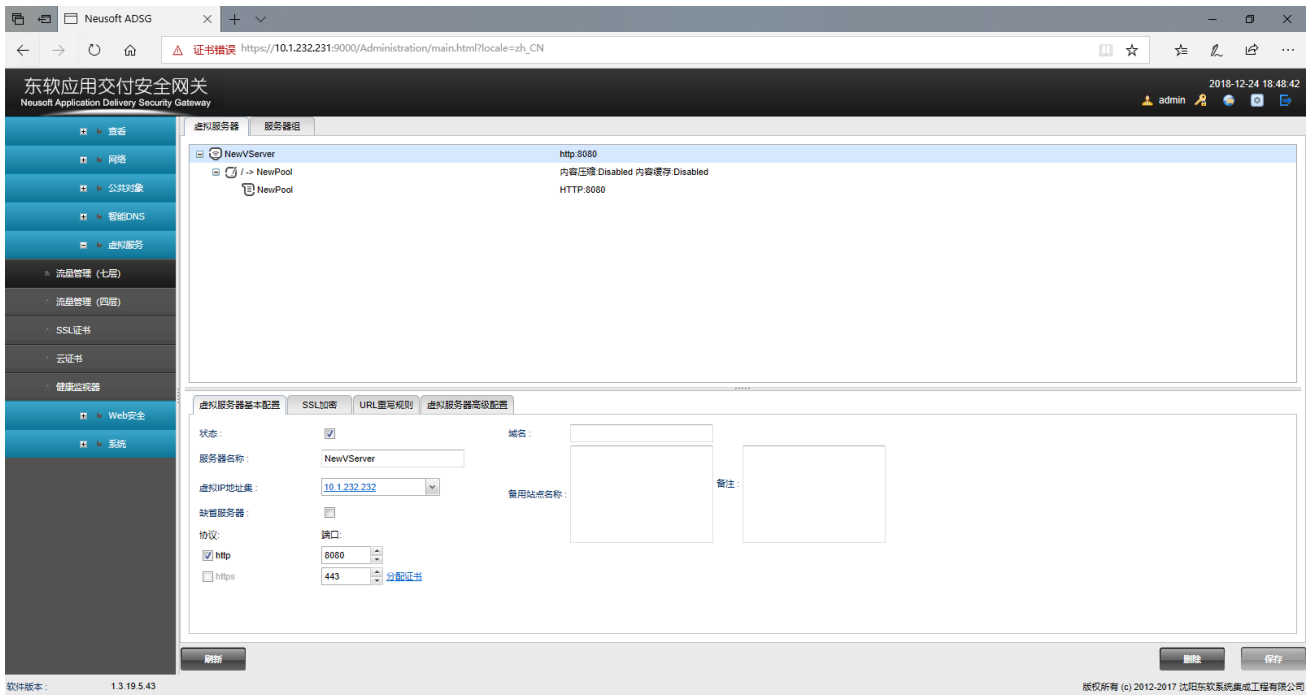
4. 选择系统>高可用性，配置高可用性。

- 状态：勾选（开启 HA 功能）
- 虚拟路由器 ID：13（主备机的虚拟路由器 ID 必须相同。）
- MAC 同步：勾选
- 角色：Backup
- 心跳口：eth-s1p3
- 配置浮动 IP 和接口：eth-s1p1 配 10.1.232.232/24, eth-s1p3 配 1.1.1.3/24。
- 配置同步设置：本地 IP 选择 1.1.1.2@eth-s1p3，远程 IP 填写备机 IP 1.1.1.1
自动同步配置选择关闭。



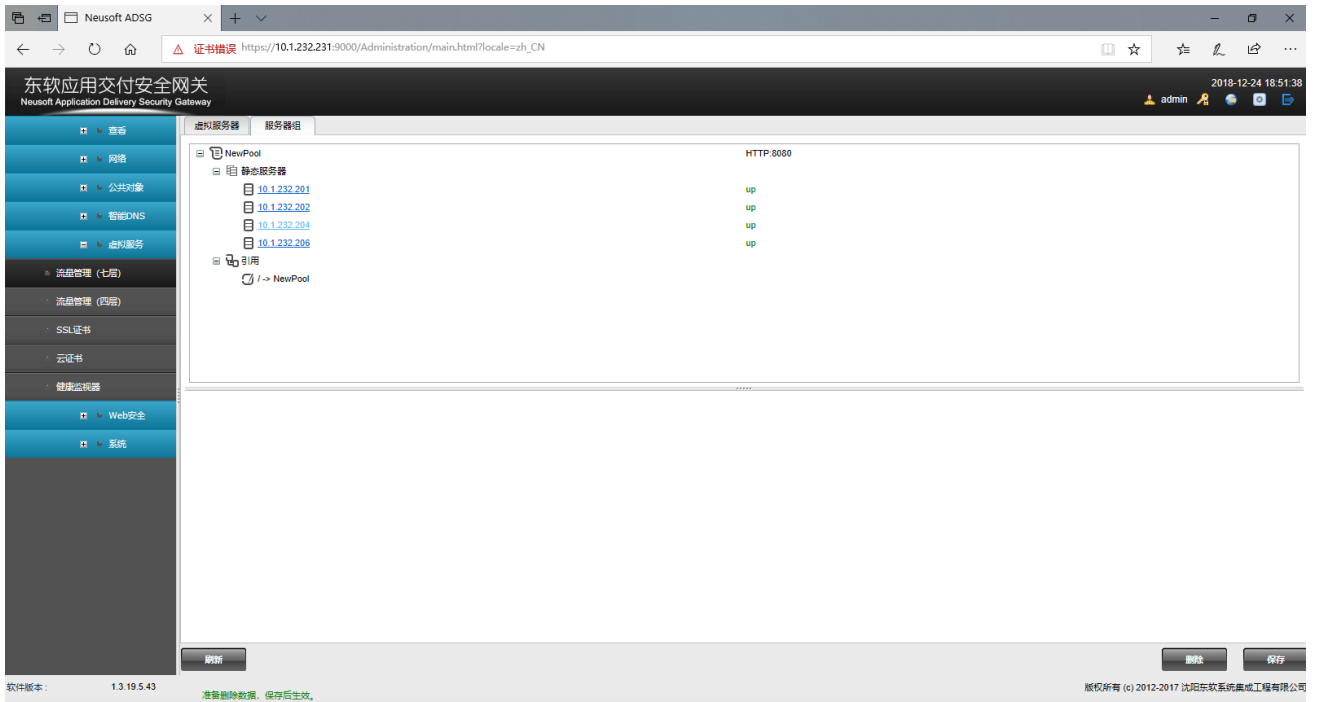
5. 选择虚拟服务>流量管理（七层）。

a. 在视图区空白处点击右键，选择添加虚拟服务器。

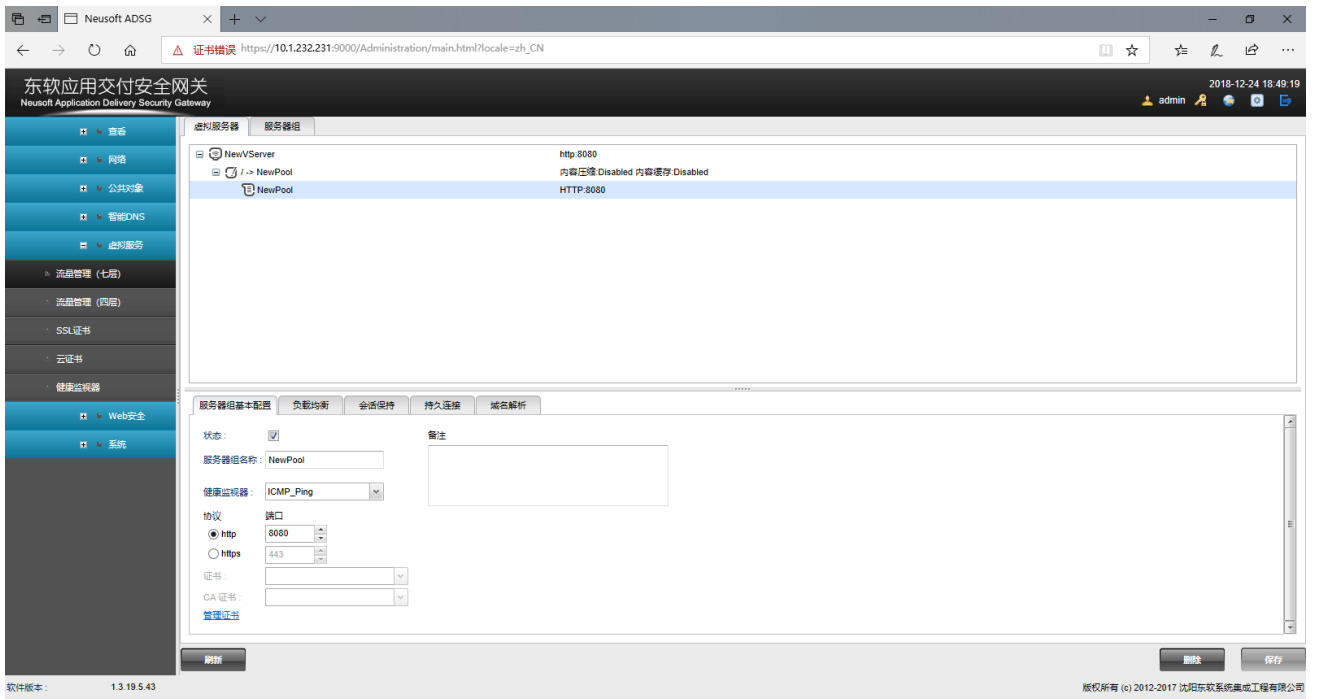


b. 右键点击静态服务器，选择添加静态服务器，添加静态服务器。

c. 点击服务器组，在视图区空白处点击右键，选择添加服务器组。



- d. 在服务器组的视图区右键点击引用，选择**添加资源路径**，双击资源路径名称，将虚拟服务器关联到虚拟服务器组。



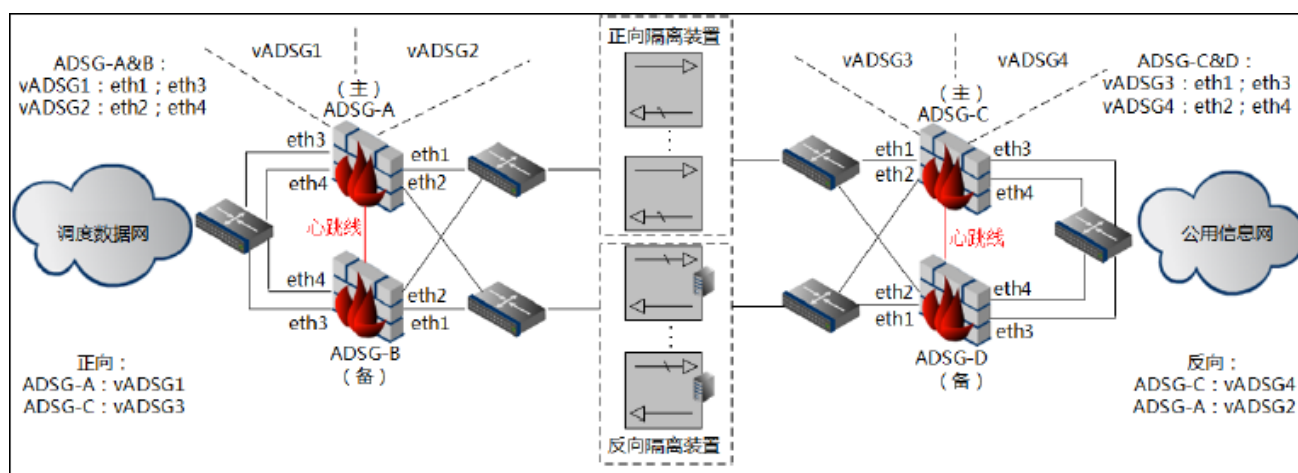
12.10. 电力网正反向虚拟隔离（虚拟系统）

背景：

如下图所示，某电力系统在调度数据网和公用信息网之间部署了正向隔离装置集群和反向隔离装置集群：正向隔离用于保护安全区 I/II 到安全区 III 的单向数据传递；反向隔离用于保护安全区 III 到安全区 IV 的单向数据传递。

在调度数据网和公用信息网的出口分别部署了主备 ADSG。现要求在两台 ADSG 主设备上分别划分出两个虚拟系统，作为正向隔离装置集群和反向隔离装置集群的统一出口。

拓扑：



配置指南：

1. 分别配置调度数据网和公用信息网出口的主备 ADSG 设备。
2. 分别在两台主备 ADSG 设备上配置两个虚拟系统，并分别配置主备。
3. 在 ADSG-A 的虚拟系统 vADSG1 中配置四层负载均衡和链路探测。
4. 在 ADSG-C 的虚拟系统 vADSG4 中配置四层负载均衡和服务器探测。

配置步骤：

配置主备设备

1. 以 admin 身份登录 ADSG。
2. 选择系统>高可用性，开启高可用性，设置主备状态，并配置相关参数。

设备名称	角色	虚拟路由器 ID	心跳口	浮动 IP	同步
ADSG-A	主	10	eth1	eth1=10.1.1.10/24	eth6

				eth3=192.168.1.10/24	本端 IP=1.1.1.1 对端 IP=2.2.2.2
ADSG-B	备	10	eth1	eth1=10.1.1.10/24 eth3=192.168.1.10/24	eth6 本端 IP=2.2.2.2 对端 IP=1.1.1.1
ADSG-C	主	9	eth1	eth2=10.1.2.20/24 eth4=192.168.2.20/24	eth6 本端 IP=3.3.3.3 对端 IP=4.4.4.4
ADSG-D	备	9	eth1	eth2=10.1.2.20/24 eth4=192.168.2.20/24	eth6 本端 IP=4.4.4.4 对端 IP=3.3.3.3

3. 点击**保存**。

创建虚拟系统

1. 以 root 身份登录 ADSG。
2. 选择**系统>虚拟系统**，创建两个虚拟系统。

- ADSG-A 和 ADSG-B:

虚拟系统	CPU数量	内存 (GB)	接口	状态	Web管理	备注
vsys1	2	2	eth1,eth3	✔		
vsys2	2	2	eth2,eth4	✔		

- ADSG-C 和 ADSG-D:

虚拟系统	CPU数量	内存 (GB)	接口	状态	Web管理	备注
vsys3	2	2	eth1,eth3	✔		
vsys4	2	2	eth2,eth4	✔		

3. 点击**保存**。
4. 选择**系统>管理用户**，创建分别为虚拟系统创建独立的管理员。

- ADSG-A 和 ADSG-B:

名称	用户类型	备注
root	Root	Root Administrator
admin	Administrator	System Default Administrator
vsys1admin	Vsys Administrator	
vsys2admin	Vsys Administrator	

- ADSG-C 和 ADSG-D:

名称	用户类型	备注
root	Root	Root Administrator
admin	Administrator	System Default Administrator
vsys3admin	Vsys Administrator	
vsys4admin	Vsys Administrator	

5. 点击**保存**。

配置四层负载均衡和链路探测（正向）

1. 以 vsys1admin 身份登录 vADSG1。
2. 选择**公共对象>IP 地址集**，创建 IP 地址集。

名称	地址集
asd1	10.175.55.175

3. 选择**虚拟服务>流量管理（四层）**，创建虚拟服务器和服务组，开启链路健康探测。

虚拟服务器
服务器组

[-] NewVServer_L4
Any

关联到 -> NewPool_L4

NewPool_L4

虚拟服务器基本配置
连接限制

状态:

服务器名称: * 虚拟IP地址集:

保持时间: 秒 协议:

本地IP:

10.175.55.113@eth-s
 10.175.55.114@eth-s
 10.175.55.123@eth-s
 10.175.55.133@eth-s
 10.175.55.143@eth-s

 *



4. 点击**保存**。
5. 选择**虚拟服务>链路探测**。
6. 分别在 vADSG1 和 vADSG3 上设置对端探测端口和本端监听端口。

基本配置	ADSG1	基本配置	ADSG3
检测端口: <input type="text" value="1234"/> (1025-50000)		检测端口: <input type="text" value="1025"/> (1025-50000)	
监听端口: <input type="text" value="1025"/> (1025-50000)		监听端口: <input type="text" value="1234"/> (1025-50000)	

7. 点击**保存**。

配置四层负载均衡和服务端探测（反向）

1. 以 vsys4admin 身份登录 vADSG4。
2. 选择**公共对象>IP 地址集**，创建 IP 地址集。

动作	
名称	地址集
asd4	10.175.55.114

3. 选择**虚拟服务>流量管理（四层）**，创建虚拟服务器和服务器组。健康监视器选择 ICMPping，开启服务器健康检测。

虚拟服务器 服务器组

NewVServer_L4 Any

关联到 -> NewPool_L4

NewPool_L4

虚拟服务器基本配置 连接限制

状态：

服务器名称：NewVServer_L4 * 虚拟IP地址集：asd4

保持时间：0 秒 协议：Any

本地IP：
 10.175.55.113@eth-s
 10.175.55.114@eth-s
 10.175.55.123@eth-s *
 10.175.55.133@eth-s
 10.175.55.143@eth-s

虚拟服务器 服务器组

NewPool_L4 NewVServer_L4

静态服务器

4.4.4.4 unknown

服务器组基本配置 会话保持

状态：

服务器组名称：NewPool_L4 * 备注：

协议：Any

负载均衡算法：轮询算法 *

健康监视器：ICMP_Ping

链路健康探测：

4. 点击**保存**。

附录 A：术语表

ADSG 术语表

英文名称	中文名称	说明
ADSG	应用交付安全网关	
Vserver	虚拟服务器	ADSG 对客户端展现出来的服务器，客户端将虚拟服务器当作真正的网站进行访问。
Pool	服务器组	虚拟服务器所使用的真正的服务器所在的组。
Location	资源路径	浏览器请求的资源在服务器中的位置。
Back-end server	后端服务器	ADSG 所保护的、真正为客户提供服务的网站服务器，位于服务器组中。
Smart DNS	智能 DNS	智能解析域名服务。能自动判断访问者的 IP 地址并解析出对应的 IP 地址，使联通用户会访问到联通服务器，电信用户会访问到电信服务器。 ADSG 的智能 DNS 支持本地站点入站链路负载均衡和多站点全局负载均衡两种场景。
Site Set	站点集合	参与实现全局负载均衡的一组服务站点，包含 Master 和 None 角色。其中，Master 负责接收 DNS 请求和解析调度，None 负责接收用户访问请求。
LDNS	本地 DNS 服务器	根据运营商、地域或用户自定义条件分类添加的一些 IP 地址集，用于 ADSG 开启智能 DNS 功能时本地解析用户 DNS 请求。
WHOIS	域名查询数据库	WHOIS 是一个用来查询域名是否已经被注册以及注册域名的详细信息的数据库。
Administrator	管理员	ADSG 产品的使用者，是 ADSG 所保护的网站的维护人员。
SQL Injection	SQL 注入	指攻击者以 URL 或 Form 输入形式变相地到数据库中执行 SQL 命令。如果攻击成功，可能让数据库执行不希望执行的命令，导致信息泄露、改变数据库内容、甚至破坏数据库。
Cross Site Scripting	跨站脚本	指攻击者在具有信任关系的 Web 服务器和客户端之间，通过在 URL 中注入恶意的脚本，来获取包含用户的身份信息、资格证书的 Cookie 或者欺骗用户提供资格证书给攻击者。

附录 B：日志信息

本附录提供关于 ADSG 日志的信息。管理员可通过本附录更好的了解日志含义及应对措施，进而更好的了解系统运行的状态。

本附录包括：

- [日志信息概述](#)
- [报警日志](#)
- [事件日志](#)
- [流量日志](#)

日志信息概述

本部分解释日志信息具体含义，包括：

- [格式](#)
- [语法](#)
- [日志类型](#)
- [日志子类型](#)
- [日志 ID 含义解释](#)
- [日志安全级别](#)

格式

系统输出日志的完整格式如下：

`date=date time=time host=host log_id=log_id level=level type=type sub-type=sub-type message.`

语法

下表解释了日志信息的参数含义。

字段	类型	说明
date	varchar	日志产生的日期。
time	varchar	日志产生的时间。
host	varchar	产生日志的主机名称。通常在分布式日志系统中使用该参数。

level	varchar	日志的级别，体现日志的严重性，具体请参见 日志安全级别 。
log_id	varchar	日志的 ID。
type	varchar	日志的类型，具体请参见 日志类型 。
sub_type	varchar	产生日志的模块的编号。
msg	varchar	日志的主体，描述日志的详细信息。
action	varchar	在攻击日志中，表示检测到攻击时采取的措施。 在事件日志中，表示管理员所执行的操作。
protocol	varchar	四层协议，如 UDP、TCP 等。
service	varchar	七层协议，如 HTTP、FTP 等。
src	varchar	源 IP 地址。
src_port	int	源端口号。
dst	varchar	目的 IP 地址。
dst_port	int	目的端口号。
vserver	varchar	虚拟服务器名称。
pool	varchar	服务器组名称。
node	varchar	服务器组中节点名称。
http_method	varchar	HTTP 请求方式。
http_uri	varchar	HTTP 请求的 URI 地址。
http_host	varchar	HTTP 请求的主机名和端口号。
http_agent	varchar	用来进行 HTTP 请求的浏览器名称。
http_session_id	varchar	HTTP 会话 ID 值。
rule	varchar	控制 HTTP 请求包的规则。
response_time	double precision	Nginx 和后端服务器间的交互时间。
bytes	int	Nginx 和后端服务器之间交互的数据包大小。
module	varchar	发布日志的模块名称。
user	varchar	执行操作的用户。
result	varchar	用户执行操作的结果，包括成功和失败两种结果。
clientip	varchar	客户端 IP 地址。

name **varchar** 执行操作的对象名称，包括对象类型和对象名称。

日志类型

下表描述了各日志类型的含义。

类型	ID	说明
Alert	01	该类型日志记录 AD SG 检测到的攻击及其采取的措施。
Traffic	02	该类型日志记录了所有经过 AD SG 的流量信息。
Event	03	该类型日志记录管理员在各个模块执行操作情况及相关的结果。

日志子类型

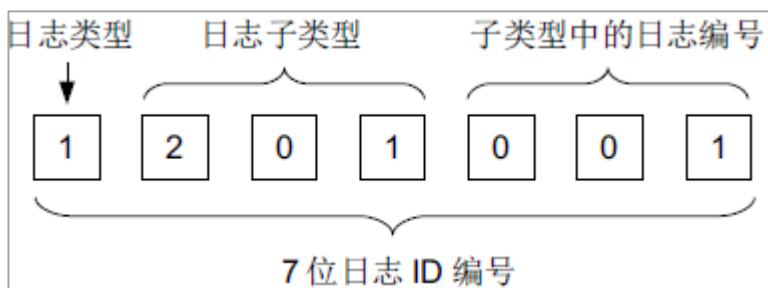
下表描述了日志子类型与 ID 号的对应关系。

子类型名称	ID
应用交付类	
Load Balancing	100
Session Persistence	101
Content Cache	102
Content Compressing	103
安全类	
Anti Robot	201
IPS	202
Captcha	203
Blacklist	206
Whitelist	207
Proactive Protection	208
Access rule control	209
Web defacement	210
DLP	211
其它	
User Management	301

System	302
Traffic	303
Report	304
System Upgrade	305
License Activate	306
HA	307
Admin	308

日志 ID 含义解释

日志 ID 解释如下所示。



日志安全级别

下表描述日志级别的具体含义。

日志级别

级别	说明
LOG_EMERG 0	系统处于不稳定状态。
LOG_ALERT 1	系统错误或被攻击，将导致一些功能不可用，需立即采取措施。如，license 到期，CPU 使用率过高，内存使用率过高，遭遇 DoS 攻击等。
LOG_CRIT 2	出现影响系统性能的事件。如，高可用主备切换。
LOG_ERR 3	所有操作失败情况，如，添加、删除和修改内容失败，病毒扫描引擎加载失败。
LOG_WARNING 4	发生有可能影响系统性能的情况或系统发生重大的配置变更，如连接升级服务器失败、超时。
LOG_NOTICE 5	发生常规事件和配置，如更新成功，进行添加、删除和修改。
LOG_INFO 6	系统操作的一般信息。
LOG_DEBUG 7	调测时产生，供技术人员进行故障处理使用。

报警日志

报警日志描述如下。

报警日志模板

子类型	日志 ID	日志消息模板
Anti Robot	1201001	<pre>date=<date> time=<time> host=<host> log_id="1201001" level="1" type="01" sub_type="201" proto="0" service="web" src=<src_IP> src_port=<src_port> dst=<dst_IP> dst_port=<dst_port> vs erver=<vserver> pool=<pool> node=<node> http_method=<http_method> http_uri=<http_uri> http_host=<http_host> http_agent=<http_agent> http_session_id=<http_session_id> action=<action> rule=<rule> msg="Active Challenge failed from <src_IP>:<src_port> to vs erver <vserver> at <dst_IP>:<dst_port>, action: <action>"</pre>
IPS	1202001	<pre>date=<date> time=<time> host=<host> log_id="1202001" level="1" type="01" sub_type="202" proto="0" s ervice="web" src=<src_IP> src_port=<src_port> dst=<dst_IP> dst_port=<dst_port> vs erver=<vserver> pool=<pool> node=<node> http_method=<http_method> http_uri=<http_uri> http_host=<http_host> http_agent=<http_agent> http_session_id=<http_session_id> action=<action> rule=<rule> msg="SQL Injection detected from <src_IP>:<src_port> to vs erver <vserver> at <dst_IP>:<dst_port>, action: <action>, rules: <rules>"</pre>
	1202002	<pre>date=<date> time=<time> host=<host> log_id="1202002" level="1" type="01" sub_type="202" proto="0" service="web" src=<src_IP> src_port=<src_port> dst=<dst_IP> dst_port=<dst_port> vs erver=<vserver> pool=<pool> node=<node> http_method=<http_method> http_uri=<http_uri> http_host=<http_host> http_agent=<http_agent> http_session_id=<http_session_id> action=<action> rule=<rule> msg="Common Injection detected from <src_IP>:<src_port> to vs erver <vserver> at <dst_IP>:<dst_port>, action: <action>, rules: <rules>"</pre>
	1202003	<pre>date=<date> time=<time> host=<host> log_id="1202003" level="1" type="01" sub_type="202" proto="0" service="web" src=<src_IP> src_port=<src_port> dst=<dst_IP> dst_port=<dst_port> vs erver=<vserver> pool=<pool> node=<node> http_method=<http_method> http_uri=<http_uri> http_host=<http_host> http_agent=<http_agent> http_session_id=<http_session_id> action=<action> rule=<rule> msg="XSS attack detected from <src_IP>:<src_port> to vs erver <vserver> at <dst_IP>:<dst_port>, action: <action>, rules: <rules>"</pre>
	1202004	<pre>date=<date> time=<time> host=<host> log_id="1202004" level="1" type="01" sub_type="202" proto="0" service="web" src=<src_IP> src_port=<src_port> dst=<dst_IP> dst_port=<dst_port> vs erver=<vserver> pool=<pool> node=<node> http_method=<http_method> http_uri=<http_uri> http_host=<http_host> http_agent=<http_agent> http_session_id=<http_session_id> action=<action> rule=<rule> msg="Buffer Over flow detected from <src_IP>:<src_port> to vs erver <vserver> at <dst_IP>:<dst_port>, action: <action>, rules: <rules>"</pre>

```

1202005  date=<date> time=<time> host=<host> log_id="1202005" level="1" type="01" sub_type="202"
         proto="0" service="web" src=<src_IP> src_port=<src_port> dst=<dst_IP> dst_port=<dst_port>
         vs erver=<vserver> pool=<pool> node=<node> http_method=<http_method> http_uri=<http_uri>
         http_host=<http_host> http_agent=<http_agent> http_session_id=<http_session_id> action=<action>
         rule=<rule> msg="Backdoor & Trojan detected from <src_IP>:<src_port> to vs erver <vserver> at
         <dst_IP>:<dst_port>, action: <action>, rules: <rules>"

1202006  date=<date> time=<time> host=<host> log_id="1202006" level="1" type="01" sub_type="202"
         proto="0" service="web" src=<src_IP> src_port=<src_port> dst=<dst_IP> dst_port=<dst_port>
         vs erver=<vserver> pool=<pool> node=<node> http_method=<http_method> http_uri=<http_uri>
         http_host=<http_host> http_agent=<http_agent> http_session_id=<http_session_id> action=<action>
         rule=<rule> msg="CSRF detected from <src_IP>:<src_port> to vs erver <vserver> at <dst_IP>:<dst_port>,
         action: <action>, rules: <rules>"

1202007  date=<date> time=<time> host=<host> log_id="1202007" level="1" type="01" sub_type="202"
         proto="0" service="web" src=<src_IP> src_port=<src_port> dst=<dst_IP> dst_port=<dst_port>
         vs erver=<vserver> pool=<pool> node=<node> http_method=<http_method> http_uri=<http_uri>
         http_host=<http_host> http_agent=<http_agent> http_session_id=<http_session_id> action=<action>
         rule=<rule> msg="Other Signature Set detected from <src_IP>:<src_port> to vs erver <vserver> at
         <dst_IP>:<dst_port>, action: <action>, rules: <rules>"

```

事件日志

事件日志描述如下。

事件日志模板

子类型	日志 ID	日志消息模板
Report	3304001	date=<date> time=<time> host=<host> log_id="3304001" level=<level> type="03" sub_type="304" vs erver=<vserver> pool=<pool> module="Report" msg="Generate <variable_parameter> successfully!"
	3304002	date=<date> time=<time> host=<host> log_id="3304002" level=<level> type="03" sub_type="304" vs erver=<vserver> pool=<pool> module="Report" msg="Generate <variable_parameter> failure!"
	3304003	date=<date> time=<time> host=<host> log_id="3304003" level=<level> type="03" sub_type="304" vs erver=<vserver> pool=<pool> module="Report" msg="Get data from unieap report file failure!"
	3304004	date=<date> time=<time> host=<host> log_id="3304004" level=<level> type="03" sub_type="304" vs erver=<vserver> pool=<pool> module="Report" msg="Read xml config failure!"

```

3304005  date=<date> time=<time> host=<host> log_id="3304005" level=<level> type="03" sub_type="304"
vs erver=<vserver> pool=<pool> module="Report" msg=" Argv is wrong!"

3304006  date=<date> time=<time> host=<host> log_id="3304006" level=<level> type="03" sub_type="304"
vs erver=<vserver> pool=<pool> module="Report" msg="Export data for report failure!"

3304007  date=<date> time=<time> host=<host> log_id="3304007" level=<level> type="03" sub_type="304"
vs erver=<vserver> pool=<pool> module="Report" msg="Create report running flag file failure!"

System  3305001  date=<date> time=<time> host=<host> log_id="3305001" level=<level> type="03" sub_type="305"
Upgrade vs erver=<vserver> pool=<pool> module="System Upgrade" msg="System Upgrade successfully!"

3305002  date=<date> time=<time> host=<host> log_id="3305002" level=<level> type="03" sub_type="305"
vs erver=<vserver> pool=<pool> module="System Upgrade" msg="System Upgrade failure!"

3305003  date=<date> time=<time> host=<host> log_id="3305003" level=<level> type="03" sub_type="305"
vs erver=<vserver> pool=<pool> module="System Upgrade" msg="No available packages!"

License 3306001  date=<date> time=<time> host=<host> log_id="3306001" level=<level> type="03" sub_type="306"
Activate vs erver=<vserver> pool=<pool> module="License Activate" msg="License activate successfully!"

3306002  date=<date> time=<time> host=<host> log_id="3306002" level=<level> type="03" sub_type="306"
vs erver=<vserver> pool=<pool> module="License Activate" msg="License activate failure!"

HA      3307001  date=<date> time=<time> host=<host> log_id="3307001" level="3" type="03" sub_type="307"
vs erver=<vserver> pool=<pool> module="HA" msg=<master_state>

3307002  date=<date> time=<time> host=<host> log_id="3307002" level="3" type="03" sub_type="307"
vs erver=<vserver> pool=<pool> module="HA" msg=<backup_state>

Admin   3308001  log_id="3308001" level="5" user=<user> action=<action> result=<result> clientip=<IP_address>
type="03" subtype="308" vs erver=<vserver> pool=<pool> module="Admin" mgs=User <user> <action>
<result> from WebUI<IP_address>

3308002  log_id="3308002" level="5" user=<user> action=<action> result=<result> name=<type:name> type="03"
subtype="308" vs erver=<vserver> pool=<pool> module="Admin" mgs=User <user> <action> <name>
<result>

```



```
3308003 log_id="3308003" level="5" user=<user> action=<action> result=<result> type="03" subtype="308"
vs erver=<vserver> pool=<pool> module="Admin" mgs=User <user> <action> <result>
```

流量日志

流量日志描述如下：

七层流量日志模板

子类

型	日志 ID	日志消息模板
---	-------	--------

Traffic	2303001	date=<date>time=<time>host=<host>log_id="2303001" level="7" type="02" sub_type="303" proto="0" service="web" src=<src_IP>src_port=<src_port>dst=<dst_IP>dst_port=<dst_port>vs erver=<vserver> pool=<pool>node=<node>http_method=<http_method>http_uri=<http_uri>http_host=<http_host>http_agent=<http_agent>http_session_id=<http_session_id>response_time=<response_time> bytes=<bytes>msg="HTTP Traffic from <src_IP>:<src_port> to vs erver <vserver> at <dst_IP>:<dst_port>"
---------	---------	--

四层流量日志模板

子类

型	日志 ID	日志消息模板
---	-------	--------

Traffic	2303003	date=<date>time=<time>log_id="2303003" level="5" pro=<pro>in_bytes=<in_bytes>out_bytes=<out_bytes>from_ip=<from_ip>from_port=<from_port>to_ip=<to_ip>to_port=<to_port>local_ip=<local_ip>local_port=<local_port>dst_ip=<dst_ip>dst_port=<dst_port>action=<action>
---------	---------	---
