

SANGFOR AD6.6

用户手册



2017 年 06 月

目录

声明.....	1
前言.....	2
手册内容.....	2
本书约定.....	2
图形界面格式约定.....	2
各类标志.....	3
技术支持.....	3
致谢.....	3
第 1 章 AD 设备的安装.....	4
1.1. 环境要求.....	4
1.2. 电源.....	4
1.3. 产品外观.....	4
1.4. 配置与管理.....	5
1.5. 设备接线方式.....	5
第 2 章 控制台的使用.....	7
2.1. 登陆 WEBUI 配置界面.....	7
2.2. 配置和使用.....	7
第 3 章 系统概况.....	10
3.1. 活动查看.....	10
3.1.1. 系统状态.....	10
3.1.2. 资源占用率.....	11
3.1.3. 网络吞吐量.....	12
3.1.4. 连接数.....	12
3.1.5. SSL TPS.....	15
3.1.6. HTTP TPS.....	15
3.2. 虚拟服务详情.....	16
3.2.1. 虚拟服务状态.....	16
3.2.2. 缓存/流量状态.....	17
3.2.3. 缓存查询.....	18
3.2.4. 缓存缺失原因.....	19
3.2.5. URL 次数统计.....	20
3.2.6. URL 实时流量.....	21
3.3. 智能 DNS 统计.....	22
3.3.1. 域名实时请求.....	22
3.3.2. 域名历史请求.....	22
3.3.3. DNS 请求数.....	23
3.3.4. LDNS 来源.....	24
3.3.5. LDNS 缺失记录.....	24
3.4. DDOS 攻击分析.....	25

3.4.1. 七层 DDOS 分析.....	25
3.4.2. 七层 DDOS 统计.....	26
3.5. 集群状态.....	27
3.6. 实时漏洞分析.....	27
3.7. 链路状态.....	30
3.7.1. 所有链路状态.....	31
3.7.2. 虚拟服务链路状态.....	32
3.8. 节点状态.....	32
3.8.1. 节点池状态.....	33
3.8.2. 节点状态.....	34
3.8.3. 调度查询.....	35
3.9. 接口状态.....	35
3.10. DNS 状态.....	36
3.11. 全局状态.....	36
3.11.1. 全局状态.....	37
3.11.2. 虚拟 IP 池状态.....	37
3.11.3. 规则测试.....	38
3.12. 动态路由表.....	38
3.13. 日志查看.....	39
3.13.1. 服务日志.....	39
3.13.2. 管理日志.....	41
3.13.3. SSL 日志.....	42
3.14. 调试信息统计.....	43
第 4 章 报表配置.....	44
4.1. 报表生成.....	44
4.1.1. 立即生成.....	44
4.1.2. 自动生成.....	45
4.1.3. 报表样式.....	46
4.2. 报表中心.....	52
4.2.1. 报表维护.....	53
4.2.2. 报表中心.....	54
第 5 章 公共对象.....	80
5.1. 用户地址集.....	80
5.2. IP 地址集.....	82
5.2.1. ISP 地址段.....	83
5.2.2. 全球地址段.....	85
5.2.3. 用户地域.....	90
5.2.4. 自动更新.....	93
5.3. 时间计划.....	94
5.4. 脚本规则.....	96
5.5. 自定义内容.....	97
第 6 章 数据中心.....	101
6.1 系统概览.....	101
6.2 数据中心.....	101

6.3 本地服务设备.....	103
第7章 应用负载.....	105
7.1. 服务.....	105
7.2. IP组.....	108
7.3. 会话保持.....	110
✓ SourceIP.....	111
✓ Cookie.....	111
✓ HTTP Passive.....	113
✓ RADIUS.....	115
✓ SSL SessionID.....	116
7.4. 节点监视器.....	117
✓ ICMP.....	119
✓ ICMPv6.....	119
✓ CONNECT(TCP).....	120
✓ CONNECT(UDP).....	122
✓ HTTP.....	123
✓ FTP.....	124
✓ HTTPS.....	125
✓ CONNECT(SSL).....	125
✓ SNMP.....	126
✓ DNS.....	128
✓ RADIUS.....	129
✓ TCP半连接.....	130
✓ TCP被动.....	131
✓ HTTP被动.....	132
✓ 复合监视器.....	133
✓ 数据库.....	134
✓ LDAP.....	137
✓ 外部应用监视器.....	139
7.5. 节点池.....	140
7.6. SSL.....	146
7.6.1. SSL证书.....	146
7.6.2. CA证书.....	152
7.6.3. CRL.....	153
7.7. 策略.....	157
7.7.1. 前置调度策略.....	157
7.7.2. 优化策略.....	166
7.7.3. HTTP改写策略.....	171
7.7.4. HTTP防护策略.....	181
7.7.5. TCP策略.....	183
7.7.6. 卸载策略.....	186
7.7.7. 加密策略.....	190
7.7.8. URL下载速度控制.....	192
7.7.9. QoS策略.....	193

7.8. 虚拟服务.....	196
7.8.1. 虚拟服务.....	196
7.8.2. 虚拟服务关联组.....	202
第 8 章 智能 DNS.....	203
8.1. DNS 服务器.....	203
8.2. 站点集合.....	205
8.3. DNS 记录.....	209
8.3.1. 本地 DNS 记录.....	209
8.3.2. 全局 DNS 记录.....	218
8.4. 虚拟 IP 池.....	219
8.4.1. 本地虚拟 IP 池.....	219
8.4.2. 全局虚拟 IP 池.....	224
8.5. DNS 映射.....	225
8.5.1. 本地 DNS 映射.....	226
8.5.2. 全局 DNS 映射.....	228
8.6. LDNS 集合.....	229
8.6.1. 本地 LDNS 集合.....	230
8.6.2. 全局 LDNS 集合.....	234
8.7. 静态就近性.....	234
8.7.1. DNS 映射级别.....	235
8.7.2. 虚拟 IP 池级别.....	236
8.8. 全局配置还原.....	238
8.8.1. 配置还原.....	238
8.8.2. 同步配置.....	239
第 9 章 路由配置.....	240
9.1. 智能路由.....	240
9.1.1. 智能路由.....	240
9.1.2. 出站高级配置.....	244
9.1.3. 路由测试.....	245
9.2. 静态路由.....	246
9.3. 虚拟 IP 路由.....	249
9.4. IP-Anycast.....	251
9.5. RIP.....	253
9.5.1. 全局配置.....	254
9.5.2. 接口配置.....	256
9.6. OSPF.....	257
9.6.1. 全局配置.....	258
9.6.2. 接口配置.....	260
9.6.3. 邻居关系表.....	262
9.7. OSPFv3.....	263
9.7.1. 全局配置.....	263
9.7.2. 接口配置.....	265
9.7.3. 邻居关系表.....	267
第 10 章 网络配置.....	268

10.1. 网络接口.....	268
10.1.1. 网络接口.....	269
10.1.2. 交换网口.....	276
10.1.3. 端口聚合.....	282
10.1.4. VLAN.....	286
10.1.5. 接口模式.....	288
10.2. 链路监视器.....	288
10.3. 源地址转换.....	292
10.3.1. 源地址转换.....	292
10.3.2. SNAT 地址集.....	297
10.3.3. 源地址转换关联组.....	298
10.4. 端口映射.....	299
10.5. DNS 代理.....	304
10.5.1. DNS 代理.....	304
10.5.2. 前置调度策略.....	306
10.5.3. 内网 DNS 记录.....	309
10.5.4. HOSTS.....	314
10.6. 网络安全.....	315
10.6.1. 网络攻击防护.....	315
10.6.2. ARP/ND 防护.....	317
10.6.3. ARP 代理.....	319
10.6.4. 高级配置.....	320
10.7. ACL 配置.....	321
10.7.1. 基础 ACL 控制.....	321
10.7.2. 高级 ACL 控制.....	324
第 11 章 系统配置.....	326
11.1. 设备管理.....	326
11.1.1. 管理网口.....	326
11.1.2. 日期/时间.....	329
11.1.3. 配置备份与恢复.....	330
11.1.4. 关机/重启.....	331
11.1.5. WebConsole.....	332
11.2. 授权信息.....	334
11.3. 用户.....	337
11.3.1. 用户.....	337
11.3.2. 角色.....	338
11.3.3. 外部认证登录.....	342
11.4. SMTP 服务器.....	343
11.5. SNMP.....	345
11.5.1. SNMP (V1, V2C)	345
11.5.2. SNMP (V3)	347
11.5.3. Traps (V1)	348
11.6. 告警.....	348
11.6.1. E-MAIL 告警.....	349

11.6.2. 短信告警.....	350
11.6.3. SNMP Trap 告警.....	353
11.7. 日志设置.....	355
11.7.1. HTTP 日志.....	355
11.7.2. Syslog 设置.....	356
11.7.3. NAT 日志服务器.....	360
11.8. 系统更新.....	361
11.8.1. 系统升级.....	361
11.8.2. 系统回滚.....	362
11.8.3. 系统安全.....	362
11.8.4. 代理设置.....	363
第 12 章 配置向导.....	365
12.1. 应用负载模板.....	365
12.2. 智能路由向导.....	365
向导第一步：配置链路信息.....	365
向导第二步：配置选路策略.....	366
向导第三步：配置策略名称.....	367
第 13 章 高可用性.....	369
13.1. 模式.....	369
13.2. 主备模式.....	371
13.2.1. 主备.....	371
13.3. 集群模式.....	375
13.3.1. 高可用集群模式.....	375
13.3.2. 高性能集群模式.....	383
第 14 章 业务分析.....	394
14.1. 安全分析.....	394
14.1.1. 实时漏洞分析.....	394
14.1.2. 服务配置.....	395
14.1.3. 漏洞识别库.....	396
14.2. 应用分析.....	398
14.2.1. WeLogic 监控.....	399
14.2.2. ORACLE 监控.....	401
14.2.3. SQLServer 监控.....	404
第 15 章 增值服务.....	408
15.1. 增值服务导航.....	408
15.1.1. 激活信息.....	408
15.1.2. 发帖求助&在线咨询.....	409
15.1.3. 社区疑问&资料搜索.....	410
第 16 章 案例集.....	412
16.1. 部署配置案例.....	412
16.1.1. 路由模式部署案例.....	412
16.1.2. 旁路模式部署案例.....	422
16.2. 服务器负载配置案例.....	427
16.3. MySQL 数据库负载配置案例.....	429

16.4. Radius 服务器负载配置案例.....	435
16.5. 传输客户端 IP 至后台服务器配置案例.....	439
16.6. 入站前置调度策略案例.....	442
16.7. HTTP 头部改写配置案例.....	445
16.8. 三角传输配置案例.....	450
16.9. SSL 策略配置案例.....	459
16.10. 智能路由配置案例.....	462
16.11. 智能 DNS 案例.....	465
16.11.1. 单站点智能 DNS 链路负载.....	465
16.11.2. 分布式部署智能 DNS 链路负载.....	475
16.12. IP-Anycast 配置案例.....	499
16.13. DNS 代理案例.....	505
16.14. 出站前置调度策略案例.....	508
16.15. ACL 配置案例.....	512
16.16. 主备双机配置案例.....	513
16.17. 集群部署配置案例.....	518
16.18. 虚拟链路健康检查案例.....	535
16.19. 综合案例.....	544
附录：网关升级客户端的使用.....	566
产品升级步骤.....	574



深信服，让IT更简单，更安全，更有价值

声明

Copyright © 2017 深信服科技股份有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书的部分或全部内容，并不得以任何形式传播。

深信服科技股份有限公司（以下简称为深信服科技、SANGFOR）。

SANGFOR 为深信服科技股份有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新用户手册，请联系深信服科技股份有限公司技术服务部。

前言

手册内容

第1部分 SANGFOR AD 产品安装。该部分主要介绍 AD 的外观特点及功能特性和安装方法。

第2部分 SANGFOR AD 控制台的使用。该部分主要介绍如何管理 AD 设备以及正确的接线方式。

第3部分 SANGFOR AD 的功能介绍与配置方法。该部分主要介绍如何配置使用 AD 设备的各项功能。

第4部分 SANGFOR AD 的功能案例。该部分主要通过案例直观说明 AD 各项功能的实现。

本书约定

图形界面格式约定

文字描述	代替符号	举例
按钮	边框+阴影+底纹	“确定”按钮可简化为确定
菜单项	『 』	菜单项“系统设置”可简化为『系统设置』
连续选择菜单项及子菜单项	→	选择『系统设置』→『接口配置』
下拉框、单选框、复选框选项	[]	复选框选项“启用用户”可简化为[启用用户]
窗口名	【 】	如点击弹出【新增用户】窗口
提示信息	“ ”	提示框中显示“保存配置成功，配置已修改，需要重启DLAN 服务才能生效，是否立即重启该服务？”

各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：



小心、注意：提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。



警告：该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。



说明、提示、窍门：对操作内容的描述进行必要的补充和说明。

技术支持

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

深信服社区：bbs.sangfor.com.cn

深信服科技服务商及服务有效期查询：<http://bbs.sangfor.com.cn/plugin.php?id=service:query>

公司网址：www.sangfor.com.cn

致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

第1章 AD设备的安装

本部分主要介绍了 SANGFOR AD 系列产品的硬件安装。硬件安装正确之后，您才可以进行配置和调试。

1.1. 环境要求

AD 设备可在如下的环境下使用。

输入电压: 110V~230V

温度: 0~45°C

湿度: 5~90%

为保证系统能长期稳定地运行，应保证电源有良好的接地措施、防尘措施，保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

1.2. 电源

SANGFOR AD 系列产品使用交流 110V 到 230V 电源。在您接通电源之前，请保证您的电源有良好的接地措施。

1.3. 产品外观

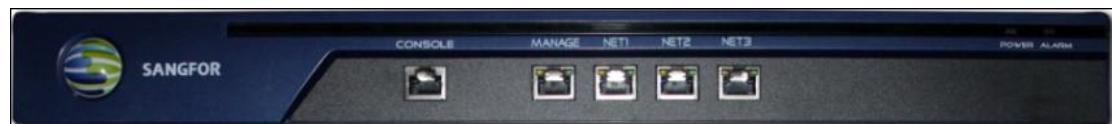


图 1 AD 网关面板（以 AD-1600 为例）

从左到右的指示灯分别是：

NET1 LINK: 用于显示 NET1 口线路连接情况

NET1 ACT: 对应显示 NET1 口数据流量情况

- NET2 LINK: 用于显示 NET2 口线路连接情况
- NET2 ACT: 对应显示 NET2 口数据流量情况
- NET3 LINK: 用于显示 NET3 口线路连接情况
- NET3 ACT: 对应显示 NET3 口数据流量情况
- MANAGE LINK: 用于显示 MANAGE 口线路连接情况
- MANAGE ACT: 对应显示 MANAGE 口数据流量情况
- POWER: AD 设备电源指示灯
- ALARM: AD 设备报警指示灯(设备启动时一分钟内长亮)



图片仅供参考，本系列其他型号产品的外观以实物为准。

1.4. 配置与管理

在配置网关之前，您需要配备一台电脑，配置之前请确定该电脑的网页浏览器（支持 IE、firefox 和 chrome 登陆）能正常使用，然后把电脑与 SANGFOR AD 连接在同一个局域网内，通过网络对设备进行配置。

1.5. 设备接线方式

在背板上连接电源线，打开电源开关，此时前面板的 Power 灯（绿色，电源指示灯）和 Alarm 灯（红色，告警灯）会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明网关正常工作。

请用标准的 RJ-45 以太网线将定义为 LAN 口的网口与内部局域网连接。



注意：如果还未定义过网口，需要先接 MANAGE 口才能进入 WEBUI，定义相应的网口后，才能从相应的网口接入 SANGFOR AD。配置方法参考 9.1 网络接口。

请用标准的 RJ-45 以太网线将定义为 WAN1 口的网口与 Internet 接入设备相连接，如路由器、光纤收发器或 ADSL Modem 等。



注意：多线路的AD设备可以支持多条Internet线路，此时将定义为WAN2口的网口与第二条Internet接入设备相连，定义为WAN3口的网口与第三条Internet线路相连，依此类推。



AD设备的WAN类别接口不支持ADSL拨号。



AD设备正常工作时POWER灯常亮，定义为WAN口和LAN口的网口LINK灯长亮，ACT灯在有数据流量时会不停闪烁。ALARM红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在安装时此红灯长亮，请将设备断电重启，重启之后若红灯一直长亮不能熄灭，请与我们联系。



定义为WAN口的网口连接路由器应使用交叉线；定义为LAN口的网口连接交换机应使用直通线、直接连接电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线序不同，如下图：

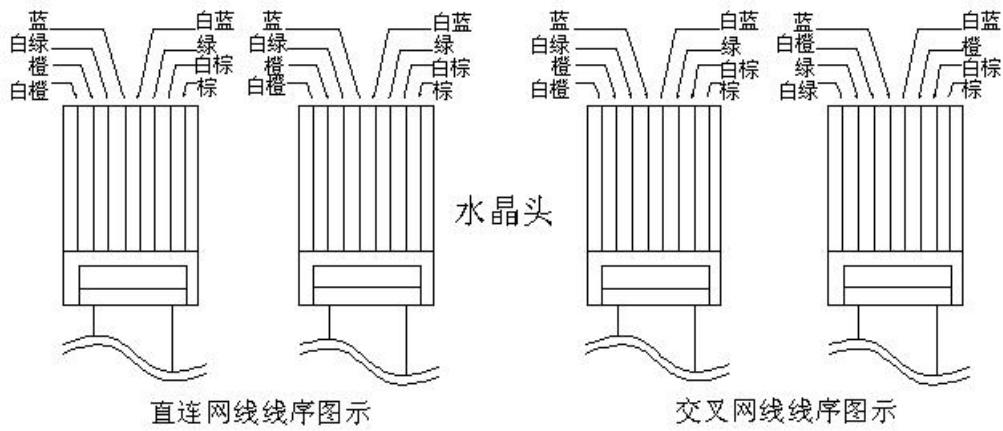


图 2 直连线、交叉线 线序

第2章 控制台的使用

2.1. 登陆 WEBUI 配置界面

按照前面所示方法接好线后（接 MANAGE 口），通过 WEB 界面来配置 SANGFOR AD 硬件设备。方法如下：

- 首先为本机器配置一个 10.252.252.X 网段的 IP（如配置 10.252.252.100），然后在浏览器（支持 IE、firefox 和 chrome 登陆）中输入网关的默认登陆 IP 及端口，输入 <https://10.252.252.252>，出现以下的界面：



在登陆框输入『用户名』和『密码』，点击**登录**按钮即可登录 AD 设备进行配置，默认情况下的用户名和密码均为 admin。

如果需要查看当前网关的版本号，点击**查看版本**，即显示当前设备的版本信息。



1.注意：如果还未定义过 LAN 口和 WAN 口，需要先接 MANAGE 口才能进入 WEBUI，定义相应的网口后，才能从相应的网口接入 SANGFOR AD。配置方法参考 9.1 网络接口。

2.MANAGE 口一共有两个出厂 IP 地址，10.252.252.252 和 10.254.254.254 。

2.2. 配置和使用

登录 WEBUI 配置界面后，可以看到以下配置模块：『系统概况』、『报表配置』、『公

『对象』、『应用负载』、『智能 DNS』、『路由设置』、『网络配置』、『系统配置』、『配置向导』、『高可用性』。



配置界面中如果有**更新**按钮，则配置完毕后，一定需要点击该按钮才能把设置保存到设备中，后面的文档不再赘述。

主页欢迎界面包括功能模块说明和用户反馈两个部分。同时系统主页有相应的高危漏洞提示，可以在系统概况下查看到具体内容。

功能模块说明可以快速了解相应模块功能。



用户反馈模块方便您的意见及建议反馈给我们。



深信服，让IT更简单，更安全，更有价值

功能模块说明 | 用户反馈 | 意见及建议反馈

尊敬的客户：

感谢您选择我们的设备为您的业务提供支持，如果您在使用过程中遇到任何问题或是对产品有好的意见和建议，可以发送电子邮件到：

ad_suggestion@sangfor.com.cn

我们将及时对您的反馈进行处理，以提供更好的产品和服务给广大客户，谢谢您的支持。

第3章 系统概况

『系统概况』用于查看AD设备的当前使用状态，虚拟服务状态，链路及服务器状态，以及系统日志查看。包括『活动查看』、『虚拟服务详情』、『智能DNS统计』、『DDOS攻击分析』、『集群状态』、『实时漏洞分析』、『链路状态』、『节点状态』、『接口状态』、『DNS状态』、『全局状态』、『动态路由表』、『日志查看』、『调试信息统计』几个部分。

界面如下图所示：



3.1. 活动查看

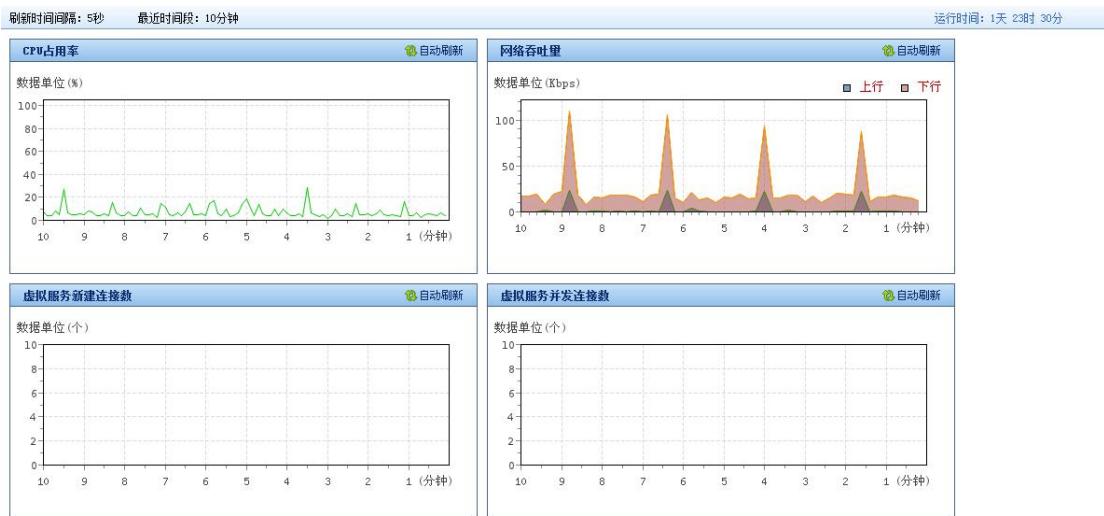
『活动查看』用于查看AD的实时状态、网络的实时状态等，包括『系统状态』、『资源占用率』、『网络吞吐量』、『连接数』、『SSL TPS』、『HTTP TPS』。

3.1.1. 系统状态

WEBUI路径：『系统概况』→『活动查看』→『系统状态』。

『系统状态』用于实时显示AD设备的CPU占用率、网络吞吐量、虚拟服务新建连接数、虚拟服务并发连接数，同时在界面右上角可以查看设备运行时间。

界面如下图所示：



点击**自动刷新**，可以切换到禁止自动刷新。

3.1.2. 资源占用率

WEBUI 路径：『系统概况』→『活动查看』→『资源占用率』。

『资源占用率』用于实时显示 AD 设备的 CPU 占用率和内存利用率，便于客户了解 AD 设备的使用状况。其中 CPU 占用率分别显示所有 CPU 和单个 CPU 核心的占用率。

界面如下图所示：



『最近时间段』用于设置显示 CPU 占用率最近多长时间内的数据，可选择[1 小时]、[1 天]或者[1 周]。

『自动刷新』每隔 5 秒自动刷新一次。点击**自动刷新**，可以切换到禁止自动刷新。

3.1.3. 网络吞吐量

WEBUI 路径：『系统概况』→『活动查看』→『网络吞吐量』。

『网络吞吐量』用于显示实时的网络上下行流量。

界面如下图所示：



『最近时间段』用于设置显示网络吞吐量最近多长时间内的数据，可选择[1 小时]、[1 天]或者[1 周]。

『网口』可以选择查看所有网口，设备流量和 WAN 口的流量。

『自动刷新』每隔 5 秒自动刷新一次。

3.1.4. 连接数

WEBUI 路径：『系统概况』→『活动查看』→『连接数』。

『连接数』用于显示实时的网络连接数，包括设备连接数、客户端连接数和服务端连接数。

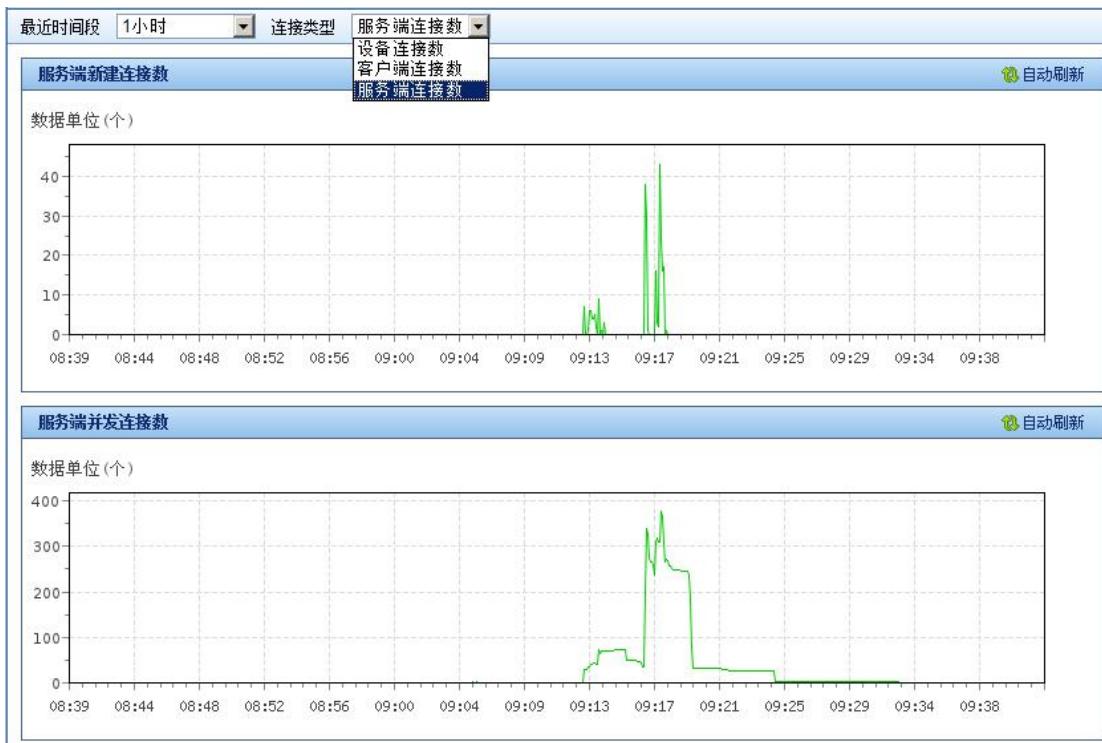
设备连接数包括系统连接数、系统并发连接数、虚拟服务新建连接数、虚拟服务并发连接数等。



客户端连接数包括客户端新建连接数、客户端并发连接数。



服务端连接数包括服务端新建连接数、服务端并发连接数。



『最近时间段』用于设置显示连接数最近多长时间内的数据，可选择[1 小时]、[1 天]或者[1 周]。

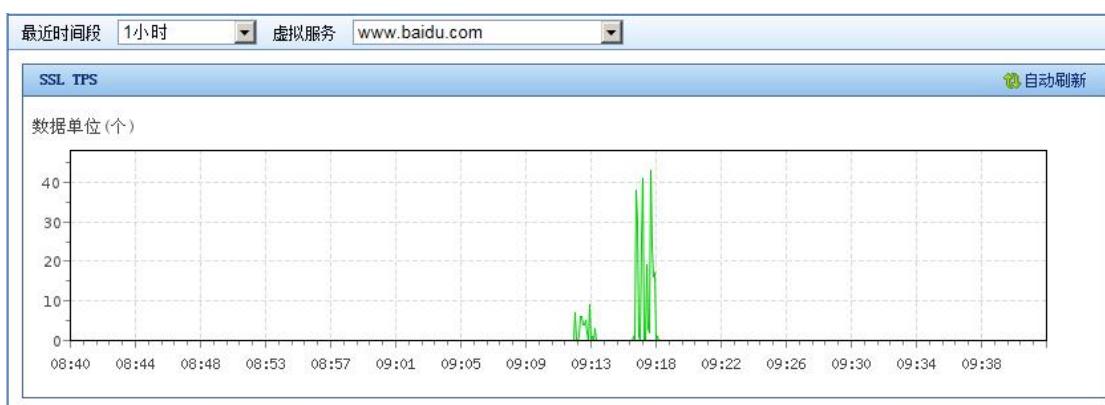
『自动刷新』每隔 5 秒自动刷新一次，点击可以禁用自动刷新。

3.1.5. SSL TPS

WEBUI 路径：『系统概况』→『活动查看』→『SSL TPS』。

『SSL TPS』用来显示 SSL 客户端的连接建立情况。

界面如下图所示：



『最近时间段』用于设置显示最近多长时间内的数据，可选择[1 小时]、[1 天]或者[1 周]。

『虚拟服务』用来选择需要查询的虚拟服务。

『自动刷新』每隔 5 秒自动刷新一次。

3.1.6. HTTP TPS

WEBUI 路径：『系统概况』→『活动查看』→『HTTP TPS』。

『HTTP TPS』用来显示 HTTP 客户端的连接建立情况。

界面如下图所示：



『最近时间段』用于设置显示最近多长时间内的数据，可选择[1 小时]、[1 天]或者[1 周]。

『虚拟服务』用来选择需要查询的虚拟服务。

『自动刷新』每隔 5 秒自动刷新一次。

3.2. 虚拟服务详情

『虚拟服务详情』用于查看虚拟服务的状态，缓存和流量情况等，包括『虚拟服务状态』、『缓存/流量状态』、『缓存查询』、『缓存缺失原因』、『URL 次数统计』、『URL 实时流量』。

3.2.1. 虚拟服务状态

WEBUI 路径：『系统概况』→『虚拟服务详情』→『虚拟服务状态』。

『虚拟服务状态』用来显示虚拟服务可用的链路情况，可用的节点池情况，以及客户端和服务端连接数的情况，相关状态可以根据需要勾选显示在列表。

界面如下图所示：



The screenshot shows the 'Virtual Service Status' page. On the left is a vertical navigation menu with sections like 'System Overview', 'Virtual Service Details', 'Smart DNS Design', 'DDoS Attack Analysis', 'Cluster Status', 'Link Status', 'Node Status', 'Interface Status', 'DNS Status', and 'Global Status'. The main content area has tabs at the top: 'Virtual Service Status', 'Cache/Flow Status', 'Cache Query', 'Cache Miss Reason', 'URL Frequency Statistics', and 'URL Real-time Traffic'. Below the tabs, there is a table with columns: 'Virtual Service', 'Status', 'Available Path', 'Available Node Pool', 'Client Connection Count', 'Established Connections', and 'Connection Reuse Rate'. The table contains three rows: 'ddos_test' (Enabled, 0/0 path, 1/1 pool, 0 clients, 0 established, -- reuse), 'aaa' (Enabled, 0/0 path, 0/1 pool, 0 clients, 0 established, -- reuse), and 'test-' (Enabled, 1/1 path, 0/1 pool, 0 clients, 0 established, -- reuse).

『虚拟服务』显示AD设备上配置的虚拟服务，点击虚拟服务名称可跳转到虚拟服务配置页面。

『状态』显示该虚拟服务是启用或者禁用。

『可用链路』显示该虚拟服务关联的线路总数以及当前可用的链路数。点击可跳转到对应的链路状态页面。

『可用节点池』显示该虚拟服务关联的节点池总数以及当前可用的节点池。点击可跳转到对应的节点池状态页面。

『客户端连接数』显示该虚拟服务的客户端连接数。

『并发连接数』显示该虚拟服务的并发连接数。

『连接数复用率』显示该虚拟服务的连接复用情况。

『自动刷新』每隔5秒自动刷新一次。

3.2.2. 缓存/流量状态

WEBUI路径：『系统概况』→『虚拟服务详情』→『缓存/流量状态』。

『缓存/流量状态』用来显示缓存命中的比率，缓存空间使用率和流量优化情况。

界面如下图所示：



『最近时间段』用于设置显示最近多长时间内的数据，可选择[1 小时]、[1 天]或者[1 周]。

『虚拟服务』用来选择需要查询的虚拟服务。

『清空流量』用来清空设备中的流量统计表。

『清空缓存』用来清空设备中的缓存数据。

『自动刷新』每隔 5 秒自动刷新一次。

3.2.3. 缓存查询

WEBUI 路径：『系统概况』→『虚拟服务详情』→『缓存查询』。

『缓存查询』用来查询虚拟服务中的某个 URL 是否被 AD 设备缓存的情况。

界面如下图所示：

虚拟服务		-- 所有 --		URL匹配 *		查询	
URL	压缩类型	文件类型	内容大小	超时时间	更新时间	命中次数	
www.baidu.com	NORMAL	text/html	514B	2014/04/10 11:16:51	1970/01/01 07:59:59	0	
www.cms.com	NORMAL	text/html	32.53KB	2014/04/10 11:53:27	2014/04/09 18:19:45	30	
www.cms.com	GZIP	text/html	11.11KB	2014/04/10 11:53:27	2014/04/09 18:19:45	0	
www.cms.com	DEFLATE	text/html	11.1KB	2014/04/10 11:53:27	2014/04/09 18:19:45	0	
www.cms.com	NORMAL	text/html	28.81KB	2014/04/10 18:17:41	2014/02/27 17:15:15	20	
www.cms.com	GZIP	text/html	10.18KB	2014/04/10 18:17:41	2014/02/27 17:15:15	0	
www.cms.com	DEFLATE	text/html	10.16KB	2014/04/10 18:17:41	2014/02/27 17:15:15	0	
www.cms.com	NORMAL	text/html	40.85KB	2014/04/10 18:17:42	2014/04/03 16:57:36	23	
www.cms.com	GZIP	text/html	14.3KB	2014/04/10 18:17:42	2014/04/03 16:57:36	0	
www.cms.com	DEFLATE	text/html	14.29KB	2014/04/10 18:17:42	2014/04/03 16:57:36	0	
www.cms.com	NORMAL	text/html	30.75KB	2014/04/10 18:17:48	2014/04/03 10:51:21	15	
www.cms.com	GZIP	text/html	10.71KB	2014/04/10 18:17:48	2014/04/03 10:51:21	0	
www.cms.com	DEFLATE	text/html	10.69KB	2014/04/10 18:17:48	2014/04/03 10:51:21	0	

『虚拟服务』用来选择需要查询的虚拟服务。

『URL 匹配』输入需要查询的 URL 地址，支持通配符。

点击 **查询**，显示缓存查询结果。缓存查询结果最多显示 10000 条。

3.2.4. 缓存缺失原因

WEBUI 路径：『系统概况』→『虚拟服务详情』→『缓存缺失原因』。

『缓存缺失原因』用来统计一段时间内某 URL 未缓存的次数和不可缓存的原因。

界面如下图所示：

虚拟服务		www.baidu.co	源IP	URL匹配条件 *	终止统计	统计中...	刷新时间
序号	URL				缺失次数	缓存缺失原因详情	
1	www.baidu.com/wordpress/?cat=1				1	<应答方向>状态码错误…	
2	www.baidu.com/wordpress/wp-login.php				2	<应答方向>状态码错误…	
3	www.baidu.com/wordpress/?m=201404				2	<应答方向>状态码错误…	
4	www.baidu.com/wordpress/?p=1				2	<应答方向>状态码错误…	
5	www.baidu.com/wordpress/wp-login.php?action=register				1	<应答方向>状态码错误…	

『虚拟服务』用来选择需要查询的虚拟服务。

『源 IP』访问虚拟服务的源 IP 地址。

『URL 匹配条件』输入需要查询的 URL 地址，支持通配符。

点击**开始统计**，则开始统计访问该 URL 无法缓存的情况，统计结束后，需要点击**终止统计**结束统计并显示最终统计结果。

『刷新时间间隔』每隔 5 秒自动刷新一次。

3.2.5. URL 次数统计

WEBUI 路径：『系统概况』→『虚拟服务详情』→『URL 次数统计』。

『URL 次数统计』用来显示访问虚拟服务中某个节点池的 HTTP 服务器的 URL 情况。

界面如下图所示：

URL 次数统计					
序号	URL	访问次数	超时次数	应答结果	响应状态
1	www.baidu.com/	7	0	301:7	最快...
2	www.baidu.com/wordpress/wp-login.php	5	5	无	最快...
3	www.baidu.com/wordpress/wp-login.php?ac...	5	5	无	最快...
4	www.baidu.com/wordpress/?m=201404	4	4	无	最快...
5	www.baidu.com/wordpress/?cat=1	3	3	无	最快...
6	www.baidu.com/wordpress/?p=1	2	2	无	最快...

『统计时长』用于设置显示统计最近多长时间内的数据。

『虚拟服务』用来选择需要查询的虚拟服务。

『节点池』用来选择需要查询的节点池。

『统计长度』用来设置此长度范围以内的 URL 相同的访问，统计到同一个 URL。

『源 IP』用来设置指定客户端的源 IP 进行统计。

设置好统计条件后，点击**开始统计**，进行访问 URL 次数情况统计。点击排除列表，页

面跳转到配置排除页面，可以添加不需要进行统计的 URL。完成添加后，点击完成保存。

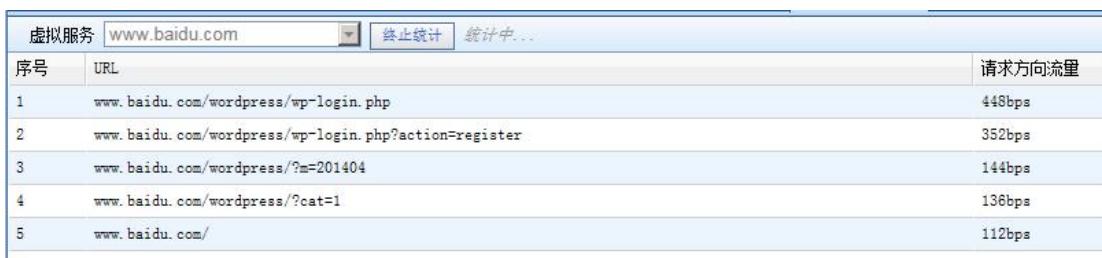


3.2.6. URL 实时流量

WEBUI 路径：『系统概况』→『虚拟服务详情』→『URL 实时流量』。

『URL 实时流量』用来显示 HTTP 和 HTTPS 的虚拟服务的 URL 实时流量情况。

界面如下图所示：



序号	URL	请求方向流量
1	www.baidu.com/wordpress/wp-login.php	448bps
2	www.baidu.com/wordpress/wp-login.php?action=register	352bps
3	www.baidu.com/wordpress/?m=201404	144bps
4	www.baidu.com/wordpress/?cat=1	136bps
5	www.baidu.com/	112bps

『虚拟服务』用来选择需要查询的虚拟服务。适用于 HTTPS 或 HTTP 类型的虚拟服务。

点击开始统计，则开始统计访问虚拟服务的 URL 流量情况，点击终止统计，显示统计结果。

3.3. 智能 DNS 统计

『智能 DNS 统计』用于查看 DNS 的实时状态等，包括『域名实时请求』、『域名历史请求』、『DNS 请求数』、『LDNS 来源』、『LDNS 缺失记录』。

3.3.1. 域名实时请求

WEBUI 路径：『系统概况』→『智能 DNS 统计』→『域名实时请求』。

『域名实时请求』用来显示每秒每域名的请求总数。

界面如下图所示：

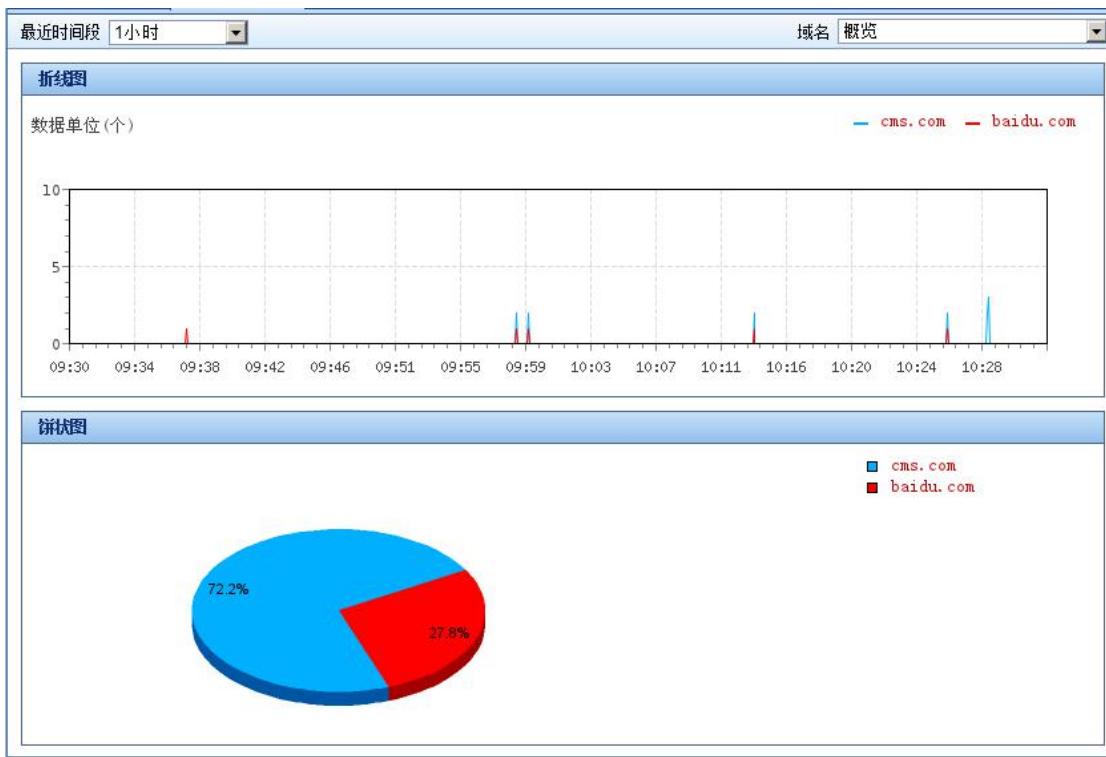
域名	次/秒
概览	7
www.cms.com	7
192.200.200.115	7

3.3.2. 域名历史请求

WEBUI 路径：『系统概况』→『智能 DNS 统计』→『域名历史请求』。

『域名历史请求』用来显示统计每域名的历史请求总数。

界面如下图所示：



『最近时间段』用于设置显示最近多长时间内的数据，可选择[1 小时]、[1 天]或者[1 周]。

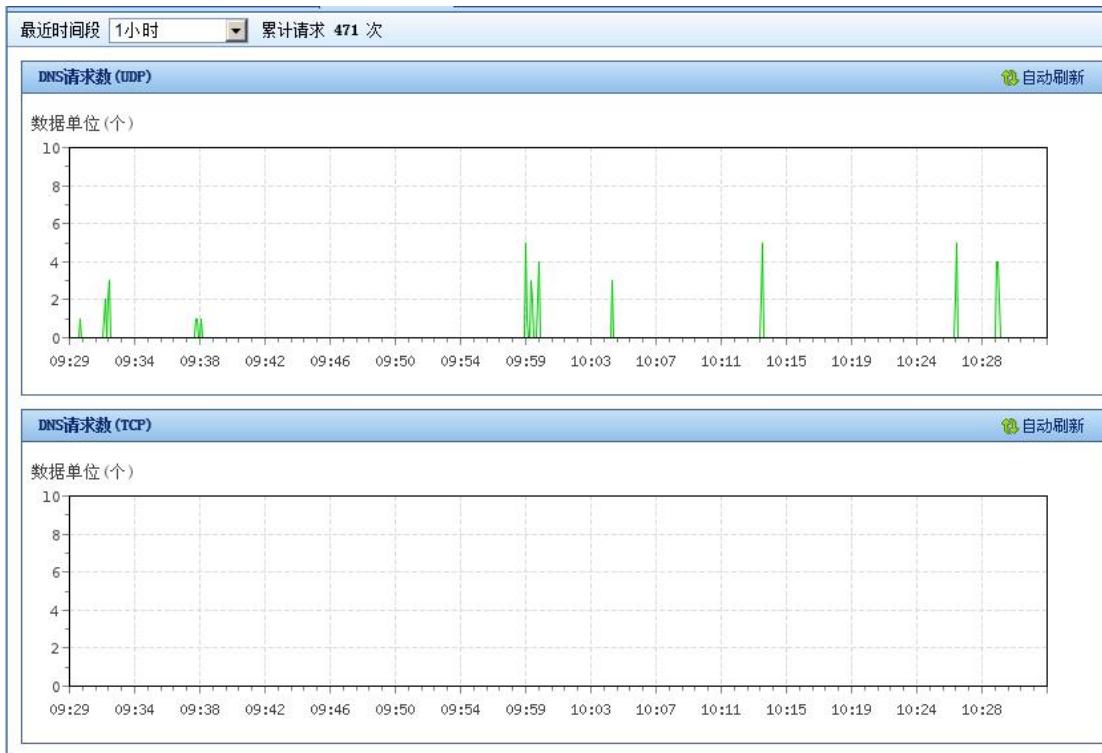
『域名』用于设置统计哪个域名的历史请求总数。

3.3.3. DNS 请求数

WEBUI 路径：『系统概况』→『智能 DNS 统计』→『DNS 请求数』。

『DNS 请求数』用来显示统计 DNS 的请求总数。

界面如下图所示：



3.3.4. LDNS 来源

WEBUI 路径：『系统概况』→『智能 DNS 统计』→『LDNS 来源』。

『LDNS 来源』用来显示统计每秒钟 DNS 请求的 LDNS 来源和访问次数。

界面如下图所示：

次数单位: 次/秒		
源IP	请求次数 ↓	操作
192.200.200.115	3	封锁 解除

3.3.5. LDNS 缺失记录

WEBUI 路径：『系统概况』→『智能 DNS 统计』→『LDNS 缺失记录』。

『LDNS 缺失记录』用来显示 ISP 地址池中缺失的 LDNS 记录。需要启用报表才能查看数据。

界面如下图所示：

查询时间段:		2014-04-03 10:33	-	2014-04-10 10:33	<input type="button" value="查询"/>	<input type="button" value="清空"/>
记录时间	源IP	不明确信息类别				
2014-04-10 10:31:00	192.200.200.115	ISP地址集	用户地域			
2014-04-10 10:31:00	172.16.253.142	ISP地址集	用户地域			
2014-04-10 10:28:00	192.200.200.115	ISP地址集	用户地域			
2014-04-10 10:26:00	172.16.253.142	ISP地址集	用户地域			
2014-04-10 10:25:00	192.200.200.115	ISP地址集	用户地域			
2014-04-10 10:21:00	192.200.200.115	ISP地址集	用户地域			

3.4. DDOS 攻击分析

『DDOS 攻击分析』用于对七层 DDOS 攻击情况进行分析，包括『七层 DDOS 分析』、『七层 DDOS 统计』两部分。

3.4.1. 七层 DDOS 分析

WEBUI 路径：『系统概况』→『DDOS 攻击分析』→『七层 DDOS 分析』。

『七层 DDOS 分析』用于对七层 DDOS 攻击情况进行分析，显示源 IP 攻击排行 TOP10，作为 ACL 限制的参考；另外显示攻击记录详情，对应时间，虚拟服务，攻击源 IP，攻击类型，攻击 URL，攻击次数，防护动作等，其中点击防护动作内容，跳转到相应策略中。

界面如下图所示：



序号	时间	虚拟服务	攻击源IP	攻击类型	攻击URL	攻击次数	防护动作
1	17:22:49	ddos_test	200.200.80.157	泛洪攻击	200.200.144.215/	507520	告警并拦截
2	17:12:48	ddos_test	200.200.80.157	泛洪攻击	200.200.144.215/	1580420	告警并拦截
3	17:04:44	ddos_test	200.200.80.157	泛洪攻击	200.200.144.215/	1298769	告警并拦截

『日期』用于选择分析的日期，选择范围一周内。

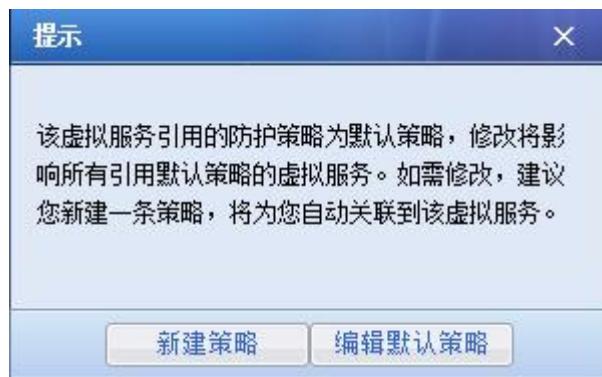
『虚拟服务』用于选择需要进行分析的虚拟服务。

点击**更新数据**，可以进行数据当前数据的更新。

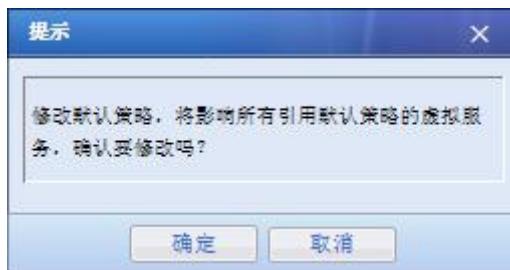
点击**清除记录**，可以删除当前的记录。

点击**导出日志**，可以导出日志，进行详细分析。

点击**防护动作**，当这条记录的虚拟服务引用的防护策略为默认策略时，弹出此提示框，提醒用户，修改默认策略将影响所有引用默认策略的虚拟服务，提供“新建策略”和编辑“默认策略”供用户选择。（“新建策略”和编辑“默认策略”详见 6.7.4 配置）



提示：如果选择“编辑默认策略”，将跳转至默认的 HTTP 防护策略编辑页面，用户可根据实际业务需求填写配置；点击“完成”时，弹出提示框，再次和用户确认是否修改默认配置，用户可根据实际需求选择。

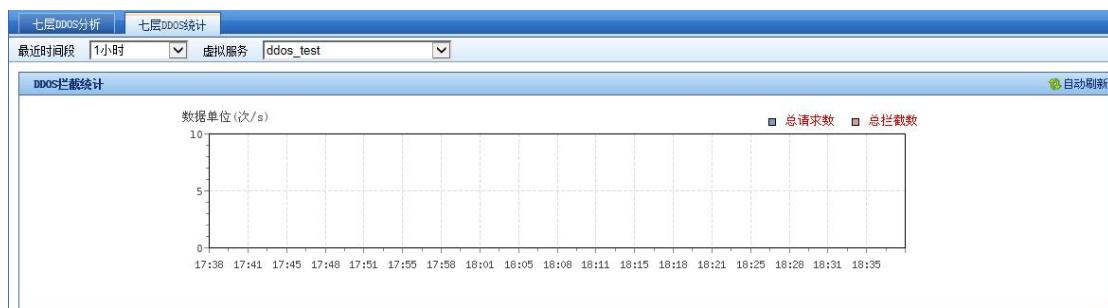


3.4.2. 七层 DDOS 统计

WEBUI 路径：『系统概况』→『DDOS 攻击分析』→『七层 DDOS 统计』。

『七层 DDOS 统计』用于对七层 DDOS 攻击情况进行统计，用户可根据 DDoS 统计页面查看 AD 设备帮助用户拦截攻击的趋势，可根据趋势调整防护策略的配置。

界面如下图所示：



『最近时间段』用于设置显示最近多长时间内的数据，可选择[1 小时]、[1 天]或者[1 周]。

『虚拟服务』用来选择需要查询的虚拟服务。

『刷新时间间隔』每隔 5 秒自动刷新一次。

3.5. 集群状态

WEBUI 路径：『系统概况』→『集群状态』。

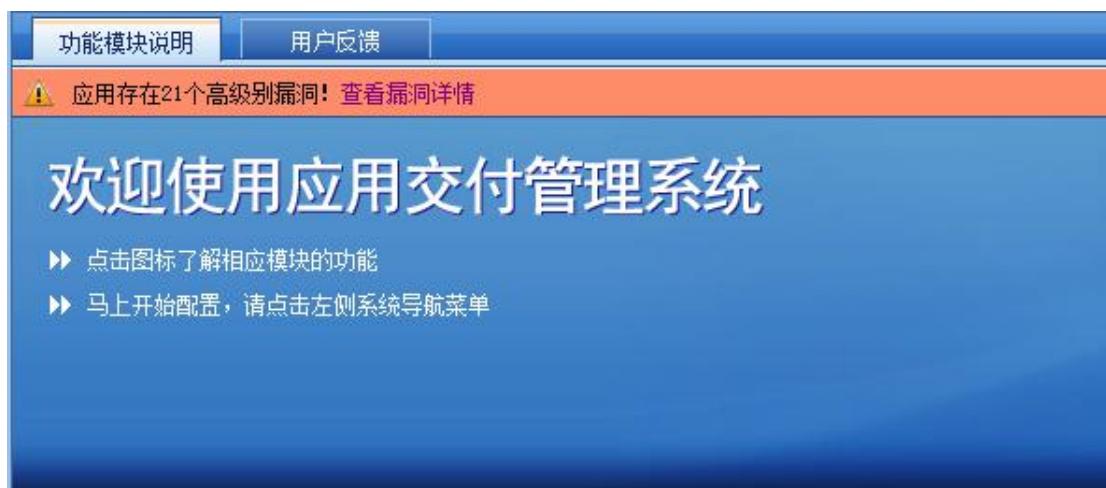
只有启用集群后，『集群状态』才会显示，可以看到设备应用组状态。

设备应用组状态	
刷新时间间隔：5秒	
名称	角色
Default	生效
Group-11	生效
Group-12	备份

3.6. 实时漏洞分析

WEBUI 路径：『系统概况』→『实时漏洞分析』。

系统主页有相应的高危漏洞提示，可以在系统概况下『实时漏洞分析』查看到具体内容。



界面如下图所示：

实时漏洞分析											
虚拟服务 全部		更新数据	清除数据	导出报告							
漏洞统计											
发现漏洞		41 个									
风险等级		高 21个 中 18个 低 2个									
漏洞列表											
序号	最近发现时间	虚拟服务	节点	漏洞名称	风险等级	详情					
1	2015-05-26 20:23:55	CMS	192.200.200.162	[15090014]DedeCMS 3.5.6 上传webshell漏洞	高	查看					
2	2015-05-26 20:23:55	CMS	192.200.200.162	[15090018]DedeCMS 6 XSS漏洞	高	查看					
3	2015-05-26 20:23:55	CMS	192.200.200.162	[15090017]DedeCMS 6 SQL注入漏洞	高	查看					
4	2015-05-26 20:23:55	CMS	192.200.200.162	[15090005]DedeCMS本地文件包含漏洞	高	查看					
5	2015-05-26 20:23:55	CMS	192.200.200.162	[15090007]DedeCMS SQL注入漏洞	高	查看					
6	2015-05-26 20:23:55	CMS	192.200.200.162	[15090008]DedeCMS 0-5 6 XSS漏洞	高	查看					
7	2015-05-26 20:23:55	CMS	192.200.200.162	[15090009]DedeCMS越权访问漏洞	高	查看					
8	2015-05-26 20:23:55	CMS	192.200.200.162	[15090010]DedeCMS 6 远程文件删除漏洞	高	查看					
9	2015-05-26 20:23:55	CMS	192.200.200.162	[15090015]DedeCMS SQL注入漏洞	高	查看					
10	2015-05-26 20:23:55	CMS	192.200.200.162	[15090012]DedeCMS 5 WebShell上传漏洞	高	查看					
11	2015-05-26 20:23:55	CMS	192.200.200.162	[15090013]DedeCMS 0-5 6 模板执行漏洞	高	查看					
12	2015-05-26 20:23:55	CMS	200.200.0.20	[15010033]Apache存在拒绝服务 (CVE-2009-1890)	高	查看					
13	2015-05-26 20:23:55	CMS	192.200.200.162	[15090011]DedeCMS 6 SQL注入漏洞	高	查看					
14	2015-05-26 20:23:55	CMS	200.200.0.20	[15010037]Apache 存多个漏洞 (CVE-2011-3192)	高	查看					
15	2015-05-26 20:23:55	CMS	200.200.0.20	[15010044]Apache HTTP 服务器存在拒绝服务 (CVE-2011-3192)	高	查看					

漏洞分为高，中，低三个风险等级，有不同高亮颜色用于区分。点击查看可以了解详细的漏洞描述及解决方案。

描述：

当前被发现风险的主机正在运行DedeCMS5.3/5.6版本，这两个版本存在一个上传webshell漏洞，由于/member/uploads_edit.php对用户上传过滤不严，导致攻击者可以上传webshell。

解决方案：

升级到织梦系统5.7或者更高的版本。
建立WAF防御策略，并开启云分析引擎。

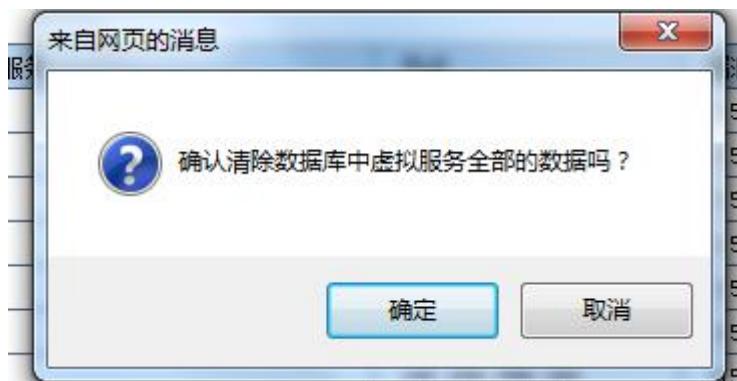
- * [推荐部署深信服下一代防火墙](#)

[更多信息请导出报告查看](#)

『虚拟服务』用来选择需要查询的虚拟服务。

点击[更新数据](#)，可以进行实时漏洞的更新。

点击[清除数据](#)，可以清除数据库中虚拟服务全部的数据。



点击[导出报表](#)，导出报告后，可以看到命中规则的关键部位会进行高亮处理，并且提供相应的解决方案，报告格式html，报告提供服务器视图、风险视图两种风险分析模式。

服务器安全风险分析报告

分析时间：截至 2015-05-28 19:12:38

虚拟服务：VS-11, CMS

服务器视图	2
节点信息	3
详情	3
风险视图	2
风险概况	3
详情	3

服务器视图 风险视图

节点信息

节点总数：3
风险总数：41

服务器漏洞风险排行前10



192.200.200.162
200.200.0.20

详情

192.200.200.162(26)

Apache httpd漏洞

风险 (1/14): Apache存在拒绝服务 (CVE-2009-1890)

应用信息	Apache httpd 2.2.9
协议	TCP
端口	80
服务类型	HTTP
实时漏洞分析规则ID	15010033
危险等级	高
CVE编号	CVE-2009-1890
最近一次发现时间	2015-05-28 20:23:54

详细信息

当前被发现风险的主机上安装的Apache版本小于2.2.12，存在以下风险问题：

CVE-2009-1890：在‘mod_proxy’模块的拒绝服务漏洞可能被利用导致消耗大量cpu资源，进而造成拒绝服务。

解决方案

方法1：升级到 Apache 2.2.12 或者更高的版本。

* 推荐部署深信服下一代防火墙

检测过程

```
RESPONSE:  
HTTP/1.1 302 Found  
Date: Tue, 26 May 2015 12:31:08 GMT  
Server: Apache/2.2.9 (APMServ) PHP/5.2.6
```

3.7. 链路状态

WEBUI 路径：『系统概况』→『链路状态』。

『链路状态』用于显示外网链路的流量及状态信息。

界面如下图所示：

所有链路状态		虚拟服务链路状态		
刷新时间间隔：5秒				
类别	名称	上行流量	下行流量	状态
WAN	wan4	0.60Kbps	69.07Kbps	正常
LAN	lan2	0.21Kbps	68.15Kbps	正常
LAN	vlan	0.00Kbps	0.00Kbps	正常

3.7.1. 所有链路状态

WEBUI 路径：『系统概况』→『链路状态』→『所有链路状态』。

『所有链路状态』用于显示全部链路的流量及状态信息。

界面如下图所示：

所有链路状态		虚拟服务链路状态		
刷新时间间隔：5秒				
类别	名称	上行流量	下行流量	状态
WAN	wan4	0.60Kbps	69.07Kbps	正常
LAN	lan2	0.21Kbps	68.15Kbps	正常
LAN	vlan	0.00Kbps	0.00Kbps	正常

『刷新时间间隔』用于显示链路状态的信息间隔多长时间刷新一次，默认[5秒]。

『名称』显示的是所有链路的名称，链路的配置请参考 9.1 网络接口的相关说明。

『上行流量』、『下行流量』用于显示各条链路的实时上下行流量。

『正常』、『繁忙』、『离线』、『禁用』分别用于显示各条链路的状态：

当链路显示“繁忙”状态时，说明此链路的流量达到了带宽繁忙比例，此带宽繁忙比例的设置请参考 9.1 网络接口的设置。

当链路显示“离线”状态时，说明链路此时不可用。

当链路显示“禁用”状态时，说明链路已经被管理员禁用了，禁用链路的设置请参考 9.1 网络接口的设置。

3.7.2. 虚拟服务链路状态

WEBUI 路径：『系统概况』→『链路状态』→『虚拟服务链路状态』。

『虚拟服务链路状态』用于显示虚拟服务对应的各条外网链路的流量情况。

界面如下图所示：

刷新时间间隔: 5秒 虚拟服务: www.baidu.com			
名称	上行流量	下行流量	状态
WAN253	29.49Kbps	8.85Kbps	正常
WAN254	0.00Kbps	0.00Kbps	正常

『刷新时间间隔』用于显示链路状态的信息间隔多长时间刷新一次，默认[5秒]。

『虚拟服务』用来选择需要查询的虚拟服务。虚拟服务设置请参 3.7.8 虚拟服务设置。

『上行流量』、『下行流量』用于显示此虚拟服务占用的外网链路的上、下行流量。

『正常』、『繁忙』、『离线』分别用于显示各虚拟服务对应的链路状态情况。

3.8. 节点状态

WEBUI 路径：『系统概况』→『节点状态』。

『节点状态』用于显示节点的状态信息。

界面如下图所示：

节点池	状态	新建连接数	并发连接数 (established)	节点总计	正常	繁忙	离线/禁用
NODE	有效	0	0	1	1	0	0
mysql-master	有效	0	0	1	1	0	0
mysql-slave	有效	0	0	2	2	0	0
httpd	有效	0	0	3	3	0	0

3.8.1. 节点池状态

WEBUI 路径：『系统概况』→『节点状态』→『节点池状态』。

『节点池状态』用于显示各个节点池的状态，如在线节点个数、繁忙节点个数等。

界面如下图所示：

节点池状态							
刷新时间间隔: 5秒							
节点池	状态	新建连接数	并发连接数 (established)	节点总计	正常	繁忙	离线/禁用
ddos_test_pool	有效	0	0	2	1	0	1
pool_local	无效	0	0	1	0	0	1
test-pool-166	无效	0	0	1	0	0	1

『刷新时间间隔』用于显示链路状态的信息间隔多长时间刷新一次，默认[5秒]。

『节点池』用于显示节点池的名称。

『节点总计』用于显示此节点池中包含的节点数。

『并发连接数』用于显示此节点池中包含的并发连接数。

『正常』、『繁忙』、『禁用』等用于显示节点池中节点的各个状态：

[正常]：表示节点可以正常连接，

[繁忙]：表示使用 SNMP 监视器时，监视的节点服务器 CPU、内存、磁盘占用超过阀值等情况。

[禁用]：表示节点被控制台用户手动禁用了。

[禁用，正在软关机]：表示该节点不再接受新连接。

[禁用，软关机完成]：表示该节点无连接。

[正常，温暖上线]：表示该新节点上线，缓慢接受新连接。

[网络不可用]：表示该节点网络不可达。

3.8.2. 节点状态

WEBUI 路径：『系统概况』→『节点状态』→『节点状态』。

『节点状态』用于显示节点池中各节点的连接数以及状态信息。

界面如下图所示：

节点池状态						
节点状态		调度查询				
刷新时间间隔：5秒		节点池		所有节点池		
节点	并发连接数 (established)	下行流量	上行流量	状态	操作	所属节点池
10.10.10.180:80	0	0.00Kbps	0.00Kbps	正常	--	NODE
10.10.10.181:3306	0	0.00Kbps	0.00Kbps	正常	--	mysql- master
10.10.10.182:3306	0	0.00Kbps	0.00Kbps	正常	--	mysql- slave
10.10.10.183:3306	0	0.00Kbps	0.00Kbps	正常	--	mysql- slave
10.10.10.181:80	0	0.00Kbps	0.00Kbps	正常	--	httpd
10.10.10.182:80	0	0.00Kbps	0.00Kbps	正常	--	httpd
10.10.10.183:80	0	0.00Kbps	0.00Kbps	正常	--	httpd

『刷新时间间隔』用于显示链路状态的信息间隔多长时间刷新一次，默认[5秒]。

『节点池』用于选择需要查看的节点池。

『节点』用于显示节点 IP 地址。

『连接数』用于显示连接到节点的连接数。

『上行流量』显示服务端节点发送的流量

『下行流量』显示服务端节点接收的流量

『正常』、『繁忙』、『禁用』、『禁用，正在软关机』、『禁用，软关机完成』、『正常，温暖上线』、『网络不可用』用于显示节点池中节点的状态，具体含义请参考 3.8.1 节点池状态。

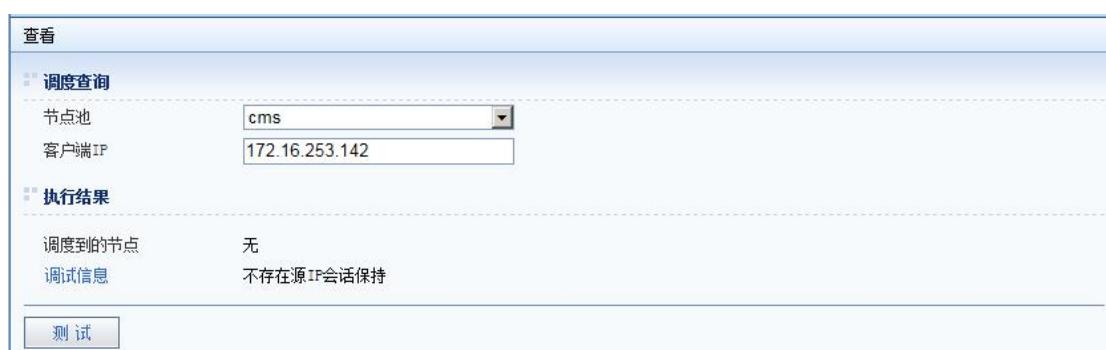
点击**刷新**，可用于手动刷新显示所选节点状态的图形。

3.8.3. 调度查询

WEBUI 路径：『系统概况』→『节点状态』→『调度查询』。

『调度查询』用于查询客户端 IP 的访问被调度到哪个节点。

界面如下图所示：



调度查询	
节点池	cms
客户端IP	172.16.253.142

执行结果	
调度到的节点	无
调试信息	不存在源IP会话保持

测试

『节点池』用于选择需要查看的节点池。

『客户端 IP』设置需要查询的客户端 IP 地址。

点击**测试**，则可查询到该客户端 IP 地址的访问被调度到节点池的那个节点。



客户端 IP 支持 IPV4 和 IPV6 地址。

3.9. 接口状态

WEBUI 路径：『系统概况』→『接口状态』。

『接口状态』用于显示设备网口的状态信息，包括上下行数据量、数据包等信息。

界面如下图所示：

接口状态							
刷新时间间隔: 5秒							
接口名称	下行数据	上行数据	下行数据包	上行数据包	下行错误包	上行错误包	下行丢弃包
eth7	0B	0B	0	0	0	0	0
eth8	0B	0B	0	0	0	0	0
eth0	0B	0B	0	0	0	0	0
eth1	168.62MB	38.95MB	289.39K	187.94K	0	0	0
eth2	15.17MB	68.64MB	185.94K	109.31K	0	0	0
eth3	12.39MB	59.56MB	155.94K	70.51K	0	0	0
eth4	0B	0B	0	0	0	0	0
eth5	0B	0B	0	0	0	0	0
bond0	0B	0B	0	0	0	0	0
bond1	0B	0B	0	0	0	0	0
bond2	0B	0B	0	0	0	0	0
bond3	0B	0B	0	0	0	0	0

3.10. DNS 状态

WEBUI 路径：『系统概况』→『DNS 状态』。

『DNS 状态』用于显示 DNS 服务的状态信息。DNS 状态需要启用 DNS 代理才能显示数据，配置见 9.5 章节。

界面如下图所示：

DNS状态		
刷新时间间隔: 5秒		
DNS服务器	网络接口	状态
192.200.200.253	WAN253	正常
192.200.200.199	WAN254	正常

『刷新时间间隔』用于显示 DNS 服务器状态的信息间隔多长时间刷新一次，默认[5 秒]。

『DNS 服务器』用于显示 DNS 服务器的 IP 地址。

『网络接口』用于显示 DNS 服务器所在的网络接口。

『状态』用于显示 DNS 的状态信息。

3.11. 全局状态

WEBUI 路径：『系统概况』→『全局状态』。

『全局状态』用于显示智能 DNS 服务的状态信息。

全局状态	虚拟IP池状态	规则测试
刷新时间间隔: 5秒		
设备列表	TCP请求	UDP请求
localhost	0 t/s	0 t/s

3.11.1. 全局状态

WEBUI 路径：『系统概况』→『全局状态』→『全局状态』。

『全局状态』用于查看全局站点信息，包括本地站点。

界面如下图所示：

全局状态	虚拟IP池状态	规则测试
刷新时间间隔: 5秒		
设备列表	TCP请求	UDP请求
localhost	0 t/s	0 t/s

『刷新时间间隔』设备列表中的站点信息默认 5 秒刷新一次。

『状态』用于显示每个站点的状态信息，包括『在线』或『离线』。

『TCP 请求』DNS 的 TCP 请求，单位次/秒。

『UDP 请求』DNS 的 UDP 请求，单位次/秒。

3.11.2. 虚拟 IP 池状态

WEBUI 路径：『系统概况』→『全局状态』→『虚拟 IP 池状态』。

『虚拟 IP 池状态』用于查看当前设备智能 DNS 中虚拟 IP 池的状态信息。

界面如下图所示：

刷新时间间隔: 5秒	虚拟IP池	apache			
虚拟IP	连接数	上行流量	下行流量	状态	
172.16.253.190	0	0 Kbps	0 Kbps	在线	
172.16.254.190	0	0 Kbps	0 Kbps	在线	

『刷新时间间隔』虚拟 IP 信息默认 5 秒刷新一次。

『虚拟 IP 池』选择需要显示状态信息的虚拟 IP 池。

3.11.3. 规则测试

WEBUI 路径：『系统概况』→『全局状态』→『规则测试』。

『DNS 映射』选择智能 DNS 中已经存在的 DNS 映射。

『LDNS 测试 IP』选择需要测试的 IP 地址。

点击 **测试**，显示测试结果，如下图所示：

规则测试

DNS映射	www.baidu.com
LDNS测试IP	200.200.0.20

测试结果

DNS映射 查找配置	成功
	获得 DNS映射 www.baidu.com
DNS映射 会话保持	启用
DNS映射 缓存记录	不存在
DNS映射 选择策略	成功
	使用策略 静态就近性
	获得 虚拟IP池 apache
虚拟IP池 首选策略	成功
	使用策略 轮询
获得结果	172.16.253.190
	测试完成

测试

3.12. 动态路由表

『动态路由表』用于查看设备通过 RIP 或者 OSPF 学习到的路由，界面如下图所示：

动态路由表				
刷新时间间隔：5秒				
目标地址	网络掩码	下一跳地址	协议类型	代价值
动态路由表为空				

3.13. 日志查看

WEBUI 路径：『系统概况』→『日志查看』。

用于查看设备的运行日志及错误提示。运行日志包括了服务日志、管理日志、SSL 日志三种类型。

界面如下图所示：



系统导航菜单			
系统概况			
» 虚拟服务详情	服务日志	管理日志	SSL日志
» 智能DNS统计	日期 20150601	类型	时间
» 实时漏洞分析	来源	详细信息	
» 链路状态	oracle监控服务 信息 04:03:23	监控管理服务初始化成功	
» 节点状态	SQLServer监控服务 信息 04:03:22	监控管理服务初始化成功	
» 接口状态	SQLServer监控服务 信息 04:03:21	SQL Server监控插件正常启动, version: v4.2.1	
» DNS状态	oracle监控服务 信息 04:03:21	Oracle监控插件正常启动, version: v2.0.1	
» 全局状态	SQLServer监控服务 信息 04:03:21	监控管理服务正在启动, 启动项ID为2, version: v2.0.1	
» 动态路由表	oracle监控服务 信息 04:03:21	监控管理服务正在启动, 启动项ID为0, version: v2.0.1	
» 日志查看	weblogic监控服务 信息 04:03:20	监控管理服务初始化成功	
» 报表配置	weblogic监控服务 信息 04:03:19	WebLogic监控插件初始化, version: v2.0.1	
» 公共对象	weblogic监控服务 信息 04:03:18	监控管理服务正在启动, 启动项ID为1, version: v2.0.1	
» 应用负载	数据采集服务 信息 04:03:18	数据采集服务启动成功, version: 4.2.0 (May 16 2015 12:52:02)	
» 智能DNS	数据导入服务 信息 04:03:18	数据导入服务启动成功, version: v3.0.0 (May 16 2015 12:51:58)	
» 策略配置	数据导入服务 信息 04:03:18	数据导入服务启动成功, version: v3.0.0 (May 16 2015 12:51:58)	
» 网络配置	数据采集服务 信息 04:02:26	服务退出, version: 4.2.0 (May 16 2015 12:52:02)	
» 系统配置	数据导入服务 信息 04:02:17	服务退出, version: v3.0.0 (May 16 2015 12:51:58)	
» 配置向导	SQLServer监控服务 信息 04:02:14	SQL Server监控插件正常退出, version: v4.2.1	
» 高可用性	SQLServer监控服务 信息 04:02:14	监控管理服务准备退出, 开始停止工作线程	
» 业务分析	weblogic监控服务 信息 04:02:11	WebLogic监控插件正常退出, version: v2.0.1	
	weblogic监控服务 信息 04:02:11	监控管理服务准备退出, 开始停止工作线程	
	oracle监控服务 信息 04:02:06	Oracle监控插件正常退出, version: v2.0.1	
	oracle监控服务 信息 04:02:06	监控管理服务准备退出, 开始停止工作线程	

3.13.1. 服务日志

WEBUI 路径：『系统概况』→『日志查看』→『服务日志』。

『服务日志』用于查看当前设备的系统日志信息。

界面如下图所示：

服务日志				管理日志	SSL日志
日期	来源	类型	时间	详细信息	
20150528	oracle监控服务	信息	04:03:33	监控管理服务初始化成功	
	SQLServer监控服务	信息	04:03:32	监控管理服务初始化成功	
	weblogic监控服务	信息	04:03:32	监控管理服务初始化成功	
	weblogic监控服务	信息	04:03:31	Weblogic监控插件初始化, version: v2.0.1	
	oracle监控服务	信息	04:03:31	Oracle监控插件正常启动, version: v2.0.1	
	SQLServer监控服务	信息	04:03:31	SQL Server监控插件正常启动, version: v4.2.1	
	oracle监控服务	信息	04:03:31	监控管理服务正在启动, 启动项ID为0, version: v2.0.1	
	SQLServer监控服务	信息	04:03:31	监控管理服务正在启动, 启动项ID为2, version: v2.0.1	
	weblogic监控服务	信息	04:03:31	监控管理服务正在启动, 启动项ID为1, version: v2.0.1	
	数据库更新服务	信息	04:02:20	服务退出, version: 4.2.0 (May 9 2015 10:14:22)	
	数据导入服务	信息	04:02:15	服务退出, version: v3.0.0 (May 9 2015 10:14:19)	
	SQLServer监控服务	信息	04:02:12	SQL Server监控插件正常退出, version: v4.2.1	
	SQLServer监控服务	信息	04:02:11	监控管理服务准备退出, 开始停止工作线程	
	weblogic监控服务	信息	04:02:07	Weblogic监控插件正常退出, version: v2.0.1	
	weblogic监控服务	信息	04:02:07	监控管理服务准备退出, 开始停止工作线程	
	oracle监控服务	信息	04:02:04	Oracle监控插件正常退出, version: v2.0.1	
	oracle监控服务	信息	04:02:04	监控管理服务准备退出, 开始停止工作线程	

『日期』选择要查看的日期，会显示相应时间下的日志记录。

『导出日志』用于导出查看系统日志、关于后台运行的重要的信息、黑盒日志等。

『选项设置』用于设置指定查看的系统日志范围。

界面如下图所示：



3.13.2. 管理日志

WEBUI 路径：『系统概况』→『日志查看』→『管理日志』。

『管理日志』可以查看当前设备管理员对设备进行的操作日志信息。

界面如下图所示：

服务日志		管理日志		SSL日志			
日期	20150528	用户名	<所有>	IP地址		操作类型	所有
admin	172.16.200.1	查看	19:24:38	系统概况	完成	查看服务日志	
admin	172.16.200.1	查看	19:24:18	系统概况	完成	查看动态路由表	
admin	172.16.200.1	查看	19:24:09	系统概况	完成	查看规则测试页面	
admin	172.16.200.1	查看	19:24:03	系统概况	完成	查看虚拟IP池状态	
admin	172.16.200.1	查看	19:23:44	系统概况	完成	查看全局状态	
admin	172.16.200.1	查看	19:23:22	系统概况	完成	查看DNS状态	
admin	172.16.200.1	查看	19:22:50	系统概况	完成	查看接口状态	
admin	172.16.200.1	查看	19:22:44	报表配置	完成	进入报表中心登录页面	
admin	172.16.200.1	查看	19:22:41	系统概况	完成	查看节点池状态	
admin	172.16.200.1	查看	19:22:31	用户登录	完成	网关控制台登录成功	
未登录	172.16.200.1	查看	19:22:26	用户登录	失败	网关控制台登录失败(用户名密码错误)	
admin	172.16.200.1	查看	19:21:58	应用负载	完成	查看服务列表	
admin	172.16.200.1	查看	19:21:53	应用负载	完成	查看前置调度策略列表	
admin	172.16.200.1	查看	19:21:35	系统概况	完成	查看调度查询页面	
admin	172.16.200.1	查看	19:21:23	系统概况	完成	查看节点状态	
admin	172.16.200.1	查看	19:20:37	系统概况	完成	查看节点池状态	
admin	172.16.200.1	查看	19:20:35	系统概况	完成	查看节点状态	
admin	172.16.200.1	查看	19:20:20	系统概况	完成	查看节点池状态	
admin	172.16.200.1	查看	19:19:46	系统概况	完成	查看虚拟服务链路状态信息	
admin	172.16.200.1	查看	19:19:17	系统概况	完成	查看所有链路状态	

『日期』选择要查看的日期，会显示相应时间下的日志记录。

『用户名』用于选择需要查看的管理员账号。

『IP 地址』用于选择需要查看的 IP 地址。

『操作类型』包括 『所有』、『查看』、『编辑』、『新建』、『删除』、『更新』、『非查看』等操作。可以选择不同的操作进行查询。

『刷新/查询』可用于手动刷新日志记录。

『导出日志』用于导出当前所选的管理日志。界面如下图所示：



『删除日志』用于删除查看系统日志。

『选项设置』用于过滤需要查看的管理日志，界面如下：



3.13.3. SSL 日志

WEBUI 路径：『系统概况』→『日志查看』→『SSL 日志』。

『SSL 日志』用来显示 SSL 客户端认证失败的日志。

界面如下图所示：

服务日志		管理日志		SSL日志	
日期	20150912				导出日志
时间	类型	源地址	目的地址	详细信息	
18:38:10	自签名证书不受信任	97.97.3.224	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.104	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.2	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.168	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.205	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.11	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.99	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.161	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.252	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.19	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.138	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.90	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	
18:38:10	自签名证书不受信任	97.97.3.235	97.97.1.1	虚拟服务：ddos_test 主题：emailAddress=ad@ad.com,CN=ad2048,OU=ad,O=ad,L=ad,ST=ad,C=CN 颁发者：ema...	

3.14. 调试信息统计

WEBUI 路径：『系统概况』→『调试信息统计』。

『调试信息统计』用于统计 TCP 握手失败，协议解析失败，DNS 解析失败，调度失败，会话保持异常，NAT 失败等统计，用于深信服技术支持通过查看设备上的异常统计息，从而做出初步的故障排查。

界面如下图所示：

调试信息统计		
模块	详细信息	出现次数
TCP协议栈	tcps_activeconnattempt	0
TCP协议栈	tcps_passiveconnattempt	0
TCP协议栈	tcps_establish	0
TCP协议栈	tcps_accepts	0
TCP协议栈	tcps_syncconnects	0
TCP协议栈	tcps_rcvconnects	0
TCP协议栈	tcps_drops	0
TCP协议栈	tcps_comdrop	0
TCP协议栈	tcps_closed	0
TCP协议栈	tcps_desitory	0
TCP协议栈	tcps_seguinized	0
TCP协议栈	tcps_xittupdated	0
TCP协议栈	tcps_delack	0
TCP协议栈	tcps_timeoutdrop	0
TCP协议栈	tcps_timeoutdropinit	0
TCP协议栈	tcps_finddrop	0
TCP协议栈	tcps_cowntdrop	0
TCP协议栈	tcps_finddrop	0
TCP协议栈	tcps_closingdrop	0
TCP协议栈	tcps_lastackdrop	0
TCP协议栈	tcps_rexmittimeo	0
TCP协议栈	tcps_fastretran	0
TCP协议栈	tcps_fastrerecovery	0

点击**更新数据**，可以进行数据当前数据的更新。

点击**清除记录**，可以删除当前的记录。

点击**导出日志**，可以导出日志，进行详细分析。

第4章 报表配置

4.1. 报表生成

WEBUI 路径：『报表配置』→『报表生成』。

『报表生成』用于使用自动或手动的方式生成所需的报表，『报表生成』包括『立即生成』、『自动生成』、『报表样式』三个部分。

界面如下图所示：



The screenshot shows a web-based configuration interface for report generation. At the top, there are three tabs: '立即生成' (selected), '自动生成', and '报表样式'. Below the tabs, the title '生成报表PDF文档' is displayed. Under the '立即生成报表' section, there are three input fields: '统计起始时间' (start date) set to '2016-01-20', '时间' (time) set to '00:00', '统计结束时间' (end date) set to '2016-01-20', '时间' (time) set to '01:00', and '报表样式' (report style) set to '默认样式' (Default Style). At the bottom of this section are two buttons: '生成' (Generate) and '重置' (Reset).

4.1.1. 立即生成

WEBUI 路径：『报表配置』→『报表生成』→『立即生成』。

『立即生成』用于设置统计时间范围，并根据报表样式立即生成报表，生成的报表可下载到本地进行查看。

界面如下图所示：



This screenshot shows the same 'Report Generation' interface as the previous one, but with different date and time settings. The '立即生成报表' section shows: '统计起始时间' (start date) '2014-04-10', '时间' (time) '00:00'; '统计结束时间' (end date) '2014-04-10', '时间' (time) '01:00'; and '报表样式' (report style) '默认样式' (Default Style). The '生成' (Generate) and '重置' (Reset) buttons are at the bottom.

『统计起始时间』用于设置生成的报表数据的起始时间。

『统计结束时间』用于设置生成的报表数据的结束时间。

『报表样式』用于选择根据哪种报表样式来生成报表。

点击**重置**，用于将『立即生成』中的配置恢复成默认值。

点击**生成**，用于立即生成报表。弹出如下对话框：



点击**确定**，系统立即生成报表，返回页面如下：



统计起始时间	日期	2015-11-05	时间	00:00
统计结束时间	日期	2015-11-05	时间	01:00
报表样式	默认样式			

点击**下载报表**，用于把生成的报表保存到本地。

点击**继续生成**，用于返回『立即生成』的页面，继续生成其他报表。

4.1.2. 自动生成

WEBUI 路径：『报表配置』→『报表生成』→『自动生成』。

『自动生成』用于设置报表生成周期，并根据报表样式自动生成报表，生成的报表可以自动发送到指定邮箱。

界面如下图所示：



更新自动生成报表配置信息

自动生成报表

每日生成	<input type="checkbox"/> 启用	报表样式	默认样式
每周生成	<input type="checkbox"/> 启用	报表样式	默认样式
每月生成	<input type="checkbox"/> 启用	报表样式	默认样式
每年生成	<input type="checkbox"/> 启用	报表样式	默认样式

SMTF服务器: --请选择smtp服务器--

邮件标题:

(长度限制为1~255个字符，且不能包含& | " " , : % < > / \ 特殊字符)

收件人:

发件人:

『每日生成』用于每日一次自动生成报表，勾选[启用]使该项生效，点击『报表样式』的下拉框，可选择根据哪种报表样式生成报表。

『每周生成』 用于每周一次自动生成报表，勾选[启用]使该项生效，点击『报表样式』的下拉框，可选择根据哪种报表样式生成报表。

『每月生成』 用于每月一次自动生成报表，勾选[启用]使该项生效，点击『报表样式』的下拉框，可选择根据哪种报表样式生成报表。

『每年生成』 用于每年一次自动生成报表，勾选[启用]使该项生效，点击『报表样式』的下拉框，可选择根据哪种报表样式生成报表。

『SMTP 服务器』用于设置是否自动将生成的报表发送到指定邮箱。

『SMTP 服务器』用于选择发送报表使用的 SMTP 服务器，点击“+”按钮进行定义，配置方法见 10.4 章节。

点击**更新**，更新并保存对『自动生成』的配置。

4.1.3. 报表样式

WEBUI 路径：『报表配置』→『报表生成』→『报表样式』。

『报表样式』：用于设置报表样式，定义生成报表所包含的信息。可设置多个报表样式，在『报表生成』中进行调用。

界面如下图所示：



『报表样式列表』用于显示已经设置完成的报表样式。

点击**删除**，用于删除选中的报表样式。

点击**新建**，用于新建报表样式。设置界面如下：



『名称』用于定义该报表样式的名称

『报表模块』用于选择该报表样式需要包含哪些模块的内容，主要分以下几个模块：[链路统计]、[节点统计]、[虚拟服务统计]、[智能路由统计]、[智能 DNS 统计]、[集群统计]。

勾选相关模块之后下面会弹出此模块的详细配置信息。

4.1.3.1. 链路统计

『链路统计』用于统计各个链路的负载情况，判断各链路的访问负载是否均衡。

界面如下图所示：

新建报表样式配置信息

属性

名称 A

报表模块 链路统计 节点统计 虚拟服务统计
 智能路由统计 智能DNS统计 集群统计

链路统计

统计类型 总流量 上行流量 下行流量
 访问次数 带宽利用率 稳定性

已选择 链路 WAN1 WAN2

待选

取消 更新



『统计类型』用于选择统计的项目，包括总流量、上行流量、下行流量、访问次数、带宽利用率、稳定性。

『链路』用于选择统计[已选择列表]中的链路的数据。

4.1.3.2. 节点统计

『节点统计』用于统计各个节点的负载情况，判断各个节点的负载是否均衡。

界面如下图所示：

新建报表样式配置信息

属性

名称

报表模块 链路统计 节点统计 虚拟服务统计
 智能路由统计 智能DNS统计 集群统计

节点统计

统计类型 总流量 上行流量 下行流量
 访问次数 并发连接数 稳定性 MySQL读写统计

已选择
节点池 NODE
 mysql-master
 mysql-slave
 httpd

待选

取消 **更新**

『统计类型』用于选择统计的项目，包括总流量、上行流量、下行流量、访问次数、并发连接数、稳定性、MySQL 读写统计。

『节点池』用于选择统计[已选择列表]中的节点池的数据。

4.1.3.3. 虚拟服务统计

『虚拟服务统计』用于统计各个虚拟服务的负载情况，判断各虚拟服务的负载是否均衡。

界面如下图所示：

新建报表样式配置信息

属性

名称

报表模块 链路统计 节点统计 虚拟服务统计
 智能路由统计 智能DNS统计 集群统计

虚拟服务统计

统计类型 总流量 上行流量 下行流量
 访问次数 稳定性

已选择
虚拟服务 web
 mysql
 httpd

待选

取消 **更新**

『统计类型』用于选择统计的项目，包括总流量、上行流量、下行流量、访问次数、稳

定性。

『虚拟服务』用于选择统计[已选择列表]中的虚拟服务的数据。

4.1.3.4. 智能路由统计

『智能路由统计』配置智能路由统计报表的统计类型，报表只生成所选统计类型的数据报表。



新建报表样式配置信息			
属性			
名称	<input type="text"/>		
报表模块	<input type="checkbox"/> 链路统计	<input type="checkbox"/> 节点统计	<input type="checkbox"/> 虚拟服务统计
	<input checked="" type="checkbox"/> 智能路由统计	<input type="checkbox"/> 智能DNS统计	<input type="checkbox"/> 集群统计
智能路由统计			
统计类型	<input type="checkbox"/> 总流量	<input type="checkbox"/> 上行流量	<input type="checkbox"/> 下行流量
	<input type="checkbox"/> 访问次数		
<input type="button" value="取消"/>		<input type="button" value="更新"/>	

『统计类型』用于选择统计的项目，包括总流量、上行流量、下行流量、访问次数。

4.1.3.5. 智能 DNS 统计

『智能路由统计』配置智能 DNS 统计报表的统计类型，报表只生成所选统计类型的数据报表。

立即生成 | 自动生成 | 报表样式

新建报表样式配置信息

属性

名称

报表模块

链路统计 节点统计 虚拟服务统计
 智能路由统计 智能DNS统计 集群统计

智能DNS统计

统计类型

站点集合 虚拟IP池 LDNS集合
 来源分布 异常请求

已选择
待选

DNS映射

取消 **更新**

『统计类型』用于选择统计的项目，包括站点集合、虚拟 IP 池、LDNS 集合、来源分布和异常请求。

『DNS 映射』选择需要生成报表的 DNS 映射，也就是智能 DNS 的一级调度策略。

完成以上所有设置后：

点击**完成**，完成此报表样式的配置。

点击**取消**，取消此报表样式的配置。

4.1.3.6. 集群统计

『集群统计』配置报表是否生成集群相关的统计数据报表。

立即生成 | 自动生成 | 报表样式

新建报表样式配置信息

属性

名称

报表模块

链路统计 节点统计 虚拟服务统计
 智能路由统计 智能DNS统计 集群统计

取消 **更新**

4.2. 报表中心

WEBUI 路径：『报表配置』 → 『报表中心』。

『报表中心』用于登录到报表中心，详细查看 AD 设备各种统计信息，包括『链路统计』、『节点统计』、『虚拟服务统计』、『智能路由统计』、『智能 DNS 统计』和『集群状态统计』。

通过『当前用户登录』和『其他用户登录』两种方式可以进入报表中心。

界面如下图所示：

配置报表功能及登录报表

报表功能

状态 启用 禁用

报表登录

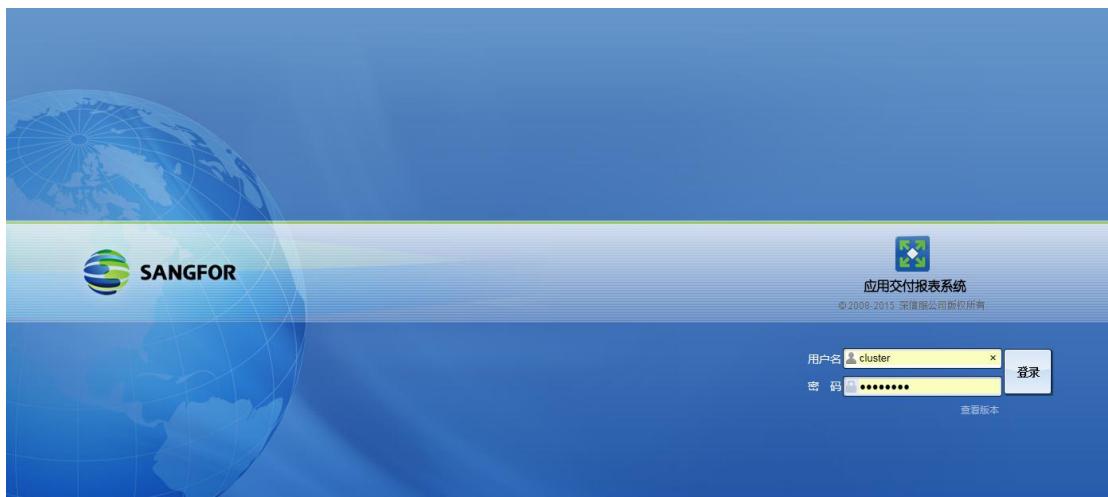
当前用户登录 其他用户登录

点击**启用**，全局启用报表中心功能。点击**禁用**，关闭报表中心功能。

点击**当前用户登录**，使用当前登录控制台的用户直接进入『报表中心』

点击**其他用户登录**，将弹出『报表中心』的登录页面，用于使用其他的用户账号登录到『报表中心』。

点击[其他用户登录](#)，登陆界面如下图所示：



输入用户名和密码，点击[登录](#)按钮就可以进入『报表中心』了。

4.2.1. 报表维护

WEBUI 路径：『报表中心』→『报表维护』。

『报表维护』用于设置自动删除报表数据的策略。

界面如下图所示：



全局查询策略	报表响应时间	8 秒	(响应时间取值范围为4~30)
报表清除策略	磁盘空间极限	90 %	
	自动删除最前面	3	天的报表数据

『报表响应时间』 报表中心每次查询全局站点数据时的超时时间。

『磁盘空间极限』 用于设置报表可以使用的磁盘空间上限。

『自动删除最前面的』用于设置当磁盘空间达到『磁盘空间极限』时，设备自动删除最前面多少天的报告数据。

点击**更新**，用于更新并保存对『报表维护』的配置。

4.2.2. 报表中心

4.2.2.1. 链路统计

『链路统计』主要是针对链路负载进行统计，对链路负载的状况进行详细的统计和查询；统计范围包括『流量』、『访问次数』、『带宽利用率』、『稳定性』。

4.2.2.1.1 流量

『流量』用来统计经过AD设备的流量信息。

WEBUI路径：『链路负载统计』→『流量』。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『链路』用于选择链路方向。可以选择全部链路、LAN、WAN。

『流量方向』用于设置统计流量的方向，包括：总流量、上行流量、下行流量。

点击[查询](#)，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是区间图。



点击[导出报表](#)，则按照以上统计选项中的设置统计出流量图，生成 pdf 格式的报表。

4.2.2.1.2 访问次数

WEBUI 路径：『报表』→『链路统计』→『访问次数』。

『访问次数』主要用来统计被访问的次数。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『链路』用于选择链路方向。可以选择全部链路、WAN。

点击**查询**，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是折线图。



点击**导出报表**，则按照以上统计选项中的设置统计出链路访问次数折线图，生成 pdf 格式的报表。

4.2.2.1.3 带宽利用率

『带宽利用率』用于统计链路的带宽利用率。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『链路』用于选择链路方向。可以选择全部链路、LAN、WAN。

『流量方向』用于设置统计流量的方向，包括：上行带宽利用率、下行带宽利用率。

点击查询，生成查询结果，生成带宽利用率折线图。



点击[导出报表](#)，则按照以上统计选项中的设置统计出流量图，生成 pdf 格式的报表。

4.2.2.1.4 稳定性

『稳定性』用于统计链路状态的稳定性。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『链路』用于选择链路方向。可以选择全部链路、WAN。

点击查询，生成查询结果，生成 WAN 口链路状态图。



点击导出报表，则按照以上统计选项中的设置统计出状态图，生成 pdf 格式的报表。

4.2.2.2. 节点统计

4.2.2.2.1 流量

『流量』 用于统计指定节点池和节点的流量信息。

界面如下图所示：

『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『节点池』用于指定统计哪个节点池的流量。

『节点』用于指定统计哪个节点的流量。

『流量方向』用于设置统计流量的方向，包括：总流量、上行流量、下行流量。

点击【查询】，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图）。

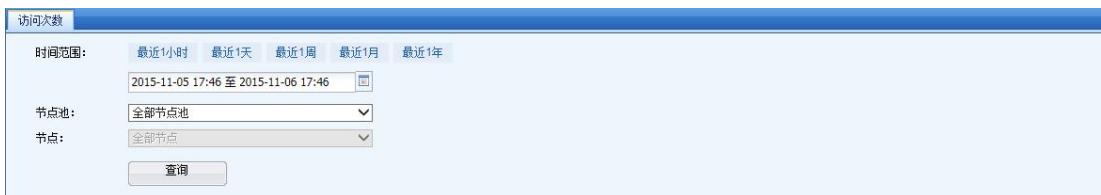


点击【导出报表】，则按照以上统计选项中的设置统计出流量图，生成 pdf 格式的报表。

4.2.2.2.2 访问次数

『访问次数』用于统计指定节点池和节点的访问次数。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『节点池』用于指定统计哪个节点池的流量。

『节点』用于指定统计哪个节点的流量。

点击【查询】，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图）。

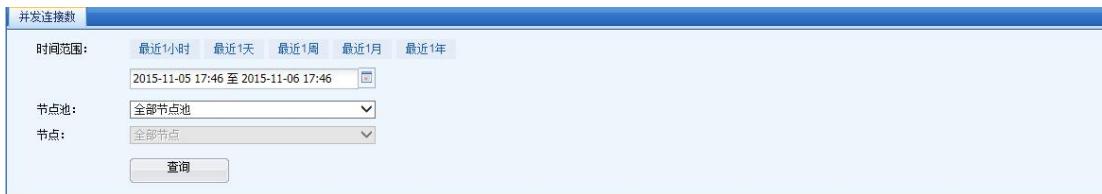


点击[导出报表](#)，则按照以上统计选项中的设置统计出节点池访问次数折线图，生成 pdf 格式的报表。

4.2.2.2.3 并发连接数

『并发连接数』 用于统计指定节点池和节点的并发连接数。

界面如下图所示：



The figure shows a query interface for concurrent connections. The title bar says '并发连接数'. The '时间范围' (Time Range) section includes buttons for '最近1小时' (Last 1 Hour), '最近1天' (Last 1 Day), '最近1周' (Last 1 Week), '最近1月' (Last 1 Month), and '最近1年' (Last 1 Year). Below this is a date range selector showing '2015-11-05 17:46 至 2015-11-06 17:46'. The '节点池' (Node Pool) dropdown is set to '全部节点池' (All Node Pools). The '节点' (Node) dropdown is set to '全部节点' (All Nodes). At the bottom is a '查询' (Query) button.

『时间范围』 用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『节点池』 用于指定统计哪个节点池的流量。

『节点』 用于指定统计哪个节点的流量。

点击[查询](#)，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图）。

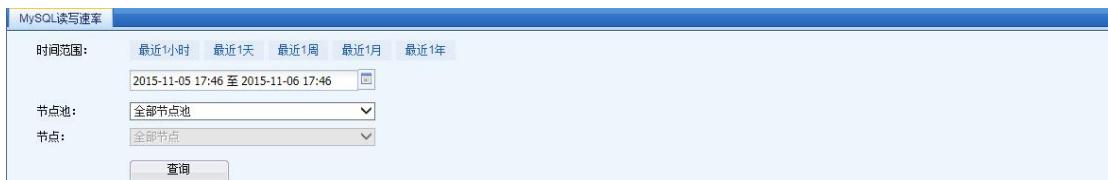


点击[导出报表](#)，则按照以上统计选项中的设置统计出节点池并发连接数区间图，生成pdf格式的报表。

4.2.2.2.4 MySQL 读写速率

『MySQL 读写速率』 用于统计指定节点池和节点的 MySQL 读写速率。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『节点池』用于指定统计哪个节点池的流量。

『节点』用于指定统计哪个节点的流量。

点击[查询](#)，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图）。



点击[导出报表](#)，则按照以上统计选项中的设置统计出节点池读速率趋势区间图，生成pdf格式的报表。

4.2.2.2.5 稳定性

『稳定性』 用于统计指定节点池和节点的稳定性。

界面如下图所示：



稳定性

时间范围： 最近1小时 最近1天 最近1周 最近1月 最近1年
2015-11-05 17:46 至 2015-11-06 17:46

节点池： 全部节点池

节点： 全部节点

查询

『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『节点池』用于指定统计哪个节点池的流量。

『节点』用于指定统计哪个节点的流量。

点击[查询](#)，生成查询结果。



点击[导出报表](#)，则按照以上统计选项中的设置统计出节点池状态图，生成 pdf 格式的报表。

4.2.2.3. 虚拟服务统计

『虚拟服务统计』主要是针对虚拟服务进行统计，对虚拟服务的状况进行详细的统计和查询；统计范围包括『流量』、『访问次数』、『URL 统计』、『稳定性』。

4.2.2.3.1 流量

『流量』用来统计虚拟服务的流量信息。

WEBUI 路径：『虚拟服务统计』→『流量』。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置

统计流量的起始时间和结束时间。

『虚拟服务』用于选择统计的虚拟服务。

『流量方向』用于设置统计流量的方向，包括：总流量、上行流量、下行流量。

点击**查询**，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是区间图。



点击**导出报表**，则按照以上统计选项中的设置统计出流量图，生成 pdf 格式的报表。

4.2.2.3.2 访问次数

WEBUI 路径：『报表』→『虚拟服务统计』→『访问次数』。

『访问次数』主要用来统计虚拟服务被访问的次数。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置

统计流量的起始时间和结束时间。

『虚拟服务』用于选择统计的虚拟服务。

『流量方向』用于设置统计流量的方向，包括：总流量、上行流量、下行流量。

点击【查询】，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是折线图。



点击【导出报表】，则按照以上统计选项中的设置统计出虚拟服务访问次数折线图，生成pdf格式的报表。

4.2.2.3.3 URL 统计

『URL 统计』用于统计虚拟服务的 URL 匹配流量。

界面如下图所示：



The screenshot shows the 'URL Statistics' search interface. It includes a 'Time Range' section with dropdowns for 'Recent 1 Hour', 'Recent 1 Day', 'Recent 1 Week', 'Recent 1 Month', and 'Recent 1 Year', with 'Recent 1 Day' selected. There is also a date range input field showing '2015-11-05 17:46 至 2015-11-06 17:46'. A 'Virtual Service' dropdown menu is open, showing 'http://www.sangfor.com.cn'. A 'URL Matching' input field contains the placeholder '*'. Under 'Traffic Direction', the 'Total Traffic' radio button is selected. At the bottom is a 'Search' button.

『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置

统计流量的起始时间和结束时间。

『虚拟服务』用于选择统计的虚拟服务。

『URL 匹配』用于定义需要匹配的 URL，统计全部填“*”。

『流量方向』用于设置统计流量的方向，包括：总流量、请求方向流量、应答方向流量。

点击查询，生成查询结果。

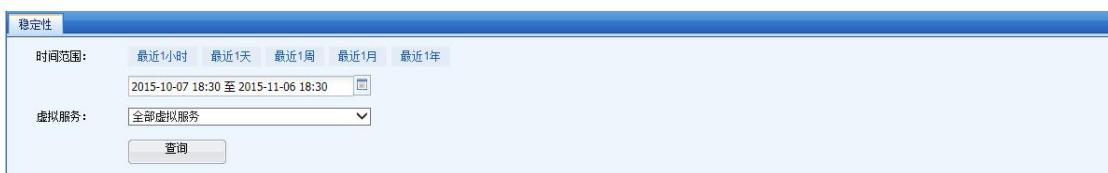


点击导出报表，则按照以上统计选项中的设置统计出结果，生成 pdf 格式的报表。

4.2.2.3.4 稳定性

『稳定性』用于统计虚拟服务的稳定性。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『虚拟服务』用于选择统计的虚拟服务。

点击查询，生成查询结果，生成虚拟服务状态图。



点击导出报表，则按照以上统计选项中的设置统计出虚拟服务状态图，生成 pdf 格式的报表。

4.2.2.4. 智能路由统计

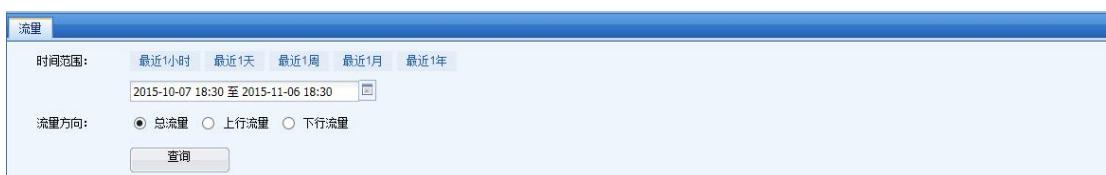
『智能路由统计』主要是针对智能路由进行统计，对智能路由的状况进行详细的统计和查询；统计范围包括『流量』、『访问次数』。

4.2.2.4.1 流量

『流量』用来统计经过 AD 设备的流量信息。

WEBUI 路径：『智能路由统计』→『流量』。

界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『流量方向』用于设置统计流量的方向，包括：总流量、上行流量、下行流量。

点击查询，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是区间图。



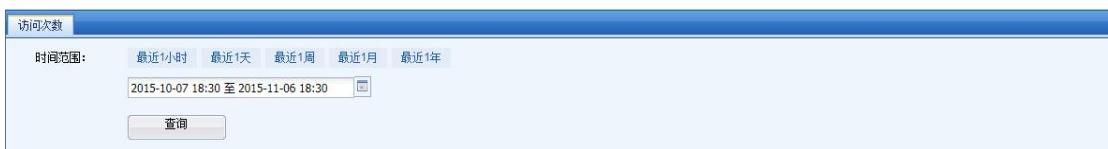
点击导出报表，则按照以上统计选项中的设置统计出流量图，生成 pdf 格式的报表。

4.2.2.4.2 访问次数

WEBUI 路径：『报表』→『智能路由统计』→『访问次数』。

『访问次数』主要用来统计被访问的次数。

界面如下图所示：



访问次数

时间范围：最近1小时 最近1天 最近1周 最近1月 最近1年
2015-10-07 18:30 至 2015-11-06 18:30

查询

『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

点击查询，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是折线图。



点击[导出报表](#)，则按照以上统计选项中的设置统计出智能路由访问次数折线图，生成pdf格式的报表。

4.2.2.5. 智能 DNS 统计

『智能 DNS 统计』包括『全局访问次数』、『全局 LDNS 来源分布』、『本地异常请求』。

4.2.2.5.1 全局访问次数

4.2.2.5.1.1 站点集合

『站点集合』用于统计站点集合访问 DNS 映射的次数，界面如下图所示：



时间范围：
最近1小时 最近1天 最近1周 最近1月 最近1年
2015-11-07 08:00 至 2015-11-07 09:00
DNS映射：
查询

『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『DNS 映射』用于设置统计的 DNS 映射。

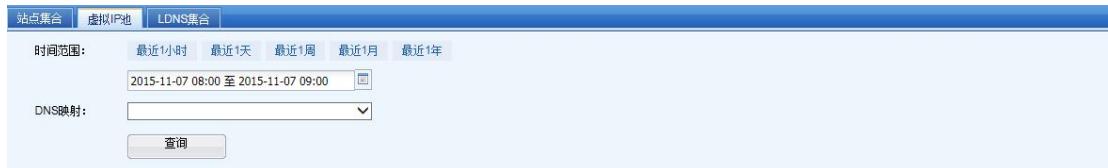
点击[查询](#)，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是区间图。



点击[导出报表](#)，则按照以上统计选项中的设置统计出结果，生成 pdf 格式的报表。

4.2.2.5.1.2 虚拟 IP 池

『虚拟 IP 池』用于根据全局虚拟 IP 池来统计访问 DNS 映射的次数，界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『DNS 映射』用于设置统计的 DNS 映射。

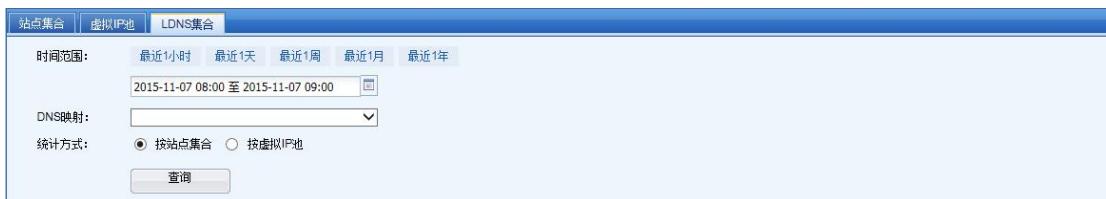
点击[查询](#)，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是区间图。



点击[导出报表](#)，则按照以上统计选项中的设置统计出结果，生成 pdf 格式的报表。

4.2.2.5.1.3 LDNS 集合

『LDNS 集合』用于根据全局站点集合或全局虚拟 IP 池来统计访问 LDNS 集合的次数，界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『DNS 映射』用于设置统计的 DNS 映射。

『统计方式』可以根据站点集合或虚拟 IP 池进行统计。

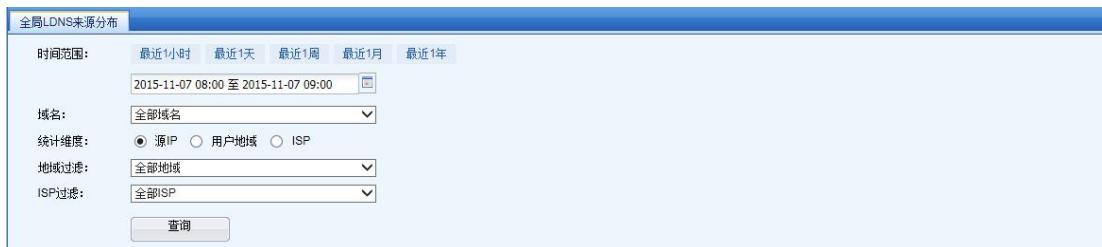
点击[查询](#)，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是区间图。



点击[导出报表](#)，则按照以上统计选项中的设置统计出结果，生成 pdf 格式的报表。

4.2.2.5.2 全局 LDNS 来源分布

『全局 LDNS 来源分布』用于根据域名、用户地域、ISP 和地址段类型来统计访问 DNS 映射的次数，界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『域名』用于选择需要统计的域名。

『统计维度』用于选择需要统计的维度，可以选择源 IP、用户地域、ISP。

『地域过滤』用于选择需要统计的地域。

『ISP 过滤』用于选择需要统计的用户运营商。

点击[查询](#)，生成查询结果，可以自主选择生成图表类型（区间图、折线图、饼状图），默认是区间图。

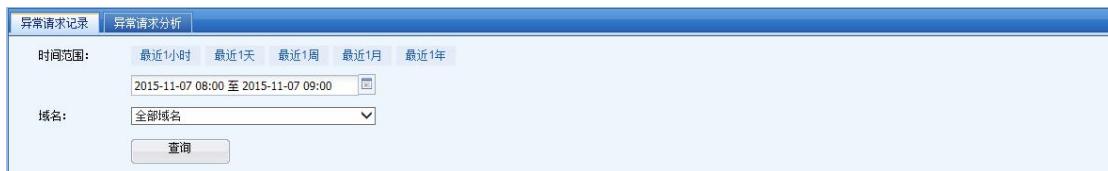


点击[导出报表](#)，则按照以上统计选项中的设置统计出结果，生成 pdf 格式的报表。

4.2.2.5.3 本地异常请求

4.2.2.5.3.1 异常请求记录

『异常请求记录』用于统计域名解析失败的次数和原因，如下图所示：



时间范围： 最近1小时 最近1天 最近1周 最近1月 最近1年
2015-11-07 08:00 至 2015-11-07 09:00

域名： 全部域名

查询

『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『域名』用于选择需要统计的域名。

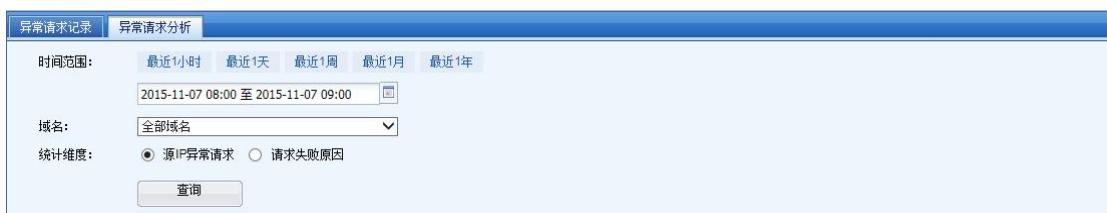
点击[查询](#)，生成查询结果。



点击[导出报表](#)，则按照以上统计选项中的设置统计出结果，生成 pdf 格式的报表。

4.2.2.5.3.2 异常请求分析

『异常请求分类』用于将域名解析失败的请求按照源 IP 统计或按照失败的原因统计，如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『域名』用于选择需要统计的域名。

『统计维度』可选择按源 IP 异常请求统计或者按请求失败原因统计。

点击[查询](#)，生成查询结果。



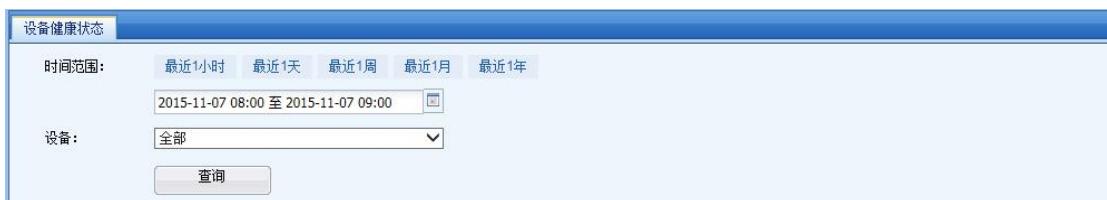
点击[导出报表](#)，则按照以上统计选项中的设置统计出结果，生成 pdf 格式的报表。

4.2.2.6. 集群状态统计

『集群状态统计』统计范围包括『设备健康状态』、『单设备生效时间』、『单应用组设备分布』。

4.2.2.6.1 设备健康状态

『设备健康时间统计』显示设备的健康状态时间分布。如下图所示：



The screenshot shows the "Equipment Health Status Statistics" interface. At the top, there is a title bar with the interface name. Below it is a search form with the following fields:

- Time Range: A dropdown menu with options: 最近1小时 (Last 1 Hour), 最近1天 (Last 1 Day), 最近1周 (Last 1 Week), 最近1月 (Last 1 Month), and 最近1年 (Last 1 Year). The "最近1小时" option is selected.
- Date Range: A text input field showing "2015-11-07 08:00 至 2015-11-07 09:00" with a calendar icon to its right.
- Device Selection: A dropdown menu labeled "设备" (Device) with "全部" (All) selected.
- Query Button: A "查询" (Query) button at the bottom of the form.

『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『设备』用于选择需统计的设备。

点击[查询](#)，生成查询结果。



点击[导出报表](#)，则按照以上统计选项中的设置统计出状态图，生成 pdf 格式的报表。

4.2.2.6.2 单设备生效时间

『单设备生效时间』显示设备的故障状态时间分布。可统计设备所有非正常状态（故障，沉默和离线）的时间。界面如下图所示：



『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『设备』用于选择需统计的设备。

点击[查询](#)，生成查询结果。



点击[导出报表](#)，则按照以上统计选项中的设置统计出状态图，生成 pdf 格式的报表。

4.2.2.6.3 单应用组设备分布

『单应用组设备分布』显示单个应用组的在集群设备上运行情况。 可统计单应用组运行设备的分布情况。

界面如下图所示：

单应用组设备分布

时间范围：

应用组：

『时间范围』用于选择时间类型，包括：一小时、一天、一个周、一个月、一年。设置统计流量的起始时间和结束时间。

『应用组』用于选择统计的应用组。

点击[查询](#)，生成查询结果。



点击[导出报表](#)，则按照以上统计选项中的设置统计出状态图，生成 pdf 格式的报表。

第5章 公共对象

『公共对象』用于配置AD设备在实现链路负载和服务器负载的时候需要调用的一些对象，包括『用户地址集』、『IP地址集』、『时间计划』和『自定义内容』几个部分，通过这几个部分的组合配置可以灵活高效地进行负载均衡。

5.1. 用户地址集

WEBUI：『公共对象』→『用户地址集』。

『用户地址集』用于定义内网的某个地址段，此处定义的『用户地址集』，可用于『智能路由』配置部分。

界面如下图所示：



『用户地址集』下显示用户地址集的『名称』、『IP地址段』。

点击**删除**，用于删除已选IP地址段。

点击**新建**，用于新建用户地址集，配置界面如下：

新建

属性

名称

配置

IP地址

起始地址:
结束地址:

当前已配置0/100个地址段



『名称』可以输入便于记忆和识别的字符串，用于标识自定义的IP地址段。

『IP地址』可以根据单个地址、IP范围、子网定义。用于自定义内网IP组的地址范围，支持IPv4或IPv6地址，不支持IPv4地址和IPv6地址的混合使用。点击**添加**按钮即可添加到下面的列表中，选中列表中的地址段，点击**删除**按钮即可从列表中删除已添加地址段。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

点击**导入**按钮，可以将IP地址通过自定义的文件来导入『用户地址集』，如下图所示：

导入用户地址集配置

导入文件

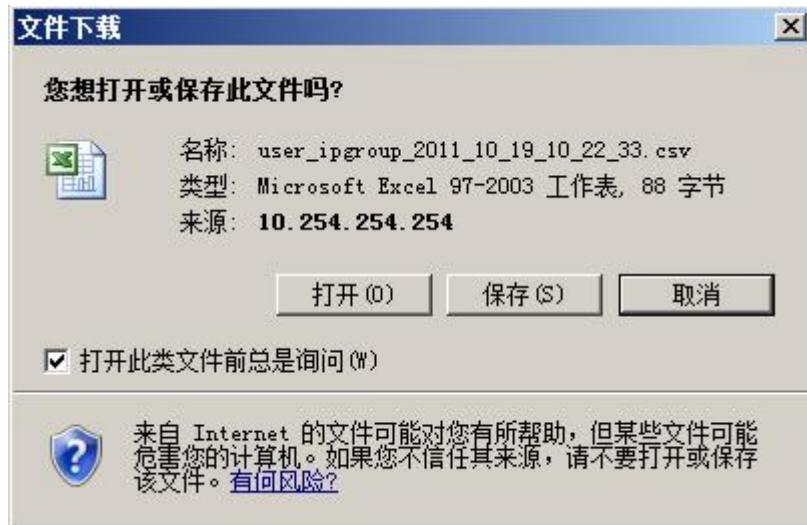
模板下载 [用户地址集CSV模板](#)



点击**浏览**按钮，选中编辑好的文件，然后点击**导入**按钮，导入完成。点击**取消**按钮可以用于取消本次配置。

点击“用户地址集CSV模板下载”，可以下载示例模板。

点击导出按钮，可以将 IP 地址从『用户地址集』中导出到 CSV 格式文件中，如下图所示：



5.2. IP 地址集

WEBUI 路径：『公共对象』→『IP 地址集』。

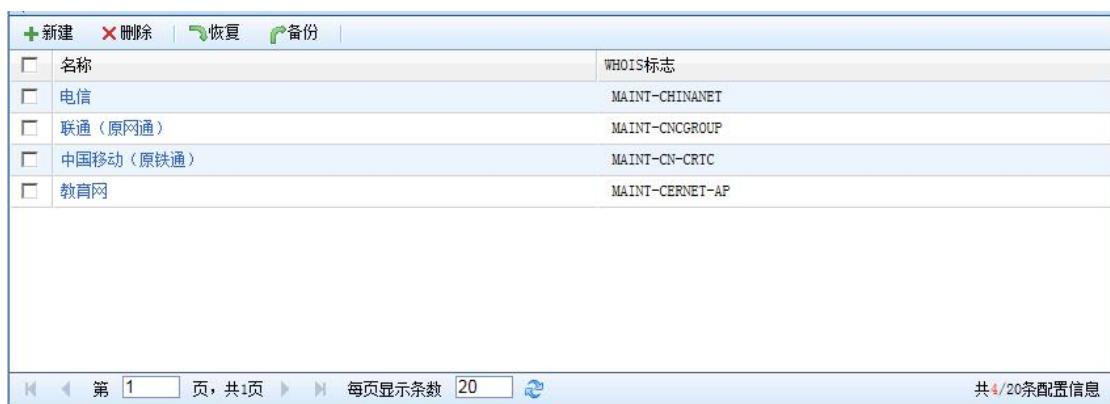
『IP 地址集』用于指定相同类别的 IP 地址，包括『ISP 地址段』、『全球地址段』、『用户地域』和『自动更新』等部分。

界面如下图所示：

5.2.1. ISP 地址段

『ISP 地址段』用于设置网络运营商的 IP 地址段，此 IP 地址段主要用于智能路由的配置。设备默认已经收集了电信、联通（原网通）、中国移动（原铁通）、教育网的 IP 地址段。

界面如下图所示：



+新建		×删除	恢复	备份
<input type="checkbox"/>	名称	WHOIS标志		
<input type="checkbox"/>	电信	MAINT-CHINANET		
<input type="checkbox"/>	联通（原网通）	MAINT-CNCGROUP		
<input type="checkbox"/>	中国移动（原铁通）	MAINT-CN-CRTC		
<input type="checkbox"/>	教育网	MAINT-CERNET-AP		

第 1 页, 共1页 每页显示条数 20 共 4/20 条配置信息

『ISP 地址段』显示已经设置完成的 ISP 信息。

点击 **删除**，用于将已选的 ISP 信息删除。

点击 **新建**，用于新建 ISP 信息，配置界面如下：

ISP地址段 全球地址段 用户地域 自动更新 帮助信息

新建

属性

名称

配置

地址范围 - **添加**

当前已配置 0/10000 个地址范围

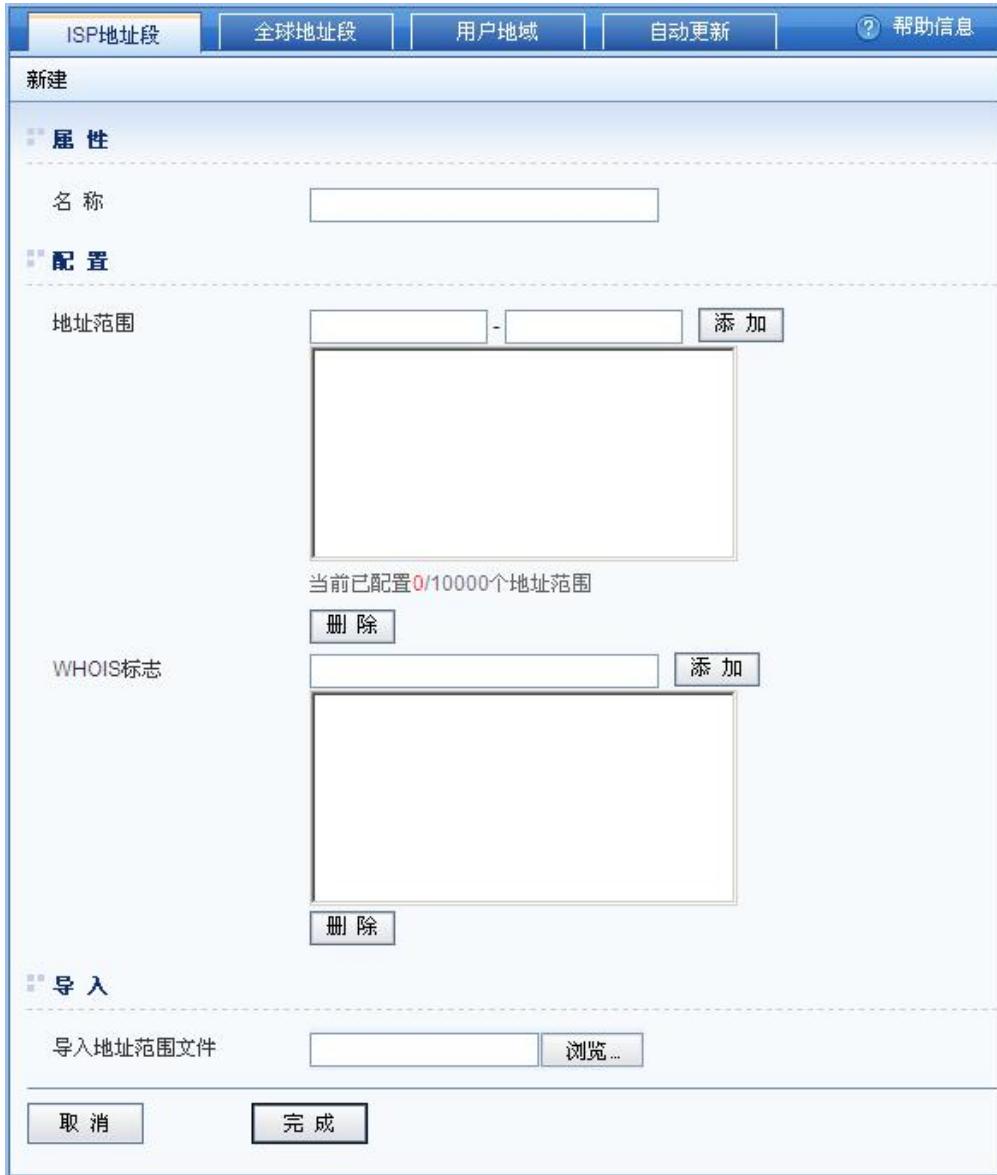
WHOIS标志

删除 **添加**

导入

导入地址范围文件 **浏览...**

取消 **完成**



『名称』用于设置 ISP 名称。

『地址范围』用于手动设置该运营商的网络 IP 段。

『WHOIS 标志』用于设置相应的 ISP 地址段对应的 WHOIS 标志，便于根据标志识别不同运营商的地址。

点击**添加**，用于添加设置的标志或地址。

点击**删除**，用于删除选中的标志和地址。

『导入地址范围文件』用于手动导入地址范围文件到AD设备，可以导入ANSI编码的txt格式文件。

配置完毕，点击**完成**，完成此ISP信息的配置。

点击**取消**，用于取消此ISP信息的配置。

5.2.2. 全球地址段

『全球地址段』用于设置全球各个国家所拥有的IP地址段。

界面如下图所示：



『全球地址段』包括亚太、欧洲、北美、拉美、非洲板块。

5.2.2.1. 国家列表

选择地区，点击『国家列表』，例如选择北美地区，如下图所示：

ISP地址段	全球地址段	用户地域	自动更新
◀板块列表 板块：北美 ▾			导出
国家			缩写 操作
Anguilla		AI	编辑 导出
Antigua and Barbuda		AG	编辑 导出
Bahamas		BS	编辑 导出
Barbados		BB	编辑 导出
Belgium		BE	编辑 导出
Bermuda		BM	编辑 导出
Canada		CA	编辑 导出
Cayman Islands		KY	编辑 导出
Grenada		GD	编辑 导出
Guadeloupe		GP	编辑 导出
Guam		GU	编辑 导出
Jamaica		JM	编辑 导出
Luxembourg		LU	编辑 导出
Montserrat		MS	编辑 导出
Puerto Rico		PR	编辑 导出
Saint-Martin		MF	编辑 导出
St. Kitts Nevis		KN	编辑 导出
St. Lucia		LC	编辑 导出
St. Pierre and Miquelon		PM	编辑 导出

点击『板块列表』返回上一层。

增加“导出”按钮。

『板块』显示当前页面的板块，可以通过下拉框选择其它板块。

例如，点击“Anguilla”，如下图所示：

ISP地址段		全球地址段	用户地域	自动更新
国家列表		板 块 :	国 家 :	新建省市
<input type="checkbox"/>	省 市			操作
	安徽省			导出
	北京市			导出
	重庆市			导出
	福建省			导出
	广东省			导出
	甘肃省			导出
	广西壮族自治区			导出
	贵州省			导出
	河南省			导出
	湖北省			导出
	河北省			导出
	海南省			导出
	香港特别行政区			导出
	黑龙江省			导出
	湖南省			导出
	吉林省			导出
	江苏省			导出
	江西省			导出
	辽宁省			导出

点击『国家列表』返回上一层。

『板块』显示当前页面显示的板块，可以通过下拉框选择其它板块。

『国家』显示当前页面显示的国家，可以通过下拉框选择其它国家。

『省市』显示当前国家的省市。

点击**新增省市**，用于新增所选国家各个省市的IP段。如下图所示：

新建省市地址段

属性

板 块	亚太
国 家	China
省 市	

配置

地址范围

<input type="text"/>	-	<input type="text"/>
<input type="button" value="添加"/>		
<input type="button" value="删除"/>		

当前已配置0/10000个地址范围

导入地址范围文件

『板块』显示当前页面显示的板块，可以通过下拉框选择其它板块。

『国家』显示当前页面显示的国家，可以通过下拉框选择其它国家。

『省市』定义当前国家的省市。

『地址范围』填写 IP 段。

点击**添加**，用于添加设置的地址。

点击**删除**，用于删除选中的地址。

『导入地址范围文件』用于手动导入地址范围文件到 AD 设备，可以导入 ANSI 编码的 txt 格式文件。

配置完毕，点击**完成**，完成配置。

点击**取消**，用于取消配置。

若点击**编辑**，如下图所示：

编辑国家地址段

属性

板 块	亚太
国 家	Afghanistan
缩 写	AF

配置

地址范围

<input type="text"/> - <input type="text"/>	<input type="button" value="添加"/>	<input type="button" value="删除"/>
27.116.56.0-27.116.59.255 58.147.128.0-58.147.159.255 111.125.152.0-111.125.159.255 111.223.244.0-111.223.247.255 117.55.192.0-117.55.207.255 117.104.224.0-117.104.231.255 119.59.80.0-119.59.87.255 121.100.48.0-121.100.55.255		

当前已配置 18 / 10000 个地址范围

导入地址范围文件

『板块』显示当前页面显示的板块。

『国家』显示当前页面显示的国家。

『缩写』显示当前国家的缩写。

『地址范围』显示默认存在的IP段。

点击**添加**，用于添加设置的地址。

点击**删除**，用于删除选中的地址。

『导入地址范围文件』用于手动导入地址范围文件到AD设备，可以导入ANSI编码的txt格式文件。

配置完毕，点击**更新**，完成配置。

点击**取消**，用于取消配置。

5.2.2.2. 板块地址段

选择地区，点击『板块地址段』，例如选择亚太地区，如下图所示：

编辑板块地址段

属性

板 块 北美

配置

地址范围

<input type="text"/>	-	<input type="text"/>
<input type="button" value="添加"/>		
<input type="button" value="删除"/>		

3.0.0.0-4.255.255.255
6.0.0.0-9.255.255.255
11.0.0.0-13.255.255.255
15.0.0.0-22.255.255.255
24.0.0.0-24.30.255.255
24.31.32.0-24.35.127.255
24.36.0.0-24.38.191.255
24.39.0.0-24.40.79.255

当前已配置 4992 / 10000 个地址范围

导入地址范围文件

『板块』显示当前页面显示的板块。

『地址范围』显示默认存在的IP段。

点击添加，用于添加设置的地址。

点击删除，用于删除选中的地址。

『导入地址范围文件』用于手动导入地址范围文件到AD设备，可以导入ANSI编码的txt格式文件。

配置完毕，点击更新，完成配置。

点击取消，用于取消配置。

5.2.3. 用户地域

『用户地域』用于配置相应地域的WHOIS标志及各地域的IP地址范围，并以此来分辨访问用户所在的地域。

界面如下图所示：

ISP地址段		全球地址段	用户地域	自动更新
		+新建	删除	
<input type="checkbox"/>	名称	描述		
<input type="checkbox"/>	北京市			
<input type="checkbox"/>	天津市			
<input type="checkbox"/>	河北省			
<input type="checkbox"/>	山西省			
<input type="checkbox"/>	内蒙古自治区			
<input type="checkbox"/>	辽宁省			
<input type="checkbox"/>	吉林省			
<input type="checkbox"/>	黑龙江省			
<input type="checkbox"/>	上海市			
<input type="checkbox"/>	江苏省			
<input type="checkbox"/>	浙江省			
<input type="checkbox"/>	安徽省			
<input type="checkbox"/>	福建省			
<input type="checkbox"/>	江西省			
<input type="checkbox"/>	山东省			
<input type="checkbox"/>	河南省			
<input type="checkbox"/>	湖北省			
<input type="checkbox"/>	湖南省			
<input type="checkbox"/>	广东省			
<input type="checkbox"/>	广西壮族自治区			

点击**新建**，添加新的用户地域，如下图所示：

ISP地址段 | 全球地址段 | 用户地域 | 自动更新 | ? 帮助信息

新建

属性

名称

描述

配置

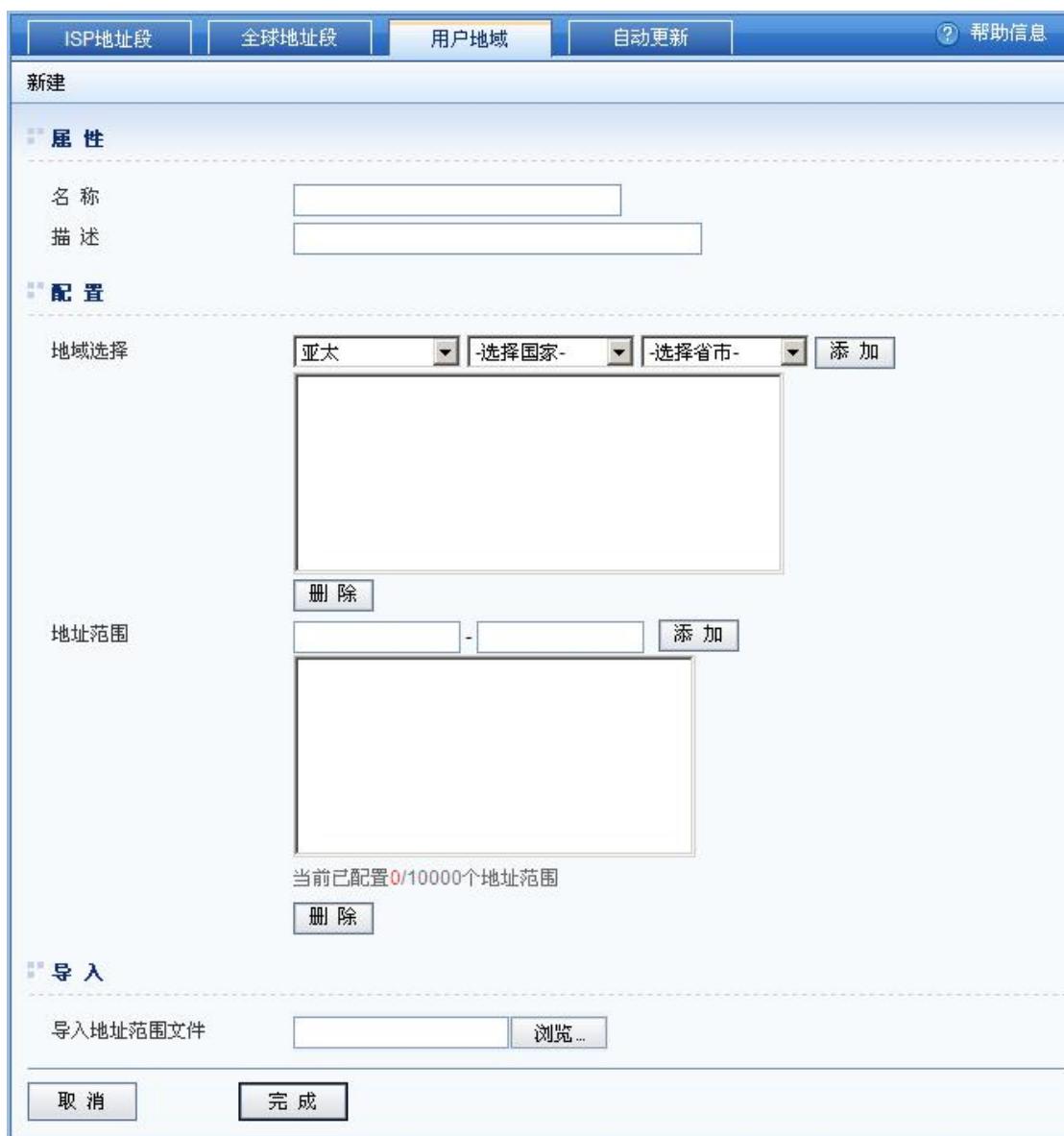
地域选择

地址范围
 -

当前已配置 0/10000 个地址范围

导入

导入地址范围文件



『名称』可以输入便于记忆和识别的字符串，用于标识自定义的用户地域。

『描述』可以输入便于记忆和识别的字符串，用于描述自定义的用户地域。

『地域选择』可以选择用户地域，包括板块、国家、省市。

『地址范围』显示默认存在的IP段。

点击 **添加**，用于添加设置的地址。

点击 **删除**，用于删除选中的地址。

『导入地址范围文件』用于手动导入地址范围文件到AD设备，可以导入ANSI编码的txt格式文件。

配置完毕，点击**更新**，完成配置。

点击**取消**，用于取消配置。

5.2.4. 自动更新

『自动更新』用于根据各个地域的WHOIS标志自动更新地址范围。

界面如下图所示：



The screenshot shows the 'Update Configuration' page with the following settings:

- 启用自动更新: 启用 禁用
- WHOIS服务器: whois.apnic.net
- 更新间隔时间: 每周
- 最近更新时间: 2014-04-09 13:22:58
- 最近更新信息: 最近更新了0个ISP地址段

A blue '更新' (Update) button is located at the bottom left.

『启用自动更新』用于设置启用或禁用自动更新功能。

『WHOIS服务器』用于设置从哪一台WHOIS服务器上去更新各个地域的地址范围。

『更新间隔时间』用于设置自动更新的周期。可以选择每天、每周或者是每月。

『最近更新时间』用于显示最近一次更新的时间。

『最近更新信息』用于显示自动更新的信息。

点击**更新**，保存配置。

5.3. 时间计划

WEBUI：『公共对象』→『时间计划』。

『时间计划』用于定义常用的时间段组合，在『路由设置』→『智能路由』中进行调用，设置在某个时间段内智能路由策略才生效。

界面如下图所示：

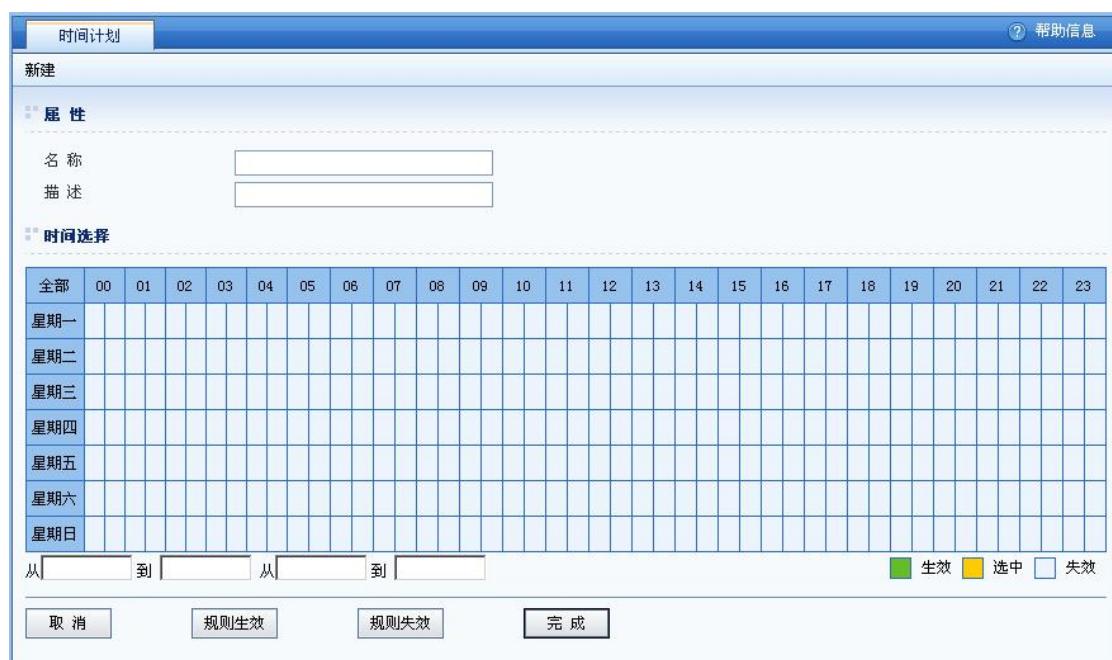


『时间计划』显示时间计划的『名称』、『时间计划描述』。

删除按钮可以用于删除时间计划，但不能删除默认时间计划。

新建按钮可以用于新建时间计划。

点击**新建**，配置页面如下：



The configuration interface for creating a new time plan. It includes fields for '名称' (Name) and '描述' (Description), and a large grid for selecting specific days and hours. At the bottom, there are buttons for '取消' (Cancel), '规则生效' (Effect Rule), '规则失效' (Invalidate Rule), and '完成' (Finish).

『名称』可以输入便于记忆和识别的字符串，用于时间计划。

『描述』可以输入便于记忆和识别的字符串。

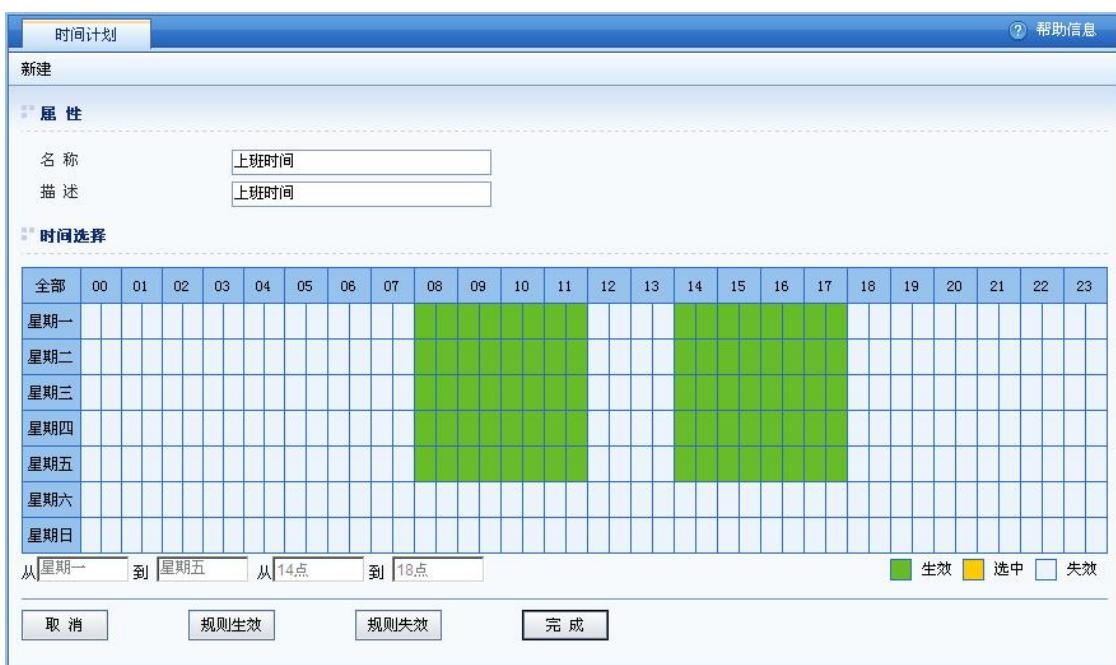
点击『规则生效』，则在时间坐标里选取的相应时间段生效。

点击『规则失效』，则在时间坐标里选取的相应时间段失效。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

例如，设置上午 8: 00-12: 00，下午 14: 00-18: 00 为上班时间，如下图所示：



The screenshot shows a 'Time Plan' configuration window. At the top, there's a toolbar with a 'Help' button. Below it is a 'New' button and a 'Properties' section containing 'Name' (上班时间) and 'Description' (上班时间). The main area is titled 'Time Selection' and features a weekly grid. The grid has columns for hours from 00 to 23. Rows represent days of the week: Monday through Sunday. Green shading covers the time slots from 08:00 to 12:00 on Monday-Friday, and from 14:00 to 18:00 on Monday-Friday, indicating active (生效) times. Below the grid, there are input fields for selecting specific days and times, and a legend at the bottom right. At the bottom of the window are four buttons: 'Cancel', 'Rule Effectiveness' (highlighted in yellow), 'Rule Ineffectiveness', and 'Finish'.

配置完成界面如下图所示：

	名称	时间计划描述
<input type="checkbox"/>	全天	全天
<input type="checkbox"/>	上班时间	上班时间

第 1 页, 共1页 每页显示条数 20 共2/50条配置信息

5.4. 脚本规则

webUI: 『公共对象』→『脚本规则』

『脚本规则』用于新建 ipro 规则，提供本地上传、在线编辑等方式。

界面如下图所示：

新建按钮用于配置所需要的 ipro 规则。

点击新建，配置页面如下：

The screenshot shows the Sangfor iPro configuration interface. On the left is a vertical navigation menu with sections such as System Overview, Report Configuration, Public Objects (which is currently selected), Data Center, Application Load Balancing, Intelligent DNS, Routing Configuration, Network Configuration, System Configuration, Configuration Wizard, and High Availability. The main right pane is titled '新建' (Create New) and '属性' (Properties). It has fields for '名称' (Name) and '描述' (Description), both with length restrictions. Below this is a section for '脚本内容' (Script Content) with a code editor. There are two radio buttons: '自定义代码' (Custom Code) (selected) and '本地文件' (Local File). A preview window shows the first line of the script: '1 |'. The overall interface is clean and modern.

『名称』标识一个脚本规则。

『描述』用以记录此脚本的作用。

『脚本来源』自定义代码时可以直接输入脚本内容；也可以通过导入本地文件的方式。

『脚本内容』Lua 语言编写的实现七层虚拟服务逻辑的文本。

完成按钮可以用于完成本次配置。



注意：新建 ipro 的右上角帮助信息中附有相关 ipro 的帮助文档，请下载阅读。

5.5. 自定义内容

WEBUI: 『公共对象』→『自定义内容』。

『自定义内容』用于定义一个返回的页面，在『应用负载』→『策略』→『前置调度策略』中引用，在前置调度策略中设置返回指定页面。

界面如下图所示：



The screenshot shows the Sangfor Cloud interface with the 'System Navigation Menu' on the left and the 'Custom Content' configuration page on the right.

System Navigation Menu:

- 系统概况
- 报表配置
- 公共对象
 - 用户地址集
 - IP地址集
 - 时间计划
 - 脚本执行
 - 自定义内容
- 数据中心
- 应用负载
- 智能DNS
- 路由配置
- 网络配置
- 系统配置
- 配置向导
- 高可用性
- 业务分析

Custom Content Configuration Page:

This page lists various custom content templates with their names and descriptions:

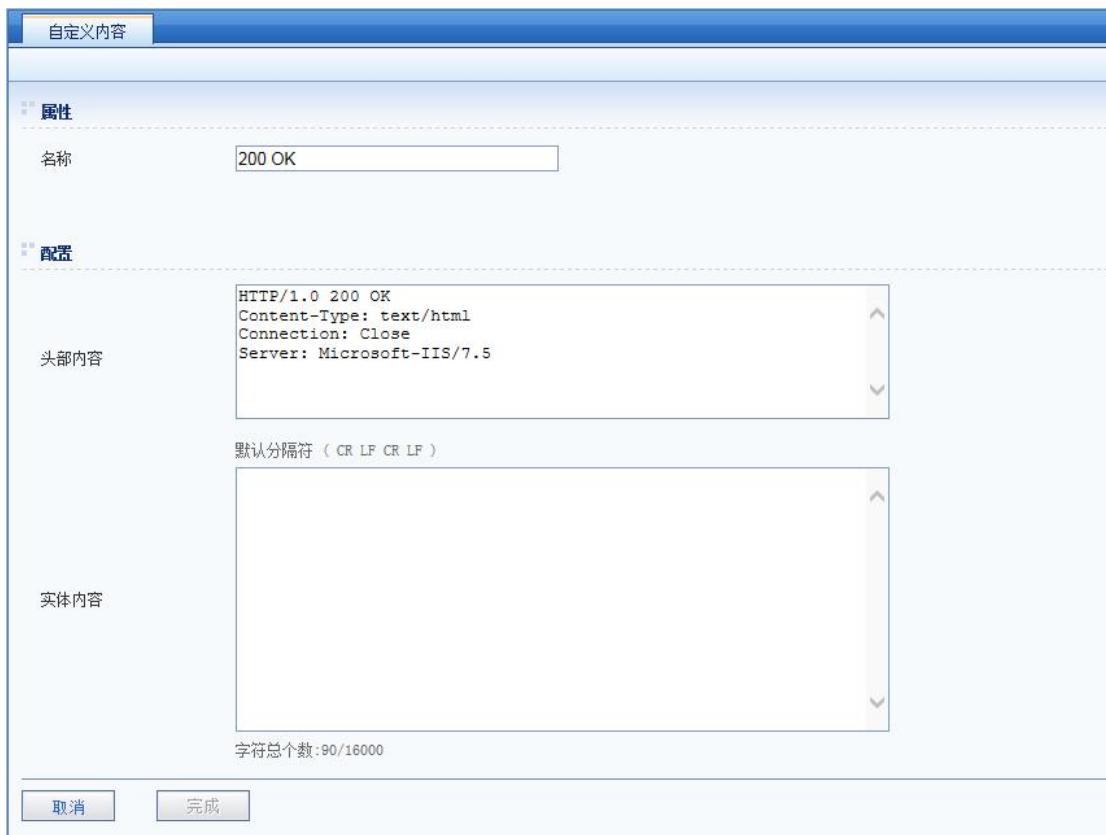
名称
200 OK
301 Moved Permanently
302 Moved Temporarily
400 Bad Request
403 Forbidden
404 Not Found
500 Internal Server Error
501 Not Implemented
502 Bad Gateway
503 Service Unavailable
认证失败默认规则
证书异常 [7] CERT_SIGNATURE_FAILURE
证书异常 [9] CERT_NOT_YET_VALID
证书异常 [10] CERT_HAS_EXPIRED
证书异常 [22] CERT_CHAIN_TOO_LONG
证书异常 [23] CERTIFICATE_REVOKED
证书异常 [27] CERT_IS_NOT_TRUSTED

『自定义内容』显示自定义页面的名称和动作。设备默认定义了一些页面返回的模板，设备自带的模板无法被前置调度策略引用，可在自定义页面中复制模板的内容。

『操作』用于复制模板内容。

新建按钮可以用于自定义内容。

点击**新建**，配置页面如下：



『名称』用于设定自定义内容的名称。

『内容』用于设定自定义的内容。头部和实体的配置用两个输入框分开。自动对头部做 unix 到 dos 格式的转换。

完成按钮可以用于完成本次配置。

例如，设置一个返回 502 Bad gateway 的页面内容，由于设备内置模版自带了这个页面，可直接复制这个模版，修改自定义页面的名称即可。点击模板“502 Bad Gateway”后面的复制按钮，如下图所示：

自定义内容

帮助信息

属性

名称: 502 Bad Gateway (长度限制为1~63字符, 且不能包含`<>|*|^:;%<>/\`特殊字符)

配置

头部内容:

```
HTTP/1.0 502 Bad Gateway
Server: Microsoft-IIS/7.5
Content-Type: text/html
Connection: Close
```

实体内容:

```
默认分隔符 (CR LF CR LF)
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<title>502 - Web 服务器在作为网关或代理服务器时收到了无效响应。</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
```

字符总个数:1462/16000

取消 完成

配置完成界面如下图所示：

自定义内容

+ 新建 X 删除 |

操作	名称
	200 OK
	301 Moved Permanently
	302 Moved Temporarily
	400 Bad Request
	403 Forbidden
	404 Not Found
	500 Internal Server Error
	501 Not Implemented
	502 Bad Gateway
	503 Service Unavailable
	502 Bad Gateway_1

第 1 页, 共1页 每页显示条数 20 共 11/100 条配置信息



默认模板不能删除，自定义的内容可以删除，本例中“502 Bad Gateway_1”自定义内容可以通过选中前面的复选框，点击删除按钮进行删除。

第6章 数据中心

数据中心用于配置数据中心设备和查看数据中心的相关状态，分为『状态概览』『数据中心』『本地服务设备』。

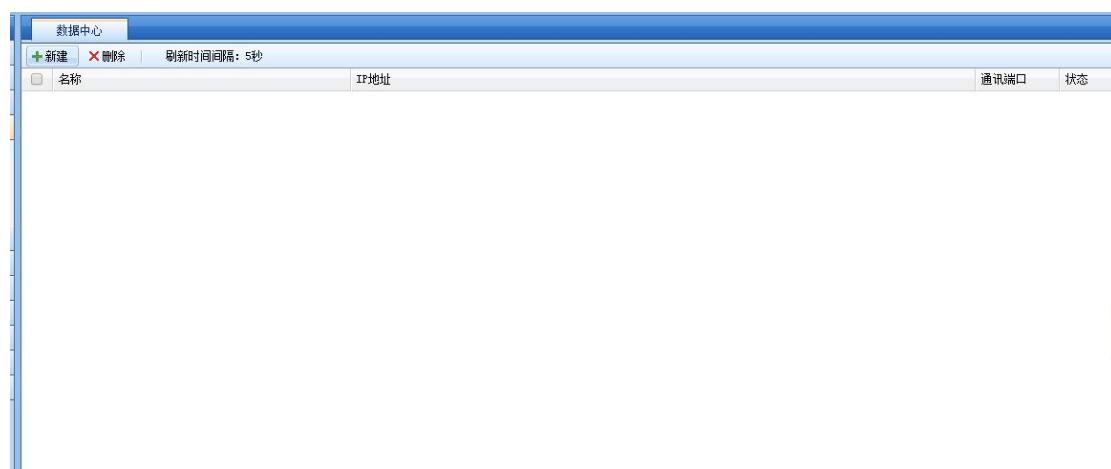
6.1 系统概览

『系统概况』用于显示数据中心服务器相关状态，可以查看数据中心的健康度，还有数据中心相关状态；比如并发连接数，新建连接数，吞吐量等，界面如下：



6.2 数据中心

数据中心用于配置数据中心服务器相关设置，界面如下图：



『删除』按钮可以用于删除数据中心。

『新建』按钮可以用于新建数据中心。点击『新建』，界面如下：



The screenshot shows the 'New Data Center' configuration dialog. At the top, there's a title bar with tabs for '数据中心' (Data Center) and '新建' (New). The '新建' tab is selected. Below the tabs, there are two sections: '普通属性' (General Properties) and '通讯配置' (Communication Configuration).

普通属性

- 名称 (Name): An input field.
- 地理位置 (Geographic Location): An input field.

通讯配置

- 地址列表 (Address List): A list box labeled '已选择' (Selected) on the left and '待选' (Available) on the right. It contains one item: 'route 1.2.3.4'. Between the two lists are left and right arrows for moving items.
- 通讯端口 (Communication Port): An input field containing '558'.
- 同步角色 (Sync Role): A dropdown menu currently set to 'None'.
- 同步公差 (Sync Tolerance): An input field containing '5' followed by '秒' (seconds).
- 通信加密密钥 (Communication Encryption Key): Two empty input fields for key entry.
- 再次输入密钥 (Re-enter Key): Two empty input fields for key re-entry.

At the bottom of the dialog are two buttons: '取消' (Cancel) and '完成' (Finish).

『名称』设置该数据中心的显示名称。

『地理位置』设置用于描述该数据中心的地理位置等相关信息。

『通讯列表』设置用于全局文件同步的地址列表。

『通讯端口』设置用于全局文件同步的通讯端口。

『同步角色』设置该数据中心在全局文件同步的角色。

None: 不参与全局文件同步。

Client：从其他数据中心下载最新的全局文件配置。

Server：向其他数据中心上传本站更新的全局文件配置。

Client & Server：同时扮演两个角色，既可上传亦可下载。

『同步公差』全局同步过程中，两个数据中心间的配置文件修改时间差的阈值。当两个数据中心配置文件修改时间差值大于[同步公差]时，表明修改时间较早的数据中心配置文件需要被更新；当两个数据中心配置文件修改时间的差值小于等于[同步公差]时，表明两个数据中心的配置文件被视为等效且不同步。

『通信加密密钥』用于数据中心之间通信的加密密钥。

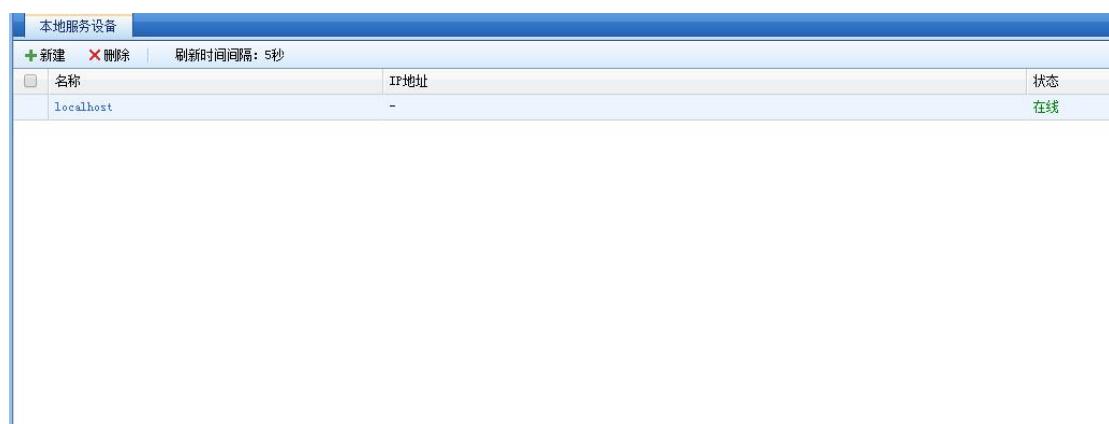
『再次输入密钥』再次输入以确认“通信加密密钥”。

点击**完成**，完成此次数据中心的配置。

点击**取消**，用于取消此次数据中心的配置。

6.3 本地服务设备

『本地服务设备』用于配置提供服务的本地设备信息。界面如下图：



本地服务设备		
+新建		删除
刷新时间间隔：5秒		
<input type="checkbox"/>	名称	IP地址
	localhost	-
		状态
		在线

删除按钮可以用于删除本地设备。

新建按钮可以用于新建本地设备。点击**新建**，界面如下：

系统导航菜单

- ▶ 系统概况
- ▶ 报表配置
- ▶ 公共对象
- ▶ **数据中心**
 - ▶ 状态概览
 - ▶ 数据中心
 - ▶ **本地服务设备**
- ▶ 应用负载
- ▶ 智能DNS
- ▶ 路由配置
- ▶ 网络配置
- ▶ 系统配置
- ▶ 配置向导
- ▶ 高可用性

本地服务设备

添加

普通属性

名称 (长度限制为1~16个字符，且不能包含<><><><>特殊字符)

地址列表

通讯端口

『名称』 标记本地数据中心服务器负载设备。

『地址列表』 服务器负载设备的 IP 地址。

『通讯端口』 服务器负载 SNMP 服务的端口

第7章 应用负载

『应用负载』用于配置需要对外发布的应用的负载，包括『服务』、『IP组』、『会话保持』、『节点监视器』、『节点池』、『SSL』、『策略』、『虚拟服务』几个部分，通过这几个部分的组合配置可以灵活高效地发布应用。

7.1. 服务

WEBUI: 『应用负载』→『服务』。

『服务』用于定义需要发布的应用属于何种服务，此处定义的『服务』，可用于『策略』、『虚拟服务』配置部分。

界面如下图所示：

名称	类型	端口
http	HTTP	80
smtp	TCP	25
pop3	TCP	110
dns	DNS	53
https	HTTPS	443
ssl	SSL	443
imap_ssl	SSL	993
smtp_ssl	SSL	465
pop3_ssl	SSL	995
radius_auth	RADIUS	1812
radius_acct	RADIUS	1813
ftp	FTP	21
mysql	MYSQL	3306
oracle	ORACLE	1521

『服务』下显示的服务的『名称』、『类型』、『端口』，包括系统默认服务和自定义服务。

删除按钮可以用于删除自定义服务，但不能删除默认服务。

新建按钮可以用于新建自定义服务。若默认服务无法满足需求，例如需要 TCP 81 端口的 HTTP 服务，可以修改默认设置，或者新建服务。

以下以新建 TCP 81 端口的 HTTP 服务为例，点击**新建**按钮，如下图所示：

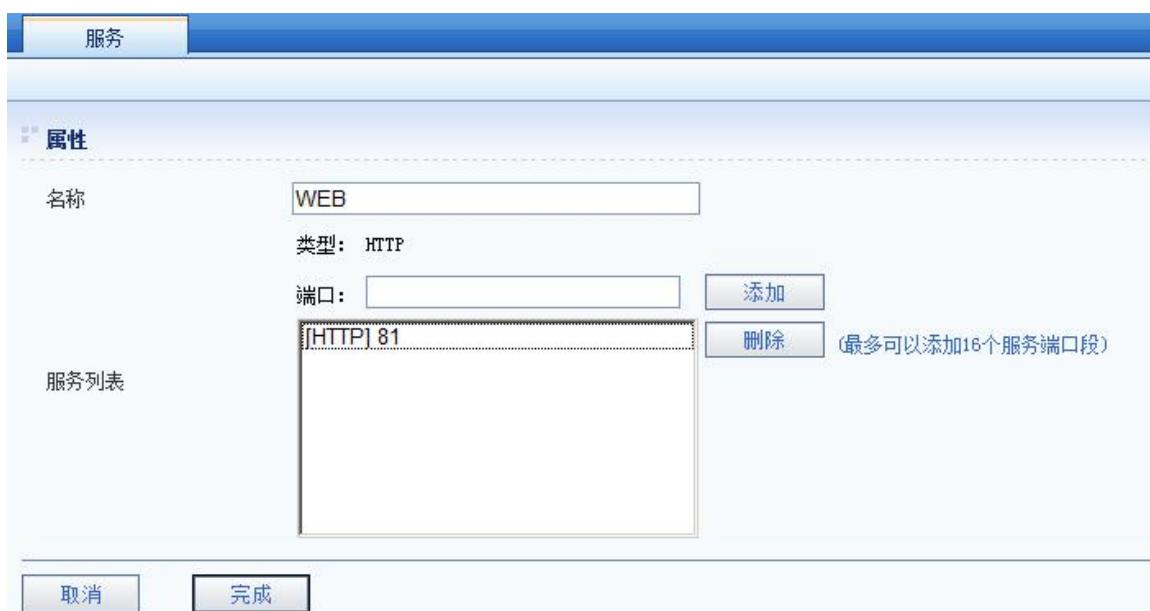


『请选择服务类型』下面显示可以选择的服务类型，包括[TCP]、[UDP]、[HTTP]、[HTTPS]、[SSL]、[Radius]、[DNS]、[FTP]、[MYSQL]。

取消按钮可以用于取消本次配置。

下一步按钮可以用于继续下一步配置。

此例中选择[HTTP]，点击**下一步**按钮，如下图所示：



『名称』可以输入便于记忆和识别的字符串，用于标识自定义的服务。

『类型』为上一步配置中选择的服务类型。

『端口列表』用于配置服务的端口或端口范围，在『端口』（或范围）处输入端口号，点击**添加**按钮即可加入『端口列表』，选中已加入『端口列表』的端口（或范围），点击**删除**按钮即可从『端口列表』中删除已添加的端口（或范围）。端口范围为1-65535，最多可以添加16个端口范围。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

此例中，输入便于记忆和识别的『名称』，例如“WEB”，输入『端口』（或范围），此例中输入“81”，点击**添加**按钮，则“81”端口添加到『端口列表』中，最后点击**完成**按钮即可完成配置。

配置完成界面如下图所示：



服务			
	名称	类型	端 口
	http	HTTP	80
	smtp	TCP	25
	pop3	TCP	110
	dns	DNS	53
	https	HTTPS	443
	ssl	SSL	443
	imap_ssl	SSL	993
	smtp_ssl	SSL	465
	pop3_ssl	SSL	995
	radius_auth	RADIUS	1812
	radius_acct	RADIUS	1813
	ftp	FTP	21
	mysql	MYSQL	3306
	oracle	ORACLE	1521
	WEB	HTTP	81



默认服务不能删除，自定义的服务可以删除，本例中“WEB”服务可以通过选中前面的复选框，点击删除按钮进行删除。

7.2. IP 组

WEBUI: 『应用负载』→『IP 组』。

『IP 组』用于定义需要发布的应用的链路 IP 地址，支持 IPV4 和 IPV6 混配。此处定义的『IP 组』，可用于『虚拟 IP 池』、『虚拟服务』配置部分。

界面如下图所示：



IP组	
+ 新建 X 删除	
名称	IP地址
IP-11	192.168.100.11 / 192.168.200.11 /
IP-12	192.168.100.12 / 192.168.200.12 /
IP-13	2000:3:4:5:0:0:0:6 / 10.10.10.1 /

右上角的搜索框可以用来从列表中查找 IP 组。

『IP 组列表』下显示 IP 组的『名称』、『IP 地址』。

删除按钮可以用于删除 IP 组。

新建按钮可以用于新建 IP 组。

点击新建按钮，如下图所示：



IP组

新建

属性

名称: test

IP地址: 2000.0.0.0-0.0.1

已选择: WAN1
192.168.100.21

IP组: 手动添加
WAN1
192.168.100.21

(最多可以添加32个IP)

显示WAN口IP对应的互联网IP

取消 完成

『名称』可以输入便于记忆和识别的字符串，用于标识 IP 组。

『IP 地址』可以在这手动添加 IP 地址到 IP 组

『IP 组』可以选择需要配置为本组的外网 IP，点击按钮左移即可将选定的 IP 加入该 IP 组。若需要将已经选定的 IP 从该 IP 组移除，选定需要移除的 IP，点击按钮右移选定的 IP 即可。如果是手动添加的 IP，点击按钮右移后，IP 则自动删除。

[显示 WAN 口 IP 对应的互联网 IP]复选框可以切换 IP 显示方式，若勾选上该选项，则 IP 地址会以『网络配置』→『网络接口』中配置的『对应互联网 IP』显示。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

此例中，输入便于记忆和识别的『名称』，例如“网通 IP 组”，选定需要加入该 IP 组的 IP 地址并左移，最后点击完成按钮即可完成配置。



说明：支持空的 IP 组。

7.3. 会话保持

WEBUI: 『应用负载』→『会话保持』。

『会话保持』用于定义需要发布的应用启用何种会话保持方法，此处定义的『会话保持方法』，可用于『节点池』配置部分。

界面如下图所示：

删除按钮可以用于删除自定义会话保持方法。

新建按钮可以用于新建自定义会话保持方法。

点击**新建**按钮，如下图所示：

『类型』下面显示可以选择的会话保持方法类型，包括[SourceIP]、[Cookie]、[HTTP Passive]、[Radius]和[SSL SessionID]。

取消按钮可以用于取消本次配置。

下一步按钮可以用于继续下一步配置。

✓ SourceIP

选择[SourceIP]，配置基于源 IP 的会话保持方式。点击**下一步**按钮，如下图所示：



『名称』可以输入便于记忆和识别的字符串，用于标识自定义的会话保持方法。

『类型』为上一步配置中选择的 SourceIP 类型。

『超时时间』用于配置会话保持方法的超时时间，单位支持秒，分钟，小时，天。

『掩码』用于配置会话保持方法 SourceIP 类型的客户端 IP 地址掩码，会话保持支持 IPV4 和 IPV6 混配。

『优先于连接限制』命中会话保持的连接是否收到节点中连接数的限制。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

✓ Cookie

选择[Cookie]，配置基于 Cookie 的会话保持方式。点击**下一步**按钮，如下图所示：

会话保持

新建

普通属性

名称	<input type="text"/>
类型	Cookie
保持方式	插入
Cookie名称	<input type="text"/>
Cookie作用域	域名： <input type="text"/> 路径： <input type="text"/>
会话Cookie	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
HttpOnly	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用

配置

优先于繁忙	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
-------	--

取消 **完成**

『名称』可以输入便于记忆和识别的字符串，用于标识自定义的会话保持方法。

『类型』为上一步配置中选择的 Cookie 类型。

『保持方式』设置 Cookie 的会话保持方式，可选择插入、被动和改写。当 AD 在收到服务端的应答时，若为插入方式，会在应答的 HTTP 协议头部添加 Set-cookie 字段创建会话保持，该字段的内容包括 Cookie 名称，cookie 作用域域名和路径，以及超时时间；若为被动方式，会通过分析应答的 HTTP 头部中 Set-cookie 字段找到对应的 Cookie 信息，将此 Cookie 和对应的节点信息记录下来，供下次调度使用；如果选择改写方式，通过匹配应答的 HTTP 头部中 Set-cookie 字段的 Cookie 名称进行改写，插入节点信息，并在请求时根据节点信息做会话保持。

『Cookie 名称』用于定义该前置调度策略返回给客户端 Cookie 名称。不同的前置调度策略 Cookie 名称要设置不一样。

『Cookie 作用域』→『域名』主要是用于如下场景：发布了某一个虚拟服务 www.test.com

采用 Cookie 会话保持，如果需要访问该页面上的链接 news.test.com，则不会匹配到会话保持，会重新调度，则可能造成访问不到，此时需要设置域名 test.com 可以保证子域名也匹配到会话保持。

『Cookie 作用域』→『路径』主要是用于如下场景：客户有两台不同的 HTTP 服务器 A 和 B，未部署 AD 的时候通过 www.test.com/test1/1.php 则可以调度到服务器 A，通过 www.test.com/test2/2.php 则可以调度到服务器 B，部署 AD 之后也需要实现该需求，此时需要使用路径来区分不同的服务器，使不同的路径调度到不同的服务器。

『会话 Cookie』用于设置启用或者禁用会话 Cookie。

『HttpOnly』用于设置启用或者禁用会话 HttpOnly。

『优先于连接限制』命中会话保持的连接是否收到节点中连接数的限制。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

✓ HTTP Passive

选择**[HTTP Passive]**，配置处理 HTTP Passive 的被动会话保持方式。点击**下一步**按钮，如下图所示：

新建

属性

名称

类型 HTTP Passive

基本配置

保持方式 启用 禁用

请求内容匹配

会话ID的查找位置
头部名称
关键字
偏移量
结束字符

(至多可以配置 4项请求内容匹配)

应答内容匹配

会话ID的学习位置
头部名称
关键字
偏移量
结束字符

(至多可以配置 4项应答内容匹配)

其他配置

超时时间 天

『名称』可以输入便于记忆和识别的字符串，用于标识自定义的会话保持方法。

『类型』为上一步配置中选择的 HTTP Passive 类型。

『保持方式』可设置根据请求方向和应答方向的某个字段做会话保持。

『优先于连接限制』命中会话保持的连接是否收到节点中连接数的限制。

『会话 ID 查找位置』可选择头部、URI 或者内容。

『头部名称』定义请求方向的HTTP头部名称。

『关键字』定义请求方向的关键字名称。

『请移量』定义请求方向从关键字开始偏移的位数。

『结束字符』定义请求方向的关键字结束的字符。

『会话ID学习位置』应答方向会话ID学习位置，包括头部和内容。

『头部名称』定义应答方向的HTTP头部名称。

『关键字』定义应答方向的关键字名称。

『偏移量』定义应答方向从关键字开始偏移的位数。

『结束字符』定义应答方向的关键字结束的字符。

『超时时间』用于配置会话保持方法的超时时间。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

✓ Radius

选择**[Radius]**，点击**[下一步]**按钮，如下图所示：



新建

属性

名称

类型 Radius

配置

属性ID User-Name 1

超时时间 1 天

优先于连接限制 启用 禁用

取消 **完成**

『名称』可以输入便于记忆和识别的字符串，用于标识自定义的会话保持方法。

『类型』为上一步配置中选择的 Radius 类型。

『属性 ID』用于定义根据 Radius 的哪个属性值进行会话保持，可以选择系统自带的属性值以及自定义属性值。

『超时时间』用于配置会话保持方法的超时时间，单位为秒。

『优先于连接限制』命中会话保持的连接是否收到节点中连接数的限制。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

✓ SSL SessionID

选择[SSL SessionID]，点击**下一步**按钮，如下图所示：



The screenshot shows a configuration dialog box titled '新建' (New). It has two tabs: '普通属性' (General Properties) and '配置' (Configuration). In the '普通属性' tab, there are fields for '名称' (Name), '类型' (Type selected as 'SSL SessionID'), and '超时时间' (Timeout, set to 1 day). In the '配置' tab, there is a checkbox '优先于连接限制' (Prioritize connection limit) which is checked. At the bottom are '取消' (Cancel) and '完成' (Finish) buttons.

『名称』可以输入便于记忆和识别的字符串，用于标识自定义的会话保持方法。

『类型』为上一步配置中选择的 SSL SessionID 类型。根据 SSL Session ID 做会话保持，确保同一用户的 SSL 访问请求能够调度到同一台应用服务器。

『超时时间』用于配置会话保持方法的超时时间，单位为天。

『优先于连接限制』命中会话保持的连接是否收到节点中连接数的限制。

取消按钮可以用于取消本次配置。

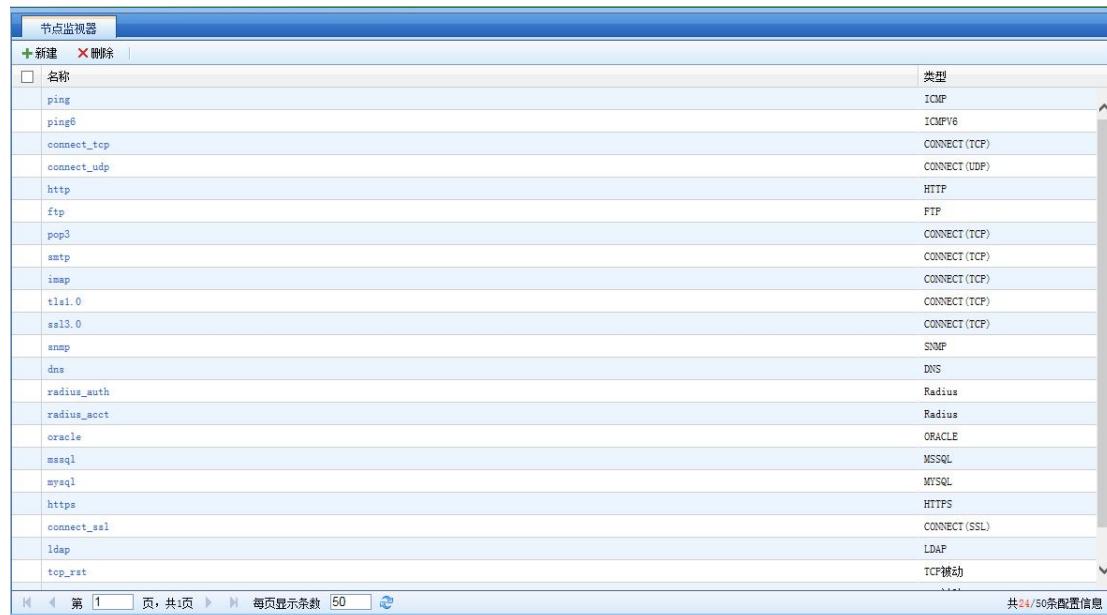
完成按钮可以用于完成本次配置。

7.4. 节点监视器

WEBUI: 『应用负载』→『节点监视器』。

『节点监视器』用于定义如何监视需要发布的应用对应的节点状态，此处定义的『节点监视器』，可用于『节点池』配置部分。

界面如下图所示：



节点监视器	
<input type="button" value="新建"/>	<input type="button" value="删除"/>
<input type="checkbox"/>	名称
<input type="checkbox"/>	ping
<input type="checkbox"/>	ping6
<input type="checkbox"/>	connect_tcp
<input type="checkbox"/>	connect_udp
<input type="checkbox"/>	http
<input type="checkbox"/>	ftp
<input type="checkbox"/>	pop3
<input type="checkbox"/>	smtp
<input type="checkbox"/>	imap
<input type="checkbox"/>	telnet
<input type="checkbox"/>	ssl3.0
<input type="checkbox"/>	snmp
<input type="checkbox"/>	dns
<input type="checkbox"/>	radius_auth
<input type="checkbox"/>	radius_acct
<input type="checkbox"/>	oracle
<input type="checkbox"/>	mssql
<input type="checkbox"/>	mysql
<input type="checkbox"/>	https
<input type="checkbox"/>	connect_ssl
<input type="checkbox"/>	ldap
<input type="checkbox"/>	tcp_rst
	类型
	ICMP
	ICMPV6
	CONNECT(TCP)
	CONNECT(UDP)
	HTTP
	FTP
	CONNECT(TCP)
	SNMP
	DNS
	Radius
	Radius
	ORACLE
	MSSQL
	MySQL
	HTTPS
	CONNECT(SSL)
	LDAP
	TCP被动

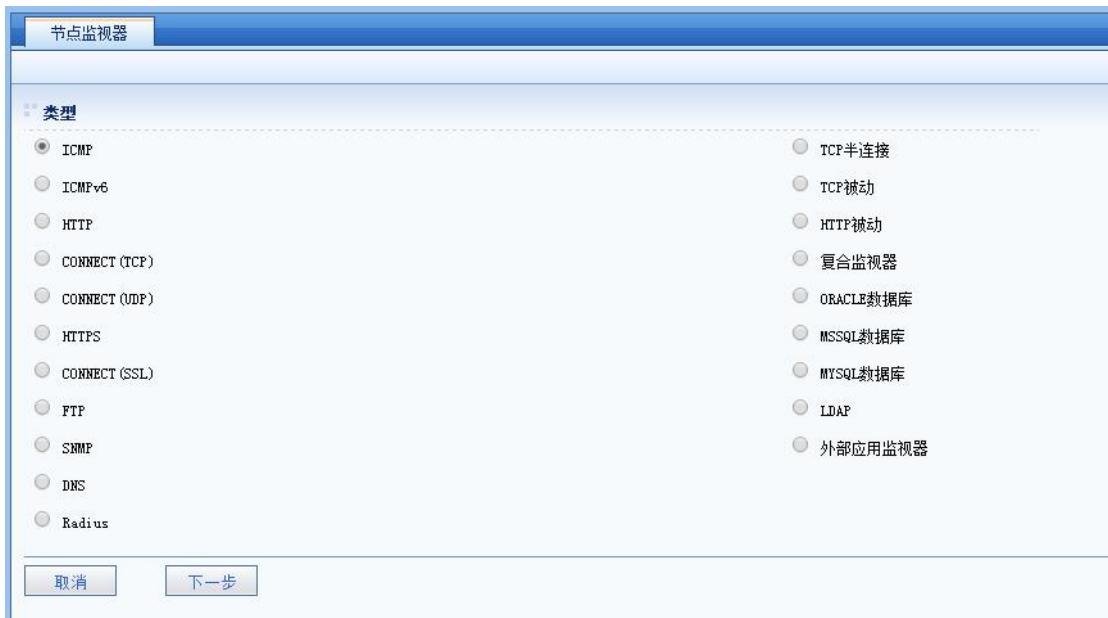
『节点监视器』下显示的节点监视器的『名称』、『类型』，包括系统默认节点监视器和自定义节点监视器。

节点监视器		类型
<input type="checkbox"/>	名称	
<input type="checkbox"/>	ping	ICMP
<input type="checkbox"/>	ping6	ICMPv6
<input type="checkbox"/>	connect_tcp	CONNECT (TCP)
<input type="checkbox"/>	connect_udp	CONNECT (UDP)
<input type="checkbox"/>	http	CONNECT (TCP)
<input type="checkbox"/>	ftp	CONNECT (TCP)
<input type="checkbox"/>	pop3	CONNECT (TCP)
<input type="checkbox"/>	smt	CONNECT (TCP)
<input type="checkbox"/>	imap	CONNECT (TCP)
<input type="checkbox"/>	telnet	CONNECT (TCP)
<input type="checkbox"/>	ssh	CONNECT (TCP)
<input type="checkbox"/>	snmp	SNMP
<input type="checkbox"/>	dns	DNS
<input type="checkbox"/>	radius_auth	Radius
<input type="checkbox"/>	radius_acct	Radius
<input type="checkbox"/>	tcp_rst	TCP被动
<input type="checkbox"/>	tcp_zero_win	TCP被动
<input type="checkbox"/>	MySQL数据库监视器	MySQL

删除按钮可以用于删除自定义节点监视器，但不能删除默认节点监视器。

新建按钮可以用于新建自定义节点监视器。

点击**新建**按钮，如下图所示：



『类型』下面显示可以选择的节点监视器类型。

取消按钮可以用于取消本次配置。

下一步按钮可以用于继续下一步配置。

✓ ICMP

选择[ICMP]，设备会发送 IPv4 地址格式的 ICMP 包对节点进行探测。点击**下一步**按钮，如下图所示：



『名称』可以输入便于记忆和识别的字符串，用于标识自定义的节点监视器。

『类型』为上一步配置中选择的类型。

『间隔时间』用于配置监视的间隔时间，单位为秒。

『超时时间』用于配置监视的超时时间，单位为秒。

『尝试次数』用于配置监视超时后的尝试次数。

『监视地址』用于配置监视的 IP 地址，“*”为监视所有。

『开启调试日志』用于配置是否启用该监视器的调试日志，启用后会在日志中显示详细的连接记录。

✓ ICMPv6

选择[ICMPv6]，设备会发送 IPv6 地址格式的 ICMP 包对节点进行探测。点击**下一步**按钮，如下图所示：

新建

属性

名称 (长度限制为1~63字符, 且不能包含& | " " , : % < > / \ 特殊字符)

类型 ICMPv6

配置

间隔时间 秒

超时时间 秒

尝试次数

监视地址

开启调试日志 是 否

『名称』可以输入便于记忆和识别的字符串，用于标识自定义的节点监视器。

『类型』为上一步配置中选择的类型。

『间隔时间』用于配置监视的间隔时间，单位为秒。

『超时时间』用于配置监视的超时时间，单位为秒。

『尝试次数』用于配置监视超时后的尝试次数。

『监视地址』配置监视的IP地址，“*”为监视所有，此处为IPv6的规范地址。

✓ CONNECT(TCP)

选择[CONNECT (TCP)]，设备会发送 TCP 的连接对节点进行探测。点击**下一步**按钮，
如下图所示：

节点监视器

新建

属性

名称

类型 CONNECT (TCP)

基本配置

间隔时间 秒
5

超时时间 秒
2

尝试次数 3

监视地址 *

监视端口 * default

调试 是 否

附加配置

回应内容的最大长度 字节
2048

发送内容

接收内容必须包含

断开之前发送的内容

启用十六进制模式 是 否

『监视端口』用于配置监视 CONNECT TCP 类型监视的端口，包括[default]、[http]、[smtp]、[pop3]、[imap]、[ftp] 、[other]，选择[other]时可以在输入框中填写自定义端口。

『回应内容最大长度』用于配置监视 CONNECT 类型回应数据内容的最大长度，单位为字节。

『发送内容』用于配置监视 CONNECT 类型建立连接之后发送的数据内容。

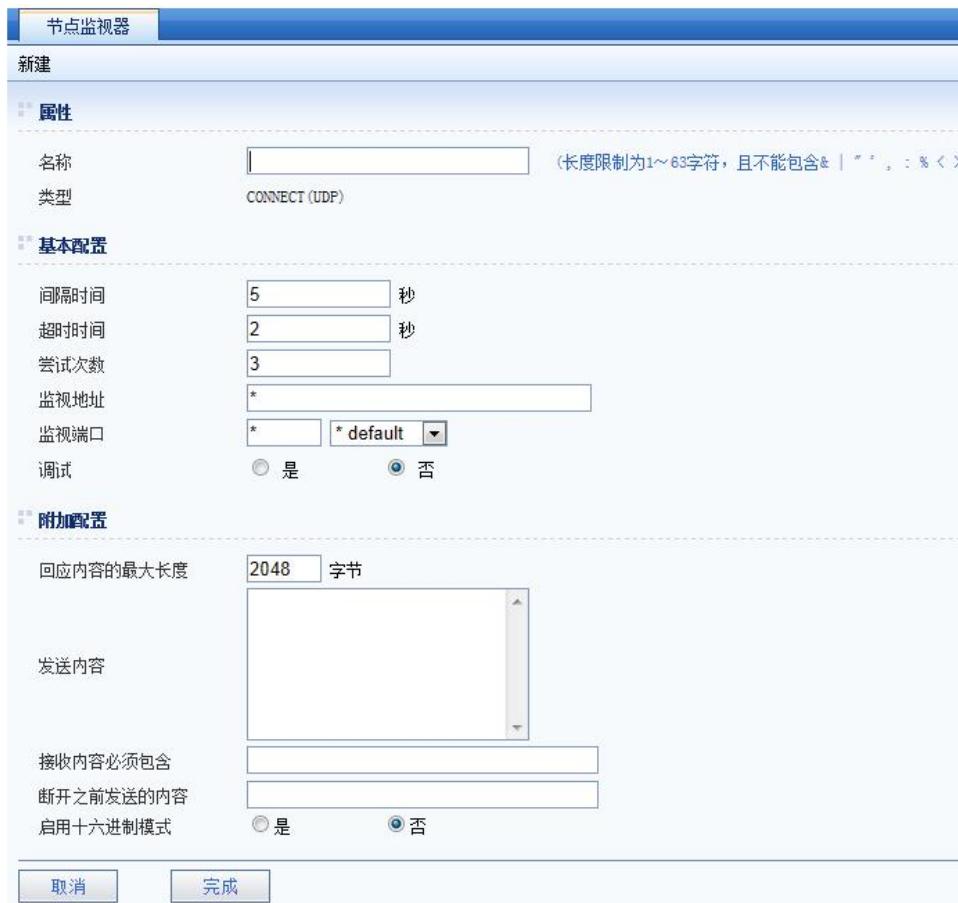
『接收内容必须包含』用于配置监视 CONNECT 类型接受数据必须包含的内容。

『断开之前发送的内容』用于配置监视 CONNECT 类型断开连接之前发送的数据内容。

『启用十六进制模式』用于配置监视 CONNECT 类型发送、接收的数据内容[是]、[否]启用十六进制模式。

✓ CONNECT(UDP)

选择[CONNECT (UDP)]，设备会发送 UDP 的连接对节点进行探测。点击[下一步]按钮，如下图所示：



『监视端口』用于配置监视 CONNECT UDP 类型监视端口，包括[default]、[http]、[smtp]、[pop3]、[imap]、[ftp]、[other]，选择[other]时可以在输入框中填写自定义端口。

『回应内容最大长度』用于配置监视 CONNECT 类型回应数据内容的最大长度，单位为字节。

『发送内容』用于配置监视 CONNECT 类型建立连接之后发送的数据内容。

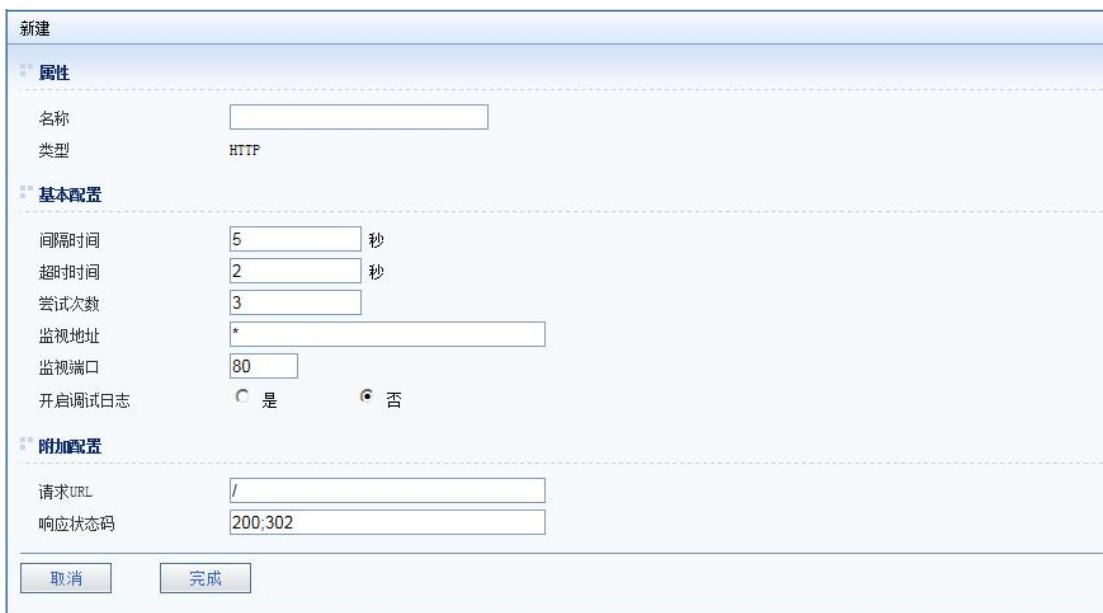
『接收内容必须包含』用于配置监视 CONNECT 类型接受数据必须包含的内容。

『断开之前发送的内容』用于配置监视 CONNECT 类型断开连接之前发送的数据内容。

『启用十六进制模式』用于配置监视 CONNECT 类型发送、接收的数据内容[是]、[否]启用十六进制模式。

✓ HTTP

选择[HTTP]，点击**下一步**按钮，如下图所示：



新建

属性

名称

类型 HTTP

基本配置

间隔时间 秒

超时时间 秒

尝试次数

监视地址

监视端口

开启调试日志 是 否

附加配置

请求URL

响应状态码

操作

取消 完成

『监视端口』用于配置监视 HTTP 类型监视的端口，默认为 80。

『请求 URL』用于设置监视的 URL，有三种填写格式，可自动识别 host 和 URI。支持填写的三种格式如下：

1. <http://www.abc.com>
2. www.abc.com
3. /a/b

『响应状态码』用于设置 HTTP 服务器的响应状态码，根据这个状态码判断服务器在线或者离线。

✓ FTP

选择[FTP]，通过登录FTP服务器对其进行监视。点击[下一步]按钮，如下图所示：

新建

属性

名称 类型 FTP

基本配置

间隔时间 秒
超时时间 秒
尝试次数
监视地址
监视端口
开启调试日志 是 否

附加配置

匿名登录 是 否
用户名
密码
路径
模式

『监视端口』用于配置监视FTP类型监视的端口，默认为21。

『匿名登录』用于是否启用FTP匿名登录。

『用户名』用于配置登录FTP服务器的用户名。

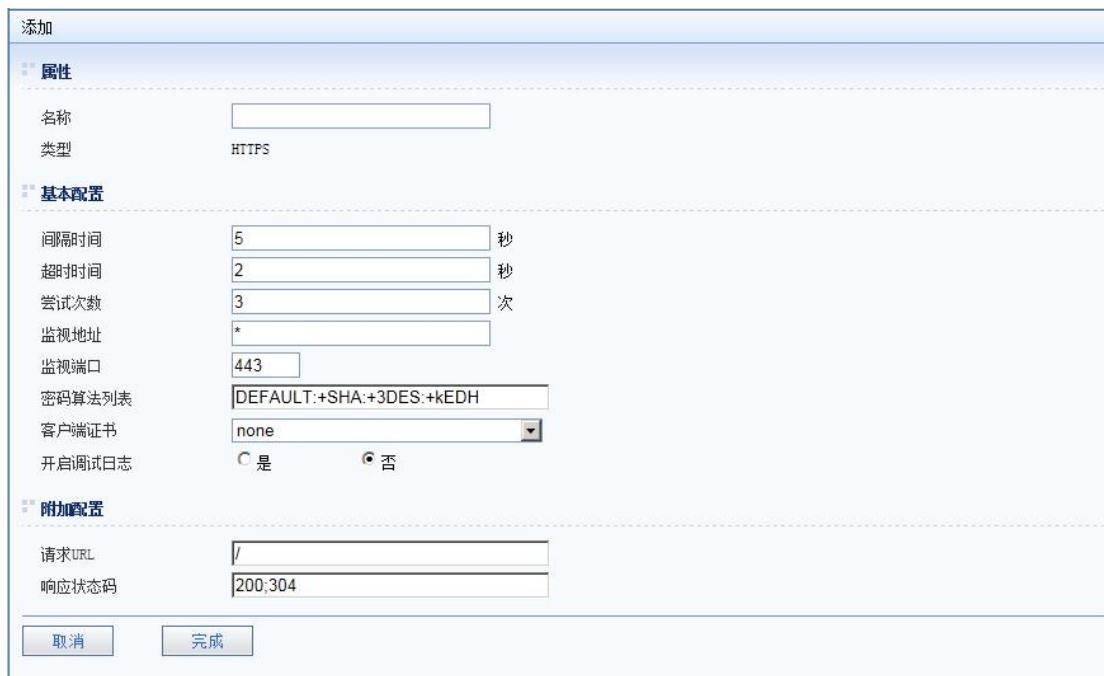
『密码』用于配置登录FTP服务器的密码。

『路径』用于配置监视FTP服务器的文件路径。

『模式』用于配置FTP服务器的工作模式，包括PASSIVE和PORT模式。

✓ HTTPS

选择[HTTPS]，设备通过发送 HTTPS 请求方式对节点进行状态监视。点击**下一步**按钮，如下图所示：



The screenshot shows the configuration interface for adding a new monitoring item. The 'Type' is set to 'HTTPS'. Under 'Basic Configuration', the 'Monitoring Port' is set to 443. Under 'Advanced Configuration', the 'Request URL' field contains a placeholder value and the 'Response Status Code' field contains 200,304.

『监视端口』用于配置监视 HTTPS 服务的监视端口，默认为 443。

『密码算法列表』配置 HTTPS 建立连接时使用到的加密和认证算法。

『客户端证书』用于配置 HTTPS 监视时是否提交客户端证书进行认证。证书配置见 6.6 章节介绍。

『请求 URL』用于设置监视的 URL，有三种填写格式，可自动识别 HOST 和 URI。

『响应状态码』用于设置 HTTP 服务器的响应状态码，根据这个状态码判断服务器在线或者离线。

✓ CONNECT(SSL)

选择[CONNECT(SSL)]，对使用 SSL 加密的服务节点进行监控，点击**下一步**按钮，如

下图所示：

属性

名称

类型 CONNECT (SSL)

基本配置

间隔时间 秒

超时时间 秒

尝试次数 次

监视地址

监视端口 https

密码算法列表

客户端证书

开启调试日志 是 否

附加配置

回应内容的最大长度

发送内容

接收内容必须包含

断开之前发送的内容

启用十六进制模式 是 否

监听端口可以选择 http、ftp、smtp、pop3、imap、https 和 other 类型的端口。选择 other 类型时可以自定义端口。

『密码算法列表』配置 HTTPS 建立连接时使用到的加密和认证算法。

『客户端证书』用于配置 HTTPS 监视时是否提交客户端证书进行认证。证书配置见 6.6 章节介绍。

✓ SNMP

选择[SNMP]，通过 SNMP 协议对主机的性能进行监控。点击**下一步**按钮，如下图所示：

节点监视器

新建

属性

名称

类型 SNMP

基本配置

间隔时间 秒

超时时间 秒

尝试次数 次

监视地址

监视端口

调试 是 否

附加配置

查询密码

CPU占用率最大值 %

CPU权重

内存占用率最大值 %

内存权重

磁盘占用率最大值 %

磁盘权重

『监视端口』用于配置监视 SNMP 类型监视的端口，默认为 161。

『查询密码』用于配置监视 SNMP 类型的查询密码，默认为“public”，可根据实际情况进行修改。

『CPU 占用率最大值』用于配置监视 SNMP 类型的 CPU 占用率最大值，超过此数值即节点繁忙。

『CPU权重』用于配置监视SNMP类型的CPU权重，用于动态反馈的节点选择策略，详情请参考 6.5 节点池。

『内存占用率最大值』用于配置监视 SNMP 类型的内存占用率最大值，超过此数值即节点繁忙。

『内存权重』用于配置监视SNMP类型的内存权重，用于动态反馈的节点选择策略，详

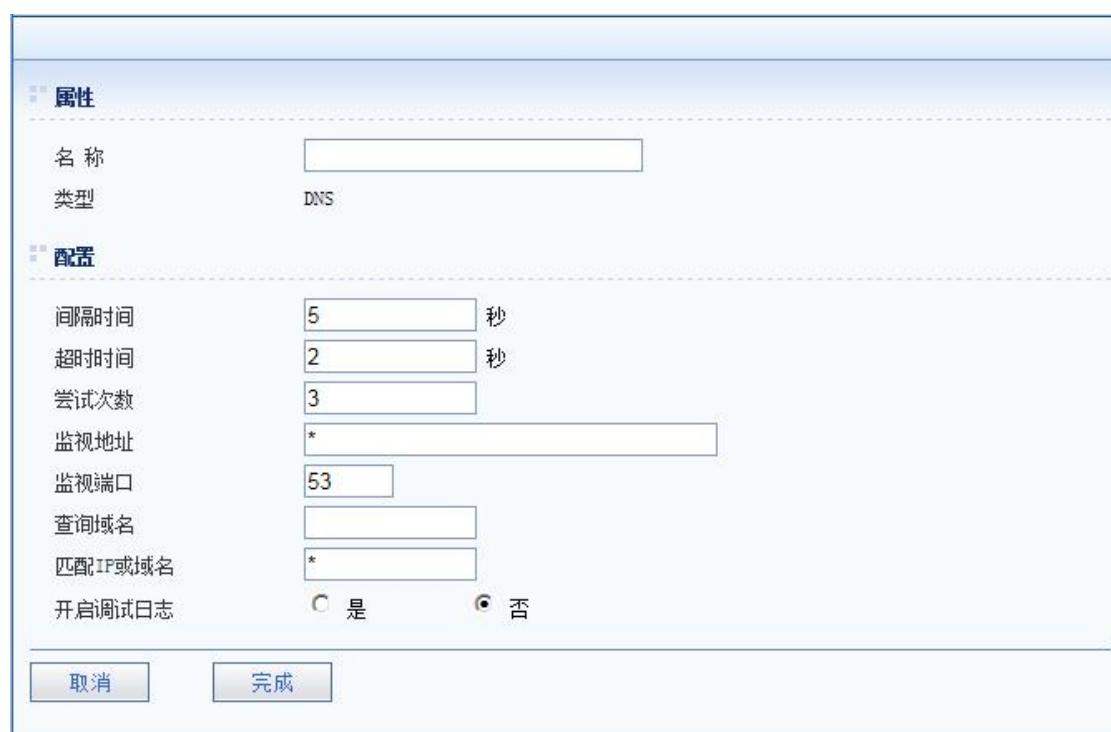
请参考 6.5 节点池。

『磁盘占用率最大值』用于配置监视 SNMP 类型的磁盘占用率最大值，超过此数值即节点繁忙。

『磁盘权重』用于配置监视SNMP类型的磁盘权重，用于动态反馈的节点选择策略，详情请参考 6.5 节点池。

✓ DNS

选择[DNS]，通过域名解析监控 DNS 服务器的状态。点击**下一步**按钮，如下图所示：



『监视端口』用于配置监视 DNS 类型监视的端口，默认为 53。

『查询域名』用于配置发送给 DNS 服务器的查询域名。

『匹配 IP 或域名』用于判断服务器返回信息是否匹配。填入 IPv4 地址，监视器发送 A 查询；填入 IPv6 地址，监视器发送 AAAA 查询；填入域名，监视器发送 CNAME 查询；填入*，监视器发送 ANY 查询。

✓ Radius

选择[Radius]，通过 Radius 认证请求的方式监视 Radius 服务器的状态。点击**下一步**按钮，如下图所示：

The screenshot shows the 'Radius' configuration page with the following settings:

- 属性 (Properties):**
 - 名称 (Name): [empty]
 - 类型 (Type): Radius
- 配置 (Configuration):**
 - 间隔时间 (Interval): 5 秒
 - 超时时间 (Timeout): 2 秒
 - 尝试次数 (Attempts): 3
 - 监视地址 (Monitoring Address): *
 - 监视端口 (Monitoring Port): 1812
 - 请求类型 (Request Type): 认证请求 (Authentication Request)
 - 用户名 (Username): [empty]
 - 密码 (Password): [empty]
 - 认证方式 (Authentication Method): PAP
 - 密钥 (Key): [empty]
 - 开启调试日志 (Enable Debug Log): 是 (否)
- 附加属性 (Additional Properties):**
 - 属性ID (Attribute ID): 自定义属性 (Custom Attribute)
 - 属性类型 (Attribute Type): 字符串 (String)
 - 属性值 (Attribute Value): [empty] (Add) [Delete]

『监视端口』用于配置监视 Radius 类型监视的端口，默认为 1812。

『请求类型』用于配置发送的请求包类型，认证请求发送认证请求包，计费请求发送计费开始和计费结束请求包。

『用户名』用于配置 RADIUS 请求使用的用户名。

『密码』用于配置 RADIUS 请求使用的密码，仅在认证请求时需要。

『认证方式』用于配置 RADIUS 请求使用的认证加密方式，支持 PAP 和 CHAP，仅在

认证请求时需要。

『密钥』用于配置 RADIUS 服务使用的密钥。

『调试』用于配置是否启用监视 Radius 类型的调试日志，启用后会在日志中显示详细的连接记录。

『属性 ID』用于配置 RADIUS 服务属性的标识，可自定义属性。

『属性类型』用于配置 RADIUS 服务携带的属性列表。包括字符串、十进制数字、十六进制字符串、IPv4 地址和 IPv6 地址。

『属性值』用于配置 RADIUS 服务属性的值。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

✓ TCP 半连接

选择[TCP 半连接]，根据 TCP 三次握手原理，发送 SYN 数据包监视主机端口监听状态。

点击**下一步**按钮，如下图所示：

新建

属性

名称

类型 TCP半连接

基本配置

间隔时间 秒

超时时间 秒

尝试次数

监视地址

监视端口

开启调试日志 是 否

附加配置

绑定源地址

『监视端口』用于配置监视服务器的端口，“*”为监视所有。可监视 HTTP, FTP, SMTP, POP3, IMAP, OTHER 类型。

『绑定源 IP 地址』用于配置发包监视目的主机的 AD 源 IP, 必须指定 AD 的网口上的 IPv4 地址。

✓ **TCP 被动**

选择[TCP 被动]，通过监听服务器节点流量的 TCP 事件，判断服务器繁忙状态。点击 **下一步** 按钮，如下图所示：

属性

名称 (长度限制为1~63字符，且不能包含& | " ' , : % < > / \ 特殊字符)

类型 TCP被动

配置

统计时间 秒

监视类型 RST关闭连接

上限值 个

动作 过载保护

保护时间 秒

过载保护无效后节点离线 启用 禁用

开启调试日志 是 否

『统计时间』配置监视器统计的时间范围。

『监视类型』选择监视的TCP事件类型，包括RST关闭连接、零窗口。

『上限值』配置在统计时间内指定的TCP事件发生的上限，超过该上限即触发节点动作。

『动作』包括过载保护和节点离线。

『保护时间』设置上述动作执行的时间。

『过载保护无效后节点离线』设置在执行过载保护超过保护时间后，节点状态依然是繁忙状态，则监视器是否执行节点离线动作。

✓ HTTP 被动

选择[HTTP 被动]，通过监听HTTP请求的响应状态码，监视节点的监控状态。点击下一步按钮，如下图所示：

节点监视器

帮助信息

属性

名称:
类型: HTTP被动

配置

检查URL: [添加] [删除]

调试: 是 否

URL失效条件

响应状态码: [添加]
 [301, 302, 400, 403, 404, 500, 501, 502]

响应超时时间: 5 秒

节点失效条件

统计时间: 1 秒
异常URL上限: 10000 个

[取消] [完成]

『响应状态码』设置判断 URL 失效的响应状态码。即当应答的响应状态码被匹配上，则判断此 URL 失效。

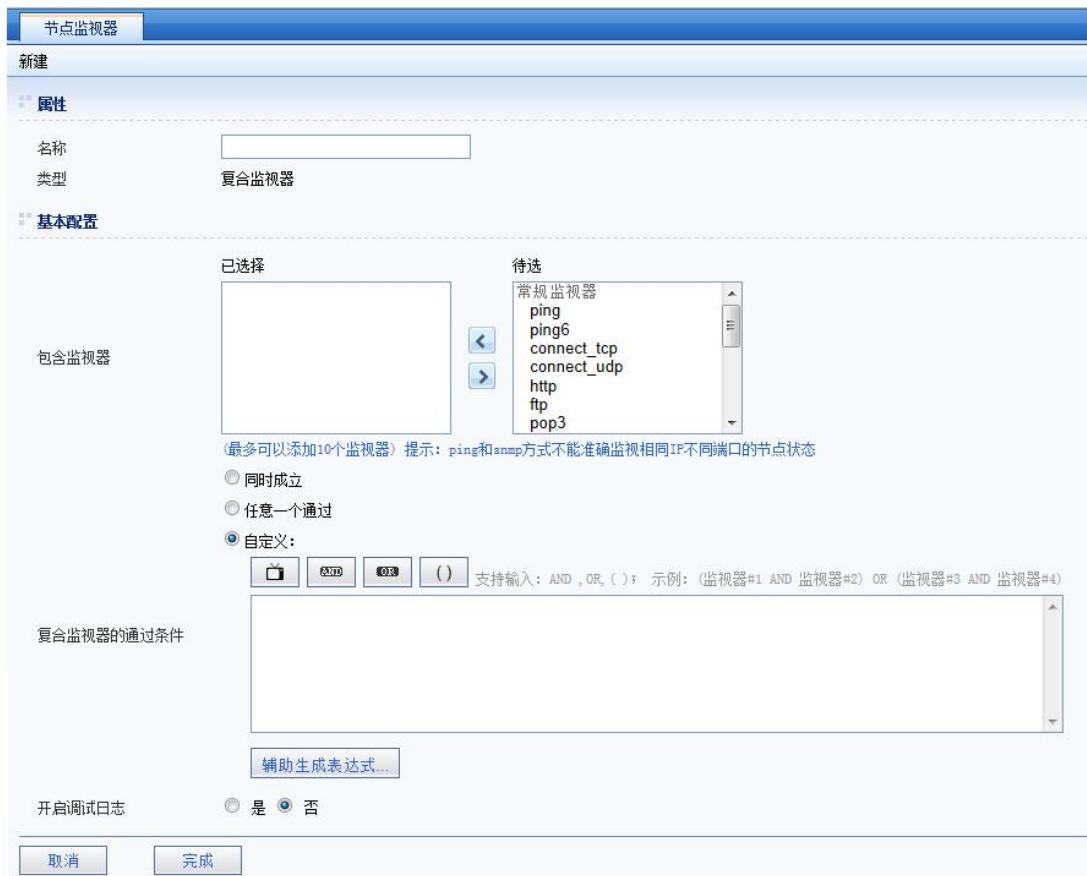
『响应超时时间』设置 URL 应答的响应超时时间。即超过响应超时时间，仍未收到应答，则判断此 URL 失效。

『统计时间』设置统计的时间范围。

『异常 URL 上限』设置在统计时间内，当异常的 URL 数量达到设定值时，则判断该节点失效。

✓ 复合监视器

选择[复合监视器]，选择一系列上述监视器的组合，同时对节点进行监控。点击**下一步**按钮，如下图所示：



『包含监视器』选择多个已经设置好的监视器。

『复合监视器的通过条件』可设置同时成立、任意一个通过、和自定义条件。复合监视器用于多个不同的服务之间存在依存关系的场景。

点击 ，插入[包含监视器]里选择的监视器；点击 ，插入与运算符；点击 ，插入或运算符；点击 ()，插入括号。

输入完复合监视器的通过条件后，再点击 辅助生成表达式。

『调试』开启调试日志的开关。

✓ 数据库

选择[MySql 数据库]，点击 下一步 按钮，如下图所示：

节点监视器

温馨提示：在填写发送内容时，请尽量使用不耗损性能、数据量小的可执行的SQL语句

属性

名称	MySql数据库监视器
类型	MYSQL

基本配置

间隔时间	10	秒
超时时间	60	秒
尝试次数	3	
监视地址	*	
监视端口	*	* default
用户名	admin	
密码	*****	
数据库名		
开启调试日志	<input type="radio"/> 是	<input checked="" type="radio"/> 否

附加配置

检测对象	查询结果集	
发送内容		
结果定位	行	列
接收内容必须包含		

『间隔时间』节点监视器监视节点从而获取节点状态的频率，即相对于前一次的监视，经过多长时间再进行监视。

『超时时间』节点监视器监视节点过程中的超时时间，即多长时间没有收到节点的回复则认为超时。

『尝试次数』监视过程中超时或是其他异常情况退出后，监视器重新进行监视的次数。

『监视地址』设置 MySql 数据库的 IP 地址。*代表所有的节点，或者输入指定地址。

『监视端口』设置 MySql 数据库的监听端口。设备默认包含 ORACLE、MSSQL、MYSQL 的监听端口，如果要设置指定端口，可选择 OTHER；还可选择 default 端口来监听节点所配

置的端口。

『用户名』设置登录数据库执行 SQL 语句的用户名。此用户名需具有执行 SQL 语句的权限。

『密码』设置登录数据库执行 SQL 语句对应的密码。

『数据库名』设置执行 SQL 语句的数据库名称。

『调试』设置是否开启调试日志。

『发送内容』设置 SQL 语句的内容，在填写发送内容时，请尽量使用不耗损性能、数据量小的可执行的 SQL 语句。

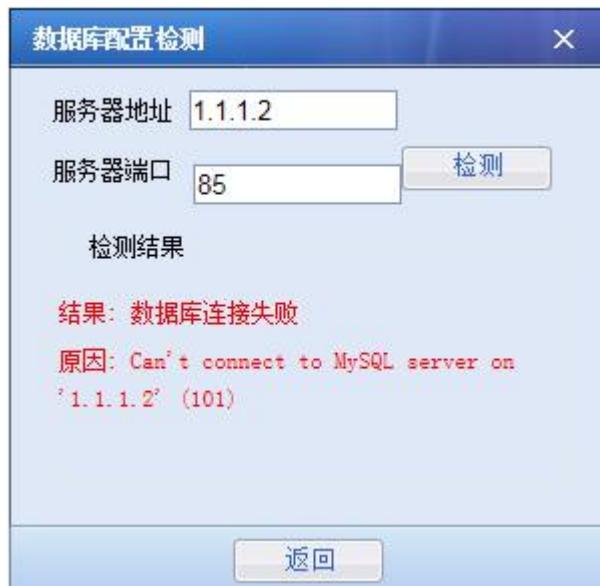
『结果定位』设置 SQL 语句执行返回结果必须满足的条件。

『接收内容必须包含』设置 SQL 语句执行返回结果必须包含的内容。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

数据库配置检测按钮可以用于数据库连接监测。输入服务器地址和端口，点击**检测**进行检测，显示检测结果。



选择[MSSQL 数据库]和[ORACLE 数据库]，新建 MSSQL 数据库的节点监视器和 ORACLE 数据库节点监视器的设置方法与[MYSQL 数据库]类似，此处不再累述。

✓ **LDAP**

选择[LDAP]，点击**下一步**按钮，如下图所示：

节点监视器

属性

名称

类型 LDAP

基本配置

间隔时间 秒
30

超时时间 秒
60

尝试次数
3

监视地址
*

监视端口 * default

用户名

密码

Base DN

Search Filter

安全加密

Mandatory Attributes 是 否

Chase Referrals 是 否

开启调试日志 是 否

『用户名』指定用户名，如果所监视的目标需要验证。

『密码』指定密码，如果被监控的目标要求身份验证。

『Base DN』指定从监视器启动健康检查的 LDAP 树中的位置。比如：

dc=bigip-test,dc=net。

『Search Filter』监视器搜索指定的 LDAP 密钥，比如：objectclass=*。

『安全加密』指定用于与目标通信的安全协议类型。

『Mandatory Attribuates』 指定目标是否必须包括其响应中的属性。。

『Chase Referrals』在收到 LDAP 引用条目后是否出现转换。默认是肯定的。

『开启调试日志』开启调试则会在服务日志中打印节点监视器的调试日志。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

✓ 外部应用监视器

选择『外部应用监视器』，点击**下一步**按钮，如下图所示：



『间隔时间』节点监视器监视节点从而获取节点状态的频率，即相对于前一次的监视，经过多长时间再进行监视。

『超时时间』节点监视器监视节点过程中的超时时间，即多长时间没有收到节点的回复则认为超时。

『尝试次数』监视过程中超时或是其他异常情况退出后，监视器重新进行监视的次数。

『开启调试日志』开启调试则会在服务日志中打印节点监视器的调试日志。

『执行命令』行监视器时执行的命令，命令可包含内置变量，\${rs_ip}代表节点 ip，\${rs_port}代表节点端口。如果节点状态正常，命令需打印 monitor:success 到标准输出，否则其他情况视为节点状态异常。以 java 为例，java -cp /usr/monitor HttpMonitorDemo \${rs_ip} \${rs_port}；以 python 为例，python /usr/monitor/HttpMonitorDemo.py \${rs_ip} \${rs_port}。（注：为保证命令正常运行，java 需指定搜索路径，python 需使用绝对路径）。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.5. 节点池

WEBUI: 『应用负载』→『节点池』。

『节点池』用于定义需要发布的应用的节点以及对应的服务器负载策略，此处定义的『节点池』，可用于『策略』、『虚拟服务』配置部分。点击到节点池名称上时，会有**查看节点**按钮出现，点击即可跳转到节点列表页面。

界面如下图所示：



节点池			
操作		节点个数	类型
【新建】	【删除】	1	IPv4
【查看节点】		2	IPv4

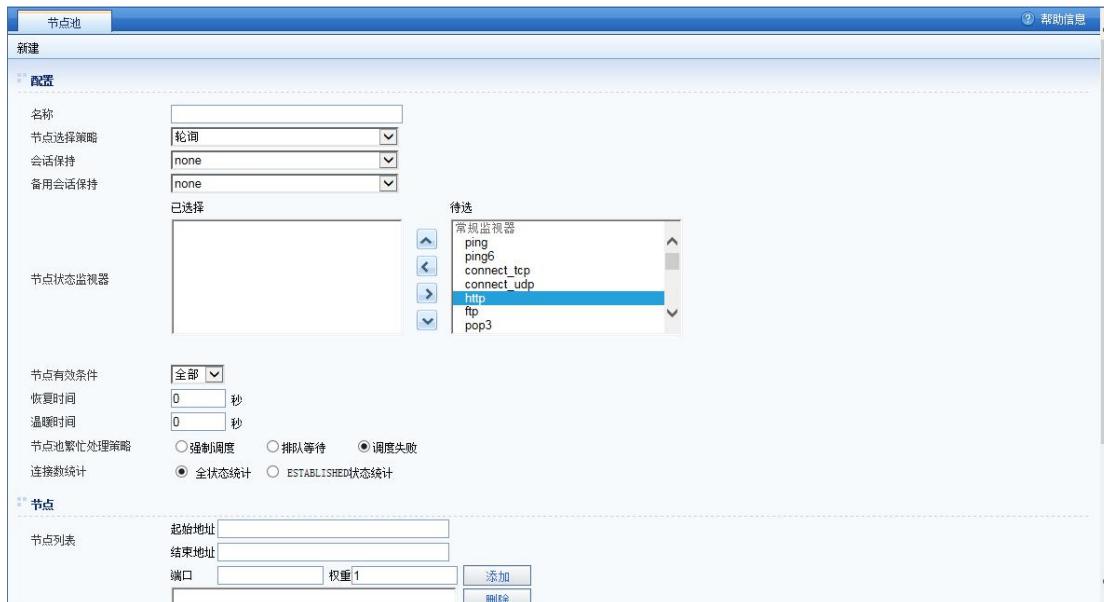
点击到节点池名称上时，会有**查看节点**按钮出现，点击即可跳转到节点列表页面。

『节点池』下显示节点池的『名称』、『类型』、『节点个数』、『操作』。

删除按钮可以用于删除节点池。

新建按钮可以用于新建节点池。

点击**新建**按钮，如下图所示：



『名称』可以输入便于记忆和识别的字符串，用于标识节点池。

『节点选择策略』用于配置节点选择的策略，包括[轮询]、[加权轮询]、[加权最少连接]、[最快响应时间]、[哈希]、[动态反馈]、[优先级]。

节点选择策略中，[轮询]表示交替返回有效的节点；[加权轮询]表示通过『节点』设置中的『权重』，按照节点权值的比例返回有效的节点；[加权最少连接]表示通过『节点』设置中的『权重』、当前节点连接数加权计算结果返回有效的节点，[最快响应时间]表示通过探测响应时间返回探测时间最短的有效的节点；[动态反馈]表示通过SNMP的监视结果、『节点监视器』中对应SNMP类型的『CPU权重』、『内存权重』、『磁盘权重』加权计算结果返回有效的节点；[哈希]根据哈希的关键字（如URL、HOST等）经过哈希运算得到哈希值，使不同的关键字尽可能平均调度节点池中各个节点；[优先级]优先调度优先级高的节点，优先级高的节点不可用时才会调度到下一级节点。

『会话保持』用于配置节点池的会话保持方式，如需要新增或修改会话保持方式，可以在『应用负载』→『会话保持方式』中进行配置。

『备用会话保持』用于配置节点池的会话保持方式，当主会话保持方式失效时，会使用备用会话保持方式进行会话保持。

『节点状态监视器』可以选择需要的监视器，点击按钮左移即可将选定的监视器启用，用于监视节点池中的节点，从而获取节点状态。若需要将已经选定的监视器禁用，选定需要禁用的监视器，点击按钮右移选定的监视器即可。

『节点有效条件』用于配置节点的有效条件，包括[至少]、[全部]两个条件。选择[至少]时，节点监视器中只要有一个或一个以上监视器监视节点生效，则该节点生效；选择[全部]时，需要全部监视器均通过，节点才有效。

『恢复时间』用于设置服务器恢复上线的时间。保证AD对该设备健康检查通过后，在一定的时间内不向该服务器发送客户请求。

『温暖时间』用于设置服务器的请求在一定时间范围内达到最大值。保证服务器在恢复时间到期后，不是马上接受负载的全部请求，而是在一定时间内逐渐增加请求，直至达到最大值。

『节点池繁忙后处理策略』有强制调度、排队等待、调度失败三种策略可以选择。“排队等待”策略需要配置“队列长度”和“超时时间”。



『连接数统计』默认使用全状态统计，即包括所有状态的连接。可以选择ESTABLISHED状态统计，即只统计建立成功的连接数。连接数显示在节点状态中。

『起始地址』、『结束地址』输入需要增加的节点地址，支持IPv4和IPv6地址的混搭。『端口』用于配置节点的监视端口，如果不填，则和虚拟服务的服务端口一致。『权重』可以输入需要增加的节点的权重，用于节点选择策略的加权运算，点击按钮进行添加，需要删除节点则选中已添加的节点，点击按钮即可。

按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

配置完成界面如下图所示：

节点池				
名称		类型	节点个数	操作
<input type="checkbox"/>	名称	IPv4/IPv6	2	
<input type="checkbox"/>	test	IPv4	1	
<input type="checkbox"/>	test1	IPv6	1	
<input type="checkbox"/>	test2	IPv6	1	

复制按钮可以用于复制所选节点池中节点部分的配置，并重新配置一个节点池。

点击 ，配置页面如下：

节点池

新建

配置

名称:

节点选择策略: 轮询

会话保持: none

备用会话保持: none

已选择:

节点状态监视器: 全部 强制调度 排队等待 调度失败 金状态统计 ESTABLISHED状态统计

恢复时间: 0 秒

重置时间: 0 秒

节点池繁忙处理策略: 强制调度 排队等待 调度失败

连接数统计: 金状态统计 ESTABLISHED状态统计

节点

节点列表: 起始地址:
结束地址:
端口: 权重:

待选: 常规监视器 ping ping6 connect_tcp connect_udp http ftp pop3

配置完成界面如下图所示：

节点池				
名称		类型	节点个数	操作
<input type="checkbox"/>	名称	IPv4/IPv6	2	
<input type="checkbox"/>	test	IPv4	1	
<input type="checkbox"/>	test1	IPv6	1	
<input type="checkbox"/>	test2	IPv6	1	
<input type="checkbox"/>	test2_1	IPv6	1	



若需要对节点进行进阶配置，例如对节点的连接数进行限制等操作，可以对已定

义的节点池内的节点进行编辑。「节点列表」用于配置节点池包括的节点。

后面的操作按钮



点击节点池后面的操作按钮或者**编辑节点**按钮，跳转到节点列表界面。



Nodes		
<input checked="" type="button"/> 新建 <input type="button"/> 删除 <input checked="" type="button"/> 启用 <input type="button"/> 禁用/软关机 <input type="button"/> 平滑退出 <input type="button"/> 返回		
地址	权重	预分配Cookie值
10.10.10.100:80	1	98184845

『节点』下显示节点的『地址』、『权重』、『预分配 Cookie 值』。

启用按钮可以用于启用节点。

禁用/软关机按钮可以用于禁用节点，被禁用的节点会维持现有活动的连接，但不会接受新的连接。

平滑退出按钮可以用于维持已有的连接和会话保持，但不调度新的请求，直到节点完全退出，确保正在运行的业务不会中断。

删除按钮可以用于删除节点。

新建按钮可以用于新建节点。点击**新建**按钮新增节点的配置和编辑原有节点类似，此处不再赘述，请参考下面的部分。

点击需要进阶配置的节点进行编辑，如下图所示：

节点

编辑

属性

IP地址: 192.168.1.2

端口:

启用 (允许所有流量)

状态:

平滑退出 (允许会话保持的流量)

禁用/软关机 (仅允许活动连接的流量)

配置

权重: 1

保持连接阈值: 0

每秒新建连接阈值: 0

每秒HTTP请求阈值: 0

关联变量:

节点健康检查

监视器类型: 继承 独立

操作

『IP 地址』用于配置节点的 IP 地址。编辑状态不可改，新建状态可以修改。

『端口』用于配置节点发布服务的端口。当『节点监视器』类型为[CONNECT]并且『监视端口』为[default]时可用。

『状态』用于配置节点的[启用]、[平滑退出]、[禁用/软关机]。被禁用的节点会维持现有活动的连接，但不会接受新的连接。

『权重』用于配置节点的权重，用于节点选择策略的加权运算。

『保持连接阈值』用于配置节点的保持连接的最大数，0 表示无限制。

『每秒新建连接阈值』用于配置节点的每秒新建连接的最大数，0 表示无限制。

『每秒 HTTP 请求阈值』用于配置节点的每秒 HTTP 请求的最大数，0 表示无限制。

『关联变量』用于 http 头部改写时，http 改写内置变量。

『监视器类型』可选择继承和独立。继承表示使用节点池中的监视器进行监视；独立则表示只用在该节点上配的监视器，主要目的是一些节点可能会单独用监视器进行监视状态。

取消按钮可以用于取消本次配置。

更新按钮用于更新改动的配置。



注意：设备会根据节点的 IP 地址类型自动判断节点池的 IP 类型，支持全是 IPv4 地址的节点池或者全是 IPv6 地址的节点池，支持 IPv4 地址与 IPv6 地址的混搭。



注意：支持空的节点池

7.6. SSL

『SSL』用于在 AD 设备和客户端之间建立一个加密的连接，对于发布服务的服务器有服务器证书的情况，也可将服务器证书导入 AD 设备，进行统一管理，可以一定程度上减少服务器的负荷；对于发布服务的服务器没有服务器证书的情况，可在 AD 设备上自生成证书或申请第三方 CA 颁发证书，实现客户端访问服务时和 AD 建立加密连接，进行数据加密。

『SSL』中的证书，可用于『虚拟服务』配置部分。

7.6.1. SSL 证书

『SSL 证书』下显示服务器证书的『名称』、『内容』、『颁发给』、『组织』、『过期时间』、『操作』。

界面如下图所示：

SSL证书						帮助信息
+新建	-删除	导入	导出为PEM	导出为DER		
名称	类型	内 容	颁发给	组织	过期时间	操作
AD	RSA	完整	AD	sangfor	2019/11/10 13:24:55	

『删除』按钮可以用于删除已选 SSL 证书，在虚拟服务中被关联的 SSL 证书则无法删除。

『导入』按钮可以用于导入第三方 SSL 证书，点击『导入』，如下图所示：



『名称』可以输入便于记忆和识别的字符串，用于标识导入的 SSL 证书。

『文件上传』点击上传按钮，可多次导入证书文件。支持 pem 和 der、pkcs12、pkcs7 等文件（后缀为 crt、cer、key、pem、der、pfx、p12、pvk、p7b、spc）。如果证书文件包含密码，会提示输入密码，如果密码输入错误则会重复弹框，可点击密码输入框右上角的“x”关闭。

『证书链』用于选择指定的证书，支持自动排序。

『SSL 证书』页面中，『新建』按钮可以用于新建设备自签名的证书。点击『新建』，配置页面如下：



SSL证书 CA证书 CRL

新建

属性

名称

颁发类型 自签名 证书请求(CSR)

颁发给

部 门

公司/机构

城 市

省 份

国 家

E-MAIL地址

公钥类型 RSA

哈希算法 SHA256

密钥长度 2048 位

证书有效期 5 年

密钥密码

确认密码

取消 完成

『名称』可以输入便于记忆和识别的字符串，用于标识新建的 SSL 证书的名称。

『颁发类型』选择 SSL 证书的颁发类型，选择自签名将会产生一份完整的证书，选择证书请求（CSR）则会产生一个证书请求用于发送到 CA 进行签名。

『颁发给』配置 SSL 证书使用者的名称。

『部门』配置 SSL 证书使用者所在的部门。

『公司/机构』配置 SSL 证书使用者所在的公司或是机构。

『城市』配置 SSL 证书使用者所在的城市。

『省份』配置 SSL 证书使用者所在的省份。

『国家』配置 SSL 证书使用者所在国家的英文缩写。

『EMAIL 地址』配置 SSL 证书使用者的 E-MAIL 地址。

『公钥类型』有 RSA、ECDSA、SM2（国密）三种。

『哈希算法』有 SHA256、SHA1、SM3（国密）三种。

『证书有效期』配置自签名类型的 SSL 证书的有效期。

取消按钮可以用于取消本次配置。

完成按钮可以用于保存配置并生成 SSL 证书。

当『颁发类型』选择[证书请求（CSR）]方式时，配置页面如下：

SSL证书 CA证书 CRL

新建

属性

名称

颁发类型 自签名 证书请求 (CSR)

颁发给

部 门

公司/机构

城 市

省 份

国 家

E-MAIL地址

公钥类型 ECDSA

哈希算法 SHA256

密钥长度 prime256v1 位

密钥密码

确认密码

『名称』可以输入便于记忆和识别的字符串，用于标识新建的 SSL 证书的名称。

『颁发类型』选择 SSL 证书的颁发类型，选择自签名将会产生一份完整的证书，选择证书请求 (CSR) 则会产生一个证书请求用于发送到 CA 进行签名。

『颁发给』配置 SSL 证书使用者的名称。

『部门』配置 SSL 证书使用者所在的部门。

『公司/机构』配置 SSL 证书使用者所在的公司或是机构。

『城市』配置 SSL 证书使用者所在的城市。

『省份』配置 SSL 证书使用者所在的省份。

『国家』配置 SSL 证书使用者所在国家的英文缩写。

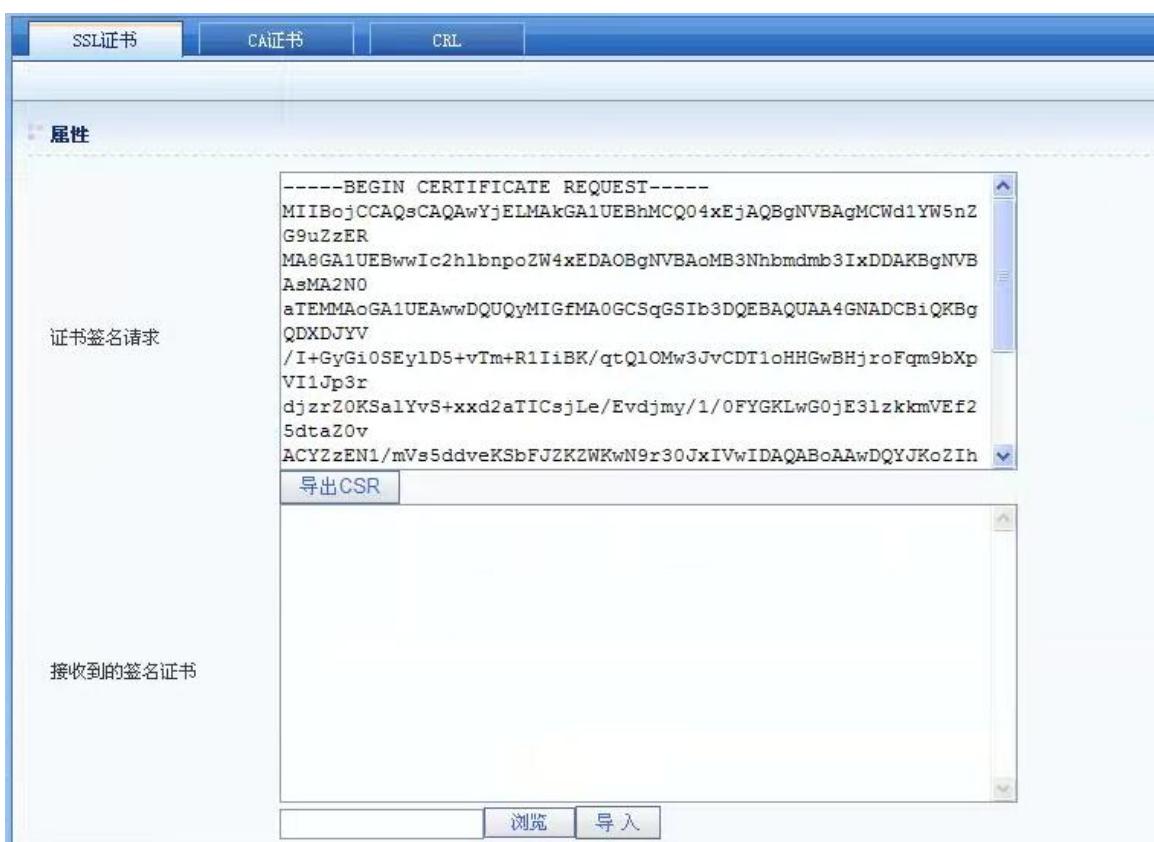
『EMAIL 地址』配置 SSL 证书使用者的 E-MAIL 地址。

『公钥类型』有 RSA、ECDSA、SM2（国密）三种。

『哈希算法』有 SHA256、SHA1、SM3（国密）三种。

『私钥长度』配置 SSL 证书的私钥长度。

点击**下一步**，可获得证书签名请求，并导入第三方 CA 颁发的证书。配置页面如下：



『证书签名请求』AD 设备生成的证书签名请求，该请求可提交给第三方 CA 申请颁发服务器证书。

导出 CSR 可将证书签名请求以 CSR 方式导出。

『接收到的签名证书』可将第三方 CA 生成的证书导入到 AD 设备。

点击**浏览**，可选定 PEM、DER 格式的证书

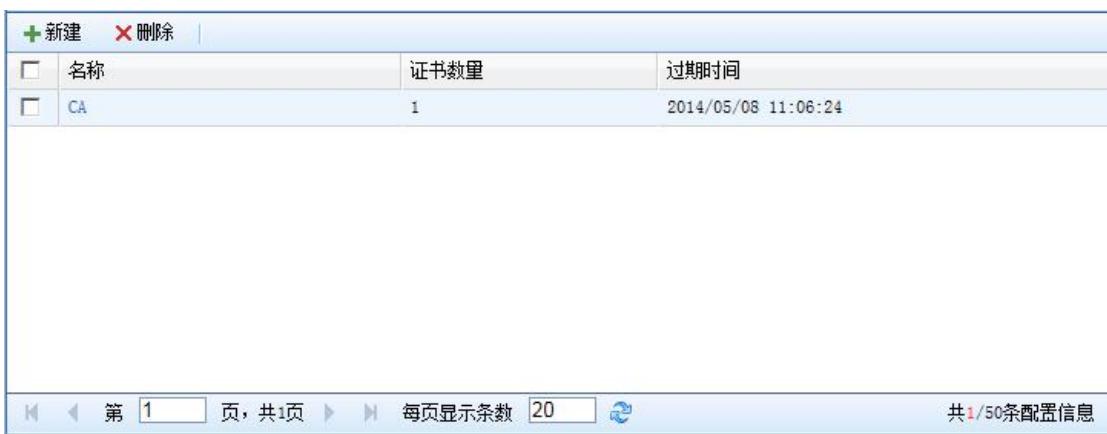
点击 **导入**，可导入第三方 CA 颁发的服务器证书到 AD 设备

取消 按钮可以用于取消本次配置。

完成 按钮可以用于保存配置并生成服务器证书。

7.6.2. CA 证书

点击 **CA 证书**，界面如下所示：



<input type="checkbox"/>	名称	证书数量	过期时间
<input type="checkbox"/>	CA	1	2014/05/08 11:06:24

第 页, 共1页 每页显示条数  共1/50条配置信息

点击 **新建**，新建 CA 证书，如下所示：

SSL证书 CA证书 CRL

新建

属性

名称 (长度限制为1~63字符，且不能包含& | " ' , : % < > / \ 特殊字符)

证书管理

文件上传

已选择

证书链

待选

当前已导入0/32个证书

取消 完成

『名称』可以输入便于记忆和识别的字符串，用于标识新建的 CA 证书的名称。

『文件上传』点击上传按钮，可多次导入证书文件。支持 pem 和 der、pkcs12、pkcs7 等文件（后缀为 crt、cer、key、pem、der、pfx、p12、pvk、p7b、spc）。如果证书文件包含密码，会提示输入密码，如果密码输入错误则会重复弹框，可点击密码输入框右上角的“x”关闭。

『证书链』用于选择指定的证书，支持自动排序。

按钮可以用于保存配置。

7.6.3. CRL

『CRL』下显示的是吊销列表的名称，获取方式，下载间隔和更新状态。如下图所示：

名称	获取方式	下载间隔(min)	更新状态	吊销证书数	文件大小

点击 ，界面如下图所示：

SSL证书 | CA证书 | CRL

新建

属性

名称

配置

获取方式

URL

下载间隔 时

超时时间 秒

重试次数

『名称』可以输入便于记忆和识别的字符串。

『获取方式』可以选择 HTTP, FTP, 或者本地上传。

『URL』填写获取 CRL 的网址。

『下载间隔』填写 CRL 的下载间隔时间，最大值可填写为 30 天。

『超时时间』填写 CRL 下载的超时时间，如果超时时间内无法获取 CRL，则重新获取。

『重试次数』填写重新获取的次数。

如果『获取方式』选择的是 FTP，界面如下所示：

SSL证书 CA证书 CRL

新建

属性

名称

配置

获取方式 FTP 本地上传
URL

匿名登录 是 否

用户名

密码

下载间隔 时 分 秒

超时时间 秒

重试次数

『URL』填写获取 CRL 的地址。

『匿名登录』可选是否匿名登录。

『用户名』填写 FTP 访问的用户名。

『密码』填写 FTP 访问的密码。

如果『获取方式』选择的是本地上传，界面如下所示：

SSL证书 CA证书 CRL

新建

属性

名称

配置

获取方式

上传

『上传』上传本地的 CRL 列表到设备里。

完成按钮可以用于保存配置。

如果『获取方式』选择的是 LDAP，界面如下所示：

SSL证书 CA证书 CRL

新建

属性

名称

配置

获取方式

LDAP

匿名登录 是 否

用户名

密码

下载间隔 时

超时时间 秒

重试次数

『名称』可以输入便于记忆和识别的字符串，用于 CRL。。

『获取方式』填写获取 CRL 的地址。

『LDAP』填写获取 CRL 的地址。

『匿名登录』可选是否匿名登录。

『用户名』填写 LDAP 访问的用户名。

『密码』填写 LDAP 访问的密码。

『下载间隔』填写 CRL 的下载间隔时间，最大值可填写为 30 天。

『超时时间』填写 CRL 下载的超时时间，如果超时时间内无法获取 CRL，则重新获取。

『重试次数』填写重新获取的次数。

完成按钮可以用于保存配置。

7.7. 策略

『策略』用于配置 AD 设备的调度策略，包括『前置调度策略』、『优化策略』、『HTTP 改写策略』、『HTTP 防护策略』、『TCP 策略』、『卸载策略』、『加密策略』、『URL 下载速度控制』和『QoS 策略』几个部分。

7.7.1. 前置调度策略

WEBUI: 『应用负载』→『策略』→『前置调度策略』。

『前置调度策略』用于将特定用户的访问调度到指定节点池。



『启用』按钮可以用于启用前置调度策略。

『禁用』按钮可以用于禁用前置调度策略。

『删除』按钮可以用于删除前置调度策略。

『新建』按钮可以用于新建前置调度策略。

点击『新建』按钮，如下图所示：



『名称』可以输入便于记忆和识别的字符串，用于标识前置调度策略。

『服务』用来选择需要启用前置调度策略的服务。

7.7.1.1. 新建 HTTP 服务类型的前置调度策略

如果选择 HTTP 类型的服务，那么新建前置调度策略的配置页面显示如下：

新建

属性

名称

关联属性

服务 源IP范围

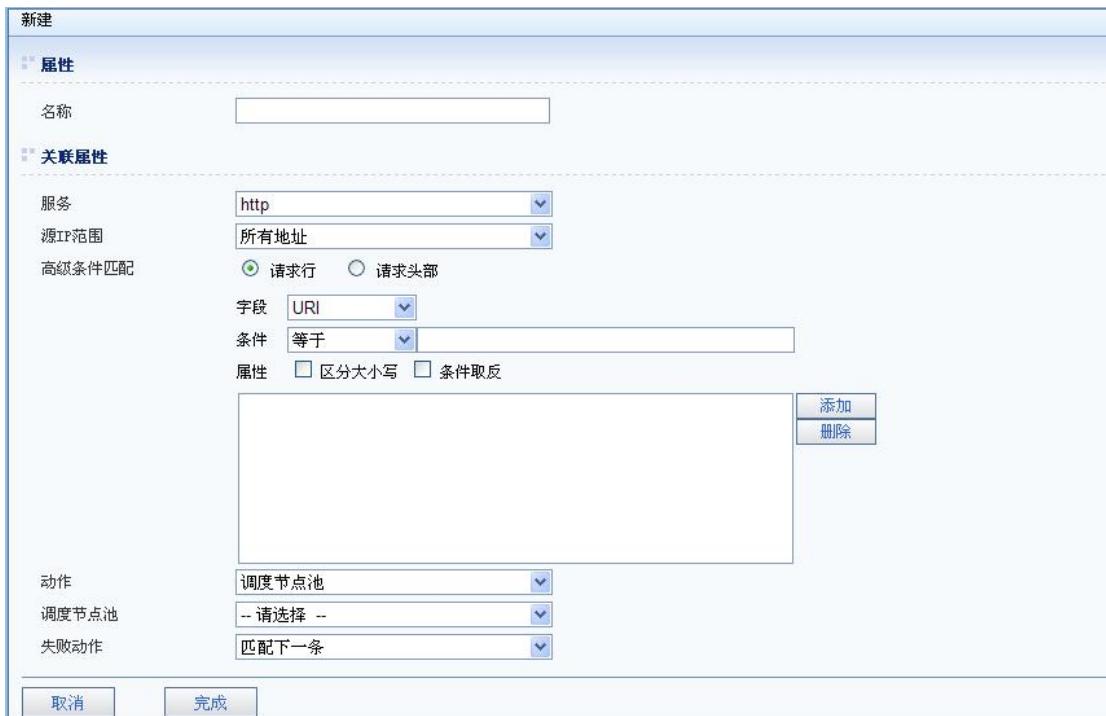
高级条件匹配 请求行 请求头部

字段 条件 属性 区分大小写 条件取反

动作 调度节点池

失败动作

取消 **完成**



『源 IP 范围』用来填写匹配前置调度策略的源 IP 地址范围，可以选择所有地址、单个地址、地址段、子网、用户地址集。

『高级条件匹配』可选择匹配请求行或者请求头部。请求行可根据[VERSION]、[METHOD]、[URI]设置匹配条件；请求头部可根据字段[HOST]、[COOKIE]、[USER-AGENT]和自定义字段设置匹配条件。

『动作』可选择调度节点池、返回指定内容、关闭连接或调度节点池并改写。

若动作选择[调度节点池]，界面显示如下：

动作

调度节点池

失败动作 匹配下一条 丢弃



『调度节点池』选择符合前置调度策略条件的用户访问某个虚拟服务时将会调度到的节点池。

『失败动作』为服务器调度失效后的动作，包括[匹配下一条]、[丢弃]两种动作。[匹配下一条] 匹配失败或前置匹配成功但节点池节点都离线调度失败后继续匹配下一条前置调度策略；[丢弃]表示匹配上前置调度策略以后，引用的节点池无节点在线，调度失败不会再调度。

若动作选择[返回指定内容]，界面显示如下：

动作	返回指定内容
返回内容	503 Service Unavailable_1

『返回内容』选择自定义好的内容，需要预先在『公共对象』→『自定义内容』中设置才可选择。

若动作选择[关闭连接]，则匹配条件的连接将会被关闭。

若动作选择[调度节点池并改写]，界面显示如下：

动作	调度节点池并改写				
调度节点池	负载均衡				
失败动作	<input checked="" type="radio"/> 匹配下一条 <input type="radio"/> 丢弃				
请求改写	<table border="1"><tr><td>已选择</td><td>待选</td></tr><tr><td><input type="button" value="<"/></td><td><input type="button" value=">"/></td></tr></table>	已选择	待选	<input type="button" value="<"/>	<input type="button" value=">"/>
已选择	待选				
<input type="button" value="<"/>	<input type="button" value=">"/>				
应答改写	<table border="1"><tr><td>已选择</td><td>待选</td></tr><tr><td><input type="button" value="<"/></td><td><input type="button" value=">"/></td></tr></table>	已选择	待选	<input type="button" value="<"/>	<input type="button" value=">"/>
已选择	待选				
<input type="button" value="<"/>	<input type="button" value=">"/>				

『调度节点池』选择符合前置调度策略条件的用户访问某个虚拟服务时将会调度到的节

点池。

『失败动作』为服务器调度失效后的动作，包括[匹配下一条]、[丢弃]两种动作。[匹配下一条] 匹配失败或前置匹配成功但节点池节点都离线调度失败后继续匹配下一条前置调度策略；[丢弃]表示匹配上前置调度策略以后，引用的节点池无节点在线，调度失败不会再调度。

『请求改写』选择请求改写的策略，需要预先在『应用负载』→『策略』→『HTTP 头部改写』设置，详见章节 6.7.3.1

『应答改写』选择应答改写的策略，需要预先在『应用负载』→『策略』→『HTTP 头部改写』设置，详见章节 6.7.3.2

7.7.1.2. 新建 TCP 服务类型的前置调度策略

若选择 TCP 类型的服务，如 SMTP，POP3 等，新建前置调度策略的配置页面显示如下：

The screenshot shows the 'New Pre-Scheduling Policy' configuration dialog. It has several sections:

- 属性 (Properties):** Contains a '名称 (Name)' input field.
- 关联属性 (Associated Properties):** Contains fields for '服务 (Service)' (set to 'smtp'), '源IP范围 (Source IP Range)' (set to '所有地址 (All Addresses)'), and '高级条件匹配 (Advanced Condition Matching)'. Under '高级条件匹配', there's a '字段 (Field)' dropdown set to 'TCP流 (TCP Flow)', a '条件 (Condition)' dropdown set to '等于 (Equal)', and a '属性 (Attribute)' section with checkboxes for '区分大小写 (Case-sensitive)' and '条件取反 (Invert Condition)'. A large list area below these fields contains a single row with a '添加 (Add)' button and a '删除 (Delete)' button.
- 动作 (Action):** Contains a '调度节点池 (Scheduling Node Pool)' dropdown set to '调度节点池 (Scheduling Node Pool)', a '调度节点池 (Scheduling Node Pool)' dropdown set to '--请选择-- (Please Select)', and a '失败动作 (Failure Action)' dropdown set to '匹配下一条 (Match Next)'.

At the bottom are '取消 (Cancel)' and '完成 (Finish)' buttons.

『源 IP 范围』用来填写匹配前置调度策略的源 IP 地址范围，可以选择所有地址、单个

地址、地址段、子网、用户地址集。

『高级条件匹配』可设置匹配 TCP 流的条件。

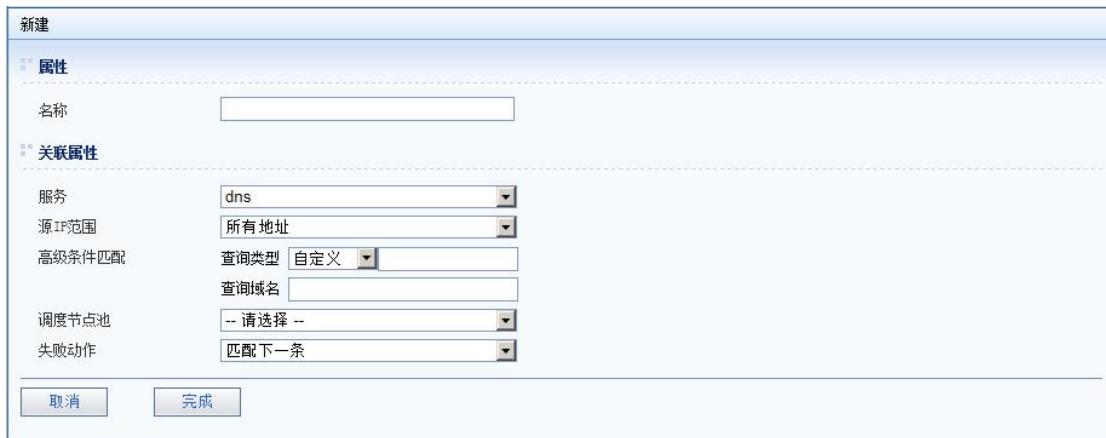
『动作』调度到节点池。

『调度节点池』选择符合前置调度策略条件的用户访问某个虚拟服务时将会调度到的节点池。

『失败动作』为服务器调度失效后的动作，包括[匹配下一条]、[丢弃]两种动作。[匹配下一条] 匹配失败或前置匹配成功但节点池节点都离线调度失败后继续匹配下一条前置调度策略；[丢弃]表示匹配上前置调度策略以后，引用的节点池无节点在线，调度失败不会再调度。

7.7.1.3. 新建 DNS 服务类型的前置调度策略

若选择 DNS 类型的服务，那么新建前置调度策略的配置页面显示如下：



The screenshot shows a configuration dialog box titled '新建' (New). It has two main sections: '属性' (Properties) and '关联属性' (Associated Properties).

属性 (Properties):

- 名称 (Name): An empty text input field.

关联属性 (Associated Properties):

- 服务 (Service): A dropdown menu set to 'dns'.
- 源IP范围 (Source IP Range): A dropdown menu set to '所有地址' (All Addresses).
- 高级条件匹配 (Advanced Matching Conditions):
 - 查询类型 (Query Type): A dropdown menu set to '自定义' (Custom).
 - 查询域名 (Query Domain Name): An empty text input field.
- 调度节点池 (Scheduling Node Pool): A dropdown menu set to '--请选择--' (Please Select).
- 失败动作 (Failure Action): A dropdown menu set to '匹配下一条' (Match Next).

At the bottom are two buttons: '取消' (Cancel) and '完成' (Finish).

『源 IP 范围』用来填写匹配前置调度策略的源 IP 地址范围，可以选择所有地址、单个地址、地址段、子网、用户地址集。

『高级条件匹配』可设置查询类型以及查询域名条件。 查询类型可选择[ALL]、[A]、[NS]、[CNAME]、[SOA]、[PTR]、[MX]、[TXT]、[AAAA]、[SPF]和自定义；查询域名填入域名地址。

『调度节点池』选择符合前置调度策略条件的用户访问某个虚拟服务时将会调度到的节点池。

『失败动作』为服务器调度失效后的动作，包括[匹配下一条]、[丢弃]两种动作。[匹配下一条] 匹配失败或前置匹配成功但节点池节点都离线调度失败后继续匹配下一条前置调度策略；[丢弃]表示匹配上前置调度策略以后，引用的节点池无节点在线，调度失败不会再调度。

7.7.1.4. 新建 HTTPS 服务类型的前置调度策略

如果选择 HTTPS 类型的服务，那么新建前置调度策略的配置页面显示如下：



『源 IP 范围』用来填写匹配前置调度策略的源 IP 地址范围，可以选择所有地址、单个地址、地址段、子网、用户地址集。

『高级条件匹配』可选择匹配请求行、请求头部或证书变量。请求行可根据[VERSION]、[METHOD]、[URI]设置匹配条件；请求头部可根据字段[HOST]、[COOKIE]、[USER-AGENT]和自定义字段设置匹配条件；证书变量可根据字段[Version]、[Issuer]、[Subject]、[Common]

Name]、[EmailAddress]、[Organization]、[Organizational Unit]、[Locality]、[State or Province]和[Country]设置匹配条件

『动作』可选择调度节点池、返回指定内容、关闭连接或调度节点池并改写。



7.7.1.5. 新建 SSL 服务类型的前置调度策略

若选择 SSL 类型的服务，新建前置调度策略的配置页面显示如下：

新建

属性

名称

关联属性

服务: ssl
源IP范围: 所有地址
高级条件匹配: 证书变量 TCP流
字段: Version
条件: v1

动作: 调度节点池
调度节点池: --请选择--
失败动作: 匹配下一条

取消 完成

『源 IP 范围』用来填写匹配前置调度策略的源 IP 地址范围，可以选择所有地址、单个地址、地址段、子网、用户地址集。

『高级条件匹配』可选择匹配证书变量或者 TCP 流条件。证书变量可根据字段[Version]、[Issuer]、[Subject]、[Common Name]、[EmailAddress]、[Organization]、[Organizational Unit]、

[Locality]、[State or Province]和[Country]设置匹配条件；TCP流可设置条件等于、包含、通配符、正则匹配。

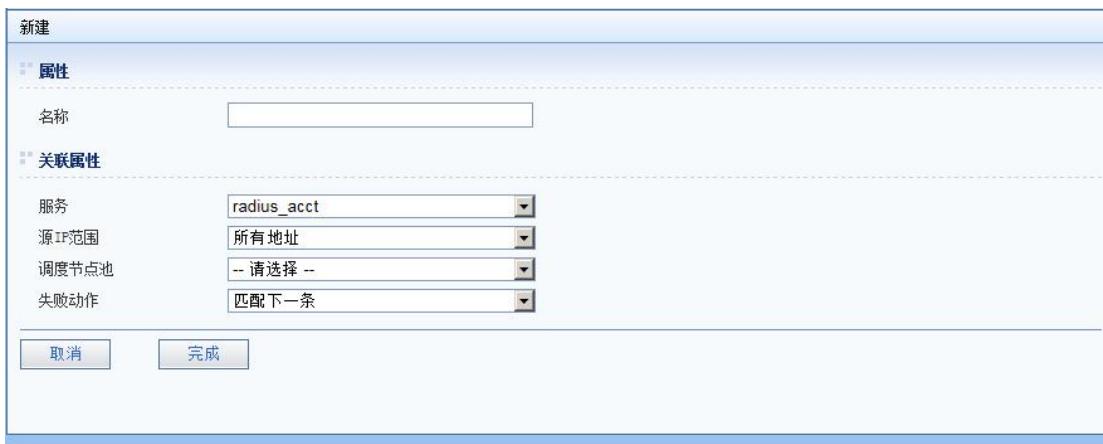
『动作』调度到节点池。

『调度节点池』选择符合前置调度策略条件的用户访问某个虚拟服务时将会调度到的节点池。

『失败动作』为服务器调度失效后的动作，包括[匹配下一条]、[丢弃]两种动作。[匹配下一条] 匹配失败或前置匹配成功但节点池节点都离线调度失败后继续匹配下一条前置调度策略；[丢弃]表示匹配上前置调度策略以后，引用的节点池无节点在线，调度失败不会再调度。

7.7.1.6. 新建 RADIUS 服务类型的前置调度策略

若选择 RADIUS 类型的服务，新建前置调度策略的配置页面显示如下：



The screenshot shows a configuration dialog titled '新建' (New) for a pre-scheduling policy. It has two main sections: '属性' (Properties) and '关联属性' (Associated Properties). In the '属性' section, there is a '名称' (Name) input field. In the '关联属性' section, there are four dropdown menus: '服务' (Service) set to 'radius_acct', '源IP范围' (Source IP Range) set to '所有地址' (All Addresses), '调度节点池' (Scheduling Node Pool) set to '-请选择-' (Please Select), and '失败动作' (Failure Action) set to '匹配下一条' (Match Next). At the bottom of the dialog are two buttons: '取消' (Cancel) and '完成' (Finish).

『源 IP 范围』用来填写匹配前置调度策略的源 IP 地址范围，可以选择所有地址、单个地址、地址段、子网、用户地址集。

『调度节点池』选择符合前置调度策略条件的用户访问某个虚拟服务时将会调度到的节点池。

『失败动作』为服务器调度失效后的动作，包括[匹配下一条]、[丢弃]两种动作。[匹配

下一条] 匹配失败或前置匹配成功但节点池节点都离线调度失败后继续匹配下一条前置调度策略；[丢弃]表示匹配上前置调度策略以后，引用的节点池无节点在线，调度失败不会再调度。

7.7.2. 优化策略

WEBUI: 『应用负载』→『策略』→『优化策略』。

点击**优化策略**，界面如下图所示：

+新建 X 删除				
<input type="checkbox"/>	名称	HTTP连接池	HTTP缓存	HTTP压缩
<input type="checkbox"/>	优化策略	启用 (1024/60)	启用	启用 (实时 缓存) 启用 (X-Forwarded-For)
◀ ◀ 第 1 页, 共1页 ▶ ▶ 每页显示条数 20	共1/50条配置信息			

『优化策略』下显示优化策略的『名称』以及该策略中『HTTP 连接池』、『HTTP 缓存』、『HTTP 压缩』、『其他』是否启用。

删除按钮可以用于删除优化策略。

新建按钮可以用于新建优化策略。

点击**新建**按钮，如下图所示：

新建

属性

名称

HTTP连接池

状态 启用 禁用

HTTP缓存

状态 启用 禁用

HTTP压缩

状态 启用 禁用

其他

传输客户端IP至后台服务器 启用 禁用

使用HTTP头部携带的IP连接服务器 启用 禁用

『名称』可以输入便于记忆和识别的字符串，用于标识优化策略。

『HTTP 连接池』实现一个 HTTP 连接能同时发多个请求，减少服务器新建连接数，降低服务器压力，并提高服务器的响应效率。如果虚拟服务开启了 HTTP 连接池，则服务端的 keep-alive 功能是默认开启的；若关闭 HTTP 连接池，则默认关闭服务端的 keep-alive 功能。不管虚拟服务是否开启 HTTP 连接池功能，客户端的 keep-alive 都是默认开启的。

若选择[启用]，则可配置『连接池大小』和『老化时间』，如下图所示：

HTTP连接池

状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
连接池大小	<input type="text" value="1024"/>
老化时间	<input type="text" value="60"/> 秒
源IP掩码	<input type="text" value="0.0.0.0"/>

[连接池大小]用于配置保持的连接的最大值。

[老化时间]用于配置一个 HTTP 连接保持的时间。

[源 IP 掩码]用于设置复用 HTTP 连接池的源 IP 地址范围。

『HTTP 缓存』设备内置 HTTP 缓存，能减轻大量重复请求对服务器的压力。若选择[启用]，则可配置[排除 URL 列表]、[缓存保持时间范围]、[默认缓存保持时间]、[单个缓存文件最大值]、[缓存 URL 控制列表]、[图片强制缓存]、[缓存调试]、[图片优化]，如下图所示：



[缓存空间大小]提供缓存的存储空间大小。

[缓存保持时间范围]用于配置缓存保持的时间范围。以上图为例，如果某个页面缓存时间小于 5 分钟，则设备缓存为 5 分钟。如果某个页面缓存时间大于 1440 分钟，则设备缓存为 1440 分钟。若设备缓存时间在 5-1440 中间，则以页面缓存时间为准。

[默认缓存保持时间]用于配置我们设备默认的缓存保持时间。当访问服务器时，服务器

应答的内容里边没有包含缓存时间或是不能依据应答内容计算出缓存超时时间，则用默认缓存保持时间。

[单个缓存文件最大值]用于配置单个缓存文件占用的最大存储空间。当某个文件大于最大存储空间时，不对该文件进行缓存。

[缓存 URL 列表]用于配置对某些访问 URL 的应答进行缓存。

[排除 URL 列表]用于配置排除掉某些 URL，对这些访问 URL 的应答不进行缓存。

[图片强制缓存]用于设置对原本不可缓存的图片强制缓存。

[缓存调试]用于设置是否开启缓存调试功能。

[图片优化]用于设置是否将图片进行转码后传输。开启该功能，会将图片格式转换成 webp 或者 jpeg 格式，减少图片传输的流量。

『HTTP 压缩』对 HTTP 缓存中的数据进行压缩和实时压缩后台服务器回的每个数据包，此功能需要额外的运算资源和客户端的支持，进而更有效地利用缓存和带宽。若选择[启用]，则可配置[压缩方式]、[最小原始长度]、[最大原始长度]、[压缩文件类型]，如下图所示：

HTTP压缩

状态 启用 禁用

压缩方式 实时 缓存

最小原始长度 KB

最大原始长度 KB

压缩文件类型
完全匹配列表

```
application/ecmascript
application/javascript
application/perlscript
application/postscript
application/rss+xml
application/rtf
application/sgml
application/vbscript
```

(最多可以添加80个完全匹配项)

通配符匹配列表

```
message/*
text/*
```

(最多可以添加16个通配符匹配)

未知文件类型 压缩 不压缩

[压缩方式]用于配置对 HTTP 进行实时压缩或者缓存压缩，如果使用缓存压缩，必须首先启用 HTTP 缓存。选择实时压缩后，如果服务器本身已经对 HTTP 进行压缩，则 AD 设备可以启用[压缩请求卸载]让服务器不进行压缩，由 AD 设备进行压缩，减轻服务器的压力，页面如下：

HTTP压缩

状态 启用 禁用

压缩方式 实时 缓存

压缩请求卸载 启用 禁用

最小原始长度 KB

最大原始长度 KB

[最小原始长度]用于配置压缩内容的最小长度，小于该长度的内容不进行压缩。

[最大原始长度]用于配置压缩内容的最大长度，大于该长度的内容不进行压缩。

[压缩文件类型]用于配置针对哪些类型的 HTTP 文件进行压缩，可以选择默认类型或者自定义。

[未知文件类型]用于设置对 WEB 应答头部没有携带 content-type 的包开启强制压缩。

『传输客户端 IP 至后台服务器』启用后可以让后台服务器获得真实的客户端源地址。主要用于旁路部署设备做了 SNAT 情况下，服务器需要获取客户端真实源 IP 地址的情况。对 HTTP 的服务生效。



『定制的 HTTP 头部名称』设定用于追加的头部名称，不能使用 HTTP 协议的标准头部名称。

『使用 HTTP 头部携带的 IP 连接服务器』开启后支持使用客户端请求头部携带的 IP 连接服务器，适用于 HTTP、HTTPS 虚拟服务的七层负载场景。



取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.7.3. HTTP 改写策略

WEBUI: 『应用负载』→『策略』→『HTTP 改写策略』。

点击 **HTTP 改写策略**，界面如下图所示：

HTTP 改写		
名称	类型	动作
请求改写	请求改写	改写头部URI
应答改写	应答改写	插入头部

『HTTP 改写』下显示 HTTP 头部改写策略的『名称』、『类型』、『动作』。

删除按钮可以用于删除 HTTP 头部改写策略。

新建按钮可以用于新建 HTTP 头部改写策略。点击**新建**按钮，如下图所示：



7.7.3.1. 请求改写

『请求改写』设置在 HTTP 请求方向的头部进行插入、删除、修改及 URI 的修改操作。

点击**下一步**，界面如下所示：

新建

属性

名称

类型 请求改写

关联属性

源IP范围

高级条件匹配 请求行 请求头部 证书变量

字段

条件

属性 区分大小写 条件取反

动作

『名称』可以输入便于记忆和识别的字符串，用于标识策略。

『源 IP 范围』设置 HTTP 头部改写的源 IP 地址范围。

『高级条件匹配』设置当 HTTP 请求方向的请求行、请求头部或者证书变量符合一定条件时进行下一步动作。

若『高级条件匹配』选择请求行，则可选的字段包括 VERSION、METHOD、和 URI，界面如下所示：



[VERSION]字段可设置条件为 HTTP/1.0 或者 HTTP/1.1，界面如下所示：

高级条件匹配

 请求行 请求头部 证书变量

字段 VERSION

条件 HTTP/1.0

HTTP/1.0
HTTP/1.1

[METHOD]字段可设置条件为 GET 或者 POST。界面如下所示：

高级条件匹配

 请求行 请求头部 证书变量

字段 METHOD

条件 GET

GET
POST

[URI]字段可设置条件等于、包含、通配符和正则匹配，并设置属性，界面如下所示：

高级条件匹配

 请求行 请求头部 证书变量

字段 URI

条件 等于

属性 区分大小写 条件取反

若『高级条件匹配』选择请求头部，则可选的字段包括 HOST、COOKIE、USER-AGENT 和自定义。

[HOST]、[COOKIE]、[USER-AGENT]和自定义字段均可设置条件等于、包含、通配符和正则匹配，并设置属性，界面如下所示：

高级条件匹配

 请求行 请求头部 证书变量

字段 HOST

条件 等于

属性 区分大小写 条件取反

若『高级条件匹配』选择证书变量，则可选的字段包括 Version、Issuer、Subject、Common Name、EmailAddress、Organization、Organizational Unit、Locality、State or Province、Country，界面如下所示：

高级条件匹配

 请求行 请求头部 证书变量

字段	Version
条件	Version Issuer Subject Common Name EmailAddress Organization Organizational Unit Locality State or Province Country

点击**添加**，将设置的条件加入选择框，如下所示：

新建

属性

名称
类型 请求改写

关联属性

源IP范围 所有地址
高级条件匹配
 请求行 请求头部 证书变量
字段 Version
条件 v1

证书变量	Version	等于	v1	aa	<input type="button" value="添加"/>	<input type="button" value="删除"/>
------	---------	----	----	----	-----------------------------------	-----------------------------------

动作

『动作』可设置插入头部，删除头部，改写头部，改写头部URI和内容改写。

若『动作』选择插入头部，则需要定义头部名称和插入内容，界面如下所示：

动作	插入头部
头部名称	<input type="text"/>
插入内容	<input type="text"/>

若『动作』选择删除头部，则需要定义删除头部的名称，界面如下所示：

动作	删除头部
头部名称	<input type="text"/>

若『动作』选择改写头部，则需要定义需要改写头部的名称，匹配内容和改写内容，界面如下所示：

动作	改写头部
头部名称	<input type="text"/>
匹配内容	<input type="text"/>
改写内容	<input type="text"/>

若『动作』选择改写头部 URI，则需要设置改写范围和改写动作，界面如下所示：

动作	改写头部URI
改写范围	<input type="text"/>
改写内容	<input type="text"/>

若『动作』选择内容改写，则需要设置匹配内容和改写内容，界面如下所示：

动作	内容改写
匹配内容	<input type="text"/>
改写内容	<input type="text"/>

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.7.3.2. 应答改写

『应答改写』设置在 HTTP 应答方向的头部进行插入、删除、修改及 URI 的修改操作。

点击**下一步**，界面如下所示：

新建

属性

名称

类型 应答改写

关联属性

源IP范围 所有地址

高级条件匹配 请求行 应答行 请求头部 应答头部

字段 URI

条件 等于

属性 区分大小写 条件取反

动作 --请选择--

『名称』可以输入便于记忆和识别的字符串，用于标识策略。

『源 IP 范围』设置 HTTP 头部改写的源 IP 地址范围。

『高级条件匹配』设置当 HTTP 请求方向的请求行、应答行、请求头部和应答头部符合一定条件时进行下一步动作。

若『高级条件匹配』选择请求行，则可选的字段包括 VERSION、METHOD、和 URI，界面如下所示：



[VERSION]字段可设置条件为 HTTP/1.0 或者 HTTP/1.1，界面如下所示：

高级条件匹配

请求行 应答行 请求头部 应答头部

字段 VERSION

条件 HTTP/1.0

HTTP/1.0
HTTP/1.1

[METHOD]字段可设置条件为 GET 或者 POST。界面如下所示：

高级条件匹配

请求行 应答行 请求头部 应答头部

字段 METHOD

条件 GET

GET
POST

[URI]字段可设置条件等于、包含、通配符和正则匹配，并设置属性，界面如下所示：

高级条件匹配

请求行 应答行 请求头部 应答头部

字段 URI

条件 等于

属性 区分大小写 条件取反

若『高级条件匹配』选择应答行，则可选的字段包括 VERSION 和 STATUS-CODE。界面如下所示：

高级条件匹配

请求行 应答行 请求头部 应答头部

字段 VERSION

条件 VERSION

STATUS-CODE

[VERSION]字段可设置条件为 HTTP/1.0 或者 HTTP/1.1，界面如下所示：

高级条件匹配

请求行 应答行 请求头部 应答头部

字段 VERSION

条件 HTTP/1.0

HTTP/1.0
HTTP/1.1

[STATUS-CODE]字段可设置条件等于、包含、通配符和正则匹配，并设置属性，界面如下所示：



若『高级条件匹配』选择请求头部，则可选的字段包括 HOST、COOKIE、USER-AGENT 和自定义。

[HOST]、[COOKIE]、[USER-AGENT]和自定义字段均可设置条件等于、包含、通配符和正则匹配，并设置属性，界面如下所示：



若『高级条件匹配』选择应答头部，则可选的字段包括 CONTENT-TYPE、LOCATION、SET-COOKIE 和自定义。

[CONTENT-TYPE]、[LOCATION]、[SET-COOKIE]和自定义字段均可设置条件等于、包含、通配符和正则匹配，并设置属性，界面如下所示：



点击[添加](#)，将设置的条件加入选择框，如下所示：

新建

属性

名称: 应答改写 (长度限制为1~63字符, 且不能包含|“”,:%<>/\特殊字符)

类型: 应答改写

关联属性

源IP范围: 所有地址

高级条件匹配:

请求行: 应答行: 请求头部: 应答头部:

字段: COOKIE

条件: 等于 aa

属性: 区分大小写 条件取反

请求头部 COOKIE 等于 aa aa

动作: --请选择--

添加 **删除**

『动作』可设置插入头部、删除头部、改写头部和内容改写。

若『动作』选择插入头部，则需要定义头部名称和插入内容，界面如下所示：

动作	插入头部
头部名称	
插入内容	

若『动作』选择删除头部，则需要定义删除头部的名称，界面如下所示：

动作	删除头部
头部名称	

若『动作』选择改写头部，则需要定义需要改写头部的名称，匹配内容和改写内容，界面如下所示：

动作	改写头部
头部名称	
匹配内容	
改写内容	

若『动作』选择内容改写，则需要设置匹配内容和改写内容，界面如下所示：

动作	内容改写
匹配内容	
改写内容	

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.7.4. HTTP 防护策略

WEBUI：『应用负载』→『策略』→『HTTP 防护策略』。

点击 **HTTP 防护策略**，界面如下图所示：

HTTP 防护策略		
+新建	×删除	
<input type="checkbox"/> 名称	慢速攻击	泛洪攻击
<input type="checkbox"/> alarm_and_intercept	启用	启用
<input type="checkbox"/> alarm	启用	启用
<input type="checkbox"/> intercept	启用	启用
<input type="checkbox"/> close	禁用	禁用
HTTP 防护策略	启用	启用

『HTTP 防护策略』下显示 HTTP 防护策略的『名称』、『慢速攻击』、『泛洪攻击』。

删除按钮可以用于删除 HTTP 防护策略。

新建按钮可以用于新建 HTTP 防护策略。点击新建按钮，如下图所示：

新建

属性

名称

慢速攻击触发DDOS防护条件

状态 启用 禁用

连接超时时间 秒

请求超时时间 秒

最小传输速率 byte/s

泛洪攻击触发DDOS防护条件

状态 启用 禁用

防护方式

防护动作 告警 拦截

取消 **完成**

『名称』 HTTP 防护策略的名称，用来标识一条改写规则。

慢速攻击触发 DDOS 防护条件：

慢速攻击触发DDOS防护条件

状态 启用 禁用

连接超时时间 秒

请求超时时间 秒

最小传输速率 byte/s

『状态』 启用或禁用 HTTP 防护策略。

『连接超时时间』 TCP 连接最大空闲时间，无数据传输的连接将被关闭。

『请求超时时间』 TCP 连接上接收一个完整 HTTP 请求的最大时间，超过此时间未发送完 HTTP 请求的 TCP 连接将被关闭。

『最小传输速率』TCP连接上发送HTTP请求的最小速率，低于此速率的TCP连接将被关闭。

泛洪攻击触发DDOS防护条件：



泛洪攻击触发DDOS防护条件

状态 启用 禁用

防护方式 插入http头部 注入JS脚本

每秒请求个数阈值 个

每秒请求个数增长率 %

请输入防护URL 每秒请求个数阈值 每秒请求个数增长率 区分大小写

URL匹配条件

(可匹配64条URL条件匹配规则)

添加 上移 下移 删除

『状态』启用或禁用泛洪攻击触发DDOS防护策略。

『防护方式』插入http头部指返回302进行重定向，注入JS脚本指返回一段JS脚本由浏览器执行。

『每秒请求个数阈值』全局配置，当每秒请求个数超过该值后，启动防御。

『每秒请求个数增长率』全局配置，当每秒请求个数超过阈值的一半，且增长率超过该值时，启动防御。

『URL匹配条件』针对URL进行限定，支持通配符*和?，匹配形式为www.xxx.com/index.html。

防护方式：可以选择告警或拦截两种方式。

7.7.5. TCP策略

配置针对TCP类型虚拟服务的连接选项。

WEBUI: 『应用负载』→『策略』→『TCP策略』。

点击 **TCP 策略**，界面如下图所示：



+ 新建		删除		
<input type="checkbox"/>	名称	策略模式	TCP单边加速	强制关闭连接
	四层虚拟服务TCP策略	四层	--	--
	七层虚拟服务TCP策略	七层	禁用	启用

系统默认的 TCP 策略不可编辑，可点击名称查看内容。

点击 **新建**，选择 TCP 策略的模式，可以选择新建四层虚拟服务或七层虚拟服务。



新建

选择TCP策略模式

四层虚拟服务

七层虚拟服务

取消 **下一步**

7.7.5.1. 四层虚拟服务

选择『四层虚拟服务』，点击**下一步**，如图所示：



新建

属性

名称 (长度为1~63字符，且不能包含# | " | : | % | < | > | \ 特殊字符)

会话超时时间 秒

取消 **完成**

『名称』：TCP 策略名称。

『会话超时时间』：四层虚拟服务 TCP 的会话超时时间。

7.7.5.2. 七层虚拟服务

选择『七层虚拟服务』，点击**下一步**，如图所示：

新建

属性

名称 (长度为1~63字符, 且不能包含`|`“`|`：“`|`%`|`<`|`>`|`\特殊字符)

关联属性

MSS	<input type="text" value="1460"/>
SYN超时时间	<input type="text" value="75"/> 秒
空闲超时时间	<input type="text" value="600"/> 秒
TIME_WAIT超时时间	<input type="text" value="10000"/> 毫秒
时间戳	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
TCP单边加速	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
强制关闭连接	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
节点离线关闭连接	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用

『名称』：TCP 策略名称。

『MSS』：最大数据报文长度，请根据网络情况配置该值。

『SYN 超时时间』：新建 TCP 连接的超时时间，协议栈中该参数的默认值为 75 秒，
请根据网络情况进行调整。

『空闲超时时间』：七层虚拟服务 TCP 的空闲超时时间。

『TIME_WAIT 超时时间』：七层虚拟服务 TIME_WAIT 超时时间。

『时间戳』：防止客户端在同一个连接中两次请求时间大于服务器的超时时间，导致服务器主动关闭连接，并将这条连接状态改变为 TIME_WAIT 状态，第二次请求到来的时候，AD 无法复用这条连接导致无法应答客户端的第二个请求。

『TCP 单边加速』：只有激活了 TCP 单边加速授权序列号，才可以配置启用或禁用 TCP 单边加速；有网络延时或丢包严重的情况下加速效果较为显著。

『强制关闭连接』：发送 RST 关闭与服务器的连接。

『节点离线关闭连接』：节点失效时关闭之前的连接。

7.7.6. 卸载策略

WEBUI: 『应用负载』→『策略』→『卸载策略』。

卸载策略支持 SM2, ECDSA, RSA 证书同端口，客户端访问时，会根据客户端支持的算法与 SSL 卸载策略的算法配置列表选择对应类型证书。

点击**卸载策略**，界面如下图所示：

名称	SSL证书	服务器名称(SNI)	会话复用	客户端认证	CA证书
test1	test1		启用(2000, 1800)	禁用	无

『卸载策略』下显示卸载策略的『名称』以及该策略中『服务器证书』、『服务器名称』、『会话复用』、『客户端认证』、『CA 证书』的相关信息。

删除按钮可以用于删除卸载策略。

新建按钮可以用于新建卸载策略。点击**新建**按钮，如下图所示：

The screenshot shows the configuration interface for an SSL/TLS profile. It includes sections for '属性' (Properties), '配置' (Configuration), and '高级' (Advanced). In the '配置' section, there are dropdown menus for 'RSA服务器证书' (RSA Server Certificate), '国密服务器证书' (National Cryptographic Server Certificate), and '国密客户端证书' (National Cryptographic Client Certificate). Under '启用协议' (Enable Protocol), 'TLS1.0' and 'TLS1.2' are selected. A note says '已选择 (选择ECDH算法必须启用客户端认证)' (Selected (Selecting ECDH algorithm must enable client authentication)). The '加密算法' (Encryption Algorithm) section lists several cipher suites: TLS_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_RC4_128_MD5, and SSL_RSA_WITH_DES_CBC_SHA. Below this is a '待选' (Pending) list containing: SSL_RSA_WITH_NULL_MD5, SSL_RSA_WITH_NULL_SHA, TLS1_TXT_ECC_SM2_WITH_SM4_128_CBC_SM3, and TLS1_TXT_ECDHE_SM2_WITH_SM4_128_CBC_SM3. The '会话复用' (Session Reuse) section has '启用' (Enable) selected. The '缓存会话数量' (Cache Session Count) is set to 2000, and '缓存超时时间' (Cache Timeout) is set to 1800 seconds. The '客户端认证' (Client Authentication) section has '启用' (Enable) selected. The 'SSL策略失败规则' (SSL Policy Failure Rule) section shows a dropdown menu with '通过' (Pass) selected, and a table with two entries: '认证失败默认规则' (Default Rule for Authentication Failure) and 'SSL协议版本未启用' (SSL Protocol Version Not Enabled), both with '拒绝' (Reject) selected. There are '添加' (Add) and '删除' (Delete) buttons for the rule table.

『名称』 卸载策略名称，可以输入便于记忆和识别的字符串，用于标识策略。

『ECDSA 服务器证书』：当协商为商密算法时，服务端使用的 ECDSA 商密证书。

『RSA 服务器证书』：当协商为商密算法时，服务端使用的 RSA 商密证书。

『国密服务器证书』：当协商为国密算法时，服务端使用的 SM2 国密证书。服务端需要提供两张证书，签名证书用于密钥协商过程中的数字签名，加密证书用于密钥协商过程中的非对称加解密。

『启用协议』：可以选择 SSL3.0、TLS1.0、TLS1.1、TLS1.2、国密 1.1 五种。

『加密算法』：SSL 服务器证书类型不同，可选择对应的加密算法。

『服务器名称 SNI』：指服务器域名。

『Session Ticket 扩展』：针对 TLS 协议的会话复用，不包括 SSL 协议的。

『会话复用』：启用会话复用可延长保持客户端认证的信息，减少客户端的重复认证。

『缓存会话数量』：设置缓存的 SSL 会话的数量。

『缓存超时时间』设置 SSL 会话缓存的超时时间。

『客户端认证』可设置是否需要开启客户端认证，如果启用客户端认证，界面如下：



『客户端认证 URI 匹配』配置需要提交客户端证书认证的是全部还是指定 URI。开启客户端认证 URI 匹配后，界面如下图：



在输入框中填写指定的 URI，指定某个 URI 是否需要客户端认证，URI 示例：/index.html，支持通配符?和*，默认*即所有 URI 无需客户端认证。

启用客户端认证的情况下，客户端证书可选择[必要]或者[可选]。

[必要]的情况下，客户端必须提供证书且通过认证才能继续访问。

客户端提供证书有可能认证失败，此时配置[认证失败规则]根据错误信息来决定下一步的行为，如下图所示：



错误信息是 SSL 认证过程中的错误代码。列举了常见的错误代码如下：

[任意错误] 默认规则
[7] CERT_SIGNATURE_FAILURE
[9] CERT_NOT_YET_VALID
[10] CERT_HAS_EXPIRED
[22] CERT_CHAIN_TOO_LONG
[23] CERTIFICATE_REVOKED
[27] CERT_IS_NOT_TRUSTED

执行动作包括通过、拒绝或返回指定页面。指定页面是在 5.4 章节中配置的自定义页面。

-- 请选择 --
200 OK
301 Moved Permanently
302 Moved Temporarily
400 Bad Request
403 Forbidden
404 Not Found
500 Internal Server Error
501 Not Implemented
502 Bad Gateway
503 Service Unavailable

『证书链深度』设置证书链的深度。

『CA 证书』选择 CA 证书，需要配置为客户端证书所属的 CA。

『CRL』选择 CA 证书对应的 CRL。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.7.7. 加密策略

WEBUI: 『应用负载』→『策略』→『加密策略』。

点击加密策略，界面如下图所示：

加密策略					
名称	SSL证书	服务器名称(SNI)	会话复用	服务器端认证	CA证书
test11	test1		启用(2000,1800)	禁用	无

『加密策略』下显示策略的『名称』以及该策略中『服务器证书』、『服务器名称』、『会话复用』、『服务器端认证』、『CA证书』的相关信息。

删除按钮可以用于删除加密策略。

新建按钮可以用于新建加密策略。点击新建按钮，如下图所示：

新建

属性

名称 (长度为1~63字符，且不能包含& | " | , | : | % | < | > | / | \ 特殊字符)

配置

客户端证书

启用协议 SSL3.0 TLS1.0 TLS1.1 TLS1.2 国密1.1

已选择

加密算法

服务器名称(SNI)

会话复用 启用 禁用

缓存会话数

缓存超时时间 秒

服务器端认证 启用 禁用

待选

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

『名称』加密策略名称，可以输入便于记忆和识别的字符串，用于标识策略。

『客户端证书』客户端使用的证书。

『启用协议』可以选择 SSL3.0、TLS1.0、TLS1.1、TLS1.2、国密 1.1 五种。

『加密算法』SSL 服务器证书类型不同，可选择对应的加密算法。

『服务器名称 SNI』指服务器域名。

『会话复用』启用会话复用可延长保持客户端认证的信息，减少客户端的重复认证。

『缓存会话数量』设置缓存的 SSL 会话的数量。

『缓存超时时间』设置 SSL 会话缓存的超时时间。

『服务器端认证』可设置是否需要开启服务器端认证，如果启用服务器端认证，界面如下：



『证书链深度』设置证书链的深度。

『CA 证书』选择 CA 证书，需要配置为客户端证书所属的 CA。

『CRL』选择 CA 证书对应的 CRL。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.7.8. URL 下载速度控制

WEBUI: 『应用负载』→『策略』→『URL 下载速度控制』。

『URL 下载速度控制』用于定义需要限制下载速度的 URL 列表。防止某个 URL 访问流量过大，引起其他页面无法访问的情况，防迅雷盗链。

点击 **URL 下载速度控制**，界面如下图所示：



<input type="checkbox"/>	名称	控制列表	控制方式	下载速度最大值
<input type="checkbox"/>	URL下载速度控制	*	全部URL	512Kbps

第 1 页, 共1页 每页显示条数 20  共1/10条配置信息

点击 **统计查看**，会跳转到『系统概况』→『虚拟服务详情』→『URL 实时流量』页面。

点击**新建**，界面如下所示：

新建

属性

名称 (长度为1~63字符，且不能包含`|“”“：“%<> / \ 特殊字符)

配置

URL控制列表
当前已配置 0/64个URL
示例：
www.sangfor.com/index.html
www.baidu.com/*

URL排除列表
当前已配置 0/64个URL

控制方式 每类URL 全部URL

下载速度最大值 20 Kbps

『名称』可以输入便于记忆和识别的字符串，用于标识虚拟服务。

『URL 控制列表』输入需要进行速度控制的 URL 地址。支持通配，比如填写：

192.200.200.55/dedecms/a/ad/*

『URL 排除列表』需要排除不限制速度的 URL 地址。

『控制方式』可选择对每类 URL 或全部 URL 做速度控制。

『下载速度最大值』设置下载流量最大值。

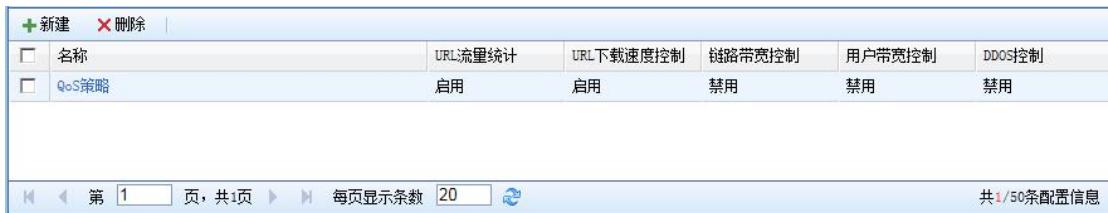
若需要设置 URL 下载速度控制功能，建议先通过『URL 实时流量』查看到 URL 的流量情况，再根据流量较大的 URL 做限制。

7.7.9. QoS 策略

WEBUI：『应用负载』→『策略』→『QoS 策略』。

『QoS 策略』用于定义针对链路和用户的带宽控制策略。

点击 **QoS 策略**，界面如下图所示：



The screenshot shows a table with columns: 名称 (Name), URL流量统计 (URL Traffic Statistics), URL下载速度控制 (URL Download Speed Control), 链路带宽控制 (Link Bandwidth Control), 用户带宽控制 (User Bandwidth Control), and DDOS控制 (DDoS Control). A single row is selected, labeled 'QoS策略'. Below the table is a pagination bar with '第 1 页, 共1页 每页显示条数 20' and a note '共1/50条配置信息'.

点击**新建**，界面如下所示：



The dialog has tabs for '编辑' (Edit) and '属性' (Properties). In the '属性' tab, there is a '名称' (Name) field containing 'QoS策略' with a note '(长度为1~63字符, 且不能包含& | " " , : % < > / \ 特殊字符)'. Under '带宽控制' (Bandwidth Control), three options are shown: '链路带宽控制' (Link Bandwidth Control) with '启用' (Enable) selected, '用户带宽控制' (User Bandwidth Control) with '禁用' (Disable) selected, and 'DDoS控制' (DDoS Control) with '启用' (Enable) selected. Under 'URL流量控制和统计' (URL Traffic Control and Statistics), 'URL流量统计' (URL Traffic Statistics) is set to '启用' (Enable) and 'URL下载速度控制' (URL Download Speed Control) is set to '禁用' (Disable). At the bottom are '取消' (Cancel) and '完成' (Finish) buttons.

『名称』可以输入便于记忆和识别的字符串，用于标识虚拟服务。

『链路带宽控制』对 IP 组使用的链路带宽进行控制。勾选启用，界面如下：



The interface shows '链路带宽控制' (Link Bandwidth Control) with '启用' (Enable) selected. It includes dropdown menus for 'IP组' (IP Group) and 'WAN口' (WAN Port), and input fields for '上行' (Upstream) and '下行' (Downstream) bandwidth limits of 100 Kbps each. Buttons for '添加' (Add) and '删除' (Delete) are also present. A note at the bottom says '(可配置128条匹配规则)'.

『用户带宽控制』对 IP 组使用的链路带宽进行控制。勾选启用，界面如下：



The interface shows '用户带宽控制' (User Bandwidth Control) with '启用' (Enable) selected. It includes input fields for '最大上行带宽' (Maximum Upstream Bandwidth) and '最大下行带宽' (Maximum Downstream Bandwidth), both set to 100000 Kbps.

『DOS 控制』防止客户端在应用层进行分布式拒绝服务攻击。可以选择针对 HTTP(HTTPS)和 DNS 类型的虚拟服务进行请求限制。

启用 DOS 控制，选择 HTTP 协议，配置界面如下：



当一个客户端在『统计时间』内对 HTTP 虚拟服务的请求次数超过设置的『请求阈值』之后，AD 会执行指定的动作，禁止请求页面。

默认动作为针对所有页面执行关闭连接动作。可以配置针对指定页面在满足 DOS 条件后，执行关闭连接或者返回指定内容。

指定页面为页面的 URL，支持通配符，勾选区分大小写以设置 URL 是否区分大小写。

关闭连接分为发送 FIN 关闭和发送 RST 关闭。



返回页面可以选择预定义的页面，见 5.4 章节配置。



启用 DOS 控制，选择 HTTP 协议，配置界面如下：



当一个客户端在『统计时间』内对 DNS 虚拟服务的请求次数超过设置的『请求阈值』之后，AD 会拒绝该客户端的 DNS 请求。

7.8. 虚拟服务

7.8.1. 虚拟服务

WEBUI: 『应用负载』→『虚拟服务』

『虚拟服务』用于定义需要发布的应用以及对应的链路负载策略。

界面如下图所示：

虚拟服务						
虚拟服务关联组						
操作		名称	负载模式	服务	IP组	前置策略
<input type="checkbox"/>	<input type="checkbox"/>	web	七层	http	IP-11	--
<input type="checkbox"/>	<input type="checkbox"/>	mysql	七层	mysql	IP-16	--
<input type="checkbox"/>	<input type="checkbox"/>	httpd	七层	http	IP-18	--

『虚拟服务』下显示节虚拟服务的『名称』、『负载模式』、『服务』、『IP 组』、

『前置策略』、『默认节点池』。

启用按钮可以用于启用虚拟服务。

禁用按钮可以用于禁用虚拟服务。

删除按钮可以用于删除虚拟服务。

新建按钮可以用于新建虚拟服务。

点击**新建**按钮，将会弹出负载模式选择框，如下图所示：



选择『四层模式』，点击**下一步**按钮，如下图所示：

虚拟服务

新建

属性

名称

状态 启用 禁用

调度配置

负载模式 四层

服务

IP 组

默认节点池

前置策略 [多选]

网络策略

TCP策略

QoS策略

SNAT地址集

三角传输 启用 禁用

『名称』可以输入便于记忆和识别的字符串，用于标识虚拟服务。

『状态』用于配置虚拟服务的[启用]、[禁用]。

『负载模式』显示上一步选择的负载模式。

『服务』用于配置虚拟服务的应用服务，如需要新增或修改服务，可以在『应用负载』→『服务』中进行配置。四层负载只能对系统自带的 SMTP、POP3、FTP 服务以及自定义的 TCP、UDP 服务进行负载。

『IP 组』用于配置虚拟服务对外发布的 IP 地址，如需要新增或修改 IP 组，可以在『应用负载』→『IP 组』中进行配置。

『默认节点池』若此虚拟服务没有关联前置调度策略或者是前置调度策略调度失败时将会对默认节点池中的节点进行调度。

『前置策略』用于关联相关服务的前置调度策略。如果有多个前置调度策略，可以点击**多选**按钮选择多个。

『QoS 策略』选择针对链路和用户的带宽控制策略。

『SNAT 地址集』开启该功能，系统会自动为该虚拟服务选择一部分 IP 组建一个转换池，并使用一定的选择算法从池中选择和分配转换地址。

『三角传输』用于设置服务器回复数据包不经过 AD 设备的情况，此时需要启用三角传输。启用三角传输后用户访问虚拟服务的数据经过 AD 设备调度到真实服务器，服务器回包不经过 AD 设备。

选择『七层模式』，点击**下一步**按钮，如下图所示：

虚拟服务

新建

属性

名称

状态 启用 禁用

调度配置

负载模式 七层

服务

IP 组

默认节点池

调度方式 首个请求 每一个请求

前置策略 [多选]

网络策略

TCP策略

QoS策略

SNAT地址集

应用策略

优化策略

HTTP防护策略

『名称』可以输入便于记忆和识别的字符串，用于标识虚拟服务。

『状态』用于配置虚拟服务的[启用]、[禁用]。

『所属虚拟服务关联组』展示该虚拟服务属于哪个虚拟服务关联组。

『负载模式』显示上一步选择的负载模式。

『服务』用于配置虚拟服务的应用服务，如需要新增或修改服务，可以在『应用负载』→『服务』中进行配置。七层负载只能对系统自带的所有服务以及自定义的 HTTP、SMTP、POP3、HTTPS、SSL、DNS、Radius、TCP、MYSQL 服务进行负载。

『IP组』用于配置虚拟服务对外发布的IP地址，如需要新增或修改IP组，可以在『应用负载』→『IP组』中进行配置。

『前置策略』用于关联相关服务的前置调度策略。多个虚拟服务支持引用同一个前置策略。如果有多个前置调度策略，可以点击**多选**按钮选择多个。

『默认节点池』若此虚拟服务没有关联前置调度策略或者是前置调度策略调度失败时将会对默认节点池中的节点进行调度。

『优化策略』启用并选择预先设定的优化策略方案。优化策略可以对“HTTP连接池”、“HTTP缓存”和“HTTP压缩”等功能进行设定。优化策略的详细配置请参考6.6.2优化策略。

『HTTP防护策略』选择新建七层虚拟服务，配置http/https服务时，默认启用“HTTP防护策略”，用户可以根据实际业务需求选择“未启用”，也可以根据业务需要在『应用负载』-『策略』-『HTTP防护策略』中新建策略。当然，也可以编辑默认的“HTTP防护策略”，但要注意，将会影响所有引用默认策略的七层虚拟服务。

『TCP策略』设置选择针对七层虚拟服务的TCP传输控制策略。

『QoS策略』设置针对用户带宽和链路带宽的控制策略。

『自动SNAT』开启该功能，系统会自动为该虚拟服务选择一部分IP组建一个转换池，并使用一定的选择算法从池中选择和分配转换地址。

『SSL卸载策略』SSL/HTTPS类型虚拟服务使用的SSL卸载策略，可以在“SSL->SSL策略->卸载策略”进行配置。如果有多个SSL卸载策略，可以点击**多选**按钮选择多个。

『SSL加密策略』SSL/HTTPS类型虚拟服务使用的SSL加密策略，可以在“SSL->SSL策略->加密策略”进行配置。如果有多个SSL加密策略，可以点击**多选**按钮选择多个。

『iPro』可以在“公共对象->iPro”进行配置，最多可以选择5条iPro。如果有多个iPro，可以点击**多选**按钮选择多个。

『自动跳转 HTTPS』用于配置当使用 HTTP 访问虚拟服务时，自动转换为 HTTPS 服务。选择[启用]则启用自动跳转功能，选择[禁用]则禁用自动跳转功能。『HTTP 端口』用于设置当通过 HTTP 某个端口访问服务的时候自动跳转到 HTTPS，而使用其他端口的 HTTP 访问不会自动跳转。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.8.2. 虚拟服务关联组

WEBUI: 『应用负载』→『虚拟服务』→『虚拟服务关联组』。

『虚拟服务关联组』开启集群模式才会显示。

虚拟服务		虚拟服务关联组
<input type="checkbox"/>	名称	虚拟服务
<input type="checkbox"/>	虚拟服务关联组_1	web/
<input type="checkbox"/>	虚拟服务关联组_5	mysql/
<input type="checkbox"/>	虚拟服务关联组_6	httpd/

『虚拟服务关联组』：发布相同 IP 或使用相同节点池的多个虚拟服务一定在同一个关联组中，该图展示这些虚拟服务之间的关联关系。



『关联应用组』：选择该虚拟服务关联组所属的应用组。应用组在哪台设备上生效，该关联组包含的虚拟服务就在哪台设备上生效。

第8章 智能DNS

『智能 DNS』用于配置 DNS 智能服务，分为本地和全局两种配置，全局配置参与各个智能站点间的信息同步，本地配置则不参与。设置包括『DNS 服务器』、『站点集合』、『DNS 记录』、『虚拟 IP 池』、『DNS 映射』、『LDNS 集合』、『静态就近性』、『全局配置还原』。



注意：此模块的『站点集合』、『DNS 记录』中的[全局 DNS 记录]、『虚拟 IP 池』中的[全局虚拟 IP 池]、『DNS 映射』的[全局 DNS 映射]、『LDNS 集合』的[全局 LDNS 集合]、『全局配置还原』需要开通智能 DNS 全局授权的序列号。未开通智能 DNS 全局授权序列号时，这些子模块和标签将被隐藏。

8.1. DNS 服务器

WEBUI：『智能 DNS』→『DNS 服务器』。

『DNS 服务器』用于定义当 AD 作为 DNS 服务器时的一些基本参数。

界面如下图所示：

DNS服务器

更新DNS服务器配置

普通属性

状态 启用 禁用

DNS服务器属性

已选择
212.10.204.26
61.139.2.34

待选

监听地址

不添加监听IP将使DNS配置失效！

DNS端口 53

不存在的域名处理 不回应 拒绝 代理

DNS探测属性

探测超时时间 2 秒

探测结果缓存时间 10800 秒

探测方法 DNS反向查询

更新



『状态』用于配置启用或禁用 DNS 服务器。禁用 DNS 服务器将不对内外网的 DNS 请求进行解析。

『监听地址』用于配置 DNS 服务器提供服务的 IP 地址，支持选择 IPv4 或 IPv6 地址。可选择列表中选定需要监听的 IP 地址，点击  按钮将选定的 IP 地址添加至已选择列表，需要取消监听则选中已选择列表中的 IP 地址，点击  按钮即可。不添加监听地址将使 DNS 配置失效。

『DNS 端口』用于配置 DNS 服务器提供服务的 TCP 和 UDP 端口，默认为 53。

『不存在的域名处理』用于配置 DNS 服务器『不回应』、『拒绝』或『代理』不存在

的域名查询处理。选择『代理』，则设备收到不存在域名的查询请求的时候，将该请求转至『DNS 代理』模块处理。

『探测超时时间』用于配置 DNS 服务器探测客户端本地 DNS 响应速度的超时时间。

『DNS 探测结果缓存时间』用于配置 DNS 服务器探测客户端本地 DNS 响应速度结果的缓存时间，单位为秒。

『探测方法』用于配置 DNS 服务器探测客户端本地 DNS 响应速度的方法，包括『DNS 根查询』、『DNS 反向查询』和『PING 方式』。『DNS 根查询』表示通过客户端本地 DNS 进行根查询的方法探测响应时间，『DNS 反向查询』表示通过客户端本地 DNS 进行反向查询的方法探测响应时间。『PING 方式』表示通过 ping 本地 DNS 的方法探测响应时间。

[更新]按钮用于更新并保存改动的配置。

8.2. 站点集合

WEBUI：『智能 DNS』→『站点集合』。

点击『站点集合』，会提示：



『站点集合』用于当 AD 做分布式部署时，添加分布式部署中的各个站点，本地站点也需要添加至站点集合中，并通过其他设置达到分布式负载的效果。

界面如下图所示：

系统导航菜单

- ▶ 系统概况
- ▶ 报表配置
- ▶ 公共对象
- ▶ 应用负载
- ▶ 智能DNS
 - ▶ DNS服务器
 - ▶ **站点集合**
 - ▶ DNS记录
 - ▶ 虚拟IP池
 - ▶ DNS映射
 - ▶ LDNS集合
 - ▶ 静态就近性
 - ▶ 全局配置还原
- ▶ 路由配置

站点集合

+ 新建 X 删除 刷新时间间隔: 5秒

站点名称	IP地址	通讯端口	状态
ALL	10.10.0.1, 10.10.1.1	558	在线

删除按钮用于删除站点集合列表中的站点。

新建按钮用于新建分布式部署中的站点。

站点集合

编辑

普通属性

站点名称	本地站点
地理位置	广州

站点通讯配置

地址列表	已选择 212.10.204.26 61.139.2.34	待选 电信 网通
通讯端口	558	
同步角色	Server	
同步公差	5	秒
通信加密密钥	*****	
再次输入密钥	*****	

取消 **完成**

『站点名称』用于自定义本地站点的名称。

『地理位置』用于对站点的地理区域的描述。

『地址列表』用于配置站点用于通讯的地址。可选择列表中选定本地需要通讯的 IP 地址，点击  按钮将选定的 IP 地址添加至已选择列表，需要取消某 IP 地址的通讯则选中已选择列表中的 IP 地址，点击  按钮即可。不添加通讯地址则其他站点无法和本地站点通讯，会导致客户端访问其他站点时，无法负载到本地站点。

『通讯端口』用于配置本地站点用于通讯的端口。

『同步角色』用于定义该站点在全局同步的角色。『None』表示不参与同步；『Client』表示仅做接收操作，当其他 Server 角色站点配置文件变更时，被动更新本站的全局配置；『Server』仅作发送操作，当本站配置文件变更时，主动同步其他 Client 角色站点的全局配置；『Client&Server』同时作为 Client 和 Server 两个角色，既可向外广播自身配置，也可同步接收全局配置。

『同步公差』全局同步过程中，两个站点间的配置文件修改时间差的阈值。当两个站点配置文件差值大于『同步公差』时，表明修改时间较早的站点配置文件需要被更新；当两个站点配置文件修改时间的差值小于等于『同步公差』时，这两个配置将被视为等效且不同步。

『通信加密密钥』和『再次输入密钥』用于加密站点间传送的数据内容。

 取消按钮可以用于取消本次配置。

 完成按钮可以用于完成本次配置。

配置好本地站点后，点击  完成，页面如下图：

站点集合				
+新建  刷新时间间隔：5秒				
	站点名称	IP地址	通讯端口	状态
	本地站点	212.10.204.26, 61.139.2.34	558	

点击**新建**按钮，开始配置其他站点，配置页面如下图：



『站点名称』用于自定义站点的名称。

『地址列表』用于添加与该站点通讯的IP地址。填写好通讯IP地址，点击**添加**，将通讯IP地址添加至地址列表。选中地址列表中的IP地址，点击**删除**，从列表中删除该IP。

『通讯端口』用于配置该站点用于通讯的端口。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

8.3. DNS 记录

WEBUI: 『智能 DNS』 → 『DNS 记录』。

『DNS 记录』用于定义当 AD 作为 DNS 服务器时需要解析的记录，包括『MX 记录』、『NS 记录』、『SRV 记录』、『CNAME 记录』、『TXT 记录』、『PTR 记录』和『SOA 记录』。

界面如下图所示：

系统导航菜单

- ▶ 系统概况
- ▶ 报表配置
- ▶ 公共对象
- ▶ 应用负载
- ▶ 智能 DNS
 - ▶ DNS服务器
 - ▶ 站点集合
 - ▶ **DNS记录**
 - ▶ 虚拟IP池
 - ▶ DNS映射
 - ▶ LDNS集合
 - ▶ 静态就近性
 - ▶ 全局配置还原
- ▶ 路由配置
- ▶ 网络配置
- ▶ 系统配置
- ▶ 配置向导
- ▶ 高可用性
- ▶ 业务分析

本地DNS记录 全局DNS记录

选择类别

- MX记录 （邮件交换记录，用于电子邮件系统发邮件时定位邮件服务器）
- NS记录 （是域名服务器记录，用来指定该域名由哪个DNS服务器来进行解析）
- SRV记录 （是服务器资源记录，用于记录一个服务器能够提供什么样的服务）
- CNAME记录 （也被称为规范名字，这种记录允许您将多个名字映射到同一台计算机）
- TXT记录 （一般指为某个主机名或域名设置的说明）
- PTR记录 （指针记录，引导至一个规范域名，常用来进行反向DNS查询）
- SOA记录 （SOA资源记录表明此DNS名称服务器是DNS域中的数据信息的最佳来源）

取消 下一步

8.3.1. 本地 DNS 记录

WEBUI: 『智能 DNS』 → 『DNS 记录』 → 『本地 DNS 记录』。

『本地 DNS 记录』用于非分布式环境，只存在本地一个站点的情况下，AD 充当本地的 DNS 服务器。

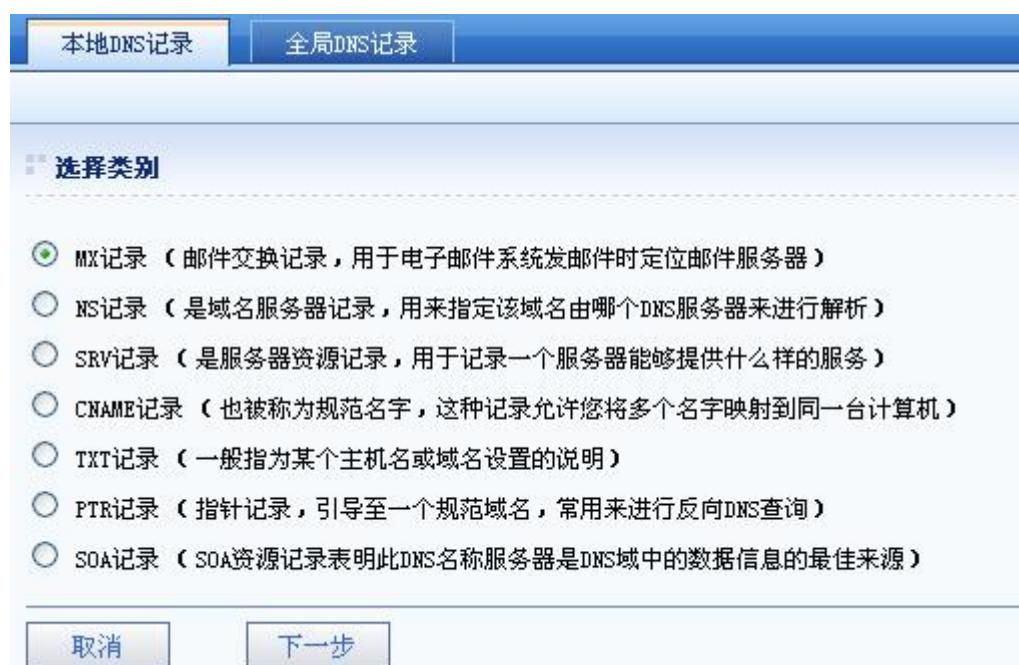
启用按钮可以用于启用选中的 DNS 记录。

禁用按钮可以用于禁用选中的 DNS 记录。

删除按钮可以用于删除选中的 DNS 记录。

新建按钮可以用于新建 DNS 记录。

点击新建按钮，如下图所示：



『选择类别』下面显示可以选择的 DNS 记录类别，包括『MX 记录』、『NS 记录』、『SRV 记录』、『CNAME 记录』、『TXT 记录』、『PTR 记录』和『SOA 记录』。

取消按钮可以用于取消本次配置。

下一步按钮可以用于继续下一步配置。

7.3.1.1 MX 记录

选择『MX 记录』，点击下一步按钮，如下图所示：

本地DNS记录 全局DNS记录 帮助信息

新建MX记录

属性

域名 (长度为1~255字符，且不能包含& | * ^ , : % < > / \ 特殊字符)

状态 启用 禁用

配置

MX记录列表

主机:	<input type="text"/>
优先级:	<input type="text"/>
TTL:	<input type="text"/> 秒

添加 **删除**

当前已配置 0/7 个地址

取消 **完成**



『域名』用于配置 DNS 记录的域名。

『状态』用于配置 DNS 记录的『启用』、『禁用』。

『MX 记录列表』用于配置 DNS 记录的域名对应的 MX 记录。MX 记录是用于电子邮件系统发送邮件时根据收信人的地址后缀来定位邮件服务器。『主机』用于配置 DNS 记录的域名对应的邮件服务器的主机名。『优先级』用于设置 MX 记录的优先级，值越小，优先级越高。『TTL』用于配置 DNS 策略的域名记录 Local DNS 的缓存时间，单位为秒。

添加 按钮用于添加 MX 记录到 MX 记录列表中。

删除 按钮用于删除 MX 记录列表中的记录。

取消 按钮可以用于取消本次配置。

完成 按钮可以用于完成本次配置。

7.3.1.2 NS 记录

若『选择类别』中选择『NS 记录』，点击**下一步**按钮，如下图所示：



『域名』用于配置 DNS 记录的域名。

『状态』用于配置 DNS 记录的『启用』、『禁用』。

『NS 记录列表』用于配置 DNS 记录的域名对应的 NS 记录。NS 记录是域名服务器记录，用来指定该域名由哪个 DNS 服务器来进行解析。『名字服务器』用于配置 DNS 记录的域名对应的名字服务器的域名。『IP 地址』用于设置名字服务器对应的 IP 地址。

添加按钮用于添加 NS 记录到 NS 记录列表中。

删除按钮用于删除 NS 记录列表中的记录。

『记录生存时间(TTL)』用于配置 DNS 记录的域名记录 Local DNS 的缓存时间，单位为秒。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.3.1.3 SRV 记录

『SRV 记录』：服务器资源记录，用于记录一个服务器能够提供什么样的服务。



『域名』用于配置 DNS 记录的域名。

『状态』用于配置 DNS 记录的『启用』、『禁用』。

『SRV 记录列表』是配置服务器资源记录，用于记录一个服务器能够提供什么样的服务。『主机』用于填写有效的主机名称。『端口』用于填写主机提供服务的端口。『优先级』用于多台主机提供相同服务时设置服务器的优先级。『权值』用于设置 SRV 记录的优先级，权值越小，优先级越高。『TTL』用于配置 DNS 策略的域名记录 Local DNS 的缓存时间，单位为秒。

添加按钮用于添加 SRV 记录到 SRV 记录列表中。

删除按钮用于删除 SRV 记录列表中选中的记录。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.3.1.4 CNAME 记录

若『选择类别』中选择『CNAME 记录』，点击下一步按钮，如下图所示：



『域名』用于配置 DNS 记录的域名。

『状态』用于配置 DNS 记录的『启用』、『禁用』。

『CNAME 记录列表』用于配置 DNS 记录的域名对应的 CNAME 记录。『规范名称』用于配置 DNS 记录的域名对应的规范名称，DNS 记录的域名即是规范名称的别名。

添加按钮用于添加 CNAME 记录到 CNAME 记录列表中。

删除按钮用于删除 CNAME 记录列表中的记录。

『记录生存时间(TTL)』用于配置 DNS 记录的域名记录 Local DNS 的缓存时间，单位为秒。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.3.1.5 TXT 记录

若『选择类别』中选择『TXT 记录』，点击下一步按钮，如下图所示：



『域名』用于配置 DNS 记录的域名。

『状态』用于配置 DNS 记录的『启用』、『禁用』。

『TXT 值』用于配置域名的文本信息。

『TTL』用于配置 DNS 记录的域名记录 Local DNS 的缓存时间，单位为秒。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.3.1.6 PTR 记录

『PTR 记录』：指针记录，引导至一个规范域名，常用来进行反向 DNS 查询



『反向域名』用于配置 PTR 记录的域名，需要一个合法的 IPv4 地址的逆序输入。

『状态』用于配置 PTR 记录的『启用』、『禁用』。

『PTR 记录列表』用于 PTR 记录信息，通常是 MX 记录对应的域名。

『TTL』用于配置 PTR 记录的域名记录 Local DNS 的缓存时间，单位为秒。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

7.3.1.7 SOA 记录

若『选择类别』中选择『SOA 记录』，点击下一步按钮，如下图所示：

本地DNS记录 | 全局DNS记录

新建SOA记录

属性

域名 (长度为1~255字符)

状态 启用 禁用

配置

源主机：

电子邮件：

序列号：

刷新时间： 秒

重试时间： 秒

到期时间： 秒

TTL：

最小TTL：

『域名』用于配置 DNS 记录的域名。

『状态』用于配置 DNS 记录的『启用』、『禁用』。

『源主机』用于配置起始授权机构 (SOA) 资源记录指明区域。

『电子邮件』用于配置有关区域问题的联系人电子邮件地址。

『序列号』该区域文件的修订版本号。每次区域中的资源记录改变时，这个数字便会增加。每次区域改变时增加这个值非常重要，它使部分区域改动或完全修改的区域都可以在后续传送中复制到其他辅助服务器上。。

『刷新时间』以秒计算的时间，它是在查询区域的来源以进行区域更新之前辅助 DNS 服务器等待的时间。当刷新间隔到期时，辅助 DNS 服务器请求来自响应请求的源服务器的区域当前 SOA 记录副本。然后，辅助 DNS 服务器将源服务器的当前 SOA 记录（如响应中所示）的序列号与其本地 SOA 记录的序列号相比较。如果二者不同，则辅助 DNS 服务器从主要 DNS 服务器请求区域传输。这个域的默认时间是 900 秒（15 分钟）。。

『重试时间』以秒计算的时间，是辅助服务器在重试失败的区域传输之前等待的时间。通常，这个时间短于刷新间隔。该默认值为 600 秒（10 分钟）。

『到期时间』以秒计算的时间，是在区域没有刷新或更新的已过去的刷新间隔之后、辅助服务器停止响应查询之前的时间。因为在这个时间到期，因此辅助服务器必须把它的本地数据当作不可靠数据。默认值是 86,400 秒（24 小时）

『TTL』用于配置区域的存在时间。

『最小 TTL』用于配置区域的默认存在时间。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

8.3.2. 全局 DNS 记录

WEBUI：『智能 DNS』→『DNS 记录』→『全局 DNS 记录』。

『全局 DNS 记录』用于分布式环境，在多个站点之间的此 AD 设备充当全局的 DNS 服务器时需要解析的记录，并且各个站点的『全局 DNS 记录』配置可以相互同步。

界面如下图所示：

		本地DNS记录	全局DNS记录		
		+新建	×删除	✓启用	✗禁用
□	域名	记录类型		别名/主机/TXT值	

配置步骤请参考 8.6.8.6.1 本地 DNS 记录。



集群部署环境下，不支持全局 DNS 负载功能，仅支持本地智能 DNS。

8.4. 虚拟 IP 池

WEBUI：『智能 DNS』→『虚拟 IP 池』。

『虚拟 IP 池』用于设置需要进行智能 DNS 二级调度，将客户端访问调度到某个发布的 IP 和端口。DNS 映射为智能 DNS 一级调度，详细配置请看章节 8.5DNS 映射。『虚拟 IP 池』包含『本地虚拟 IP 池』和『全局虚拟 IP 池』。『本地虚拟 IP 池』用于单个站点，非分布式环境中；『全局虚拟 IP 池』用于多个站点，分布式环境中，并且各个站点的『全局虚拟 IP 池』配置可以相互同步。

界面如下图所示：



8.4.1. 本地虚拟 IP 池

WEBUI：『智能 DNS』→『虚拟 IP 池』→『本地虚拟 IP 池』。

『本地虚拟 IP 池』用于非分布式环境，只存在本地一个站点的情况下，对本地的 IP 和端口进行智能 DNS 二级调度。

界面如下图所示：



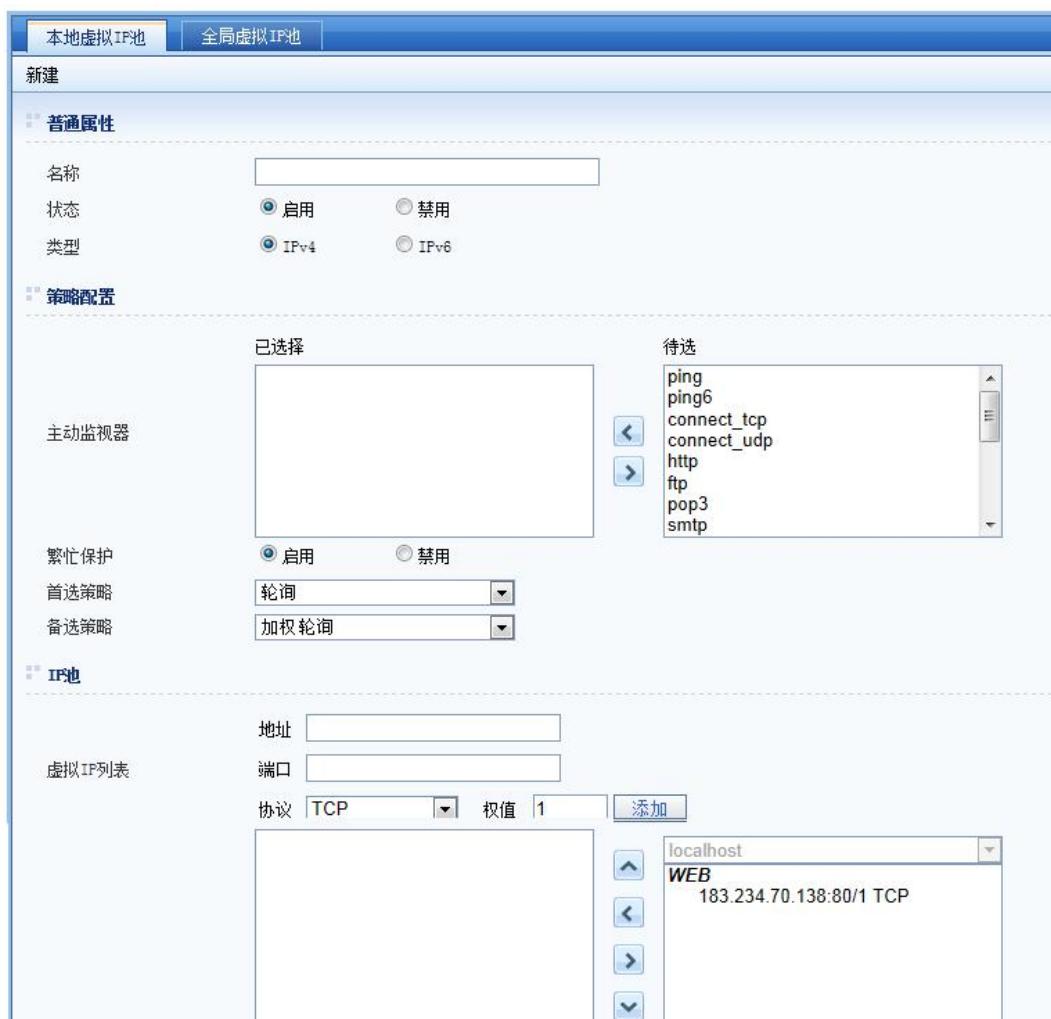
『启用』按钮可以用于启用选中的虚拟IP池。

『禁用』按钮可以用于禁用选中的虚拟IP池。

『删除』按钮可以用于删除选中的虚拟IP池。

『新建』按钮可以用于新建虚拟IP池。

点击『新建』按钮，如下图所示：



『名称』用于定义虚拟IP池的名称。

『状态』用于配置该虚拟IP池的『启用』、『禁用』。

『类型』用于定义该虚拟IP池的类型，是IPv4虚拟IP池还是IPv6虚拟IP池。

『主动监视器』选择需要启用的监视器，用于监视虚拟 IP 池中 IP 和端口是否正常。在可选择列表中，选定监视器，点击  按钮左移即可将选定的监视器启用。若需要将已经选定的监视器停用，在已选择列表中选定需要停用的监视器，点击  按钮右移选定的监视器即可。

『繁忙保护』用于设置『启用』或『禁用』繁忙保护，『启用』时，当某条链路繁忙，该链路上的 IP 和端口不参与调度。

『首选策略』用于配置虚拟 IP 池调度的首选策略，包括『轮询』、『加权轮询』、『首个可用』、『哈希』、『加权最小连接』、『动态就近性』、『加权最小流量』、『静态就近性』、『返回所有 IP』。

『备选策略』用于配置虚拟 IP 池调度的备用策略，包括『轮询』、『加权轮询』、『首个可用』、『哈希』、『加权最小连接』、『动态就近性』、『加权最小流量』、『静态就近性』、『返回所有 IP』、『返回备用 IP』、『拒绝』、『丢弃』。备选策略失败时，按轮询策略处理。选择策略说明如下：

- 1、『轮询』表示交替返回虚拟 IP 池中的某个 IP；
- 2、『加权轮询』表示通过设置中的『权重』加权计算结果返回虚拟 IP 池中的某个 IP；
- 3、『首个可用』表示在虚拟 IP 池中从上往下匹配，当匹配到某个 IP 有效则返回该 IP；
- 4、『哈希』表示通过哈希算法对 DNS 请求的源 IP 进行运算，由此确定返回的 IP；
- 5、『加权最小连接』表示通过设置中的『权重』、当前该 IP 所在链路连接数加权计算结果返回某个 IP；
- 6、『动态就近性』根据 DNS 服务器中配置的探测方法探测虚拟 IP 池中各个 IP 所在链路到客户端 Local DNS 的往返时延，返回往返时延最小的链路对应的 ip；
- 7、『加权最小流量』表示通过设置中的『权重』、当前该 IP 所在链路的流量加权计算结果返回虚拟 IP 池中的某个 IP；

8、『静态就近性』调度算法在『智能 DNS』→『静态就近性』→『虚拟 IP 池级别』中进行配置，根据所设置的 LDNS 集合来选择将客户端访问调度到虚拟 IP 池中的某个 IP。详细配置参考 8.7 静态就近性；

9、『返回所有 IP』则不对 IP 进行任何筛选，将虚拟 IP 池中的所有 IP 返回给客户端；

10、『拒绝』当首选策略调度失败，则返回拒绝信息到客户端；

11、『丢弃』当首选策略调度失败则对 DNS 请求数据包直接丢弃，不回应；

12、『返回备用 IP』表示可以设定某个 IP，当首选策略调度失败，则返回该 IP，设置如下图：



『虚拟 IP 列表』用于配置虚拟 IP 池中需要参与智能 DNS 二级调度的 IP 和端口。『地址』用于配置需要添加到虚拟 IP 池并发布出去的 IP。『端口』用于配置该 IP 所要发布的端口。

添加按钮用于手动添加需要参与智能 DNS 二级调度的地址和端口到虚拟 IP 池列表中。

点击  按钮，删除手动添加的 IP 地址和端口。

虚拟 IP 池列表右边框中显示的 IP 和端口为本地虚拟服务发布的公网 IP 和端口。在右边框中选中 IP 和端口，点击  按钮将选中的 IP 和端口添加至虚拟 IP 池列表。

选中虚拟 IP 池列表中的 IP 和端口，点击  按钮将选中的 IP 和端口上移，点击  按钮将选中的 IP 和端口下移。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置，如下图所示：

本地虚拟IP池			
全局虚拟IP池			
+ 新建		X 删除	
名称	类别	虚拟IP列表	
web	IPv4	183.234.70.138	

点击已经设置好的虚拟IP池的名称 **web**，可编辑虚拟IP池，并编辑虚拟IP，如下图所示：

编辑

普通属性

名称: web (长度限制为1~63个字符, 且不能包含* | " " , : % < > / \ 特殊字符)

状态: 启用 禁用

类型: IPv4 IPv6

策略配置

主动监视器: 已选择 ping, http 待选 ping6, connect_tcp, connect_udp, ftp, pop3, smtp, imap, tls1.0

虚拟IP有效条件: 至少 1 个监视器通过

繁忙保护: 启用 禁用

首选策略: 轮询 备选策略: 加权轮询

虚拟IP

虚拟IP列表 编辑虚拟IP

取消 完成

点击**编辑虚拟IP**，跳转到如下虚拟IP的设置页面：

虚拟IP			
+ 新建 X 删除 ⏪ 返回			
地址	权值	协议	
183.234.70.138:80	1	TCP	

点击地址列表中的虚拟IP **183.234.70.138:80**，可为每个虚拟IP单独设置监视器，如下图所示：

虚拟IP

编辑

普通属性

IP地址	183.234.70.138
端口	80
协议	TCP
权值	1

虚拟IP健康检查

监视器类型 继承 独立

8.4.2. 全局虚拟 IP 池

WEBUI：『智能 DNS』→『虚拟 IP 池』→『全局虚拟 IP 池』。

『全局虚拟 IP 池』用于分布式环境，在多个站点之间的 IP 和端口做智能 DNS 二级调度，各个站点的全局虚拟 IP 池配置会互相同步。

界面如下图所示：

本地虚拟IP池 全局虚拟IP池

新建

普通属性

名称 状态 启用 禁用

虚拟IP有效条件

主动监视器

已选监视器
无监视器时，将不关心链路状态

待选监视器
ping
connect_tcp
connect_udp
http
ftp
pop3
smtp
imap

关联虚拟服务

已选虚拟服务
无虚拟服务时，将不关心链路状态

待选虚拟服务
guangzhou
local
none
190.1.1.10
http
http1
http2
http3

关联虚拟服务全部在线时，虚拟IP有效

策略

繁忙保护 启用 禁用

首选策略：最佳资源调度

调度依据：维度 CPU 占用率，最大值，权重

当前已配置 0/4 个调度依据

备选策略：加权轮询

IP池

虚拟IP列表：地址，端口，协议（TCP），权值（1），添加

guangzhou/local

『全局虚拟 IP 池』中的具体配置步骤与『本地虚拟 IP 池』配置步骤一致。区别是：在『虚拟 IP 列表』右边框中可以看到其他站点发布的 IP 和端口并进行添加。

『繁忙保护』检测本地站点链路状态是否繁忙的同时，不同站点之间每 10S 会互相通报本站点的繁忙状态。当某站点的链路繁忙时，其他站点将这条链路的参与调度的 IP 和端口自动排除，不进行调度。

其他设置请参考 8.4.1 本地虚拟 IP 池。



集群部署环境下，不支持全局 DNS 负载功能，仅支持本地智能 DNS。

8.5. DNS 映射

WEBUI：『智能 DNS』 → 『DNS 映射』。

『DNS 映射』用于设置对客户端的域名请求进行智能 DNS 一级调度，将客户端访问调度到某个虚拟 IP 池，再对该虚拟 IP 池进行智能 DNS 二级调度。『DNS 映射』包含『本地 DNS 映射』和『全局 DNS 映射』。『本地 DNS 映射』用于单个站点，非分布式环境中；『全局 DNS 映射』用于多个站点，分布式环境中，并且各个站点的『全局 DNS 映射』配置可以相互同步。

8.5.1. 本地 DNS 映射

WEBUI：『智能 DNS』→『DNS 映射』→『本地 DNS 映射』。

『本地 DNS 映射』用于非分布式环境，只存在本地一个站点的情况下，对本地的 IP 和端口进行智能 DNS 一级调度。

界面如下图所示：



The screenshot shows the Sangfor WEBUI interface. On the left is the 'System Navigation Menu' with the following items: 系统概况, 报表配置, 公共对象, 数据中心, 应用负载, and 智能DNS. Under 智能DNS, there are several sub-items: DNS服务器, DNS记录, 虚拟IP池, DNS映射 (highlighted in yellow), LDNS集合, 静态就近性, and 全局配置还原. On the right is the 'Local DNS Mapping' configuration page. At the top, there are three tabs: 本地DNS映射 (selected), 全局DNS映射, and 规则测试. Below the tabs are four buttons: 新建 (New), 删除 (Delete), 启用 (Enable), and 禁用 (Disable). A table below these buttons has two columns: 名称 (Name) and IP类型 (IP Type). The table is currently empty.

启用按钮可以用于启用选中的 DNS 映射。

禁用按钮可以用于禁用选中的 DNS 映射。

删除按钮可以用于删除选中的 DNS 映射。

新建按钮可以用于新建 DNS 映射。

点击**新建**按钮，如下图所示：



『名称』用于定义 DNS 映射的名称。

『状态』用于配置该 DNS 映射的『启用』、『禁用』。

『类型』用于配置 IPv4 或 IPv6。

『域名列表』用于配置需要进行 DNS 映射的域名。

添加按钮用于添加需要进行 DNS 映射的域名到域名列表中。选中域名列表中的域名，点击删除，从列表中删除该域名。

『选择策略』用于配置 DNS 映射调度的策略，包括『静态就近性』、『轮询』、『加权轮询』。选择策略说明如下：

1、『静态就近性』调度算法在『智能 DNS』→『静态就近性』→『DNS 映射级别』中进行配置，根据所设置的 LDNS 集合来选择将客户端访问调度到某个虚拟 IP 池。详细配置参考 8.7 静态就近性；

2、『轮询』表示交替调度到不同虚拟 IP 池；

3、『加权轮询』表示通过设置中的『权重』加权计算结果并调度到某个虚拟 IP 池；

『会话保持』用于配置是否对客户端访问 DNS 映射域名返回的虚拟 IP 池做会话保持。在超时时间内，使相同来源的多次请求调度到相同的虚拟 IP 池。

『会话超时时间』用于配置会话保持方法的超时时间，单位为秒。

『TTL』用于配置通过 DNS 映射调度的域名记录在 Local DNS 的缓存时间，单位为秒。

『虚拟 IP 池列表』用于配置用于本地 DNS 映射调度的本地虚拟 IP 池。可选择列表中选定的本地虚拟 IP 池，点击  按钮将选定本地虚拟 IP 池添加至已选择列表，需要取消某本地虚拟 IP 池的调度则选中已选择列表中的虚拟 IP 池，点击  按钮即可。

8.5.2. 全局 DNS 映射

WEBUI：『智能 DNS』→『DNS 映射』→『全局 DNS 映射』。

『全局虚拟 IP 池』用于分布式环境，在多个站点之间的多个虚拟 IP 池中做智能 DNS 一级调度，各个站点的全局 DNS 映射配置会互相同步。

界面如下图所示：

全局DNS映射

新建

普通属性

名称:

状态: 启用 禁用

策略配置

域名列表:

选择策略: 静态就近性

延迟切换: 启用 禁用

延迟时间:

会话保持: 启用 禁用

会话超时时间: 300 秒

TTL: 60 秒

已选择列表 可选择列表

『全局 DNS 映射』中的具体配置步骤与『本地 DNS 映射』配置步骤一致。区别是：在『虚拟 IP 池列表』右边框中可以选择『全局虚拟 IP 池』中配置的虚拟 IP 池。



集群部署环境下，不支持全局 DNS 负载功能，仅支持本地智能 DNS。

8.6. LDNS 集合

WEBUI: 『智能 DNS』 → 『LDNS 集合』。

『LDNS 集合』用于定义各个区域 Local DNS 所在网段，用于静态就近性配置中进行调用。『LDNS 集合』包含『本地 LDNS 集合』和『全局 LDNS 集合』。『本地 LDNS 集合』

用于单个站点，非分布式环境中；『全局 LDNS 集合』用于多个站点，分布式环境中，并且各个站点的『全局 LDNS 集合』配置可以相互同步。

8.6.1. 本地 LDNS 集合

WEBUI：『智能 DNS』→『LDNS 集合』→『本地 LDNS 集合』。

『本地 LDNS 集合』用于在静态就近性中，配置范围选择『本地』时，在『LDNS 集合』项中进行调用。

界面如下图所示：



删除按钮可以用于删除选中的 LDNS 集合。

新建按钮可以用于新建 LDNS 集合。

点击**新建**按钮，如下图所示：



深信服，让IT更简单，更安全，更有价值

本地LDNS集合

全局LDNS集合

② 帮助信息

新建

属性

名称

(长度限制为1~63个字符，且不能包含& | " ' , : % < > / \ 特殊字

地圖集

教材类型

地圖範例

IP地址段

添加

第十一章

ANSWER

当前已配置0/10000个地址范围

删除

取消

完成

『名称』用于定义 LDNS 集合的名称。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

『地址类型』用于选择添加地址的类型，包含『IP 地址段』、『ISP 地址段』、『全球地址段』和『用户地域』。

当选择『IP 地址段』时，页面如下图：



『地址范围』填入要进行地址访问的『起始 IP』和『结束 IP』。

添加按钮用于添加地址段到地址列表中。选中地址列表中的地址段，点击**删除**，从列表中删除该地址段。

当选择『ISP 地址段』时，页面如下图：



『地址段』用于选择在『网络配置』→『IP 地址集合』→『ISP 地址段』中定义好的 ISP 地址段。

添加按钮用于添加 ISP 地址段中的地址到地址列表中。选中地址列表中的地址段，点击**删除**，从列表中删除该地址段。

当选择『全球地址段』时，页面如下图：



『地址段』用于选择在『网络配置』→『IP 地址集合』→『全球地址段』中定义好的某国家省市的地址段。

添加按钮用于添加全球地址段中的地址到地址列表中。选中地址列表中的地址段，点击**删除**，从列表中删除该地址段。

当选择『用户地域』时，页面如下图：



『地址段』用于选择在『网络配置』→『IP 地址集合』→『用户地域』中定义好的某地域的地址段。

添加按钮用于添加某地域地址段中的地址到地址列表中。选中地址列表中的地址段，

点击[删除](#)，从列表中删除该地址段。

8.6.2. 全局 LDNS 集合

WEBUI: 『智能 DNS』→『LDNS 集合』→『全局 LDNS 集合』。

『全局 LDNS 集合』用于在静态就近性中，配置范围选择『全局』时，在『LDNS 集合』项中进行调用。

界面如下图所示：



本地LDNS集合 全局LDNS集合 帮助信息

新建

属性

名称 (长度限制为1~63个字符，且不能包含& | " ' , : % < > / \ 特殊字符)

地址集

地址类型 IP地址段 添加

地址范围 -

当前已配置 0/10000个地址范围

删除

取消 完成

配置步骤请参考 8.6.1 本地 LDNS 集合。



集群部署环境下，不支持全局 DNS 负载功能，仅支持本地智能 DNS。

8.7. 静态就近性

WEBUI: 『智能 DNS』→『静态就近性』。

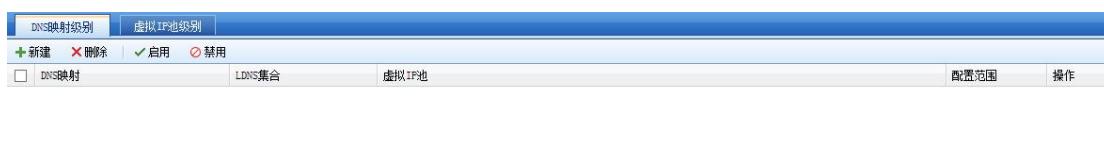
『静态就近性』用于定义调度算法，并在 DNS 映射和虚拟 IP 池中进行调用。

8.7.1. DNS 映射级别

WEBUI：『智能 DNS』→『静态就近性』→『DNS 映射级别』。

『DNS 映射级别』用于定义 DNS 映射中设置的静态就近性的调度策略。

界面如下图所示：



删除按钮可以用于删除选中的 DNS 映射。

新建按钮可以用于新建 DNS 映射。

启用按钮可以用于启用选中的 DNS 级别。

禁用按钮可以用于禁用选中的 DNS 级别。

点击**新建**按钮，如下图所示：



『状态』可以根据需要启用或者禁用 DNS 映射。

『配置范围』包含『本地』和『全局』。当选择『本地』时，该静态就近性就是选定的

『本地 DNS 映射』中的调度算法；当选择『全局』时，该静态就近性就是选定的『全局 DNS 映射』中的调度算法。

『DNS 映射』选择目标域名所在的 DNS 映射，当『配置范围』选择『本地』时，可选择『本地 DNS 映射』中设置的该域名的 DNS 映射，当『配置范围』选择『全局』时，可选择『全局 DNS 映射』中设置的该域名的 DNS 映射。

『LDNS 集合』选择客户端所在区域的 LDNS 集合。当『配置范围』选择『本地』时，可选择『本地 LDNS 集合』中设置的 LDNS 集合，当『配置范围』选择『全局』时，可选择『全局 LDNS 集合』中设置的该域名的 LDNS 集合。

『虚拟 IP 池』设定由『DNS 映射』和『LDNS 集合』联合匹配的策略调度结果，当客户端访问 DNS 映射中设置的域名且 Local DNS 属于 LDNS 集合定义的范围内时，返回指定 DNS 映射内配置的虚拟 IP 池。

取消按钮可以用于取消本次配置。

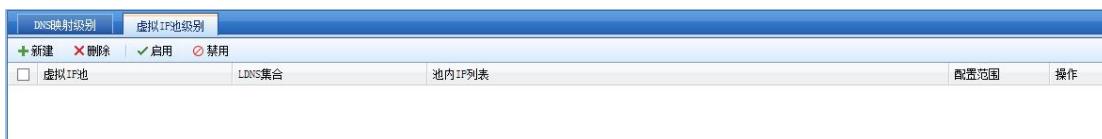
完成按钮可以用于完成本次配置。

8.7.2. 虚拟 IP 池级别

WEBUI：『智能 DNS』→『静态就近性』→『虚拟 IP 池级别』。

『虚拟 IP 池级别』用于定义虚拟 IP 池中设置的静态就近性的调度策略。

界面如下图所示：



删除按钮可以用于删除选中的虚拟 IP 池级别。

新建按钮可以用于新建虚拟 IP 池级别。

【启用】按钮可以用于启用选中的虚拟IP池级别。

【禁用】按钮可以用于禁用选中的虚拟IP池级别。

点击【新建】按钮，如下图所示：



『配置范围』包含『本地』和『全局』。当选择『本地』时，该静态就近性就是选定的『本地虚拟IP池』中的调度算法；当选择『全局』时，该静态就近性就是选定的『全局虚拟IP池』中的调度算法。

『状态』可以根据需要启用或者禁用虚拟IP池级别。

『虚拟IP池』选择需要做调度的虚拟IP池，当『配置范围』选择『本地』时，可选择『本地虚拟IP池』中设置的该域名的虚拟IP池，当『配置范围』选择『全局』时，可选择『全局虚拟IP池』中设置的该域名的虚拟IP池。

『LDNS集合』选择客户端所在区域的LDNS集合。当『配置范围』选择『本地』时，可选择『本地LDNS集合』中设置的LDNS集合，当『配置范围』选择『全局』时，可选择『全局LDNS集合』中设置的该域名的LDNS集合。

『池内IP』设定由『虚拟IP池』和『LDNS集合』联合匹配的策略调度结果。可选择列表为指定虚拟IP池内配置的IP地址，点击【<】按钮将选定的IP地址添加至已选择列表，

则当访问匹配同时匹配到设定的『虚拟 IP 池』和『LDNS 集合』时，调度到该 IP，需要取消该 IP 的调度则选中已选择列表中的 IP 地址，点击  按钮即可。

 取消按钮可以用于取消本次配置。

 完成按钮可以用于完成本次配置。

8.8. 全局配置还原

8.8.1. 配置还原

WEBUI：『智能 DNS』 → 『全局配置还原』 → 『配置还原』。

界面如下图所示：



时间点：记录了创建还原点的时间。

描述：对当前还原点的内容用途等描述信息(系统还原点不可编辑)。

备份配置：显示了当前还原点的备份内容，由当前还原点创建时的“同步配置”决定。可以选择『智能 DNS』和『用户管理』两部分。

8.8.2. 同步配置

WEBUI：『智能 DNS』→『全局配置还原』→『同步配置』。

界面如下图所示：



同步选项：设置参与全局配置同步和配置还原的项目。

智能 DNS 包含[全局 DNS 记录]、[全局虚拟 IP 池]、[全局 DNS 映射]、[全局 LDNS 集合]以及[静态就近性]全局部分的配置信息。

用户管理 包含[用户]和[角色]的配置信息。

第9章 路由配置

『路由配置』用于配置设备的路由信息，让AD能够满足多种网络环境的部署，包括『智能路由』、『静态路由』、『虚拟IP路由』、『IP-Anycast』、『RIP』、『OSPF』和『OSPFv3』几个部分。

9.1. 智能路由

WEBUI：『路由配置』→『智能路由』。

SANGFOR AD 提供的『智能路由』功能，主要用于具有多条 WAN 口线路时，根据源/目的 IPv4 地址、链路选择策略等条件，设定基于某些策略的路由，以确定数据从哪个 WAN 口转发，实现手动选路功能，达到对多链路实现流量分隔，优化带宽的目的。

界面如下图所示：



9.1.1. 智能路由

『智能路由』下显示智能路由的『源 IP』、『目的 IP』、『协议』、『使用链路』、『生效时间』和『操作』，包括系统默认智能路由和自定义智能路由。

界面如下图所示：

The screenshot shows the Sangfor Cloud Intelligent Routing configuration page. At the top, there are tabs for '智能路由' (Intelligent Routing), '出站高级配置' (Advanced Outbound Configuration), and '路由测试' (Route Testing). Below the tabs is a toolbar with buttons for '+新建' (New), '删除' (Delete), '启用' (Enable), '禁用' (Disable), '导入' (Import), '导出' (Export), and '配置向导' (Configuration Wizard). A table lists four configured routes:

名称	源IP	目的IP	协议	使用链路	生效时间	操作
电信	所有	电信	ALL	WAN1	全天	
联通	所有	联通(原网通)	ALL	WAN_GFAD	全天	
教育	所有	教育网	ALL	教育	全天	
Default	所有	所有	ALL	WAN1, WAN_GFAD, 教育	全天	

At the bottom, there are navigation buttons for '第 1 页, 共1页' (Page 1, 1 page), a '每页显示条数' (Items per page) dropdown set to 20, and a '共4/100条配置信息' (Total 4/100 configuration items) status bar.

启用按钮可以用于启用智能路由。

禁用按钮可以用于禁用智能路由，但不能禁用默认智能路由。

删除按钮可以用于删除智能路由，但不能删除默认智能路由。

配置向导可以链接到『配置向导』→『智能路由向导』页面。

导入按钮可以用于导入智能路由，所导入智能路由文件为在『智能路由列表』中导出的文件，点击**导入**如下图所示：



点击**浏览**可以选择本地备份的智能路由文件，点击导入可将备份的智能路由文件导入

到设备。点击**取消**，取消本次导入配置。

导出按钮可以用于备份自定义的智能路由。点击**导出**按钮，如下图：



点击**保存**，可将智能路由保存到本地PC。

新建按钮可以用于新建智能路由。点击**新建**，配置界面如下：

『名称』用于定义智能路由名称，建议使用便于标识的文字。

『状态』用于设置智能路由的状态，包括[启用]和[禁用]。

『插入位置』将该条智能路由插放的位置，默认情况下为用户配置的最后一条。

『源 IP 地址』用于设置匹配此条智能路由的源 IP 地址。可以是单个 IP、IP 范围、子网或者是用户地址集中定义的 IP 段。

『目的 IP 地址』用于设置匹配此条智能路由的目标 IP 地址。可以是单个 IP、IP 范围、子网、ISP 地址段或者是域名。

『TOS』 区分应用层流量，提供给智能路由选择不同链路。支持应用引流，应用识别智能选路。

『协议条件』用于设置匹配此条智能路由的协议，包括[所有协议]和[指定类型]，[指定类型]包括 TCP、UDP、ICMP、其他，选择[指定类型]可以自定义端口号或协议号。

『使用链路范围』用于设置匹配此条智能路由时所选择的外网链路。

『生效时间』用于设置此条智能路由生效的时间，在生效时间以外，则智能路由不生效。

『链路选择策略』用于设置匹配此条智能路由、并且使用链路范围为两个或两个以上时，采用的选路策略，包括[轮询]、[带宽比例]、[加权最小流量]、[动态就近性]。

『链路繁忙保护』用于设置匹配此条智能路由时，选路是否受链路繁忙状态影响，开启时，如果某条链路处于繁忙状态，则不选择这条链路；如果该规则所有链路都繁忙，则链路调度失败。

『链路调度失败的默认动作』用于设置匹配此条智能路由时，链路调度失败采取的动作，建议选择匹配下一条规则。

点击**完成**，完成此智能路由的配置。

点击**取消**，用于取消此智能路由的配置。

9.1.2. 出站高级配置

『出站高级配置』可以设置出站数据控制的高级属性。

界面如下图所示：



『子网掩码』通过此子网掩码对属于同一网络号的不同外网 IP 的访问进行同一个会话保持。

『TCP 探测方法』表示当智能路由中的链路选择策略是[动态就近性]时，基于 TCP 协议的出站请求某一个目的地址，设备向该目的地址发送 TCP SYN 进行探测。

『其他协议探测方法』除了 TCP 类型请求外，基于其他协议的请求，使用此探测方法。

『缓存子网掩码』通过此子网掩码对属于同一网络号的不同外网 IP 使用同一个动态就近性选择出的链路。

『缓存默认超时时间』用于设置动态就近性往返延时缓存的超时时间。

9.1.3. 路由测试

『路由测试』可以用来进行智能路由测试。

界面如下图所示：



The screenshot shows the 'Route Test' configuration page. At the top, there are three tabs: 'Intelligent Routing' (智能路由), 'Outbound Advanced Configuration' (出站高级配置), and 'Route Test' (路由测试). The 'Route Test' tab is selected. Below the tabs, the title 'Route Test Configuration' (路由测试配置) is displayed. The configuration fields include:

- Source IP Address (源IP地址): An input field.
- Destination IP Address (目的IP地址): An input field.
- Protocol (协议): A dropdown menu set to 'TCP'.
- TOS (TOS): An input field containing '0'.
- Port (端口): Two input fields for source and destination ports.

At the bottom of the configuration area are two buttons: 'Test' (测试) and 'Recent Test Results' (最近一次测试结果).

『源 IP 地址』要进行路由测试的源 IPv4 地址，当协议为 TCP/UDP 时需要端口号。

『目的 IP 地址』要进行路由测试的源 IPv4 地址，当协议为 TCP/UDP 时需要端口号。

『协议』选择将要测试的协议，若列表中不存在请选择“其他”并填写协议号。

『TOS』区分应用层流量，提供给智能路由选择不同链路。支持应用引流，应用识别智能选路。

点击测试，将按照设置进行路由测试，如下图所示：

The screenshot shows the 'Route Test' configuration page. In the 'Route Test Configuration' section, the source IP is 192.200.200.14, destination IP is 202.96.134.133, protocol is TCP, and TOS is 0. The test result table shows one step: '目的地址为直连网络，将直接转发。' (The destination address is a direct connection network, it will be forwarded directly). Buttons for 'Test' and 'Recent Test Result' are at the bottom.

点击[最近一次测试结果](#)，可以查看最近一次的路由测试结果，以及最近一次测试的时间，如下图所示：

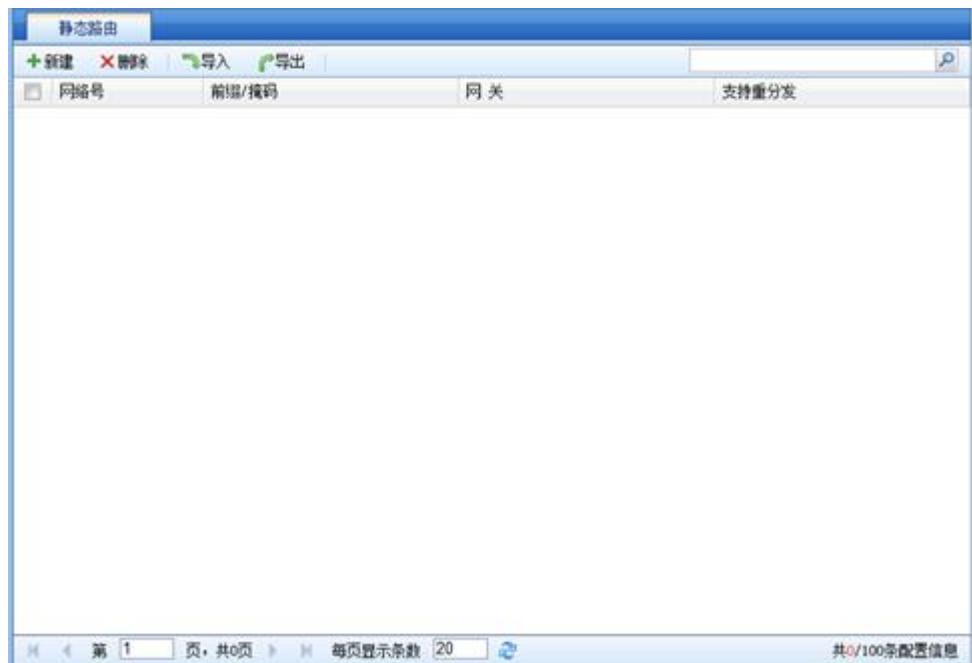
The screenshot shows the 'Route Test' configuration page with the same parameters as before. Below the configuration, a 'Recent Test Result' section is expanded, showing the date (2016-01-25 19:44:40) and the same test result: '目的地址为直连网络，将直接转发。'. Buttons for 'Test' and 'Recent Test Result' are at the bottom.

9.2. 静态路由

WEBUI 路径：『路由配置』→『静态路由』。

『静态路由』用于指定静态路由，一般用于设置到达非 AD 设备直连网段的路由。

界面如下图所示：



『静态路由』用于显示已经设置完成的路由信息。

点击 **删除**，用于删除选中的静态路由。

点击 **新建**，用于新建静态路由，弹出界面如下图所示：



『网络号』用于设置需要到达的目标网段。

『子网掩码』用于设置目标网段的子网掩码。

『网关』用于设置到达目标网段的下一跳IP地址。

『支持重分发』用于设置是否允许将此条静态路由条目通过动态路由协议分发出去。当目标网段为IPv6时，此项目不可配置。

点击**完成**，完成此静态路由的配置。

点击**取消**，用于取消此静态路由的配置。

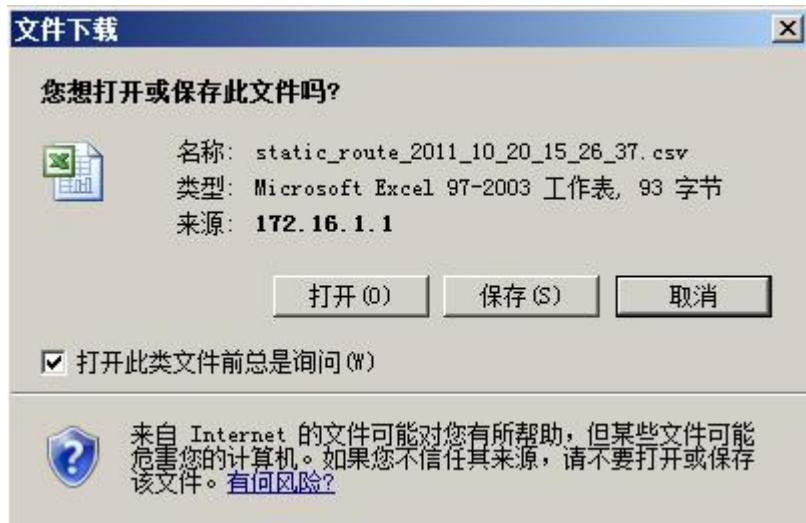
导入按钮可以用于导入静态路由，所导入静态路由文件为在『静态路由列表』中导出的文件或者自定义的文件，点击**导入**如下图所示：



点击**浏览**可以选择本地备份的静态路由文件或者自定义的文件，点击**导入**可将文件导入到设备。点击**取消**，取消本次导入配置。

点击“静态路由CSV模板下载”即可下载默认模板手动编辑静态路由。

导出按钮可以用于备份自定义的静态路由。点击**导出**按钮，如下图：



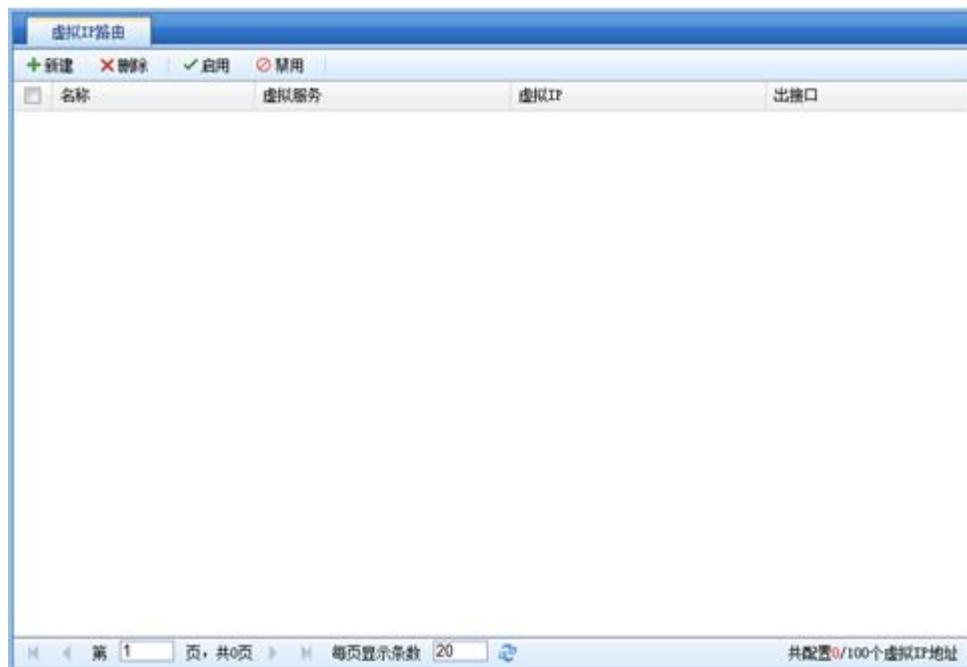
点击 保存，可将静态路由文件保存到本地 PC。

9.3. 虚拟 IP 路由

『虚拟 IP 路由』用于强制指定虚拟服务发布 IP 的出接口。当公网访问虚拟服务的某个发布 IP 的时候，可以匹配虚拟 IP 路由，强制走某条线路。例如客户有两条线路，电信 IP 为 A 和网通 IP 为 B，发布了虚拟服务 IP 组为 A 和 B，那么可以设置虚拟 IP 路由，公网访问 A 的时候强制走电信线路回包，公网访问 B 的时候强制走网通线路回包。

WEBUI 路径：『路由配置』→『虚拟 IP 路由』。

界面如下图所示：



点击**启用**，用于启用选中的虚拟IP路由。

点击**禁用**，用于禁用选中的虚拟IP路由。

点击**删除**，用于删除选中的虚拟IP路由。

点击**新建**，用于新建虚拟IP路由，设置界面如下：



『名称』可以输入便于记忆和识别的字符串，用于标识虚拟 IP 路由。

『状态』启用，该条虚拟 IP 路由配置生效；禁用，则虚拟 IP 路由失效。

『虚拟服务』用于配置一个虚拟服务，并列出虚拟服务的发布 IP，效果如下：

『虚拟 IP』用于配置虚拟 IP 选择列表，使该条虚拟 IP 路由应用于这些虚拟 IP。

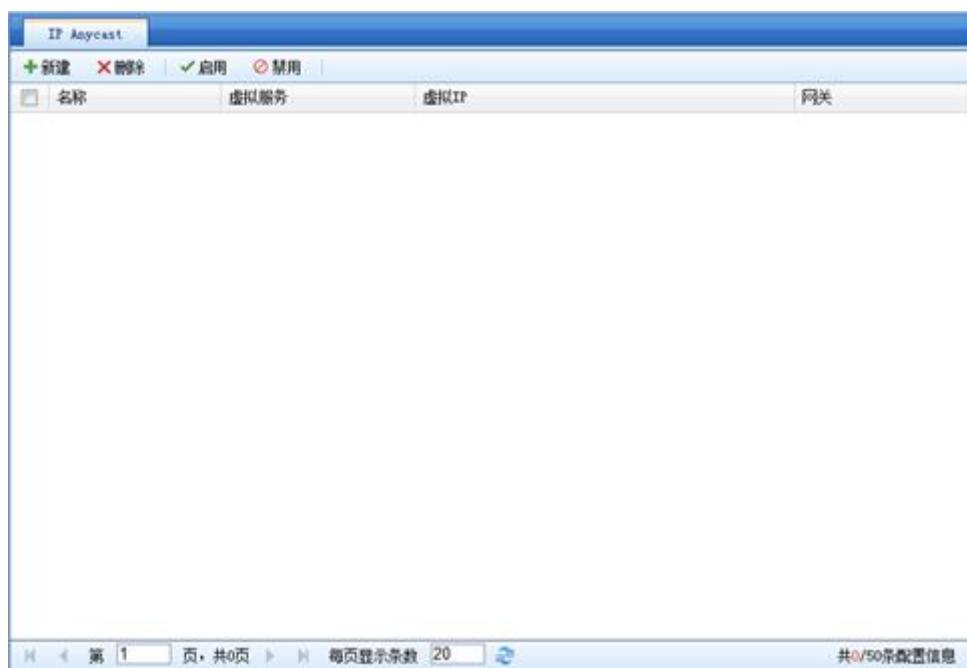
『出接口』用于设置上述选择的虚拟 IP 的出接口。

9.4. IP-Anycast

『IP-Anycast』用于配置全局发布的虚拟服务，以及相应的动态路由网关，是实现多个数据中心负载的一种方式。

WEBUI 路径：『路由配置』→『IP-Anycast』。

界面如下图所示：



点击**启用**，用于启用选中的 IP-Anycast 条目。

点击**禁用**，用于禁用选中的 IP-Anycast 条目。

点击**删除**，用于删除选中的 IP-Anycast 条目。

点击**新建**，用于新建 IP-Anycast 条目，设置界面如下：



『名称』可以输入便于记忆和识别的字符串，用于标识 IP-Anycast 条目。

『状态』启用，该条 IP-Anycast 配置生效；禁用，则 IP-Anycast 失效。

『虚拟服务』用于配置一个虚拟服务，并列出虚拟服务的发布 IP。

『虚拟 IP』用于配置虚拟 IP 选择列表，使该条 IP-Anycast 应用于这些虚拟 IP。

『网关』用于设置上述选择的虚拟 IP 的下一跳 IP 地址。

9.5. RIP

『RIP』用于配置 AD 设备需要通过 RIP 路由协议宣告的网络。用于支持将 AD 部署在使用 RIP 路由协议的环境中。

WEBUI 路径：『路由配置』→『RIP』。

界面如下图所示：



9.5.1. 全局配置

『全局配置』用于设置需要通过 RIP 协议宣告的网络以及是否支持使用 RIP 协议将其他路由协议学习到的路由条目广播出去。

WEBUI 路径：『网络配置』→『RIP』→『全局配置』。

界面如下图所示：

The screenshot shows the 'Global Configuration' tab selected in the header. Under 'Basic Configuration', the 'RIP Status' is set to '禁用' (Disabled). In the 'Route Redistribution Configuration' section, 'Default Route强制重分发' and 'OSPF Route重分发' are both set to '禁用' (Disabled), while 'Static Route重分发' is set to '启用' (Enabled). The 'Running Network Segment' section allows configuration of IP address and subnet mask for a specific segment, with '添加' (Add) and '删除' (Delete) buttons available for managing multiple entries. A note at the bottom indicates 0/16 segments are currently configured.

『RIP 状态』用于启用或者是禁用设备运行 RIP 路由协议。

『默认路由强制重分发』用于设置是否允许 RIP 协议将默认路由广播出去，让相邻的路由器把默认路由指向 AD 设备。

『静态路由重分发』用于设置是否允许 RIP 协议将设备上配置的静态路由广播出去。

『OSPF 路由重分发』用于设置是否允许 RIP 协议将设备学习到的 OSPF 路由信息广播出去。

『运行网段』用于配置需要通过 RIP 协议宣告给对方的网段，输入『IP 地址』和『掩码』，点击**添加**按钮即可。

9.5.2. 接口配置

『接口配置』用于设置运行 RIP 协议的接口所使用的 RIP 协议版本。默认情况下，宣告网络中若包含了接口所在的网络，则该接口就会运行 RIP V2，且不需要认证。

WEBUI 路径：『网络配置』→『RIP』→『接口配置』。

界面如下图所示：



点击**新建**，用于设置运行 RIP 协议接口的 RIP 版本信息，配置界面如下：



『网络接口』用于选择需要设置版本信息的接口。

『RIP 版本』用于选择该接口上运行的 RIP 协议的版本，支持 V1 和 V2 版本。

『认证类型』用于设置 RIP V2 的认证方式。认证类型可以选择无认证、明文认证或者是 MD5 认证。如果选择明文认证，需要填写认证码；如果选择 MD5 认证，则需要填写认证 KeyID 和认证码。

9.6. OSPF

『OSPF』用于配置 AD 设备需要通过 OSPF 路由协议宣告的网络。用于支持将 AD 部署在使用 OSPF 路由协议的环境中。

WEBUI 路径：『路由配置』→『OSPF』。

界面如下图所示：



9.6.1. 全局配置

『全局配置』用于设置需要通过 OSPF 协议宣告的网络以及是否支持使用 OSPF 协议将其他路由协议学习到的路由条目广播出去。

WEBUI 路径：『网络配置』→『OSPF』→『全局配置』。

界面如下图所示：

全局配置 | 接口配置 | 邻居关系表

全局配置

基本配置

路由器ID

OSPF状态 启用 禁用

路由重分发配置

默认路由强制重分发 启用 禁用

静态路由重分发 启用 禁用

RIP路由重分发 启用 禁用

Metric-type Type-1 Type-2

Metric-value

区域配置

区域ID

接受自治系统外部路由 启用 禁用

运行网段

运行网段 IP地址:

掩码/前缀:

『路由器 ID』填写用户便于记忆的信息，用于标识该路由器的身份。填写形式为数字形式（1-4294967295）或者是点分十进制形式。

『OSPF 状态』用于启用或者是禁用设备运行 OSPF 路由协议。

『默认路由强制重分发』用于设置是否允许 OSPF 协议将默认路由广播出去，让相邻的路由器把默认路由指向 AD 设备。

『静态路由重分发』用于设置是否允许 OSPF 协议将设备上配置的静态路由广播出去。

『RIP 路由重分发』用于设置是否允许 OSPF 协议将设备学习到的 RIP 路由信息广播出去。

『Metric-type』用于设置 OSPF 计算路径开销的类型。

『Metric-value』用于设置 OSPF 的链路度量值。

『区域 ID』用于设置该路由器所在的区域标识。

『接受自治系统外部路由』用于设置设备是否接收自治系统外部链路状态通告。若『启用』了该选项，则当邻居路由器的路由条目发生了变化，此路由器会接收邻居路由器的链路状态通告；若『禁用』了该选项，则此路由器不会接收邻居路由器的链路状态通告。

『运行网段』用于配置需要通过 OSPF 协议宣告给对方的网段，输入『IP 地址』和『掩码/前缀』，点击**添加**按钮即可。

9.6.2. 接口配置

『接口配置』用于设置运行 OSPF 协议的接口信息。

WEBUI 路径：『网络配置』→『OSPF』→『接口配置』。

界面如下图所示：

全局配置				接口配置				邻居关系表			
+ 新建		- 删除									
<input type="checkbox"/>	优先级	<input type="text"/>	Hello间隔(秒)	<input type="text"/>	失效时间(秒)	<input type="text"/>	代价值	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

点击**新建**，用于设置运行 OSPF 协议接口的接口信息，配置界面如下：

全局配置 接口配置 邻居关系表

新建

基本配置

网络接口

时间配置

Hello间隔 秒
重传间隔 秒
失效间隔 秒

认证配置

认证类型

属性配置

优先级
链路代价
网络类型

『网络接口』选择需要设置 OSPF 协议接口信息的接口。

『Hello 间隔』发送方路由器连续两次发送 hello 数据包之间的时间间隔。

『重传间隔』发送方路由器重传链路状态通告数据包的时间间隔。

『失效间隔』用于设置发送方路由器在多长时间内未收到对方发来的 hello 包，就拒绝与对方形成邻居关系。

『认证类型』用于设置 OSPF 的认证方式。认证类型可以选择无认证、明文认证或者是 MD5 认证。如果选择明文认证，需要填写认证码；如果选择 MD5 认证，则需要填写认证 KeyID 和认证码。

『优先级』用于设置运行 OSPF 协议接口的接口优先级，该接口优先级用于 DR/BDR 的选举过程。填写的数字越大，其接口优先级越高。

『链路代价』用于设置当前接口的链路开销。填写的数字越大，其链路开销越高。

『网络类型』用于设置当前接口的网络类型。

9.6.3. 邻居关系表

『邻居关系表』用于查看哪些路由器与 AD 设备形成了邻居关系。

WEBUI 路径：『网络配置』→『OSPF』→『邻居关系表』。

界面如下图所示：

邻居关系表					
刷新时间间隔: 5秒					
邻居路由表ID	优先级	邻接状态	超时时间	邻居邻接IP	邻接网口
192.200.200.22	1	Full/Backup	38.730s	192.200.200.22	eth2:192.200.200.171

『邻居路由器 ID』显示邻居路由器的路由器 ID。

『优先级』显示邻居路由器接口的接口优先级。

『邻接状态』显示邻居路由器与 AD 设备之间形成的邻居状态。

『超时时间』显示邻居路由器与 AD 设备之间的失效时间剩余值。该超时时间会从 40s 开始倒计时，收到邻居发来的数据包后更新，收不到就一直递减，直到减为 0 后，将删除邻居关系。

『邻居邻接 IP』显示与 AD 设备直连的邻居路由器的接口 IP 地址。

『邻接网口』显示与邻居路由器直连的 AD 设备的接口及接口 IP 地址。

9.7. OSPFV3

『OSPFV3』用于配置 AD 设备需要通过 OSPFV3 路由协议宣告的网络。用于支持将 AD 部署在使用 OSPFV3 路由协议的环境中。

WEBUI 路径：『路由配置』→『OSPFV3』。

界面如下图所示：



全局配置

基本配置

路由器ID:

OSPFV3状态: 启用 禁用

路由重分发配置

静态路由重分发: 启用 禁用

直连路由重分发: 启用 禁用

区域间路由汇聚

区域间路由汇聚: 区域ID:
汇聚IPv6前缀/掩码:

当前已配置0/16个路由汇聚

9.7.1. 全局配置

『全局配置』用于设置需要通过 OSPFV3 协议宣告的网络以及是否支持使用 OSPFV3 协议将其他路由协议学习到的路由条目广播出去。

WEBUI 路径：『网络配置』→『OSPFV3』→『全局配置』。

界面如下图所示：

全局配置 接口配置 邻居关系表

全局配置

基本配置

路由器ID

OSPFV3状态 启用 禁用

路由重分发配置

静态路由重分发 启用 禁用

直连路由重分发 启用 禁用

区域间路由汇聚

区域间路由汇聚 区域ID

汇聚IPv6前缀/掩码：

当前已配置0/16个路由汇聚

『路由器 ID』填写用户便于记忆的信息，用于标识该路由器的身份。填写形式为数字形式（1-4294967295）或者是点分十进制形式。

『OSPFV3 状态』用于启用或者是禁用设备运行 OSPFV3 路由协议。

『默认路由强制重分发』用于设置是否允许 OSPFV3 协议将默认路由广播出去，让相邻的路由器把默认路由指向 AD 设备。

『静态路由重分发』用于设置是否允许 OSPFV3 协议将设备上配置的静态路由广播出去。

『RIP 路由重分发』用于设置是否允许 OSPFV3 协议将设备学习到的 RIP 路由信息广播出去。

『Metric-type』用于设置 OSPFV3 计算路径开销的类型。

『Metric-value』用于设置 OSPFV3 的链路度量值。

『区域 ID』用于设置该路由器所在的区域标识。

『接受自治系统外部路由』用于设置设备是否接收自治系统外部链路状态通告。若『启用』了该选项，则当邻居路由器的路由条目发生了变化，此路由器会接收邻居路由器的链路状态通告；若『禁用』了该选项，则此路由器不会接收邻居路由器的链路状态通告。

『运行网段』用于配置需要通过 OSPF 协议宣告给对方的网段，输入『IP 地址』和『掩码/前缀』，点击**添加**按钮即可。

9.7.2. 接口配置

『接口配置』用于设置运行 OSPFV3 协议的接口信息。

WEBUI 路径：『网络配置』→『OSPFV3』→『接口配置』。

界面如下图所示：



全局配置			
接口配置			
邻居关系表			
+ 新建 - 删除			
□	优先级	Hello间隔 (秒)	失效时间 (秒)
代价值			

点击**新建**，用于设置运行 OSPFV3 协议接口的接口信息，配置界面如下：

全局配置 接口配置 邻居关系表

新建

基本配置

网络接口

时间配置

Hello间隔	10	秒
重传间隔	5	秒
失效间隔	40	秒
传输延迟	1	秒

属性配置

优先级	1
链路代价	10
instance-id	0
区域	

『网络接口』选择需要设置 OSPFV3 协议接口信息的接口。

『Hello 间隔』发送方路由器连续两次发送 hello 数据包之间的时间间隔。

『重传间隔』发送方路由器重传链路状态通告数据包的时间间隔。

『失效间隔』用于设置发送方路由器在多长时间内未收到对方发来的 hello 包，就拒绝与对方形成邻居关系。

『传输延迟』由于 LSA 在本路由器的链路状态数据库 LSDB 中会随时间老化，但在网络的传输过程中却不会，所以有必要在发送之前将 LSA 的老化时间增加一定的延迟时间。

『优先级』用于设置运行 OSPF 协议接口的接口优先级，该接口优先级用于 DR/BDR 的选举过程。填写的数字越大，其接口优先级越高。

『链路代价』用于设置当前接口的链路开销。填写的数字越大，其链路开销越高。

『instance-id』接口实例 id，两端接口实例 id 必须相同，邻居关系才能协商成功。

『区域』网口所属 OSPFv3 区域 id。

9.7.3. 邻居关系表

『邻居关系表』用于查看哪些路由器与 AD 设备形成了邻居关系。

WEBUI 路径：『网络配置』→『OSPFV3』→『邻居关系表』。

界面如下图所示：

全局配置	接口配置	邻居关系表		
刷新时间间隔：5秒				
邻居路由表ID	优先级	邻接状态	超时时间	邻接网口
邻居关系表为空				

『邻居路由器 ID』显示邻居路由器的路由器 ID。

『优先级』显示邻居路由器接口的接口优先级。

『邻接状态』显示邻居路由器与 AD 设备之间形成的邻居状态。

『超时时间』显示邻居路由器与 AD 设备之间的失效时间剩余值。该超时时间会从 40s 开始倒计时，收到邻居发来的数据包后更新，收不到就一直递减，直到减为 0 后，将删除邻居关系。

『邻居邻接 IP』显示与 AD 设备直连的邻居路由器的接口 IP 地址。

『邻接网口』显示与邻居路由器直连的 AD 设备的接口及接口 IP 地址。

第 10 章 网络配置

『网络配置』用于设置 AD 设备的网络相关配置，包括『网络接口』、『链路监视器』、『源地址转换』、『端口映射』、『DNS 代理』、『网络安全』和『ACL 配置』七个部分。

界面如下图所示：



10.1. 网络接口

要通过 MANAGE 口之外的接口接入 SANGFOR AD 设备，必须先使用 MANAGE 口进行网络接口的配置。MANAGE 口的初始 IP 为 10.252.252.252/24 或者是 10.254.254.254/24。

WEBUI 路径：『网络配置』→『网络接口』。



10.1.1. 网络接口

『网络接口』用于设置AD设备的网络接口，并且定义网络接口的类别。

界面如下图所示：



『网口连接实时状态』用于显示已经接上网线并处于正常工作的网口的状态，其中连接



启用 用于启用选中的网络接口。

禁用 用于禁用选中的网络接口。

删除 用于删除选中的已定义完成的网络接口。

点击**新建**，弹出『网络接口』的选择页面，用于新建网络接口。弹出界面如下图所示：



『选择类别』用于选择新建网络接口的类型，包括内网接口 LAN 和外网接口 WAN。

第一步：『选择类别』，选择[LAN]用于定义一个内网接口，选择[WAN]用于定义一个外网接口，勾选所需的接口类别，点击**下一步**，进入下一步的配置。

点击**取消**，用于退出配置。

10.1.1.1. LAN

如果『选择类别』选择的是内网接口 LAN，如下图所示：



点击**下一步**后，弹出『网络接口』的详细配置页面。

弹出界面如下图所示：

网络接口 | 交换网口 | 端口聚合 | VLAN子接口 | 接口模式

新建LAN口

属性

名称:
网络接口: -请选择网络接口-
类别: LAN
状态: 启用 禁用

网络地址配置

地址列表 起始IP:
结束IP:
掩码/前缀: 添加 删除

当前已配置 0 / 512 个地址

健康检查

健康状态: 启用 禁用
插拔网线检测: 启用 禁用
ARP检查: 启用 禁用

取消 完成

『名称』 网络接口的名称。

『网络接口』 配置网络接口时可供选择的网口。

『类别』 用来显示新建网络接口的类型，现在是 LAN。

『状态』 启用，网络接口的所有配置生效；禁用，网络接口的所有配置失效且无法使用。

『地址列表』 定义网络接口绑定的 IP 地址，支持 IPV4 和 IPV6 地址混配。

『健康检查』 用来开启或禁用 LAN 口的健康状态监测，仅支持 IPV4 地址。

[插拔网线检测]开启，通过检测 LAN 口的插拔网线情况来判断 LAN 口的健康状态。

[ARP 检查]开启，通过获取监视 IP 的 ARP 地址来判断 LAN 口的健康状态。



点击**完成**，设置 LAN 口完成。

点击**取消**，用于取消此接口的配置。

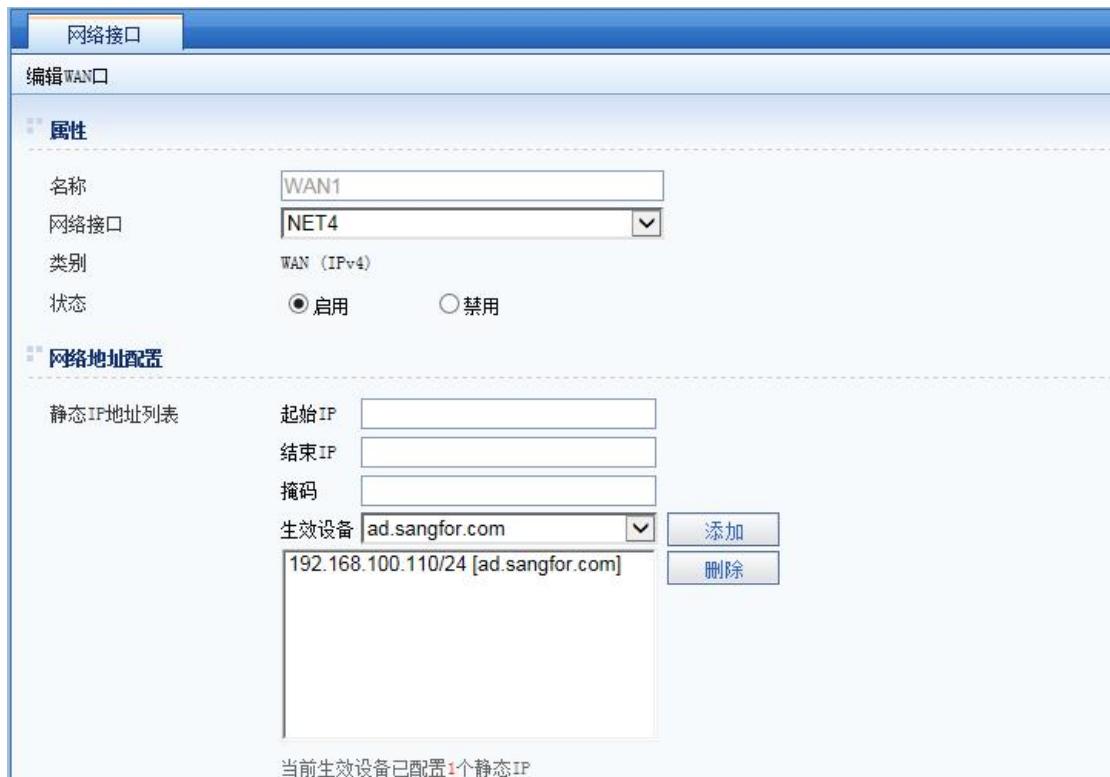
10.1.1.2. WAN

如果『选择类别』选择的是外网接口 WAN，如下图所示：



点击**下一步**后，弹出『网络接口』的详细配置页面。

弹出界面如下图所示：



『名称』 网络接口的名称。

『网络接口』 配置网络接口时可供选择的网口。

『类别』 用来显示新建网络接口的类型，现在是 WAN。

『状态』 启用，网络接口的所有配置生效；禁用，网络接口的所有配置失效且无法使用。

『地址列表』 输入『起始 IP』、『结束 IP』和『掩码/前缀』，点击添加按钮即可，您可以添加多个不同的 IP，或者是一个 IP 段，但是添加的 IP 必须是一个可以实际分配给网卡使用的 IP。

『网关』 用于设置此接口的网关 IP 地址。

『对应互联网 IP』 当公网 IP 配置在 AD 设备上，对应互联网 IP 就不用填写；当公网 IP 不在 AD 设备上，对应互联网 IP 需填写，且互联网 IP 地址与网口 IP 地址必须一一对应。



『线路带宽』配置网络接口的真实带宽，可实现带宽管理和带宽控制，若链路流量超过指定带宽的繁忙百分比，则判断该链路处于繁忙状态。

『上行带宽』、『下行带宽』用于设置公网线路真实的上下行带宽，单位可选择 Kbps 和 Mbps，此处的设置在带宽控制以及链路负载中使用。

『上行带宽繁忙比例』、『下行带宽繁忙比例』用于设置当使用带宽达到总带宽的 $\%$ 时，线路状态标识为“繁忙”。



- 1、线路状态可以在『系统概况』→『链路状态』→『所有链路状态』中查看。
- 2、每种接口 IP 设置支持最多 512 个 IP 地址。
- 3、IPv4 地址和 IPv6 地址可以混合配置于同一个网络接口。

『健康检查』用于监视链路的活动状态，设置包括『网关 ARP 检查』、『有效监视器』、『监视主机』、『插拔网线检测』等部分。点击启用后，默认界面如下图所示：

健康检查

监视器状态 启用 禁用

网关ARP检查 启用 禁用

有效监视器

监视主机

插拔网线检测 启用 禁用



『启用』可以用来启用健康检查。

『禁用』可以用来禁用健康检查。

『网关 ARP 检查』开启网关 ARP 检查，通过检测接口的网关 IP 对应的 ARP 地址来判断线路的健康状态，如果不能获取到网关的 ARP 地址，则认为线路故障。

『有效监视器』可以选择需要启用的监视器。

『监视主机』可以输入需要监视的主机。可以添加 IP 也可以添加域名。

『插拔网线检测』用于设置是否检测网口的接线状态，没接线就判断为线路故障。选择[启用]则开启插拔网线检测功能，选择[禁用]则禁用插拔网线检测功能。



『浮动 IP 地址列表』高可用集群模式下，多台设备共享的 IP 地址，浮动 IP 在哪台设备上生效，取决于其所属应用组在哪台设备上生效。

浮动IP地址列表

起始IP	<input type="text"/>								
结束IP	<input type="text"/>								
掩码/前缀	<input type="text"/>								
<table border="1"><tr><td>192.168.100.11/24</td></tr><tr><td>192.168.100.12/24</td></tr><tr><td>192.168.100.13/24</td></tr><tr><td>192.168.100.14/24</td></tr><tr><td>192.168.100.15/24</td></tr><tr><td>192.168.100.16/24</td></tr><tr><td>192.168.100.17/24</td></tr><tr><td>192.168.100.18/24</td></tr></table>		192.168.100.11/24	192.168.100.12/24	192.168.100.13/24	192.168.100.14/24	192.168.100.15/24	192.168.100.16/24	192.168.100.17/24	192.168.100.18/24
192.168.100.11/24									
192.168.100.12/24									
192.168.100.13/24									
192.168.100.14/24									
192.168.100.15/24									
192.168.100.16/24									
192.168.100.17/24									
192.168.100.18/24									
<input type="button" value="添加"/> <input type="button" value="删除"/>									

当前已配置 11/512个地址，其中静态IP为1个，浮动IP为10个。

网关

对应互联网IP

起始IP:	<input type="text"/>
结束IP:	<input type="text"/>
<input type="button" value="添加"/> <input type="button" value="删除"/>	

当前已配置 0/512个地址



修改网络接口配置（线路带宽，繁忙比例，网关，健康检查，互联网 IP，调整已有 IP 顺序），动态路由进程不重启，避免动态路由重新学习造成网络中断；如果启用/禁用网口，修改 IP 地址，修改引用网络接口依然会重启动态路由进程。

10.1.2. 交换网口

WEBUI：『网络配置』→『网络接口』→『交换网口』。

『交换网口』用于将 AD 设备的多个网口从逻辑上合并成一个二层交换机的接口，其中 AD 的每个网口都可以当做一个二层交换机的接口来处理。

它主要应用于当 AD 设备部署在网络出口下，透过 AD 后面的防火墙设备来做负载均衡。为了保证网络的高可用性与高可靠性，防火墙使用了双机热备功能，即在同一个网络节点使用两个配置相同的防火墙。此时，在不增加多余网络节点（如：交换机）的情况下，使用

AD 的交换网口功能可以解决主-备防火墙动态切换的问题以及实现 AD 与防火墙、防火墙与防火墙之间的互联。

界面如下图所示：



点击**启用**，用于使选中的交换网口生效。

点击**禁用**，用于使选中的交换网口失效。

点击**删除**，用于删除选中的交换网口。

点击**新建**，用于新建交换网口，交换网口的配置页面如下图所示：

网络接口 交换网口 端口聚合 VLAN子接口 接口模式

新建

属性

名称: (长度限制为1~63个字符, 且不能包含& | " ' , : % < > / \ 特殊字符)

状态: 启用 禁用

已选择:

待选: NET3
NET4
NET5

STP协议

协议状态: 启用 禁用

取消 **完成**



『名称』可以输入便于记忆和识别的字符串，用于标识交换网口名称。

『状态』用于设置“启用”或“禁用”该交换网口。

『网络接口』用于选择将要参与当前交换网口的网络接口，点击按钮左移即可将选定的网口加入该交换网口。若需要将已经选定的网口从该交换网口中移除，选定需要移除的网口，点击按钮右移选定的网口即可。

『STP协议』用于，设置包括『优先级』、『Hello间隔』、『老化时间』、『转发延时』等部分。点击后，默认界面如下图所示：



『协议状态』用于设置“启用”或“禁用”该交换网口上的 STP 协议。

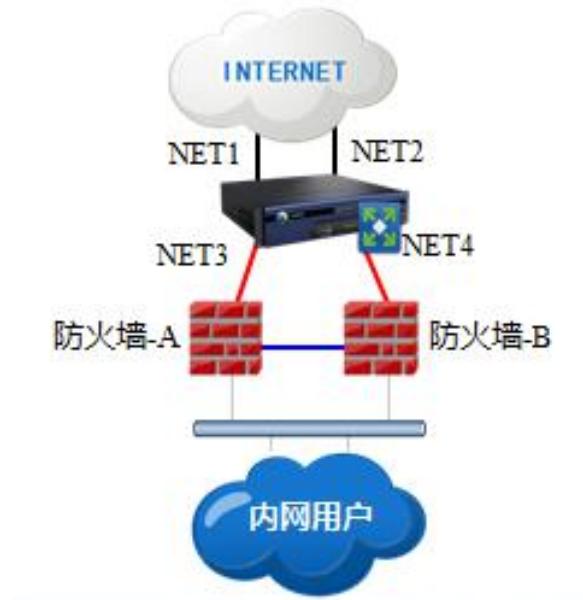
『优先级』用于设置协议优先级，值越小，成为根网桥的机会越大。

『Hello 间隔』用于设置交换网口发送 BPDU 的时间间隔，发送的 BPDU 会被接收的交换机/网桥转发。

『老化时间』用于设置交换网口判定拓扑改变需要等待的时间，通常该值是 Hello 间隔时间的倍数。

『转发延迟』用于设置接口从阻塞状态转换成转发状态的时延。

例如，某客户两个防火墙做双机热备，两个防火墙一主一备，从而满足高可用性与高可靠性的要求，此时 AD 如果部署到网络出口，则要求 NET3 与 NET4 接口 IP 地址一样，相当于 NET3 与 NET4 属于同一个 VLAN，且防火墙发送的数据通过 NET3 与 NET4 均能与该 VLAN IP 通信。



此时需要将 NET3 和 NET4 口组合成交换网口。首选，选中 NET3 和 NET4，点击 按钮左移，点击 保存即可。界面如下图所示：



接下来，给该交换网口配置一个可用的 IP 地址。在『网络配置』→『网络接口』中新建一个 LAN 类别的网络接口，点击 ，可以看到此时网络接口处可以选择刚才新建的交换网口，并给该交换网口配置一个可用的 IP 地址。（注意：在给交换网口配置一个可用

的 IP 地址时，接口类别可以选择 LAN 口，也可以选择 WAN 口，请根据实际情况做选择。)

界面如下图所示：



配置完成后，可看到网络接口的配置界面如下图所示：

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

网口连接实时状态

名称	网络接口	上行带宽	下行带宽	类别
交换网口	交换网口 (交换)			LAN
电信	NET1	100Kbps	100Kbps	WAN

+ 新建 X 删除 ✓ 启用 ✘ 禁用 1个LAND口, 1个WAN口, 0条虚拟链路



在选择合并为交换网口的网络接口时，不仅可以选择多个网口，也可以选择聚合网口和其他网口合并。有关聚合网口的描述请参考 9.1.3 端口聚合。

10.1.3. 端口聚合

WEBUI：『网络配置』→『网络接口』→『端口聚合』。

『端口聚合』用于将 AD 设备的多个物理接口当作一个单一的逻辑接口来处理，它允许多个端口并行连接同时传输数据以提供更高的带宽、更大的吞吐量。

界面如下图所示：



点击**启用**，用于使选中的聚合口生效。

点击**禁用**，用于使选中的聚合口失效。

点击**删除**，用于删除选中的聚合口。

点击**新建**，用于新建聚合口，聚合口的配置页面如下图所示：



『名称』可以输入便于记忆和识别的字符串，用于标识聚合口名称。

『状态』用于设置“启用”或“禁用”端口聚合。

『绑定策略』用于设置端口聚合的工作模式，包括哈希、轮询、802.3ad 和冗余双网卡。

1、『哈希』基于源 IP 和目标 IP 计算 hash 值，选择相应的接口。

2、『轮询』将数据包一个一个轮询发往对应的接口。

3、『802.3ad』自动选择带宽链路最大的为主链路，其余为备用链路。如果带宽一样，则采用哈希算法发送数据。

4、『冗余双网卡』将多个物理网口绑定为一个逻辑接口，只有其中一个物理网口处于工作状态，当主网口宕掉时，备份网口切换成主网口继续工作。

『网络接口』用于选择聚合在一起的网络接口，点击按钮左移即可将选定的网口加入端口聚合。若需要将已经选定的网口从端口聚合中移除，选定需要移除的网口，点击按钮右移选定的网口即可。

例如，此时需要将 NET2 和 NET3 口做端口聚合。首选，选中 NET2 和 NET3，绑定策略选择哈希，点击 **下一步** 按钮左移，点击 **完成** 保存即可。界面如下图所示：



接下来，给该聚合口配置一个可用的 IP 地址。在『网络配置』→『网络接口』中新建一个 LAN 类别的网络接口，点击 **下一步**，可以看到此时网络接口处可以选择刚才新建的聚合口，并给该聚合口配置一个可用的 IP 地址。（注意：在给聚合口配置一个可用的 IP 地址时，接口类别可以选择 LAN 口，也可以选择 WAN 口，请根据实际情况做选择。）界面如下图所示：



网络接口 交换网口 端口聚合 VLAN子接口 接口模式 ? 帮助信息

新建LAN口

属性

名称	端口聚合
网络接口	端口聚合(聚合)
类别	LAN
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

网络地址配置

地址列表

起始IP	(起始地址必须小于或等于结束地址, 如果只有一个地址, 只填写起始地址即可)
结束IP	
掩码/前缀	<input type="text"/> 添加
192.168.10.1/24 <input type="button" value="删除"/>	

配置完成后，可看到网络接口的配置界面如下图所示：

网络接口 交换网口 端口聚合 VLAN子接口 接口模式

网口连接实时状态

MANAGE	NET1	端口聚合	NET4	NET5
--------	------	------	------	------

+ 新建 X 删除 启用 禁用 | 1个LAN口, 1个WAN口

名称	网络接口	I...	上行带宽	下行带宽	类别
端口聚合	端口聚合(聚合)	1...			LAN
电信	NET4	2...	10.24Mbps	10.24Mbps	WAN

10.1.4. VLAN

WEBUI：『网络配置』→『网络接口』→『VLAN』。

『VLAN』用于将 AD 设备的网口从逻辑上划分成多个虚拟子接口，从而实现虚拟工作组。

界面如下图所示：



点击**启用**，用于使选中的 VLAN 生效。

点击**禁用**，用于使选中的 VLAN 失效。

点击**删除**，用于删除选中的 VLAN。

点击**新建**，用于新建 VLAN，VLAN 的配置页面如下图所示：



『名称』可以输入便于记忆和识别的字符串，用于标识 VLAN 名称。

『状态』用于设置“启用”或“禁用”VLAN。

『网络接口』用于选择想要划分的物理设备接口

『Vlan ID』用于设置在指定网络接口内，该 VLAN 的唯一标识 ID。

配置完 VLAN 接口后，然后在『网络接口』里新建接口，配置每一个 VLAN 接口的 IP 地址。



VLAN 接口支持端口聚合网口。

10.1.5. 接口模式

WEBUI：『网络配置』→『网络接口』→『接口模式』。

『接口模式』用于设置网口的工作模式，界面如下所示：

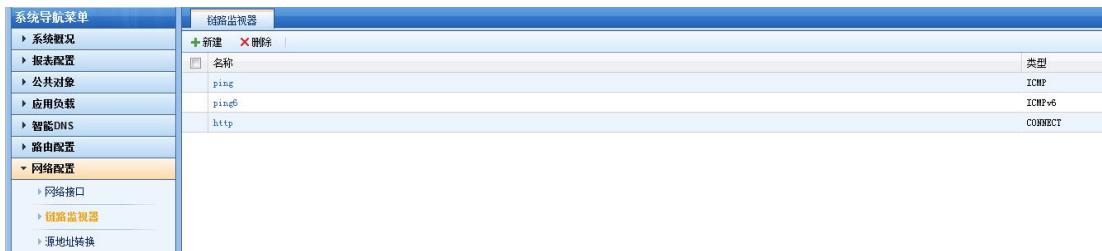
端口	速率/双工	模式
NET1	100baseT/Full	Auto
NET2	1000baseT/Full	Auto
NET3	模式未协商	Auto
NET4	模式未协商	Auto
NET5	模式未协商	Auto

10.2. 链路监视器

WEBUI：『网络配置』→『链路监视器』。

『链路监视器』用于监视需要发布的应用的链路状态。

界面如下图所示：

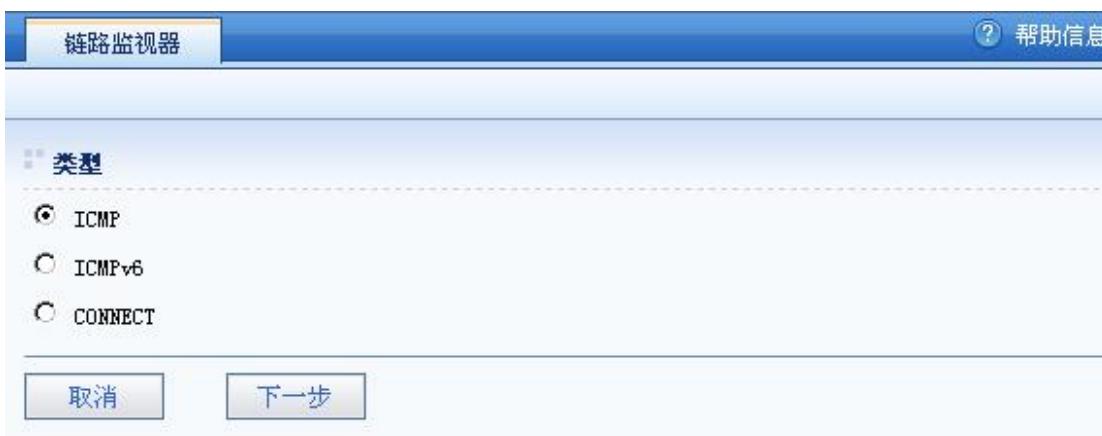


『链路监视器』下显示链路监视器的『名称』、『类型』，包括系统默认链路监视器和自定义链路监视器。

删除按钮可以用于删除自定义链路监视器，但不能删除默认链路监视器。

新建按钮可以用于新建自定义链路监视器。

点击**新建**按钮，如下图所示：

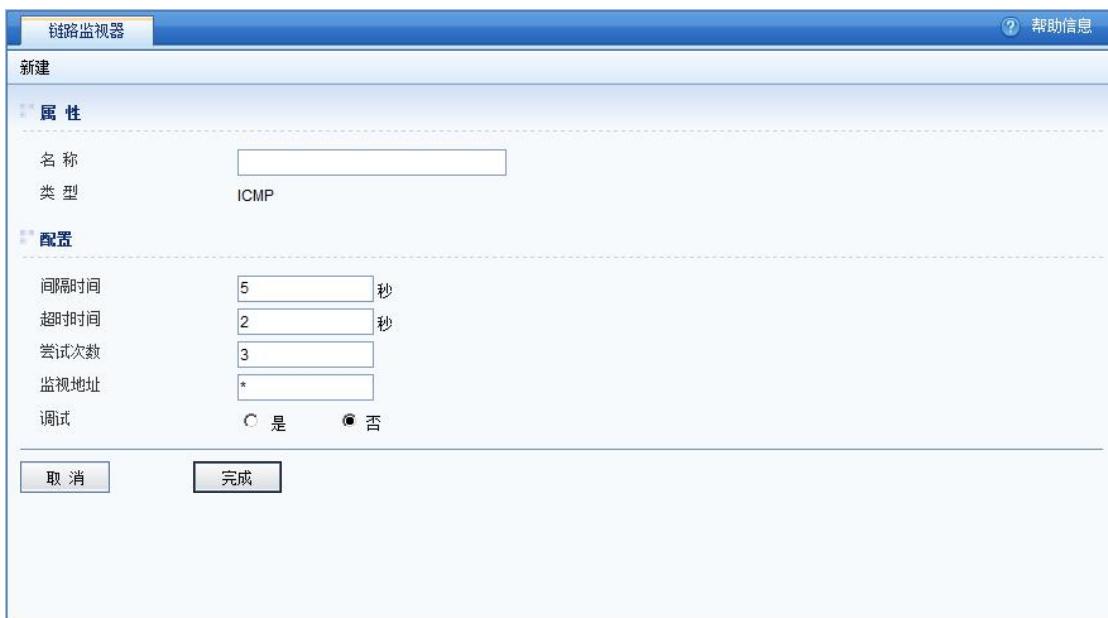


『类型』下面显示可以选择的监视类型，包括[ICMP]、[ICMPv6]、[CONNECT]。

取消按钮可以用于取消本次配置。

下一步按钮可以用于继续一下步配置。

选择[ICMP]或者[ICMPv6]，点击**下一步**按钮，如下图所示：



链路监视器

帮助信息

新建

属性

名称:

类型: ICMP

配置

间隔时间: 5 秒

超时时间: 2 秒

尝试次数: 3

监视地址: *

调试: 是 否

取消 完成

『名称』可以输入便于记忆和识别的字符串，用于标识自定义的链路监视器。

『类型』为上一步配置中选择的类型，此处为 ICMP/ICMPv6。

『间隔时间』用于配置监视的间隔时间，单位为秒。

『超时时间』用于配置监视的超时时间，单位为秒。

『尝试次数』用于配置监视超时后的尝试次数。

『监视地址』用于配置监视的 IP 地址，“*”为监视所有。

『调试』用于配置是否启用监视 ICMP 类型的调试日志。

若选择[CONNECT]，点击**下一步**按钮，如下图所示：

链路监视器 帮助信息

新建

属性

名称

类型 CONNECT

基本配置

间隔时间 秒

超时时间 秒

尝试次数

监视地址

监视端口

调试 是 否

附加配置

回应内容的最大长度 字节

发送内容

接收内容必须包含

断开之前发送的内容

启用十六进制模式 是 否

『名称』可以输入便于记忆和识别的字符串，用于标识自定义的链路监视器。

『类型』为上一步配置中选择的类型，此处为 CONNECT。

『间隔时间』用于配置监视的间隔时间，单位为秒。

『超时时间』用于配置监视的超时时间，单位为秒。

『尝试次数』用于配置监视超时后的尝试次数。

『监视地址』用于配置监视的 IP 地址，“*”为监视所有。

『监视端口』用于配置监视 CONNECT 类型监视的 TCP 端口，包括[http]、[smtp]、[pop3]、[imap]、[other]，可以在输入框中填写自定义的 TCP 端口。

『调试』用于配置是否启用监视 CONNECT 类型的调试日志。

『回应内容最大长度』用于配置监视 CONNECT 类型回应数据内容的最大长度，单位为字节。

『发送内容』用于配置监视 CONNECT 类型建立连接之后发送的数据内容。

『接收内容必须包含』用于配置监视 CONNECT 类型接受数据必须包含的内容。

『断开之前发送的内容』用于配置监视 CONNECT 类型断开连接之前发送的数据内容。

『启用十六进制模式』用于配置监视 CONNECT 类型发送、接收的数据内容[是]、[否]启用十六进制模式。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

10.3. 源地址转换

10.3.1. 源地址转换

『源地址转换』用于设置经过 AD 设备的数据进行源地址转换，适用于 IPv4 和 IPv6 网络，常见应用是代理内网用户上网。

WEBUI 路径：『网络配置』→『源地址转换』。

界面如下图所示：

点击**启用**，用于启用选中的 NAT 规则。

点击**禁用**，用于禁用选中的 NAT 规则。

点击**删除**，用于删除选中的 NAT 规则。

点击『操作』的 用于上下移动 NAT 规则，NAT 规则是由上往下匹配的。

点击『操作』的 用于复制 NAT 规则。

点击**新建**，用于新建 NAT 规则，设置界面如下：

上图是『初级配置视图』，如果想要详细设置，可以点击右上角的『高级配置视图』。

界面如下图所示：



The screenshot shows the Sangfor Cloud interface for configuring a NAT rule. The top navigation bar has tabs for '源地址转换' (Source Address Translation) and 'SNAT地址集' (SNAT Address Set). A '帮助信息' (Help Information) link is in the top right. The main area is titled '新建' (New) and contains two sections: '属性' (Properties) and '配置' (Configuration). In the Properties section, '名称' (Name) is empty, '状态' (Status) is set to '启用' (Enabled), and '类型' (Type) is set to 'IPv4'. In the Configuration section, under '出接口' (Output Interface), '指定网口' (Specify Port) is selected. Under '代理网段' (Proxy Subnet), '代理所有IPV6地址' (Proxy all IPv6 addresses) is selected. Under '目的IP地址转换条件' (Destination IP Address Translation Conditions), '所有目的IPV4地址' (All destination IPv4 addresses) is selected. Under '协议转换条件' (Protocol Conversion Conditions), '所有协议' (All protocols) is selected. Under '转换源IP地址为' (Convert Source IP Address To), '使用网口地址' (Use port address) is selected. Under '转换策略' (Conversion Strategy), '源IP和目的IP哈希' (Source IP and Destination IP Hash) is selected.



提示：1.源地址转换支持 IPv4 和 IPv6 的地址转换。

2.源地址转换的源 IP 地址支持配置“所有 IP”，“子网”，“IP 范围”，“用户地址集”

例如，要建立一条代理局域网内部所有人上网的规则，局域网网段为：
192.168.1.0/255.255.255.0，设置如下：

『规则名称』用于定义 NAT 规则的名称，建议使用便于标识的文字。

『出接口』用于选择数据的输出网口，选择『指定网口』则该规则只会从对应 WAN 口或 MANAGE 口出去的数据包进行匹配。

『代理网段』用于填写需要进行源地址转换的网段，可以选择[代理所有 IP 地址]或者[代理指定网段]。例如填写需要代理上网的网段，在这里我们填写『子网』：192.168.1.0，『掩码』：255.255.255.0。

『转换源 IP 地址为』指定一段 IP 范围，设置『起始地址』和『结束地址』，用于指定将源 IP 转换成的 IP 地址范围，例如代理内网上网，在这里我们填写 AD 设备上分配的外网 IP：202.96.137.75。

『转换策略』用于设置源 IP 地址转换条件，例如相同的源 IP 地址转换成同一个公网 IP

地址，则选择源IP哈希。

界面如下图所示：



The screenshot shows the 'Source Address Translation' (SAT) configuration page. At the top, there are tabs for 'Source Address Translation' and 'SNAT Address Set'. Below the tabs, it says 'New' and 'Properties'.

Properties:

- Name: 代理上网-电信
- Status: Enabled (selected)
- Type: IPv4 (selected)

Configuration:

- Output Interface: Selectable interface (dropdown menu)
- Proxy Network Segment:
 - Proxy all IPv6 addresses (radio button)
 - Proxy specific network segment - source IP must belong to the specified network range to pass through NAT (radio button selected).
 - Subnet: 192.168.1.0
 - Mask: 255.255.255.0
- Convert Source IP Address To:
 - Use interface address (radio button)
 - Use specified address (radio button selected).
 - Start Address: 202.96.137.75
 - End Address: 202.96.137.75
- Conversion Strategy:
 - Source IP and Destination IP Hash (radio button)
 - Source IP Hash (radio button selected)

如果选择『高级配置视图』，界面如下图所示：

名称

状态 启用 禁用

类型 IPv4 IPv6

配置

出接口 指定网口

代理网段 代理所有IPv6地址 代理指定网段 - 源IP地址属于如下设置的网段才可以经过NAT源地址转换

子网

掩码

目的IP地址转换条件 所有目的IPv4地址 指定目的地址网段 - 目的IP地址属于如下设置的网段才可以经过NAT源地址转换

协议转换条件 所有协议 指定协议类型

转换源IP地址为 使用网口地址 使用指定地址

起始地址

结束地址

转换策略 源IP和目的IP哈希 源IP哈希

『目标 IP 地址转换条件』用于设置目标条件，当数据包中的目标 IP 匹配此条件时进行地址转换，可以选择[所有目标 IP 地址]，也可以选择[指定目标地址网段]设置一段指定的 IP 地址。

『协议转换条件』用于设置协议条件，当数据包中的协议满足此条件时进行地址转换，选择[所有协议]，代表所有的协议，选择[指定协议类型]用于设置特定的协议类型及端口。

点击**完成**，完成此 NAT 规则的配置。

点**取消**，用于取消此 NAT 规则的配置。

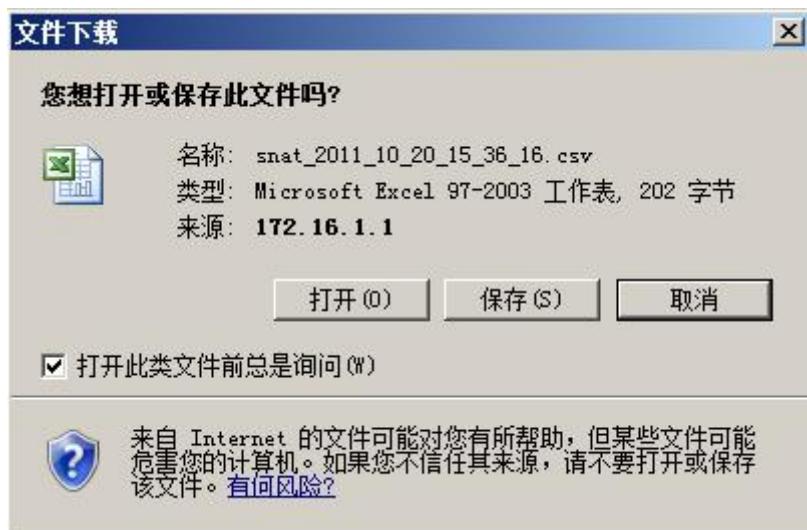
导入按钮可以用于导入 NAT 规则，所导入 NAT 规则文件为在『源地址转换列表』中导出的文件或者自定义的文件，点击**导入**如下图所示：



点击**浏览**可以选择本地备份的 NAT 规则文件或者自定义的文件，点击导入可将文件导入到设备。点击**取消**，取消本次导入配置。

点击“代理上网 CSV 模板下载”即可下载默认模板手动编辑 NAT 规则。

导出按钮可以用于备份自定义的 NAT 规则。点击**导出**按钮，如下图：



点击**保存**，可将 NAT 规则文件保存到本地 PC。

10.3.2. SNAT 地址集

WEBUI 路径：『网络配置』→『源地址转换』→『SNAT 地址集』。

界面如下图所示：

点击**新建**，用于新建 NAT 规则，设置界面如下：

『名称』 SNAT 地址集的名称。

『IP 地址段』可以配置单个地址、IP 范围和子网，属于同一 SNAT 地址集的 IP 地址段之间不能重叠，属于不同 SNAT 地址集的 IP 地址段可以相互重叠，支持 IPV4 和 IPV6 地址混配。

10.3.3. 源地址转换关联组

『源地址转换关联组』开启集群模式，模块才会显示，如图：

	名称	源地址转换规则
<input type="checkbox"/>	源地址转换关联组_10	代理上网WAN1_ad1/
<input type="checkbox"/>	源地址转换关联组_12	代理上网WAN2_ad1/
<input type="checkbox"/>	源地址转换关联组_11	代理上网WAN1_ad2/
<input type="checkbox"/>	源地址转换关联组_13	代理上网WAN2_ad2/

『源地址转换关联组』：转换源地址相同的多条规则一定在同一个关联组中，该图展示这些规则之间的关联关系。



『关联应用组』：选择该源地址转换关联组所属的应用组。应用组在哪台设备上生效，该关联组包含的规则就在哪台设备上生效。

10.4. 端口映射

WEBUI 路径：『网络配置』→『端口映射』。

『端口映射』用于将局域网内的服务器所提供的服务直接发布到公网上，适用于 IPv4 和 IPv6 网络。

界面如下图所示：



点击**启用**，用于使选中的端口映射规则生效。

点击**禁用**，用于使选中的端口映射规则失效。

点击**删除**，用于删除选中的端口映射规则。

点击**新建**，用于新建新端口映射规则，端口映射规则配置页面如下图所示：



属性	
名称	<input type="text"/>
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6

配置	
入接口	<input type="text" value="MANAGE"/>
源IP符合条件	<input type="checkbox"/> 发布服务器 (入接口同时包含所有lan口) <input checked="" type="radio"/> 所有IPV4地址 <input type="radio"/> 指定范围
目的IP符合条件	起始地址： <input type="text"/> 结束地址： <input type="text"/>
指定协议	<input type="text" value="ALL"/>
映射目的IP地址	起始地址： <input type="text"/> 结束地址： <input type="text"/>
关联应用组	<input type="text" value="Default"/>

『名称』用于设置该端口映射规则的名称。

『状态』用于设置“启用”或“禁用”该端口映射规则。

『类型』用于设置该端口映射规则的类型，可以选择 IPv4 或 IPv6

『入接口』用于设置发布内网服务的接口。

『源 IP 符合条件』用于设置一个 IP 范围，当访问数据的源 IP 符合该条件时，匹配该端口映射规则。

『目的 IP 符合条件』用于设置一个 IP 地址或 IP 地址段，当访问数据的目标 IP 地址符合该条件时，匹配该端口映射规则。

『指定协议』用于设置局域网服务器所发布的服务。其中：

[ALL]表示发布所有服务。

[TCP]表示 TCP 服务，并且可以设置发布服务的端口。

[UDP]表示 UDP 服务，并且可以设置发布服务的端口。

[ICMP]表示 ping 服务。

[OTHER]选择 OTHER，可以自定义发布服务的具体协议。

『映射目的 IP 地址』用于设置局域网发布服务的服务器地址。

『映射目的端口范围』可不填写，存在默认值。

『关联应用组』启用高可用集群才显示。选择该规则所属的应用组。应用组在哪台设备上生效，该规则就在哪台设备上生效。

点击**完成**，表示完成并可不填写，存在默认值新该配置。

点击**取消**，取消配置并退回端口映射列表页面。

例如，现在局域网内部有一台 IP 为 192.168.100.250 的电脑要对外网提供 Web 服务，WAN 口地址为 202.96.137.75，所使用的端口为 80，那么设置如下：

在『端口映射列表』页面，点击**新建**，配置新端口映射规则如下：



The screenshot shows the "Port Mapping" configuration page. The "Properties" section is selected, showing:

- Name: web
- Status: Enabled (radio button selected)
- Type: IPv4 (radio button selected)

The "Configuration" section contains the following settings:

- Interface: WAN1
- Source IP Condition: All IPv4 addresses (radio button selected)
- Destination IP Condition: Start address: 202.96.137.75, End address: 202.96.137.75
- Protocol: TCP
- Source Port Range: 0
- Destination Port Range: 80
- Mapping Destination IP Address: Start address: 192.168.100.250, End address: 192.168.100.250
- Mapping Destination Port Range: 80

点击『完成』后规则生效，则外网可通过 AD 的端口映射访问到内网提供的 Web 服务。

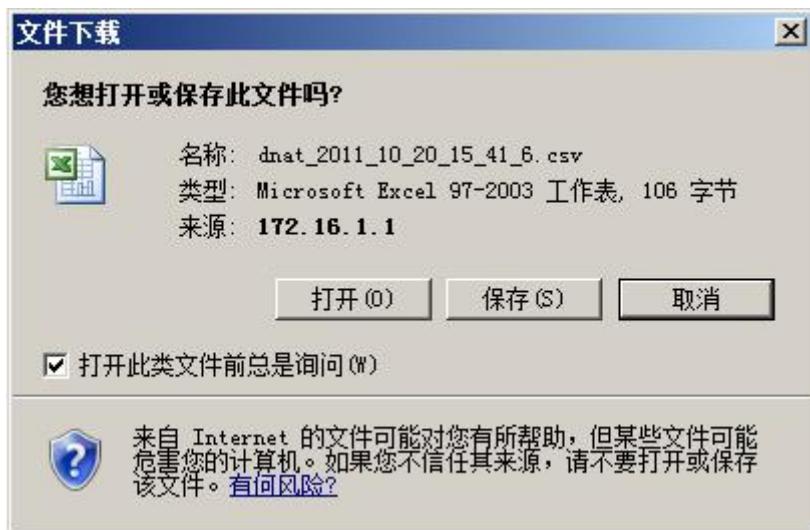
导入按钮可以用于导入端口映射规则，所导入端口映射规则文件为在『端口映射列表』中导出的文件或者自定义的文件，点击**导入**如下图所示：



点击**浏览**可以选择本地备份的端口映射规则文件或者自定义的文件，点击**导入**可将文件导入到设备。点击**取消**，取消本次导入配置。

点击“端口映射 CSV 模板下载”即可下载默认模板手动编辑端口映射规则。

导出按钮可以用于备份自定义的端口映射规则。点击**导出**按钮，如下图：



点击**保存**，可将端口映射规则文件保存到本地 PC。

列表页面增加规则冲突提示，支持规则冲突检测。



10.5. DNS 代理

10.5.1. DNS 代理

『DNS 代理』用于设置 DNS 服务器地址，此处的 DNS 服务器是 AD 设备需要解析域名时，连接的 DNS 服务器地址，并可代理内网 PC 转发 DNS 请求。

WEBUI 路径：『网络配置』→『DNS 代理』。

界面如下图所示：



DNS代理 前置调度策略 内网DNS记录 HOSTS 帮助信息

网关DNS设置

网口： -请选择网络接口-

DNS服务器列表

IP地址：

权值：

(设备本机发出的域名解析请求仅使用最前面的三个DNS服务器)

DNS透明代理

启用DNS代理

『DNS 服务器列表』配置系统网口的 DNS 服务器，可以配置每个 WAN 口的 DNS 服务 器和权值，AD 设备本身只会使用前面三个 DNS。选择[网口]，填写对应 DNS 服务器的[IP] 和[权值]，点击**添加**则添加到下面的 DNS 服务器列表中。点击**删除**则删除选中的 DNS 服务 器。

『启用 DNS 代理』用于设置[启用]或[禁用]DNS 透明代理，启用 DNS 代理后，将会对 内网 PC 的 DNS 请求进行代理。如下图所示：



『IPv4 监听地址』设置监听地址后，内网用户可以将 DNS 服务器设置为该监听地址。

『IPv6 监听地址』设置监听地址后，内网用户可以将 DNS 服务器设置为该监听地址。

『监听端口』 DNS 代理内部使用的端口。

『缓存』开启缓存后，会将 ldns 的应答缓存下来，后续收到 dns 查询时，先查找缓存，如果缓存存在，则使用缓存应答客户端。

『并发查询』收到客户端查询时，会将查询转发给所有可用的 ldns，并使用第一个有效 应答答复客户端。(前置调度策略会优先于并发查询)。

『选择策略』用于配置 DNS 透明代理的 DNS 选择策略。包括[轮询]、[加权轮询]、[加权最小流量]、[优先级]。

- 1、『轮询』轮流选择 DNS 服务器列表中的 DNS 服务器，机会均等。
- 2、『加权轮询』按照 DNS 服务器的权值比例选择 DNS 服务器列表中的 DNS 服务器。
- 3、『加权最小流量』从流量最小的链路里根据权值选择 DNS 服务器。
- 4、『优先级』始终选择权值最高的服务器，只有在权值较高的 DNS 离线或繁忙时才会选择权值较低的 DNS 服务器。

『代理目标范围』代理全部 DNS 请求、指定的服务器、指定的域名。代理目标范围为“全部 DNS 请求”时，需要指定“代理内网网段”为部分网段，否则智能 DNS 失效；代理“指定域名”指的是前置策略中配置的域名。

『代理内网网段』用来设置需要提供 DNS 代理的内网网段。

『监视域名』通过对此域名的监视来判断 DNS 的有效性，从而进行 DNS 透明代理。

『前置调度策略』用于将特定用户的访问调度到指定的服务器上。

『链路繁忙保护』用于设置 DNS 代理时，选路是否受链路繁忙状态影响，开启时，如果某条链路处于繁忙状态，则不选择这条链路；如果该规则所有链路都繁忙，则随机调度链路绑定的 DNS 服务器。

点击[更新](#)，将此 DNS 设置保存生效。

10.5.2. 前置调度策略

『前置调度策略』用于将特定用户的访问调度到指定的服务器上。

界面如下图所示：

DNS代理 | 前置调度策略 | 内网DNS记录 | HOSTS

+ 新建 × 删除 | ✓ 启用 ⚡ 禁用 |

<input type="checkbox"/>	名称	内网用户	域名	DNS服务器	操作

共0/16条配置信息

点击**启用**，用于使选中的前置调度策略生效。

点击**禁用**，用于使选中的前置调度策略失效。

点击**删除**，用于删除选中的前置调度策略。

点击**新建**，用于新建前置调度策略，前置调度策略配置页面如下图所示：

DNS代理 前置调度策略 内网DNS记录 HOSTS

新建

普通属性

名称:

状态: 启用 禁用

策略配置

内网用户:

域名:

已选择:

待选:

DNS服务器:

链路繁忙保护: 启用 禁用

失效动作: 匹配下一条策略 强制调度

操作

『名称』可以输入便于记忆和识别的字符串，用于标识自定义的策略。

『状态』点击[启用]则启用前置调度策略，点击[禁用]则禁止前置调度策略。

『内网用户』选择启用前置调度策略的内网 IP 地址段。

『域名』配置用于匹配前置调度策略的目标域名。

『DNS 服务器』指定 DNS 服务器为本项前置调度策略返回结果。

『链路繁忙保护』设置是否根据链路繁忙状态来分配链路。

『失效动作』当列表内 DNS 服务器失效后的处理方式。[匹配下一条策略]略过本规则匹配下一条策略，[强制调度]始终返回列表中的 DNS 服务器。

点击**完成**，完成此规则的配置。

点击**取消**，用于取消此规则的配置。

10.5.3. 内网 DNS 记录

『内网 DNS 记录』在设备上添加 DNS 条目用于 DNS 解析。

界面如下图所示：

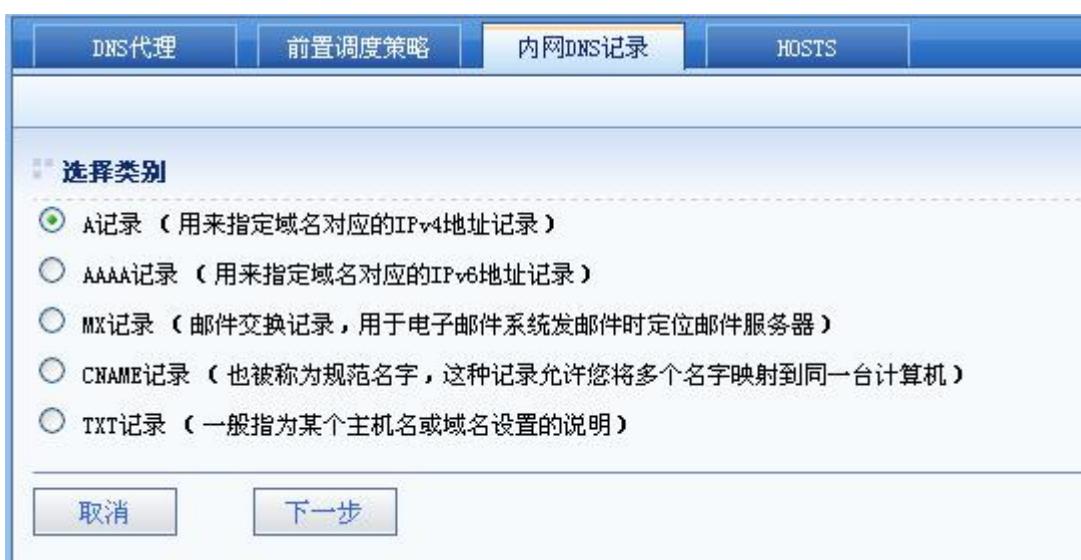


点击**启用**，用于使选中的内网 DNS 记录生效。

点击**禁用**，用于使选中的内网 DNS 记录失效。

点击**删除**，用于删除选中的内网 DNS 记录。

点击**新建**，用于新建内网 DNS 记录，内网 DNS 记录配置页面如下图所示：



『选择类别』下面显示可以选择的 DNS 记录类别，包括[A 记录]、[AAAA 记录]、[MX 记录]、[CNAME 记录] 和[TXT 记录]。

取消按钮可以用于取消本次配置。

下一步按钮可以用于继续下一步配置。

选择[A 记录]，点击**下一步**按钮，如下图所示：

DNS代理 前置调度策略 内网DNS记录 HOSTS

新建A记录

属性

域名 (长度为1~255字符, 且不能包含& | " , : % < > / \ 特殊字符)

状态 启用 禁用

配置

A记录列表 IP:
TTL: 秒

添加 删除

取消 完成

『域名』用于配置 A 记录的域名。

『状态』用于配置 A 记录的[启用]、[禁用]。

『IP』用于配置 A 记录的域名对应的 IP 地址。

『TTL』用于配置 A 记录 Local DNS 的缓存时间，单位为秒。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

选择[AAAA 记录]，点击下一步按钮，如下图所示：



The screenshot shows the '新建AAAA记录' (Create AAAA Record) dialog box. It has two main sections: '属性' (Properties) and '配置' (Configuration).
属性 (Properties):

- 域名 (Domain): An input field.
- 状态 (Status): A radio button group with '启用' (Enabled) selected and '禁用' (Disabled) unselected.

配置 (Configuration):

- AAAA记录列表 (List of AAAA records): A table with columns 'IP:' and 'TTL'. It contains one row with IP '60' and TTL '60 秒'. To the right of the table are '添加' (Add) and '删除' (Delete) buttons.

At the bottom are '取消' (Cancel) and '完成' (Finish) buttons.

『域名』用于配置 AAAA 记录的域名。

『状态』用于配置 AAAA 记录的[启用]、[禁用]。

『IP』用于配置 AAAA 记录的域名对应的 IP 地址。

『TTL』用于配置 AAAA 记录 Local DNS 的缓存时间，单位为秒。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

若『选择类别』中选择[MX 记录]，点击下一步按钮，如下图所示：

DNS代理 | 前置调度策略 | **内网DNS记录** | HOSTS

新建MX记录

属性

域名

状态 启用 禁用

配置

MX记录列表

主机:	优先级:	TTL:	秒	操作
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	添加
				删除

当前已配置 0 / 8 个地址

取消 **完成**



『域名』用于配置 MX 记录的域名。

『状态』用于配置 MX 记录的[启用]、[禁用]。

『主机』用于配置 MX 记录的域名。

『优先级』用于设置列表中 MX 记录的优先级别。

『TTL』用于配置 MX 记录 Local DNS 的缓存时间，单位为秒。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

若『选择类别』中选择[CNAME 记录]，点击**下一步**按钮，如下图所示：

DNS代理 前置调度策略 内网DNS记录 HOSTS

新建CNAME记录

属性

域名 (长度为1~255字符，且不能包含& | " " , : % < > / \ 特殊字符)

状态 启用 禁用

配置

CNAME记录列表 规范名称:
TTL: 秒

当前已配置 0/8 个地址



『域名』用于配置 CNAME 记录的域名。

『状态』用于配置 CNAME 记录的[启用]、[禁用]。

『规范名称』用于配置 CNAME 记录的域名。

『TTL』用于配置 CNAME 记录 Local DNS 的缓存时间，单位为秒。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

若『选择类别』中选择[TXT 记录]，点击**下一步**按钮，如下图所示：

DNS代理 前置调度策略 内网DNS记录 **HOSTS**

新建TXT记录

属性

域名

状态 启用 禁用

配置

TXT值

记录生存时间(TTL) 秒

取消 **完成**



『域名』用于配置 TXT 记录的域名。

『状态』用于配置 TXT 记录的[启用]、[禁用]。

『TXT 值』用于配置 TXT 记录的域名对应的 TXT 值。

『TTL』用于配置 TXT 记录 Local DNS 的缓存时间，单位为秒。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

10.5.4. HOSTS

『HOSTS』用于设置 AD 设备的 HOST 表，用于设备本身访问域名时的域名解析。

WEBUI 路径：『网络配置』→『DNS 代理』→『HOSTS』。

界面如下图所示：

DNS代理		前置调度策略		内网DNS记录		HOSTS	
+ 新建 × 删除							
	HOST					IP 地址	
	ad.sangfor.com					127.0.0.1	
	localhost					127.0.0.1	

点击**删除**用于将选中的 hosts 删除。

点击**新建**用于新建 hosts 条目，设置界面如下：

DNS代理	前置调度策略	内网DNS记录	HOSTS	帮助信息
新建				
配置				
HOST	<input type="text"/>	(长度限制为1~63字符，必须以英文字符开始，只能包含字母(不区分大小写)、数字 - _ . 等)		
IP地址	<input type="text"/>			
<input type="button" value="取消"/> <input type="button" value="完成"/>				

『HOST』用于设置域名或主机名。

『IP 地址』用于设置以上设置的主机名对应的 IP 地址。

配置完毕，点击**完成**，完成此 HOSTS 规则的配置。

点击**取消**，用于取消此 HOSTS 规则的配置。

10.6. 网络安全

10.6.1. 网络攻击防护

DOS 攻击（拒绝服务攻击），通常是以消耗服务器端资源、迫使服务停止响应为目标，通过伪造超过服务器处理能力的请求数据造成服务器响应阻塞，从而使正常的用户请求得不到应答，以实现其攻击目的。SANGFOR AD 网关的防 DOS 攻击功能可以防止外网对内网

的 DOS 攻击并通过 IP 来判断攻击者。

WEBUI 路径：『网络配置』→『网络安全』→『网络攻击防护』。

界面如下图所示：



网络攻击防护

ICMP-Flood防护

○ 启用 ● 禁用

每目的IP阈值: 2048 包/秒 (必须是整数, 取值范围 0~2147483647)

UDP-Flood防护

○ 启用 ● 禁用

每目的IP阈值: 20480 包/秒

SYN-Flood防护

○ 启用 ● 禁用

每目的IP激活阈值: 4096 包/秒

白名单

IP地址: 单个地址

单个地址: [输入框] [添加] [删除]

当前已配置 0 / 100 个地址段

更新

『ICMP-Flood 防护』用于配置 ICMP-Flood 防护的[启用]、[禁用]。

『UDP-Flood 防护』用于配置 UDP-Flood 防护的[启用]、[禁用]。

『SYN-Flood 防护』用于配置 SYN-Flood 防护的[启用]、[禁用]。

『每目的 IP 阈值』用于配置防护模块对 ICMP/UDP 包的每秒数量限制。

『每目的 IP 激活阈值』用于配置防护模块对网口受到 SYN-Flood 的判定标准值。

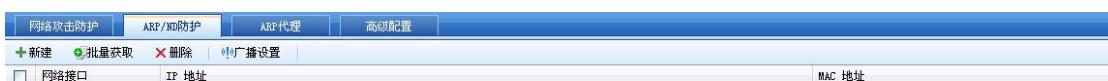
『白名单』用于设置不进行防护的源地址列表。

10.6.2. ARP/ND 防护

WEBUI 路径：『网络配置』→『网络安全』→『ARP/ND 防护』。

『ARP/ND 防护』用于设置静态的 ARP 条目，通常用于绑定重要设备与服务器的 ARP 信息，防止内网有 ARP 欺骗时，影响 AD 设备与其他设备的正常通信。

界面如下图所示：



点击**删除**，用于删除选中的 ARP 条目。

点击**新建**，用于新建 ARP 条目，设置界面如下：



『网络接口』用于设置绑定 IP/MAC 的网络接口。

『IP 地址』用于设置对应的 IP 地址信息。

『MAC 地址』用于设置上面配置的 IP 地址对应的 MAC 地址信息。

点击**自动获取**用于获取指定 IP 地址的 MAC 地址，如果无法获得该 MAC 地址则提示获取失败。

配置完毕，点击**完成**，完成此条 ARP 信息的配置。

点击取消，用于取消此条 ARP 信息的配置。

AD 设备提供自动获取 MAC 地址的功能，点击批量获取，用于自动扫描对应 IP 地址段的 MAC 地址，界面配置如下：



输入需要扫描的[起始 IP]和[结束 IP]，点击自动获取，设备通过发送 ARP 广播获取对应 IP 的 MAC 地址。

『MAC 地址列表』用于显示扫描后的 ARP 信息。

点击完成，即可将自动扫描的 ARP 信息加入 ARP 列表中。

点击取消，取消该 ARP 信息搜索，并返回 ARP 防护默认页面。

点击广播设置，用于设置主动广播网关 MAC 地址。



『广播间隔时间』用于配置 AD 网关每过多少分钟发送一次 ARP 广播包。

点击立即广播，即可将自动扫描的 ARP 信息加入 ARP 列表中。

点击更新，完成配置。

点击取消，取消该配置。

10.6.3. ARP 代理

WEBUI 路径：『网络配置』→『网络安全』→『ARP 代理』。

界面如下图所示：

名称	代理IP	出接口

点击删除，用于删除选中的 ARP 代理条目。

点击新建，用于新建 ARP 代理条目，设置界面如下：

新建

属性

名称

状态 启用 禁用

配置

地址列表 起始IP：
结束IP：

当前共配置0/2048个代理IP

出接口



『名称』： ARP 代理的名称。

『状态』： 启用时，ARP 代理的所有配置生效；禁用时，ARP 代理的所有配置失效且无法使用。

『地址列表』： 手动添加 IP 到地址列表中。

『出接口』： 匹配此 ARP 代理时，数据的出接口。一条配置可选择多个出接口，其中选择自动出接口则不能选择其它业务口，选择其它业务口则不能选择自动出接口。自动出接口：根据 arp 请求的入接口来选择 arp 应答的目标 MAC

10.6.4. 高级配置

『高级配置』用于配置路由转发选项。

WEBUI 路径：『网络配置』→『网络安全』→『高级配置』。

界面如下图所示：



选择启用[WAN 网卡的入站路由转发]则对于 WAN 口收到的需要路由转发的数据包进行转发。

选择禁用[WAN 网卡的入站路由转发]则对于 WAN 口收到的需要路由转发的数据包直接丢弃。

如果 WAN 网卡的入站路由转发功能为禁用状态，则 WAN 口与 LAN 口无法进行除虚拟服务、DNS、代理上网、端口映射、远程登录、匹配智能路由或静态路由之外的数据传输，启用后才可以进行数据传输。

『对称路由模式』设置设备进行路由转发时，该网络环境下是对称路由模式还是非对称路由模式。选择[启用]为对称路由模式，选择[禁用]为非对称路由模式。默认情况下为对称路由模式。

10.7. ACL 配置

10.7.1. 基础 ACL 控制

WEBUI 路径：『网络配置』→『ACL 配置』→『基础 ACL 控制』。

『基础 ACL 控制』用于配置链路级别的访问控制，。

界面如下图所示：



名称	入接口	源IP	源端口	目的IP

点击**启用**，用于启用选中的 ACL 规则。

点击**禁用**，用于禁用选中的 ACL 规则。

点击**删除**，用于删除选中的 ACL 规则。

点击『操作』的   用于上下移动 ACL 规则，ACL 规则是由上往下匹配的。

点击**新建**，用于新建 ACL 规则，设置界面如下：

基本ACL控制 高级ACL控制

新建基本ACL

属性

名称

状态 启用 禁用

规则配置

协议 协议名： 自定义

协议号：

指定入接口

源IP地址

IP地址

目的IP地址

IP地址

动作 允许 拒绝

『名称』用于定义 ACL 规则的名称，建议使用便于标识的文字。

『协议』用于设定一个协议号，当通信符合此协议号时，则匹配当前 ACL 规则。0 表示所有协议号。

『指定入接口』允许选择“ALL/面板接口”，支持“指定入接口”的 ACL 控制。

『源 IP 地址』用于配置一个 IP 段，当源 IP 符合此 IP 段时，则匹配当前 ACL 规则。

『目的 IP 地址』用于配置一个 IP 段，当目的 IP 符合此 IP 段时，则匹配当前 ACL 规则。

『动作』用于配置一个动作，当上述条件都符合时，执行此动作。

1、『允许』放通匹配五元组的访问。

2、『拒绝』丢弃匹配五元组的访问。



说明：选择 ICMP 协议，自定义 ICMP 类型可以选择设定常规类型



10.7.2. 高级 ACL 控制

WEBUI 路径：『网络配置』→『ACL 配置』→『高级 ACL 控制』。

『高级 ACL 控制』用于配置虚拟服务级别的访问控制，。

界面如下图所示：

点击 **启用**，用于启用选中的 ACL 规则。

点击 **禁用**，用于禁用选中的 ACL 规则。

点击删除，用于删除选中的 ACL 规则。

点击『操作』的   用于上下移动 ACL 规则，ACL 规则是由上往下匹配的。

点击新建，用于新建 ACL 规则，设置界面如下：



基本 ACL 控制 高级 ACL 控制 帮助信息

新建高级 ACL 控制

属性

名称

状态 启用 禁用

规则配置

源IP地址

虚拟服务

每IP连接限制

取消 完成

『名称』用于定义 ACL 规则的名称，建议使用便于标识的文字。

『源 IP 地址』用于配置一个 IP 段，当源 IP 符合此 IP 段时，则匹配当前 ACL 规则。

『虚拟服务』用于配置虚拟服务，此规则将应用于此虚拟服务。

『每 IP 连接限制』用于配置外部访问虚拟服务的最大连接数限制，当虚拟服务连接数达到限制以后，新的外部访问将会被拒绝。

第 11 章 系统配置

『系统配置』用于配置设备的系统信息，包括『设备管理』、『授权管理』、『用户』、『SMTP 服务器』、『SNMP』、『告警』、『双机维护』、『日志设置』、『系统更新』等几个部分。界面如下图所示：



11.1. 设备管理

11.1.1. 管理网口

WEBUI 路径：『系统配置』→『设备管理』→『管理网口』。

『管理网口』用于设置 AD 设备的管理网口的相关信息，另外还包括主机名、WEBUI 的设置。

界面如下图所示：

The screenshot shows the Sangfor Cloud Management interface under the 'System Configuration' section. On the left sidebar, 'System Configuration' is selected. The main panel has tabs for 'Manage Port', 'Date/Time', 'Backup & Recovery', 'Power Off/Restart', and 'WebConsole'. The 'Manage Port' tab is active, displaying basic device management information. It includes a table for managing IP addresses, a field for the management gateway, and sections for system configuration and WEB UI settings.

地址列表	IP	掩码	操作
	10.252.252.215/24		添加
	200.200.144.215/22		删除

当前已配置 2/16 个IP
管理网关: 200.200.147.254

系统配置
主机名称: yhao
远程维护: 启用 禁用

WEB UI
HTTPS端口: 443
HTTP会话超时时间: 6000 秒
报表端口: 85
报表UI会话超时时间: 600 秒
设备根证书: 下载

更新

『管理网口』用于设置 AD 设备管理网口 MANAGE 的相关信息。

在『地址列表』中输入[IP 地址]和[掩码]，点击**添加**，将 IP 加入地址列表中。

点击**删除**，用于删除选中的管理 IP。

『管理网关』用于设置 AD 设备管理网口 MANAGE 的网关信息。

『主机名称』用于设置 AD 设备的主机名，一般填写申请过的 DNS 主机名即可。
『远程维护』用于设置是否启用 AD 设备的远程维护，勾选[启用]时，管理员可以通过 WAN 方向的接口访问设备并进行管理。

『WEB UI』用于设置 WEBUI 控制台等相关配置。

『HTTPS 端口』用于设置登录 AD 设备控制台页面的登录端口，默认是 443 端口。

『HTTP 会话超时时间』用于设置控制台用户的控制超时时间。

『报表端口』用于设置连接报表服务器的端口，默认是 85 端口。

『报表 UI 会话超时时间』用于配置报表数据中心登录用户的会话超时时间，此超时时间内用户没有进行任何操作，将会清空会话，需要重新登录。

『设备根证书』登录控制台的根证书下载，用户下载的根证书，导入浏览器中，登录控制台不再提示证书错误。



点击更新，用于完成及保存以上设置。



说明：MAD 中，『虚拟化管理』-『vAD 管理』也增加了『管理网关』用于设置 AD 设备管理网口 MANAGE 的网关信息。



11.1.2. 日期/时间

WEBUI 路径：『系统配置』→『设备管理』→『日期/时间』。

『时间』用于设置 AD 设备的系统时间。

界面如下图所示：



『刷新』用于刷新界面上的时间。

点击获取 PC 当前时间用于将设备系统时间与登录控制台的电脑系统时间同步。

『自动与时间服务器同步』勾选后，将自动与时间服务器进行时间同步。

『时间服务器』填写 INTERNET 时间服务器。

『备份服务器』填写备用的 INTERNET 时间服务器。

『同步间隔』可配置与时间服务器同步时间的间隔，取值范围是 1-604800s，默认为 86400s。

点击立即与服务器同步用于将设备系统时间与时间服务器的时间立即进行同步。

点击**更新**用于保存并更改设备系统时间。



如果更新的时间在原时间之后的话，会导致中间一段时间的数据没有记录，如果更新的时间在原时间之前的话，对于报表中的分钟视图、小时视图是以最新的数据显示，对于报表中的天视图和月视图是以数据叠加后的结果显示数据的。

11.1.3. 配置备份与恢复

WEBUI 路径：『系统配置』→『设备管理』→『配置备份与恢复』。

『配置备份与恢复』AD 设备控制台提供在界面上进行备份配置与恢复配置的操作。

界面如下图所示：

管理网口		日期/时间	配置备份与恢复	关机/重启	WebConsole
	新建		删除		从文件恢复
	恢复默认配置				
<input type="checkbox"/>	时间点		描述	版本	操作
<input type="checkbox"/>	2015-10-29 23:29:41		配置文件备份	AD-6.3_B	恢复 导出

点击**新建**，就可以对当前的配置进行备份：

管理网口		日期/时间	配置备份与恢复	关机/重启	WebConsole
新建					
属性					
时间点	2015-05-28 21:23:29				
描述	配置文件备份				
<input type="button" value="取消"/>		<input type="button" value="完成"/>			

点击**恢复**，即可恢复到所选备份的配置状态。

点击**导出**，把备份的配置保存到电脑。

点击 **从文件恢复**，选择本地的配置恢复，如下图所示：



点击  恢复默认配置，恢复出厂配置，如下图所示：



1. 恢复备份配置会自动重启设备。
2. 设备加入集群前会自动备份配置。

11.1.4. 关机/重启

WEBUI 路径：『系统配置』→『设备管理』→『关机/重启』。

『关机/重启』提供界面上的重启按钮，方便客户进行重启操作。

界面如下图所示：



点击**关机**，用于关闭 AD 设备。

点击**重启设备**，用于重启 AD 设备。

点击**重启服务**，用于重启 AD 设备的所有服务，硬件不重启。

11.1.5. WebConsole

WEBUI 路径：『系统配置』→『设备管理』→『WebConsole』。

『WebConsole』用于让客户能通过 web 页面进行命令行操作，查看后台的一些基本信息。

界面如下图所示：



『命令帮助列表』列出 webconsole 所支持的命令以及命令的作用，在页面最下方的 [Sangfor Webconsole#] 后面输入命令 help，按键盘 Enter 键就能查看到系统的相应信息。

界面如下图所示：

		3.ethhtool -S DEVNAME
free	查看内存占用率	free
ifconfig	查看设备网卡信息	ifconfig
iptables	查看设备的iptables规则	iptables -t tableName
ip link	查看设备的网卡信息	ip link
ip route	查看设备的路由表	1.ip route list 2.ip route list table tableName
ip rule	查看设备的路由规则	ip rule
netstat	查看设备的服务侦听情况	同linux下的netstat命令，输入netstat默认执行netstat -an
ping	查看设备与其他主机的连接情况	同linux下的ping命令（注意：不使用-c参数默认ping四个包，若使用-c参数，需放在“ping”之后）
ping6	查看设备与其他主机的连接情况，IPv6地址专用。	同linux下的ping6命令（注意：不使用-c参数默认ping四个包，若使用-c参数，需放在“ping”之后）
route	查看系统路由	route
sock	检测连接，检测某个主机的指定端口是否在侦听	sock host port (如:sock 192.168.1.1 4009)
tcpdump	抓取数据包命令	同linux下的tcpdump命令，需加-c参数 (如:tcpdump -i eth0 -c 10)
top	查看进程的CPU占用率	top
traceroute	查看设备到达其他网络的中间路径	traceroute host
whoisp	查看IP地址所属的ISP和地域名称	whoisp ip (如: whoisp 202.96.134.133)
check	检测系统状态	check
regexmatch	测试正则表达式	regexmatch (如: regexmatch -es ".+" "sangfor")
nslookup	查询域名信息	nslookup [-option] [name -] [server] (如: nslookup -querytype=A www.163.com) (注意：“=”两边不能有空格) (帮助: nslookup -all 可以查看option)
clear	清除屏幕	clear
help	帮助命令列表	help或?

11.2. 授权信息

『授权信息』包括『设备信息』和『序列号』两部分。『设备信息』用于显示设备的网关序号、授权模块、电话服务有效期、硬件质保服务有效期。『序列号』用于控制链路数量、SSL 卸载授权、TCP 单边加速授权（即 TCP 加速）、HTTP 缓存授权、智能 DNS 全局授权、应用分析模块，安全分析模块、软件升级授权，不同的序列号对应着不同功能模块。

WEBUI 路径：『系统配置』→『授权信息』。

界面如下图所示：

序列号

告警：该用户未授权！ | 声明：非授权客户使用，深信服科技不提供任何技术支持！

设备信息

网关序号	1C0C95ED
授权模块	基本模块, SSL卸载模块, TCP单边加速模块, HTTP缓存模块, 智能DNS模块
电话服务有效期	-
硬件质保服务有效期	-

基本授权

序列号	8R2CTBXXF3E3HDBD
激活状态	已激活
链路数量	8

SSL卸载授权

序列号	RJTFFSJFT3D6LJRQ
激活状态	已激活

TCP单边加速授权

序列号	CQWBPAPBBR24A5LF
激活状态	已激活

HTTP缓存授权

序列号	EXCGPRGAAT27ATY8
激活状态	已激活

智能DNS全局授权

设备信息：用于显示设备的网关序号、授权模块、电话服务有效期、硬件质保服务有效期。

『激活状态』显示 AD 设备是否被激活，当没有设置序列号或者序列号错误时，AD 设备会处于未激活状态。

基本授权：激活基本授权序列号才能使用 AD 设备提供的主要功能（如应用负载、链路负载等）。

『链路数量』显示的是此 AD 设备最多支持的外网链路即 WAN 类别接口数量。

SSL 卸载授权：激活 SSL 卸载授权序列号才能配置 SSL 相关的虚拟服务。

TCP 单边加速授权：激活 TCP 单边加速授权序列号才能启用虚拟服务的 TCP 单边加速功能。

HTTP 缓存授权：激活 HTTP 缓存授权序列号才能启用虚拟服务优化策略的 HTTP 缓存和 HTTP 压缩功能。

智能 DNS 全局授权：激活智能 DNS 全局授权序列号才能启用全局配置还原、站点集合等全局关功能。

应用分析授权：激活应用分析授权序列号才能启用业务分析中的应用分析功能，进行 WebLogic、ORACLE、SQLServer 服务器的监视。

安全分析授权：激活安全分析授权序列号才能启用业务分析中的安全分析功能，进行实时漏洞分析。

软件升级授权：软件升级授权序列号只在一定时间内有效，超过有效期后将不能进行系统软件升级。

虚拟多租户授权：激活虚拟多租户授权序列号才能新建和启动 vAD，可新建的 vAD 数目受序列号中的 vAD 数量限制。

软件升级授权：可进行软件系统升级。



说明：在虚拟 AD 下隐藏授权告警提示以及隐藏掉序列号输入的文本框。

序列号	
设备信息	
网关序号	FDEB55CC
授权模块	基本模块, SSL卸载模块, TCP单边加速模块, HTTP缓存模块, 智能DNS模块, 应用分析模块, 安全分析模块
电话服务有效期	2016-11-29
硬件质保服务有效期	2016-11-29
基本授权	
激活状态	已激活
链路数量	2
SSL卸载授权	
激活状态	已激活
TCP单边加速授权	
激活状态	已激活
HTTP缓存授权	
激活状态	已激活
智能DNS全局授权	
激活状态	已激活

11.3. 用户

11.3.1. 用户

『用户』用来设置能够通过控制台管理 AD 硬件设备的登录用户。

WEBUI 路径：『系统配置』→『用户』→『用户』。

界面如下图所示：



『用户列表』用于显示已经设置完成的控制台用户及此用户所属角色。

[启用]、[禁用]：用于启用或者禁用选中的控制台用户。

[删除]：用于删除选中的控制台用户。

点击相应的用户名用于修改用户用户信息和用户密码。

在『用户列表』右上方点击新建，用于新建控制台用户。

配置界面如下：

用 户 角 色 外部认证登录

新建

属性

名称	<input type="text"/>
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
角 色	-请选择角色-
描 述	<input type="text"/>
认 证 方 式	<input checked="" type="radio"/> 本地密码 <input type="radio"/> 外部认证
密 码	<input type="password"/>
确认密码	<input type="password"/>

『名称』用于设置控制台用户名。

『状态』用于[启用]或[禁用]此控制台用户。

『角色』用于选择此用户所属的角色。

『描述』用于设置用户的描述信息。

『认证方式』提供“本地密码/外部认证”两个选项。

『密码』用于设置用户的登录密码。

『确认密码』用于确认用户的登录密码，与『密码』中设置的密码要一致。

配置完毕，点击**完成**，完成此用户的配置。

点击**取消**，用于取消此用户的配置。

11.3.2. 角色

『角色列表』用于显示已经设置完成的控制用户角色。

用户	角色	外部认证登录
+ 新建	X 删除	
<input type="checkbox"/> 角色名称		描述
admin		管理员角色，拥有所有权限，不可删除修改
<input type="checkbox"/> guest		只读权限

『角色列表』用于显示已经设置完成的控制台用户及其用户所属角色。

[删除]：用于删除选中的控制台用户。

在『角色列表』右上方点击**新建**，用于新建控制台角色。

列表中的“admin”角色和用户默认无法删除，此用户管理员，拥有所有权限，密码为“admin”。

在建立控制台用户之前需要先确定此控制台用户所使用的角色，『用户角色』用于设置不同的控制权限以及其他相关配置，在『用户角色列表』上方，点击**新建**，用于新建角色，配置界面如下：

属性	名称	描述	
AD API 访问	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用	
SSH	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用	
登录限制	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用	
权限	温馨提示：点击“+”展开子模块		
系统概况	<input checked="" type="radio"/> 无	<input type="radio"/> 查看	<input type="radio"/> 所有
报表配置	<input checked="" type="radio"/> 无	<input type="radio"/> 查看	<input type="radio"/> 所有
公共对象	<input checked="" type="radio"/> 无	<input type="radio"/> 查看	<input type="radio"/> 所有
数据中心	<input checked="" type="radio"/> 无	<input type="radio"/> 查看	<input type="radio"/> 所有
应用负载	<input checked="" type="radio"/> 无	<input type="radio"/> 查看	<input type="radio"/> 所有
智能DNS	<input checked="" type="radio"/> 无	<input type="radio"/> 查看	<input type="radio"/> 所有
路由配置	<input checked="" type="radio"/> 无	<input type="radio"/> 查看	<input type="radio"/> 所有
网络配置	<input checked="" type="radio"/> 无	<input type="radio"/> 查看	<input type="radio"/> 所有

『名称』用于设置此角色的名称，建议设置容易标识的文字。

『描述』用于设置角色的描述信息。

『ADAPI 访问』设置用户 ADAPI 的控制权限。

『SSH』若启用 SSH 访问，则允许引用该角色的用户访问后台命令行功能，若禁用 SSH 访问，则禁止访问后台命令行功能。

命令行功能是指可以将 SSL、虚拟服务、网络配置、路由配置、系统配置菜单下所有功能的配置通过登陆 SSH 将配置命令导入导出。

此功能的应用场景：客户部署了大量的 AD 设备，配置都差不多，不想一台一台的设置，想要批量修改服务器负载的配置，例如：增加一个 HTTP 头部改写，只需在一台设备通过 UI 配置妥当，然后登陆 SSH 将配置命令导出，在其他设备的 SSH 上执行即可。

如下图可以导出虚拟服务配置命令：

```
[gaosu@ad66]:~$ ad_cli vs export
vs export
export:
ad_cli vs vs { name="https" } add
ad_cli vs vs[ name="https" ] name {"https"}
ad_cli vs vs[ name="https" ] enable {true}
ad_cli vs vs[ name="https" ] type {FAMILY_INET}
ad_cli vs vs[ name="https" ] mode {VS_MODE_L7}
ad_cli vs vs[ name="https" ] service {https}
ad_cli vs vs[ name="https" ] ip_group {111.76}
ad_cli vs vs[ name="https" ] node_pool {https}
ad_cli vs vs[ name="https" ] force_close_conn {true}
ad_cli vs vs[ name="https" ] sched_mode {HTTP_SCHED_MODE_EVERY_REQ}
ad_cli vs vs[ name="https" ] fast_tcp {false}
ad_cli vs vs[ name="https" ] ssl sess_resume_enable {false}
ad_cli vs vs[ name="https" ] ssl http_redir_enable {false}
ad_cli vs vs[ name="https" ] ssl http_port {80}
ad_cli vs vs[ name="https" ] ssl ssl_profile {gaosu_卸载} add
ad_cli vs vs[ name="https" ] auto_snat {true}
ad_cli vs vs[ name="https" ] qos_profile {}
ad_cli vs vs[ name="https" ] tcp_profile {七层虚拟服务TCP策略}
ad_cli vs vs[ name="https" ] ddos_profile {HTTP防护策略}
```

『登录限制』用于设置使用此角色登录的控制台用户是否需要限制其登录的IP地址。

勾选[启用]，启用此角色的限制IP登录。



『许可地址列表』用于设置IP地址，填入『IP地址』和『子网掩码』，点击**添加**即可设置登录IP地址。

『权限』用于分模块设置控制台角色的权限，控制模块包括『系统概况』、『报表配置』、『应用负载』、『链路配置』、『智能DNS』、『网络配置』、以及『系统配置』。

可设置的权限包括：

[无]：没有查看和编辑的权限，

[查看]：只有查看权限，没有编辑权限，

[所有]：既有查看权限也有编辑权限。

[自定义]：可自定义对各个模块的查看或者编辑权限。

配置完毕，点击**完成**，完成此角色的配置。

点击**取消**，用于取消此角色的配置。



如果是升级的设备，想要给之前的用户命令行权限，需要更改下老用户的密码。

11.3.3. 外部认证登录

『外部认证登录』用于配置 Web 控制台支持“外部认证”。可以选择 Radius、AD 域或禁用三种方式。

The screenshot shows the 'External Authentication Login' configuration interface. At the top, there are three tabs: 'User', 'Role', and 'External Authentication Login'. The 'External Authentication Login' tab is selected. Below the tabs, there is a section titled '属性' (Properties). Under 'Authentication Method', the 'Radius' option is selected. In the 'Active Directory Configuration' section, the 'Host' field is empty, 'Port' is set to 636, 'SSL Communication' is enabled, and both 'Service CA Certificate' and 'Client Certificate' dropdown menus show 'Not Enabled'. The 'Search Method' is set to 'Login Account' (selected), and the 'User Name Extension' is set to \${user}. At the bottom left is a 'Update' button.

认证方式：根据实际情况选择外部认证服务器的类型，默认禁用。

主机：服务器的 IP 地址。

端口：服务器端口。

共享密钥：“Radius 认证”时，服务器与客户端通信的“共享密钥”。

授权属性 ID：“Radius 认证”时，通过 Radius 应答所携带的指定属性(STRING 类型)，获取登陆账户的角色名称；“本地授权”则需在设备上创建用户(外部认证)并关联角色。

SSL 通讯：“AD 域认证”时，选择是否开启 SSL 通讯，默认禁用。

目录树：搜索路径的起点，非 SSL 的服务器如果获取目录树成功，可以从列表中选择。

搜索方式：配置以何种方式向服务器发起第一次绑定，默认匿名搜索。

用户名扩展：当选择搜索方式为“登录帐户”时需要配置这个字段，比如配置这个字段为\${user}@sangfor.com，则会将用户登录时的用户名替换\${user}。

DN：指系统使用这里输入的域用户来读取 LDAP 上的用户信息。需要确保这里输入的域用户具有足够的权限，例如输入 LDAP 管理员的用户。这里的用户名需要填写完整的 DN 名，一个例外是 MS Active Directory 时可以写成 user@domain 的形式。

密码：输入域用户的密码。

11.4. SMTP 服务器

『SMTP 服务器』用于设置 SMTP 服务器信息，此处 SMTP 服务器设置主要被『EMAIL 告警』和『自动生成报表』等使用。

WEBUI 路径：『系统配置』→『SMTP 服务器』。

界面如下图所示：

SMTP服务器	
+ 新建 - 删除	
<input type="checkbox"/> 名称	地址
<input type="checkbox"/> SMTP	smtp.sangfor.com
第 1 页, 共1页 每页显示条数 20	
共 1/20 条配置信息	

『SMTP 服务器列表』用于显示已经设置完成的 SMTP 服务器。

点击**删除**用于删除选中的 SMTP 服务器。

点击**新建**用于新建 SMTP 服务器。

设置界面如下：

SMTP服务器

新建

属性

名称	SMTP
SMTP主机地址	192.168.10.1
SMTP端口	25
验证用户名和密码	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
用户名：	sangfor
密码：	*****
SMTP服务器检测	测试有效性 无效！

取消 **完成**

『名称』用于定义 SMTP 服务器的名称，建议使用便于标识的文字。

『SMTP 主机地址』用于设置 SMTP 服务器的地址，此处即可填写 IP 地址也可以填写域名地址。

『SMTP 端口』用于设置 SMTP 使用的端口，默认是 25 端口。

如果 SMTP 服务器需要验证用户名密码，则需要勾选[启用]验证用户名和密码，输入『用户名』和『密码』即可。

『SMTP 服务器检测』可以辅助性检测配置的 SMTP 服务器是否有效，网络状况良好情况下，检测的准确性更高。点击**测试有效性**，开始检测。

配置完毕，点击**完成**，完成此 SMTP 服务器的配置。

点击**取消**，用于取消此 SMTP 服务器的配置。

11.5. SNMP

『SNMP』用于设置 AD 设备的 SNMP 信息，主要是用于网络管理设备通过 SNMP 协议获取 AD 设备的一些状态信息，如 CPU 占用率、内存以及网卡接口状态等。界面设置如下：



11.5.1. SNMP (V1, V2C)

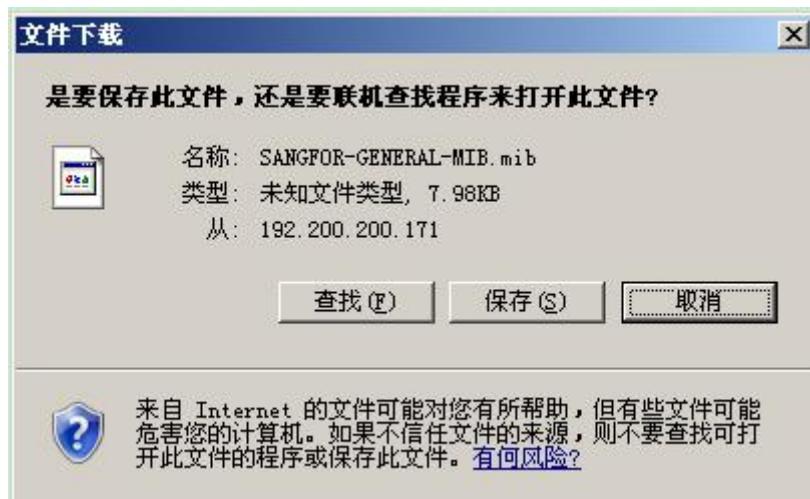
『SNMP (V1, V2C)』用于设置通过 snmp 协议的 V1 或者 V2C 版本获取设备信息的参数，界面如下：

点击**删除**，用于将已选目标条目删除。

点击**启用**，用于启用已选目标条目。

点击**禁用**，用于禁用已选目标条目。

点击**MIB库**，用于下载设备所使用的 MIB 库文件，可保存到本地 PC，界面如下：



点击**新建**，配置界面如下：

『共同体』用于设置与对端设备相同的密钥信息，该信息与对端设备设置一致。

『允许访问的 IP 来源』用于设置允许哪些 IP 地址通过 SNMP 获取到 AD 设备的信息，

此处可以选择所有 IP、单个 IP 或者网络。

『访问权限』用于设置对端设备通过 SNMP 对 AD 设备的访问权限，此处可以选择只读或者读写。

11.5.2. SNMP (V3)

『SNMP (V3)』用于其他设备通过 snmp 协议的 V3 版本获取设备信息的参数，点击 **新建**，界面如下：

The screenshot shows the configuration interface for SNMP (V3). At the top, there are three tabs: 'SNMP (V1, V2C)', 'SNMP (V3)' (which is selected), and 'Traps (V1)'. Below the tabs, there is a '新建' (New) button. The main area is divided into sections: '属性' (Properties) and '配置' (Configuration). In the '属性' section, there is a radio button for '启用' (Enable) which is selected. In the '配置' section, there are several fields:

- 用户名:** A text input field with a note: '(长度限制为1~31字符, 且不能包含& | " ' , : % < > / \ 特殊字符)'.
- 认证:** A radio button for '启用' (Enable) which is selected.
- 认证算法:** A dropdown menu showing 'MD5'.
- 密码 (认证):** An empty text input field.
- 再次输入密码 (认证):** An empty text input field.
- 加密:** A radio button for '启用' (Enable) which is selected.
- 加密算法:** A dropdown menu showing 'DES'.
- 使用认证密码:** A checkbox which is unchecked.
- 密码 (加密):** An empty text input field.
- 再次输入密码 (加密):** An empty text input field.
- 访问权限:** A dropdown menu showing '只读' (Read-only).

At the bottom of the interface are two buttons: '取消' (Cancel) and '完成' (Finish).

『用户名』用于设置本端 AD 设备的名称

『认证』用于设置是否启用认证。

『认证算法』用于设置认证算法和密码，此处需要设置与对端一致。

『加密』用于设置是否启用加密。

『加密算法』用于设置加密算法和加密密码等信息，此处需要设置与对端一致。

『访问权限』用于设置对端设备通过 SNMP 对 AD 设备的访问权限，此处可以选择只

读或者读写。

11.5.3. Traps (V1)

『Traps (V1)』用于 AD 设备主动向某个 IP 地址发送本机的状态信息，点击**新建**，界面如下：



The screenshot shows the 'Traps (V1)' configuration page. At the top, there are tabs for 'SNMP(V1,V2C)', 'SNMP(V3)', and 'Traps(V1)', with 'Traps(V1)' selected. A 'Help' button is also present. Below the tabs, there's a 'New' button. The main area has two sections: 'Properties' (属性) and 'Configuration' (配置). Under 'Properties', the 'Status' (状态) is set to 'Enabled' (启用). Under 'Configuration', there are three input fields: 'Community' (共同体), 'Target IP' (目的IP), and 'Port' (端口) with the value '162'. At the bottom are 'Cancel' (取消) and 'Finish' (完成) buttons.

『共同体』用于设置与对端设备相同的密钥信息，该信息与对端设备设置一致。

『目的 IP』设置 AD 设备主动向该 IP 发送本机的状态信息。

『端口』设置对端的监听端口。

11.6. 告警

WEBUI 路径：『系统配置』→『告警』。

『告警』是 AD 设备通过 E-MAIL、短信或者 SNMP Trap 的方式发送告警信息。

11.6.1. E-MAIL 告警

WEBUI 路径：『系统配置』→『告警』→『E-MAIL 告警』。

『E-MAIL 告警』是 AD 设备自动发送 E-mail 邮件信息告警的功能。界面如下：



勾选[启用]，启用 EMAIL 事件告警，将启用设备自动发送告警邮件的功能，

勾选[禁用]，用于禁用此邮件告警功能。

『告警触发事件』用于设置发生哪些事件时会发送告警邮件：

事件包括：

[链路故障]：每条链路断掉或者繁忙或恢复时会告警，

[虚拟服务故障]：所有链路或所有节点都断开或者恢复时会告警，

[节点故障]：某个节点断开或者恢复时会告警，

[网络攻击]：发现有不合规范的 http 请求或者无法识别洪水攻击时会告警。

[CRL 更新失败]：发现 CRL 更新失败时会告警。

[高可用性故障]：若启用了双机或者集群，当进行切换时会有告警。

[CPU 负荷百分比]: 当 AD 设备的 CPU 使用率超过设定比例时进行告警。

[内存占用]: 当 AD 设备的内存使用率超过设定比例时进行告警。

[磁盘占用]: 当 AD 设备的磁盘使用率超过设定比例时进行告警。

[系统连接数]: 当 AD 设备的全局连接数超过设定的上限时进行告警。

[虚拟服务连接数]: 当 AD 设备的虚拟服务连接数超过设定的上限时进行告警。

[日志匹配]: 当 AD 设备上有匹配上设置的日志时进行告警。

『SMTP 服务器』用于设置发送告警邮件使用的 SMTP 服务器，SMTP 服务器的设置请参见 10.4 章节『SMTP 服务器』的相关说明，点击按钮“+”也可跳转到新增服务器页面，用于新增 SMTP 服务器。

『邮件标题』用于设置发送告警邮件的邮件标题。

『收件人』用于设置告警邮件的接收邮箱。

『发件人』用于设置告警邮件的发送邮箱，一般需要使用已选的 SMTP 服务器对应的邮箱。

点击 **更新** 完成此配置。

『邮件发送频率』用于自定义邮件发送频率时间。

11.6.2. 短信告警

WEBUI 路径：『系统配置』→『告警』→『短信告警』。

『短信告警』是 AD 设备自动发送手机短信告警的功能。界面如下：



The screenshot shows the configuration interface for SMS alerts. At the top, there are three tabs: E-MAIL告警 (Email Alert), 短信告警 (SMS Alert), and SNMP Trap告警 (SNMP Trap Alert). The current tab is 短信告警 (SMS Alert).

配置短信告警

基本配置

短信告警: 启用 (Selected) | 禁用

告警触发事件:

- 链路故障
- 节点故障
- 虚拟服务故障
- 日志匹配
- 网络攻击
- CRL更新失败
- 高可用性故障

CPU负载超限: 80 % | 系统连接超限: 80000 条 | 内存占用超限: 90 % | 虚拟服务连接超限: 240000 条 | 磁盘占用超限: 90 %

短信模块: 内置 (Selected) | 外置

接收方: (最多可以添加20个接收方手机号码)

短信网关配置

发送方式: GSM短信猫

SMSC号码: (Input field)

波特率: 115200

勾选启用[短信告警]，将启用设备自动发送手机短信的功能。

勾选禁用[短信告警]，将禁用设备自动发送手机短信的功能。

『告警触发事件』用于设置发生哪些事件时会发送告警短信：

事件包括：

[链路故障]: 每条链路断掉或者繁忙或恢复时会告警，

[虚拟服务故障]: 所有链路或所有节点都断开或者恢复时会告警，

[节点故障]: 某个节点断开或者恢复时会告警，

[网络攻击]: 发现有不合规范的 http 请求或者无法识别洪水攻击时会告警。

[CRL 更新失败]: 发现 CRL 更新失败时会告警。

[高可用性故障]: 若启用了双机或者集群，当进行切换时会有告警。

[CPU 负荷百分比]: 当 AD 设备的 CPU 使用率超过设定比例时进行告警。

[内存占用]: 当 AD 设备的内存使用率超过设定比例时进行告警。

[磁盘占用]: 当 AD 设备的磁盘使用率超过设定比例时进行告警。

[系统连接数]: 当 AD 设备的全局连接数超过设定的上限时进行告警。

[虚拟服务连接数]: 当 AD 设备的虚拟服务连接数超过设定的上限时进行告警。

[日志匹配]: 当 AD 设备上有匹配上设置的日志时进行告警。

『短信模块』使用内置或者外置的短信模块来发送短信。如果选择[内置]，则必须在 AD 设备上接短信猫设备；如果选择[外置]，则 AD 设备必须连接短信网关设备。

如果短信模块选择[外置]，还需要配置短信中心的地址和端口，配置页面如下：



『接收方』填写接收告警短信的手机号码。

『发送方式』可以选择 GSM 短信猫，中国移动 V2，中国移动 V3 和中国联通。

如果发送方式选择[GSM 短信猫]，则还需要配置 SMSC 号码和波特率；如果发送方式选择为[中国移动 V2]，[中国移动 V3]和[中国联通]，则还需要配置如下参数：

[网关服务器地址]填写短信网关服务器的 IP 地址。

[网关服务器端口]填写短信网关服务器的端口。

[企业代码] 按照短信服务提供商提供的相关参数填写。

[业务代码]按照短信服务提供商提供的相关参数填写。

[SP 接入号]按照短信服务提供商提供的相关参数填写。

[网关编号]按照短信服务提供商提供的相关参数填写。

[登录账号]按照短信服务提供商提供的相关参数填写。

[登录口令]按照短信服务提供商提供的相关参数填写。

[确认口令]按照短信服务提供商提供的相关参数填写。



说明：外置短信猫不支持电信 4G。

11.6.3. SNMP Trap 告警

WEBUI 路径：『系统配置』→『告警』→『SNMP Trap 告警』。

『SNMP Trap 告警』是 AD 设备通过 SNMP Trap 来发送告警日志，界面如下：



The screenshot shows the 'SNMP Trap 告警' configuration page. At the top, there are three tabs: 'E-MAIL告警', '短信告警', and 'SNMP Trap告警'. The 'SNMP Trap告警' tab is selected. Below the tabs, there's a title '配置SNMP Trap告警'. The main area is divided into sections:

- 基本配置**:
 - SNMP Trap告警: A radio button group with '启用' (Enabled) selected.
 - 告警触发事件: A list of checkboxes including '链路故障', '节点故障', '虚拟服务故障', '日志匹配', '网络攻击', 'CRL更新失败', '高可用性故障', 'CPU负荷超', '内存占用超', '磁盘占用超', '系统连接超', and '虚拟服务连接超'. Most checkboxes have percentage values next to them: 80%, 90%, 90%, 800000, 90%, 90%, and 240000.
- 告警频率**: A section with a '频率' input field containing '6' and a dropdown menu showing '时'.

At the bottom left is a '更新' (Update) button.

勾选启用[SNMP Trap 告警]，将启用设备通过 SNMP Trap 发送手机告警的功能。

勾选禁用[短信告警]，将禁用设备通过 SNMP Trap 发送手机告警的功能。

『告警触发事件』用于设置发生哪些事件时会发送告警短信。

事件包括：

[链路故障]：每条链路断掉或者繁忙或恢复时会告警，

[虚拟服务故障]：所有链路或所有节点都断开或者恢复时会告警，

[节点故障]：某个节点断开或者恢复时会告警，

[网络攻击]：发现有不合规范的 http 请求或者无法识别洪水攻击时会告警。

[CRL 更新失败]：发现 CRL 更新失败时会告警。

[高可用性故障]：若启用了双机或者集群，当进行切换时会有告警。

[CPU 负荷百分比]：当 AD 设备的 CPU 使用率超过设定比例时进行告警。

[内存占用]：当 AD 设备的内存使用率超过设定比例时进行告警。

[磁盘占用]：当 AD 设备的磁盘使用率超过设定比例时进行告警。

[系统连接数]：当 AD 设备的全局连接数超过设定的上限时进行告警。

[虚拟服务连接数]：当 AD 设备的虚拟服务连接数超过设定的上限时进行告警。

[日志匹配]：当 AD 设备上有匹配上设置的日志时进行告警。

11.7. 日志设置

WEBUI 路径：『系统配置』→『日志设置』。

『日志设置』包括 HTTP 日志、Syslog 设置、NAT 日志服务器。



11.7.1. HTTP 日志

WEBUI 路径：『系统配置』→『日志设置』→『HTTP 日志』。

『HTTP 日志』可以自定义虚拟服务的日志变量，通过 Syslog 服务器发送。

界面如下图所示：

+新建		
日志名称	虚拟服务名称	自定义日志头部
cms	www.cms.com	[\$client_ip]:[\$client_port][\$method][\$time]\$...

点击**新建**，如下图所示：



新建

属性

HTTP日志名称: cms

虚拟服务名称: www.cms.com

自定义日志头部: \${method}
[\$client_ip]:[\$client_port]
[\$method][\$time]\$method

取消 完成

『HTTP 日志名称』设置 HTTP 日志名称。

『虚拟服务名称』选择 HTTP 或者 HTTPS 类型的虚拟服务，一个虚拟服务只能被添加一次。

『自定义日志头部』选择日志的变量，点击下拉框，显示如下类型：



如下是各字段的说明：

自定义字段	字段解释	自定义字段	字段解释
`\${client_ip}`	客户端 IP	`\${rs_ip}`	服务器端 IP
`\${client_port}`	客户端端口号	`\${rs_port}`	服务器端口号
`\${vip}`	虚拟服务 IP	`\${user_agent}`	浏览器版本信息
`\${vport}`	虚拟服务端口号	`\${method}`	请求方法
`\${uri}`	请求 URL	`\${time}`	请求时间
`\${host}`	请求 host		

11.7.2. Syslog 设置

WEBUI 路径：『系统配置』→『日志设置』→『Syslog 设置』。

『Syslog 设置』用来设置将设备的日志发送给设定的 Syslog 服务器。

支持 2 个 syslog 服务器，可同时发送日志，界面如下图所示：



『状态』用于开启将日志发送给 Syslog 服务器。

『IP 地址』用于填写 Syslog 服务器的 IP 地址。

『端口』用于填写 Syslog 服务器的服务端口。

『编码格式』用于定义日志的编码格式，可以选择 UTF-8、GBK、GB2312。客户可根据实际需求进行选择，避免乱码问题。

『日志设备设置』用于设置将信息日志、告警日志、错误日志、SSL 日志、管理日志、HTTP 日志、NAT 日志打上对应的标记，发送给 Syslog 服务器，这样的目的是可以在 Syslog 服务器上根据不同的标记做分类。LACAL0 到 LOCAL7 代表标记，无论选择哪种都会发送到 Syslog 服务器，NONE 则表示不发送到 Syslog 服务器。

系统配置-日志设置-Syslog 设置中状态设为“启用”，配置 HTTP 日志：

『HTTP 日志』可以自定义虚拟服务的日志变量，通过 Syslog 服务器发送。

界面如下图所示：

+ 新建 × 删除		
<input type="checkbox"/>	日志名称	虚拟服务名称
<input type="checkbox"/>	cms	www.cms.com [\$(client_ip):\$(client_port)][\$(method)][\$(time)]\$...

点击新建，如下图所示：



The screenshot shows the 'Syslog Settings' configuration page. At the top, there are three tabs: 'HTTP日志' (selected), 'Syslog设置' (current tab), and 'NAT日志服务器'. Below the tabs, there is a '更新Syslog设置' (Update Syslog Settings) button. The main area is divided into sections: '属性' (Properties), '日志编码' (Log Encoding), and '日志设备设置' (Log Device Settings). In the '属性' section, '状态' is set to '启用' (Enabled). In the '日志编码' section, '编码格式' is set to 'UTF-8'. In the '日志设备设置' section, various log levels have their device settings changed from 'NONE' to 'LOCAL0'. A '更新' (Update) button is located at the bottom left.

HTTP日志 | Syslog设置 | NAT日志服务器

新建

属性

HTTP日志名称:

虚拟服务名称:

自定义日志头部:

`[$client_ip]:{$client_port}
[$method] [$time]`

『HTTP 日志名称』设置 HTTP 日志名称。

『虚拟服务名称』选择 HTTP 或者 HTTPS 类型的虚拟服务，一个虚拟服务只能被添加一次。

『自定义日志头部』选择日志的变量，点击下拉框，显示如下类型：



如下是各字段的说明：

自定义字段	字段解释	自定义字段	字段解释
`\${client_ip}`	客户端 IP	`\${rs_ip}`	服务器端 IP
`\${client_port}`	客户端端口号	`\${rs_port}`	服务器端口号

<code> \${ vip }</code>	虚拟服务 IP	<code> \${ user_agent }</code>	浏览器版本信息
<code> \${ vport }</code>	虚拟服务端口号	<code> \${ method }</code>	请求方法
<code> \${ uri }</code>	请求 URL	<code> \${ time }</code>	请求时间
<code> \${ host }</code>	请求 host		

11.7.3. NAT 日志服务器

WEBUI 路径：『系统配置』→『日志设置』→『NAT 日志服务器』。

『NAT 日志服务器』用来设置将设备更新 NAT 日志导出。

界面如下图所示：

The screenshot shows the 'NAT Log Server' configuration page. At the top, there are three tabs: 'HTTP 日志' (disabled), 'Syslog 设置' (disabled), and 'NAT 日志服务器' (enabled). Below the tabs, the page title is '更新NAT日志导出'. Under the title, there is a section titled '属性' (Properties) with the following fields:

状态	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
IP地址	<input type="text"/>	
FTP端口	21	
用户名	admin	
密码	*****	
路径	/	

At the bottom left of the form is a blue '更新' (Update) button.

『状态』用于开启将日志发送给 NAT 服务器。

『IP 地址』用于填写 NAT 服务器的 IP 地址。

『FTP 端口』用于填写 NAT 服务器的服务端口。

『用户名』用于填写 NAT 服务器的用户名。

『密码』用于填写NAT服务器的密码。

『路径』用于填写NAT服务器的路径。

11.8. 系统更新

11.8.1. 系统升级

『系统升级』可以直接在页面上对设备进行升级。

界面如下图所示：



点击[查看升级历史](#)，可以查看设备的升级历史。



11.8.2. 系统回滚

『系统回滚』支持页面直接回滚升级包即降级。

界面如下图所示：



当在系统回滚页面能看到当前回滚包时，说明可回滚，点击回滚数分钟后刷新即可。

11.8.3. 系统安全

『系统安全』可以配置系统自动更新和隐私的相关选项。

界面如下图所示：



『系统自动更新』选择[启用]则系统会自动下载并安装从深信服科技有限公司网站上公布的补丁；选择[禁用]则系统不会自动下载补丁。

『系统隐私』可以设置是否发送系统质量报告给深信服科技有限公司。

11.8.4. 代理设置

『代理设置』当使用代理服务器时，请确认其支持 HTTP 和 HTTPS，启用以后，系统将用他来获取配置的更新。。

界面如下图所示：



系统安全 代理设置

启用代理服务器

IP地址:

端口:

验证用户

用户名:

密码:

『启用代理服务器』：当使用代理服务器时，请确认其支持 HTTP 和 HTTPS，启用以后，系统将用它来获取更新。

『IP 地址』：代理设置的 IP 地址（支持 IPv4 地址）

『端口』：代理设置的端口（端口范围 1~65535）

『验证用户』：如果您的代理服务器需要身份验证，可以开启用户验证。



深信服，让IT更简单，更安全，更有价值

『用户名』：代理服务器的用户名

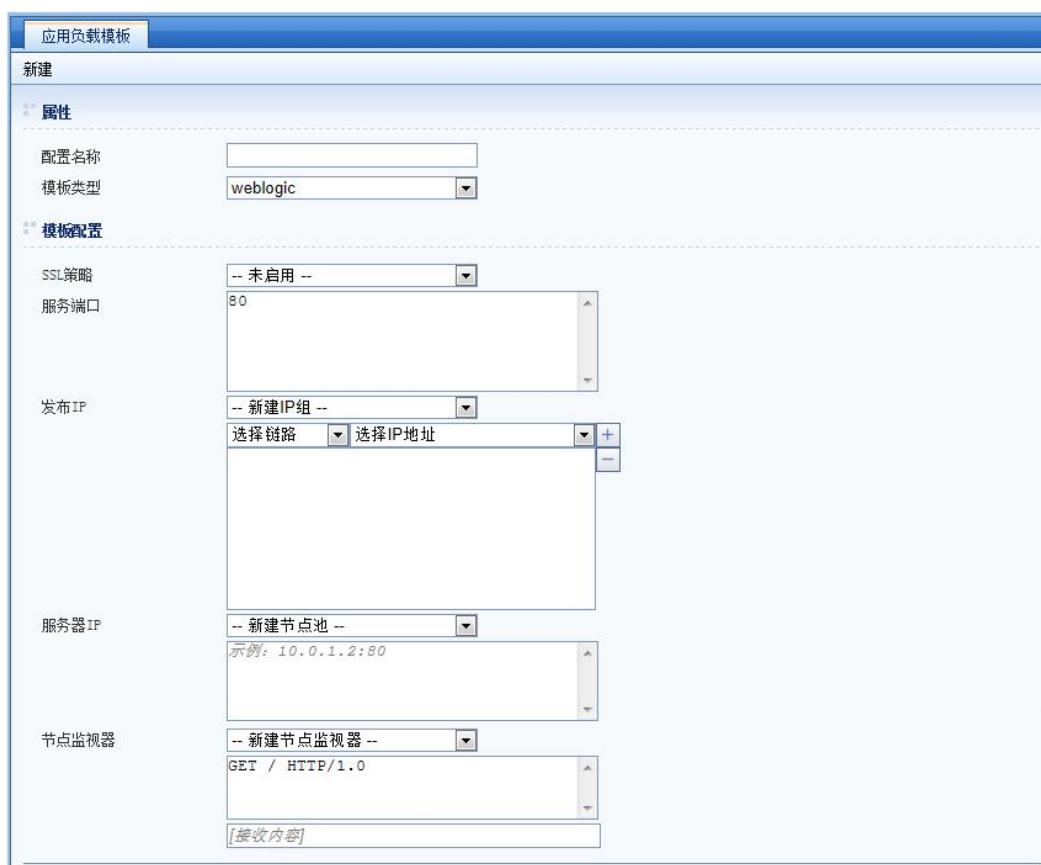
『密码』：代理服务器的密码

第 12 章 配置向导

通过向导的方式，分步骤快速配置应用负载和智能路由。

12.1. 应用负载模板

通过模板方式，快速配置应用负载。



12.2. 智能路由向导

通过向导的方式，分步骤快速配置智能路由。

向导第一步：配置链路信息

选择各个链路所对应的 ISP 地址段。

界面如下图所示：



为每条链路选定一个 ISP 地址段，标识这条链路对应的运营商。

点击 **下一步**，则进入下一个配置步骤。

向导第二步：配置选路策略

配置上网数据的选路策略。

界面如下图所示：



点击 **上一步**，可返回上一个配置步骤。

点击**下一步**，则进入下一个配置步骤。

向导第三步：配置策略名称

配置出站策略的名称。

界面如下图所示：



『出站策略名称』可以输入便于记忆和识别的字符串，用于标识智能路由。

点击**上一步**，可返回上一个配置步骤。

点击**完成**，则保存智能路由配置向导中的所有配置。

界面如下图所示：



如图所示，根据我们配置的选路策略，AD设备自动添加了两个策略来实现。

点击[返回向导首页](#)，可返回配置向导的首页。

点击[智能路由管理](#)，可链接到『链路负载』→『智能路由』页面。

界面如下图所示：



智能路由		出站高级配置		路由测试			
+ 新建		X 删除		✓ 启用	✗ 禁用	导入	导出
名称	源IP	目的IP	协议	使用链路	生效时间	操作	
智能路由_0	所有	电信	ALL	电信	全天		
智能路由_1	所有	联通（原网通）	ALL	网通	全天		
Default	所有	所有	ALL	电信,网通	全天		

第 13 章 高可用性

可对多台 AD 设备设置主备或者集群的工作方式，避免出现单点故障，对用户的网络和应用造成影响。

13.1. 模式

『模式』选择主备、高可用集群、高性能集群三种工作方式。设备出厂是主备的模式。

『主备模式』用于两台 AD 做主备的环境。主备模式下，正常情况下只有主机一台设备工作，备机处于监听状态；网络发生异常时，备机自动切换成主机接替工作，保障用户的网络不受影响。



该模式支持单台设备的所有功能。

『高可用集群模式』该模式下，可以将最多 16 台设备组建成集群的方式部署，一个服务只运行于一台设备之上，提供服务的这台设备即为这个服务的主设备，集群会另外选出一台设备作为该服务的备设备，当主设备故障时，备设备切换为主设备，继续提供该服务。多个服务可以分别运行在不同的设备之上，并互相作为备份。

模式

选择模式

主备模式

高可用集群模式

高性能集群模式

完成

高可用集群模式

该模式下，可以将最多16台设备组建成集群的方式部署，一个服务只运行于一台设备之上，提供服务的这台设备即为这个服务的主设备，集群会另外选出一台设备作为该服务的备设备，当主设备故障时，备设备切换为主设备，继续提供该服务。多个服务可以分别运行在不同的设备之上，并互相作为备份。

该模式工作于服务器负载场景，不支持链路负载。

『高性能集群模式』该模式下，可以将最多 8 台设备组建成集群方式部署，通过在与集群业务口相连的交换机上配置链路聚合，一个服务的数据会被分发给集群中的每台设备，这些设备都能接收并处理该服务的数据，从而达到性能提升的效果。当集群中有设备因故障退出集群或重新加入集群时，都可保证流量在设备间均衡分配，业务不会中断。

选择模式

主备模式

高可用集群模式

高性能集群模式

完成

该模式下，可以将最多8台设备组建成集群方式部署，通过在与集群业务口相连的交换机上配置链路聚合，一个服务的数据会被分发给集群中的每台设备，这些设备都能接收并处理该服务的数据，从而达到性能提升的效果。当集群中有设备因故障退出集群或重新加入集群时，都可保证流量在设备间均衡分配，业务不会中断。

该模式工作于服务器负载场景，不支持链路负载、IPv6、SSL 会话复用、动态路由功能。

13.2. 主备模式

『主备模式』路径：『高可用性』→『模式』→『主备模式』。

需选择『主备模式』后才能配置双机维护功能，界面如下图所示：



点击『完成』，进行模式切换。需重启设备，重新登录控制台。

13.2.1. 主备

『主备』设置双机热备功能。界面如下图所示：



『名称』自定义设备的名称，方便区分当前哪台设备处于主模式。

『状态』中[启用]用来启用双机，[禁用]用来禁用双机。

『超时时间』当在超时时间内备机一直无法收到主机发送的心跳包，则认为主机超时，备机主动切换成主机。

『通信介质』选择连接双机的接口，可以用串口和空闲的网口。选择网口后，需要为该网口配置一个IP地址，只要不与正在使用的IP地址冲突即可。建议选择网口作为通信介质，通过网口来做双机切换比串口切换花费的时间短。通信介质选择网口，则可以实现会话同步。

『MAC同步』用于设置双机切换是否同步MAC地址。

『同步网口列表』用于设置切换双机的时候同步哪些接口的MAC地址，需要开启MAC同步才会显示该选项。

『通信介质故障检测』通过网络数据包来检测对端是否存在，避免两台设备成为主机导致IP冲突。两台设备的通信介质故障检测网口需要接到同一个广播域，可以选择已经使用的网口，也可以选择空闲网口，选择空闲网口需要设置IP地址。

『启用备机交换网口』可以很好的控制交换网口开启与关闭。

『同步配置』点击向备机同步配置。

『故障切换』用于设置双机切换条件，符合此处设置的条件则进行主备切换，界面如下：



『状态』用于设置是否启用双机故障切换检测，『检测类型』分为『掉线检测』、『ARP 检测』、『健康检查』3 种，设置后点击【添加】可以组合使用多种检测方法，【删除】可以取消选中的检测方法。

『掉线检测』当检测到网口物理状态不正常则进行切换。

『ARP 检测』AD 设备向选择的接口发送 ARP 广播，如果监视主机里填写的 IP 地址有回应 ARP，则判断正常。该监视主机地址需要填写与 AD 设备接口同一网段的地址。界面如下：



『健康检查』通过网络接口处设置的链路健康检查机制来检测，当选择健康检查后，只

有启用了链路健康检查的链路才可选，界面如下：



『主备状态』分为“主机”、“备机”，可通过右边的切换按钮进行主备切换。界面如下：



『升级模式』升级模式在有升级需要时才手动启用，启用时不会发生主备切换，并且不会同步配置。请在客服的指导下进行升级。

『服务状态』显示目前双机状态。

『最近一次切换时间』显示最近一次发生主备切换的时间。

『最近一次同步配置时间』显示最近一次向备机同步配置的时间，可通过右边的同步配置按钮重新同步配置。

13.3. 集群模式

『集群模式』分为『高可用集群模式』和『高性能集群模式』两种。

13.3.1. 高可用集群模式

『高可用集群模式』路径：『高可用性』 → 『模式』 → 『高可用集群模式』。

需选择『高可用集群模式』后才能配置高可用集群维护功能，界面如下图所示：



点击『完成』，进行模式切换。需重新登录控制台。

13.3.1.1. 集群

『集群』路径：『高可用性』 → 『集群』。

『集群』用于启用和设置集群，如下图所示：

系统导航菜单

- ▶ 系统概况
- ▶ 报表配置
- ▶ 公共对象
- ▶ 应用负载
- ▶ 智能DNS
- ▶ 路由配置
- ▶ 网络配置
- ▶ 系统配置
- ▶ 配置向导
- ▶ 高可用性
 - ▶ 模式
 - ▶ 集群
 - ▶ 成员管理
 - ▶ 应用组管理

集群维护

集群维护

设备集群状态

状态 启用 禁用

动作 加入集群 创建集群

集群管理IP

本地设备配置

设备管理IP

HA网口

IP地址

掩码

密钥

再次输入密钥

『状态』开启或者禁用设备的集群功能。

『动作』可选择加入集群或者创建集群。第一台配置集群的设备必须创建集群，其余的设备才能加入集群。选择[创建集群]，界面如下所示：

设备集群状态

状态 启用 禁用

动作 加入集群 创建集群

本地设备配置

设备管理IP

HA网口

IP地址

掩码

密钥

再次输入密钥

集群配置

集群名称

集群管理IP

子网掩码

HA网口

密钥

心跳检测时间 毫秒

心跳间隔时间 毫秒

集群远程维护 启用 禁用

连接客户端检测 启用 禁用

网络接口

『设备管理 IP』本设备管理口（MANAGE 口）的 IP 地址，用于主控设备通过管理口发送心跳和管理其余设备。

『HA 网口』用于集群设备发送心跳，同步会话和连接跟踪的网口。HA 网口必须一致，才能加入集群。

[IP 地址]和[掩码]设置 HA 网口的 IP 地址和掩码，集群设备的 HA 网口的 IP 地址必须在同一网段。HA 的 IP 地址不能和其他网口的 IP 地址在同网段。

『密钥』用于集群设备的身份校验，必须输入相同的密钥，才能加入集群。

『集群名称』自定义集群的名称。

『集群管理 IP』用来管理和配置集群，登陆集群控制中心。设备加入集群后，只能通过集群管理 IP 来配置设备。

『子网掩码』设置集群管理 IP 的掩码。

『心跳超时时间』设置集群设备心跳包的超时时间。超过时间未收到心跳包则判断为故障，进行切换。

『心跳间隔时间』设置发送心跳包的间隔时间。

『集群远程维护』开启后，可通过维护 IP 登陆该设备，配置如下图所示：

集群远程维护	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
维护 IP	10.0.0.4	
使用互联网IP	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
互联网IP	202.96.128.6	
管理端口	443	
报表端口	85	

『维护 IP』填入设备 WAN 口的浮动 IP 地址。

『使用互联网 IP』启用互联网 IP 后，可通过互联网 IP 登陆设备。

『互联网 IP』填入 WAN 口的互联网 IP 地址。

『管理端口』登陆控制台的端口。

『报表端口』登陆报表中心的端口。

点击更新后，保存和生效配置，如下图所示：



The screenshot shows the 'Cluster Maintenance' interface. Under 'Device Cluster Status', the 'Status' is set to 'Enabled' (启用) and the 'Action' is 'Log in to Cluster' (登陆集群). Under 'Local Device Configuration', the 'Management IP' is 10.252.252.74/24, the 'HA Interface' is NET1, and the 'IP Address' is 123.0.0.74 with a 'Mask' of 24. The 'Cluster Configuration' section shows the 'Cluster Name' as sangfor, 'Management IP' as 10.252.252.77, and the 'Subnet Mask' as 24. A 'More Advanced Configuration' link is also present. At the bottom left is a 'Update' button.

『启用通信介质检测』可以防止集群内各节点间的心跳出现故障时而带来的灾害，点击启动后，选择网络接口。

若动作选择加入集群，界面如下图所示：

集群维护

集群维护

设备集群状态

状态	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
动作	<input checked="" type="radio"/> 加入集群	<input type="radio"/> 创建集群
集群管理IP	10.252.252.77	

本地设备配置

设备管理IP	10.252.252.75/24
HA网口	NET1
IP地址	123.0.0.75
掩码	24
密钥	*****
再次输入密钥	*****

更新

『集群管理 IP』填入创建集群时设置的集群管理 IP 地址，只支持 IPV4 地址及掩码。

『设备管理 IP』选择设备管理口的 IP 地址，只支持 IPV4 地址及掩码。

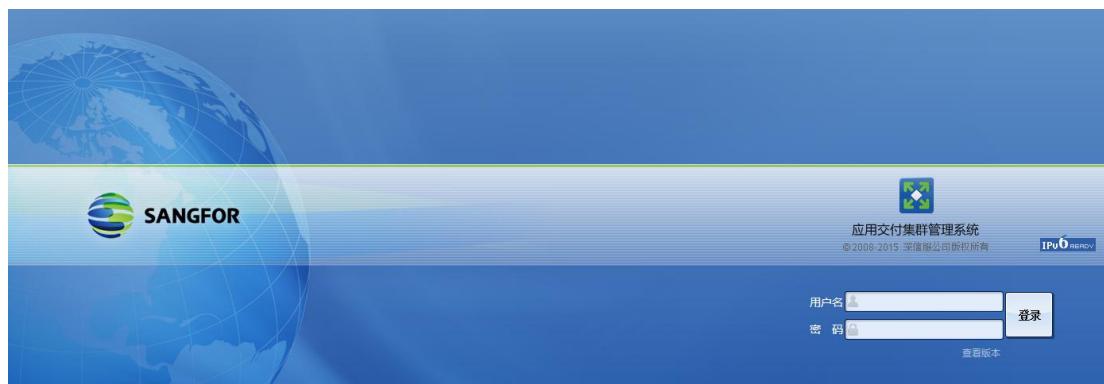
『HA 网口』选择与其他集群设备相同的 HA 网口，只支持 IPV4 地址及掩码。

[IP 地址]和[掩码]设置 HA 网口的 IP 地址和掩码，需与其他集群设备的 HA 网口地址在相同的网段。

『密钥』输入加入集群的密钥。

点击更新后，保存和生效配置。

点击 **登陆集群**，可跳转到集群管理系统的登陆页面，如下图所示：



集群管理系统默认的账号密码是“cluster”，加入集群后只能通过集群管理系统对设备进行配置。

通过集群管理 IP 登录设备，集群状态如下图：



集群状态：包括禁用、加入集群、创建集群。若想组建一个集群，先进入第一台设备，选择创建集群，然后在成员管理页面，将其他设备加入到集群中，其他各台设备选择加入集群。

『设备管理 IP』设备管理口上的 IP 地址，用于集群控制连接的建立，和设备间的心跳监视。

『HA 网口』设备的一个物理接口(可使用聚合口)，并需配置 IP 地址，用于数据连接的建立，和设备间的心跳监视。

『密钥』用于集群认证和传输加密，所有设备必须有相同的密钥，才能组建集群。

『集群名称』集群的名称，用于标识一个集群。

『集群管理 IP』用于管理整个集群的 IP 地址，用该 IP 可登录到集群管理界面。

『心跳超时时间』集群中的设备，如果在超时时间内收不到其他设备的心跳，就认为其他设备已离线，然后接替该设备的工作。

『心跳间隔时间』集群中的设备每隔一个间隔时间，广播心跳包给集群中的其他设备。

『集群远程维护』启用集群远程维护时，用户可以通过远程维护IP地址登录集群控制台或各台设备的控制台进行管理。

『通信介质检测』启用通信介质检测，可以防止集群内各节点间的心跳出现故障时而带来的灾害（当启用通信介质检测时，如若修改了业务口，需要同步修改业务口引用的物理口）。

13.3.1.2. 成员管理

『成员管理』路径：『高可用性』→『成员管理』。



名称	管理IP	角色	健康状态	管理状态	跳转
A	10.252.252.74	主控	在线	启用	
B	10.252.252.75	备控	在线	启用	

点击**添加**，新建成员。



新设备

属性

名称 (长度限制为1~63字符，且不能包含& | “ ‘ ’ : % < > / \ 特殊字符)

配置

设备管理IP

设备信息

HA口IP 未知

取消 完成

『名称』要加入集群的名称。

『设备管理 IP』用来管理和配置集群，登陆集群控制中心。设备加入集群后，只能通过集群管理 IP 来配置设备。

13.3.1.3. 应用组管理

『应用组管理』路径：『高可用性』→『应用组管理』。



应用组管理					
+ 新建		- 删除		刷新时间间隔: 5秒	
<input type="checkbox"/>	名称	默认设备	生效设备	备份设备	会话同步状态
	Default		ad.sangfor.com	ad2.sangfor.com	同步完成
<input type="checkbox"/>	Group-11	ad.sangfor.com	ad.sangfor.com	ad2.sangfor.com	同步完成
<input type="checkbox"/>	Group-12	ad2.sangfor.com	ad2.sangfor.com	ad.sangfor.com	同步完成

点击**新建**，新建应用组。

『名称』：一个应用组的名称，用于标识一个应用组。

『会话同步』：若开启，该应用组的生效设备会同步会话到备份设备之上，如果生效设备故障，备份设备成为生效设备，可保证原有连接不中断。

『默认设备』：若选择一个默认设备，这个默认设备具有最高的优先级被选举为生效设备。

『抢占模式』：若开启了抢占模式，该应用组的默认设备如果健康，会主动成为生效设备，而使原生效设备成为应用组的备份设备。

『故障检测』：选择与应用组关联的链路，如果一台设备的关联链路故障，若该设备是生效设备，则发生故障切换，应用组会切换到其他设备上，若该设备不是生效设备，则应用组生效设备故障时，该设备不具有成为应用组生效设备的能力。

『虚拟 MAC』：若为应用组在某条链路上配置一个虚拟 MAC 地址，应用组在该链路上的所有 IP 地址，都用这个伪装的 MAC 与外部通讯，如果发生了故障切换，新的生效设备能够继续使用这个伪装 MAC 与外部通讯。

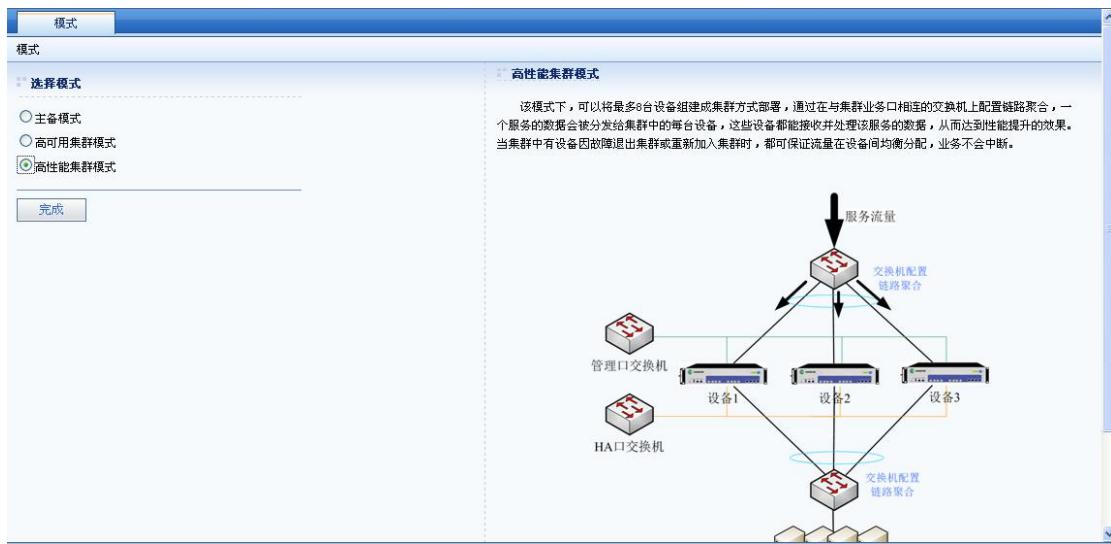
『权重』：若应用组在某台设备上生效，则该设备的负载会根据应用组的权重相应增加，当应用组在集群中切换时，会根据设备的负载状况选择设备。

『应用组关联信息』：该应用组包含的一组配置，包括浮动 IP、虚拟服务、NAT 规则。这些配置使该应用组具有发布服务的能力。

13.3.2. 高性能集群模式

『高性能集群模式』路径：『高可用性』→『模式』→『高性能集群模式』。

需选择『高性能集群模式』后才能配置高性能集群维护功能，界面如下图所示：



点击『完成』，进行模式切换。需重新登录控制台。

13.3.2.1. 集群

『集群』路径：『高可用性』→『模式』→『集群』。

『集群』包括集群维护和网络检测两个部分，用于启用和设置集群，如下图所示：

系统导航菜单

- ▶ 系统概况
- ▶ 报表配置
- ▶ 公共对象
- ▶ 应用负载
- ▶ 智能DNS
- ▶ 路由配置
- ▶ 网络配置
- ▶ 系统配置
- ▶ 配置向导
- ▼ 高可用性
 - ▶ 模式
 - ▶ 集群
 - ▶ 成员管理

集群维护

集群维护

设备集群状态

状态 启用 禁用

动作 加入集群 创建集群

本地设备配置

设备管理IP: 172.16.200.111/24

HA网口:

IP地址:

掩码: admin

密钥: *****

再次输入密钥:

集群配置

集群名称:

集群管理IP:

子网掩码: 24

高级配置

心跳超时时间: 2000 毫秒

心跳间隔时间: 200 毫秒

『状态』开启或者禁用设备的集群功能。

『动作』可选择加入集群或者创建集群。第一台配置集群的设备必须创建集群，其余的设备才能加入集群。选择[创建集群]，界面如下所示：

状态 启用 禁用

动作 加入集群 创建集群

本地设备配置

设备管理IP: 172.16.200.111/24

HA网口: IP地址: []
掩码: admin

密钥: [*****]
再次输入密钥: []

集群配置

集群名称: []

集群管理IP: []

子网掩码: 24

高级配置

心跳超时时间: 2000 毫秒
心跳间隔时间: 200 毫秒

会话同步: 启用 禁用
集群远程维护: 启用 禁用

维护IP: []
使用互联网IP: 启用 禁用
互联网IP: []
管理端口: 443
报表端口: 85

更新

『设备管理 IP』本设备管理口（MANAGE 口）的 IP 地址，用于主控设备通过管理口发送心跳和管理其余设备。

『HA 网口』用于集群设备发送心跳，同步会话和连接跟踪的网口。HA 网口必须一致，才能加入集群。

[IP 地址]和[掩码]设置 HA 网口的 IP 地址和掩码，集群设备的 HA 网口的 IP 地址必须在同一网段。HA 的 IP 地址不能和其他网口的 IP 地址在同网段。

『密钥』用于集群设备的身份校验，必须输入相同的密钥，才能加入集群。

『集群名称』自定义集群的名称。

『集群管理IP』用来管理和配置集群，登陆集群控制中心。设备加入集群后，只能通过集群管理IP来配置设备。

『子网掩码』设置集群管理IP的掩码。

『心跳超时时间』设置集群设备心跳包的超时时间。超过时间未收到心跳包则判断为故障，进行切换。

『心跳间隔时间』设置发送心跳包的间隔时间。

『会话同步』若开启，集群中的设备会相互同步会话。若有设备发生故障，可保证原有连接不中断。

『集群远程维护』开启后，可通过维护IP登陆该设备，配置如下图所示：



『维护IP』填入设备WAN口的浮动IP地址。

『使用互联网IP』启用互联网IP后，可通过互联网IP登陆设备。

『互联网IP』填入WAN口的互联网IP地址。

『管理端口』登陆控制台的端口。

『报表端口』登陆报表中心的端口。

点击【更新】后，保存和生效配置，如下图所示：

集群维护

集群维护

设备集群状态

状态 启用 禁用

动作 [登陆集群](#)

本地设备配置

设备管理IP: 10.252.252.74/24

HA网口: NET1

IP地址: 123.0.0.74

掩码: 24

密钥: [REDACTED]

集群配置

集群名称: sangfor

集群管理IP: 10.252.252.77

子网掩码: 24

[>>高级配置](#)

[更新](#)

若动作选择加入集群，界面如下图所示：

集群维护

集群维护

设备集群状态

状态 启用 禁用

动作 加入集群 创建集群

集群管理IP: 10.252.252.77

本地设备配置

设备管理IP: 10.252.252.75/24

HA网口: NET1

IP地址: 123.0.0.75

掩码: 24

密钥: [REDACTED]

再次输入密钥: [REDACTED]

[更新](#)

『集群管理 IP』填入创建集群时设置的集群管理 IP 地址，只支持 IPV4 地址及掩码。

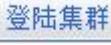
『设备管理 IP』选择设备管理口的 IP 地址，只支持 IPV4 地址及掩码。

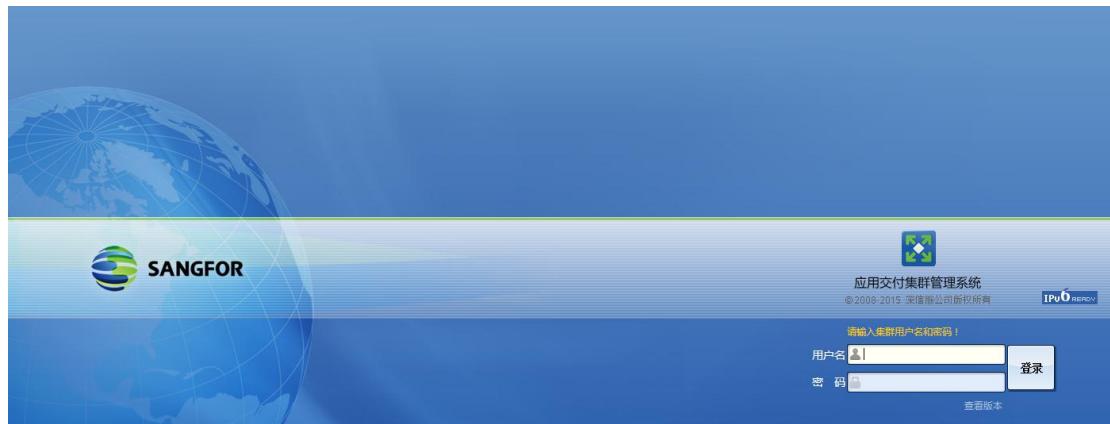
『HA 网口』选择与其他集群设备相同的 HA 网口，只支持 IPV4 地址及掩码。

[IP 地址]和[掩码]设置 HA 网口的 IP 地址和掩码，需与其他集群设备的 HA 网口地址在相同的网段。

『密钥』输入加入集群的密钥。

点击更新后，保存和生效配置。

点击 ，可跳转到集群管理系统的登陆页面，如下图所示：



集群管理系统的账号密码是“cluster”，加入集群后只能通过集群管理系统对设备进行配置。

通过集群管理 IP 登录设备，集群状态如下图：

The screenshot shows the Sangfor Cloud management interface. On the left is a vertical navigation menu under 'System Navigation Menu' with several sections: System Overview, Report Configuration, Public Objects, Application Load Balancing, Intelligent DNS, Route Configuration, Network Configuration, System Configuration, Configuration Wizard, and High Availability. 'High Availability' is currently selected. The main content area is titled 'Cluster Maintenance' and contains two sections: 'Cluster Configuration' and 'Advanced Configuration'. In 'Cluster Configuration', fields include 'Cluster Name' (ad-ha-cluster), 'Management IP' (172.16.200.112), 'Subnet Mask' (24), 'HA Port' (NET1), and 'Secret Key' (a series of asterisks). In 'Advanced Configuration', fields include 'Heartbeat Timeout' (3000 ms), 'Heartbeat Interval' (1000 ms), 'Enable Remote Maintenance' (radio button selected for 'Enable'), 'Maintenance IP' (empty), 'Use Internet IP' (radio button selected for 'Enable'), 'Internet IP' (0.0.0.0), 'Management Port' (443), 'Report Port' (85), 'Communication Medium Detection' (radio button selected for 'Enable'), and 'Network Interface' (dropdown menu set to 'Please select'). At the bottom is a 'Update' button.

集群状态：包括禁用、加入集群、创建集群。若想组建一个集群，先进入第一台设备，选择创建集群，然后在成员管理页面，将其他设备加入到集群中，其他各台设备选择加入集群。

『设备管理 IP』设备管理口上的 IP 地址，用于集群控制连接的建立，和设备间的心跳监视。

『HA 网口』设备的一个物理接口(可使用聚合口)，并需配置 IP 地址，用于数据连接的建立，和设备间的心跳监视。

『密钥』用于集群认证和传输加密，所有设备必须有相同的密钥，才能组建集群。

『集群名称』集群的名称，用于标识一个集群。

『集群管理 IP』用于管理整个集群的 IP 地址，用该 IP 可登录到集群管理界面。

『心跳超时时间』集群中的设备，如果在超时时间内收不到其他设备的心跳，就认为其他设备已离线，然后接替该设备的工作。

『心跳间隔时间』集群中的设备每隔一个间隔时间，广播心跳包给集群中的其他设备。

『集群远程维护』启用集群远程维护时，用户可以通过远程维护IP地址登录集群控制台或各台设备的控制台进行管理。

『通信介质检测』启用通信介质检测，可以防止集群内各节点间的心跳出现故障时而带来的灾害（当启用通信介质检测时，如若修改了业务口，需要同步修改业务口引用的物理口）。

『网络检测』判断网络故障，如下图所示：



『检测列表』判断故障的依据，可以选择检测链路或者检测节点池。

『切换条件』根据切换条件来判断是否发生切换。

13.3.2.2. 成员管理

『成员管理』路径：『高可用性』→『模式』→『成员管理』。

成员管理					
<input type="button"/> 添加 <input type="button"/> 删除		<input checked="" type="checkbox"/> 启用 <input type="checkbox"/> 禁用	<input type="checkbox"/> 切换主控	刷新时间间隔：5秒	
<input type="checkbox"/>	名称	管理IP	角色	健康状态	管理状态
<input type="checkbox"/>	ad.sangfor.com.cn	172.16.200.110	主控	在线	启用
<input type="checkbox"/>	ad2.sangfor.com.cn	172.16.200.111	备控	在线	启用
<input type="checkbox"/>	ad3.sangfor.com	172.16.200.109	成员	离线	添加失败(连接超时)

点击**添加**，新建成员。

新建设备

新建设备

属性

名称 (长度限制为1~63字符，且不能包含& | " ' , : % < > / \ 特殊字符)

配置

设备管理IP

设备信息

HA口IP 未知

『名称』要加入集群的名称。

『设备管理 IP』用来管理和配置集群，登陆集群控制中心。设备加入集群后，只能通过集群管理 IP 来配置设备。



1. HA 网口引用网口不支持交换口和 VLAN 接口，只能选择普通网口和端口聚合网口。
2. 加入集群后，可通过管理 IP 登陆主控和受控设备控制台进行查看；若要对设备进行配置，必须登陆集群管理系统。
3. 加入集群时，会备份设备的配置；退出集群时，则会恢复默认配置。
4. 设备加入集群，必须满足的条件：
 - 1) 设备的软件版本和硬件平台均需一致。且选型时需考虑极端情况，即单台设备能负载所有的流量，避免切换后设备负载过重导致异常的情况。
 - 2) 设备的授权需一致，升级序列号除外。
 - 3) 设备的网口位置，顺序需一致。

13.3.2.3. 应用组管理

『应用组管理』路径：『高可用性』→『应用组管理』。



The screenshot shows the 'Application Group Management' interface. At the top, there are buttons for 'New' (+), 'Delete' (X), and 'Refresh' (5s). Below is a table with columns: 'Name' (with 'Default' entry), 'Default Device' (empty), 'Effective Device' (empty), 'Backup Device' (empty), 'Session Sync Status' (empty), and a 'Switch' button. A small blue gear icon is in the top right corner.

点击**新建**，新建应用组。



The screenshot shows the 'Properties' dialog for a new application group. It has three sections:

- 属性**:
 - 名称: Text input field.
 - 会话同步: Radio buttons for '启用' (selected) and '禁用'.
 - 默认设备: Dropdown menu showing '未选择'.
 - 故障检测: Two dropdown menus: '链路' (selected) and '请选择关联链路'. To the right are '添加' and '删除' buttons.
- 高级配置**:
 - 应用组权重: Text input field showing '20'.
 - 虚拟MAC: Two dropdown menus: '链路' (selected) and '请选择关联链路'. To the right are '添加' and '删除' buttons.
- 应用组关联信息**: This section is currently empty.

『名称』：一个应用组的名称，用于标识一个应用组。

『会话同步』：若开启，该应用组的生效设备会同步会话到备份设备之上，如果生效设备故障，备份设备成为生效设备，可保证原有连接不中断。

『默认设备』：若选择一个默认设备，这个默认设备具有最高的优先级被选举为生效设备。

『抢占模式』：若开启了抢占模式，该应用组的默认设备如果健康，会主动成为生效设备，而使原生效设备成为应用组的备份设备。

『故障检测』：选择与应用组关联的链路，如果一台设备的关联链路故障，若该设备是生效设备，则发生故障切换，应用组会切换到其他设备上，若该设备不是生效设备，则应用组生效设备故障时，该设备不具有成为应用组生效设备的能力。

『虚拟 MAC』：若为应用组在某条链路上配置一个虚拟 MAC 地址，应用组在该链路上的

所有 IP 地址，都用这个伪装的 MAC 与外部通讯，如果发生了故障切换，新的生效设备能够继续使用这个伪装 MAC 与外部通讯。

『权重』：若应用组在某台设备上生效，则该设备的负载会根据应用组的权重相应增加，当应用组在集群中切换时，会根据设备的负载状况选择设备。

『应用组关联信息』：该应用组包含的一组配置，包括浮动 IP、虚拟服务、NAT 规则。这些配置使该应用组具有发布服务的能力。

第 14 章 业务分析

14.1. 安全分析

『安全分析』用于配置『实时漏洞分析』启用禁用，扫描『服务配置』，『漏洞识别库』管理等功能。

WEBUI 路径：『业务分析』→『安全分析』。

界面如下图所示：



14.1.1. 实时漏洞分析

WEBUI 路径：『业务分析』→『安全分析』→『实时漏洞分析』。

『实时漏洞分析』用于配置实时漏洞分析功能启用禁用。

界面如下图所示：



状态栏勾选启用或禁用，进行选择实时漏洞分析功能的开启和禁用。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

14.1.2. 服务配置

WEBUI：『业务分析』→『安全分析』→『服务配置』。

『服务配置』用于定义需要进行扫描的虚拟服务。

界面如下图所示：



虚拟服务	漏洞数量（高/中/低）	状态
VS-11	1/0/0	启用
CMS	20/18/2	启用

启用按钮可以用于启用服务配置。

禁用按钮可以用于禁用服务配置。

选择一个虚拟服务名称，点击进行编辑：



实时漏洞分析 | 服务配置 | 漏洞识别库

安全项的基本配置

基本配置

虚拟服务: VS-11

实时漏洞分析: 启用 禁用

示例:
www.sangfor.com/index.html
www.baidu.com/*

URL排除列表

当前已配置 1/128个URL

取消 **完成**

虚拟服务名称不能修改。

点击『启用』或『禁用』选择对该虚拟服务进行实时漏洞分析开启或禁用。

在 URL 排除列表进行自定义添加不需要实时漏洞分析的域名，最多可以添加 128 条。

取消按钮可以用于取消本次配置。

完成按钮可以用于完成本次配置。

14.1.3. 漏洞识别库

WEBUI: 『业务分析』→『安全分析』→『漏洞识别库』。

『漏洞识别库』用于更新漏洞识别库和了解漏洞详细信息。

界面如下图所示：

实时漏洞分析 | 服务配置 | 漏洞识别库

启用 禁用 立即更新 离线升级 当前版本：20150227

ID	名称	类别	威胁	状态
15090284	Drupal拒绝服务漏洞	cms漏洞	高	启用
15090283	WordPress拒绝服务漏洞	cms漏洞	高	启用
15090282	JCMS 2010 数据库配置文件读取漏洞	cms漏洞	高	启用
15090281	JCMS 2010 SQL注入漏洞	cms漏洞	高	启用
15090280	JCMS 2010 文件上传漏洞	cms漏洞	高	启用
15090279	JCMS 2010 文件包含漏洞	cms漏洞	高	启用
15090278	KingCMS 0 Fckeditor上传webshell漏洞	cms漏洞	高	启用
15090277	Joomla Zap Calendar组件跨站脚本漏洞	cms漏洞	高	启用
15090276	Joomla Flexicontent 组件远程代码执行漏洞	cms漏洞	高	启用
15090275	Joomla Explorer组件跨站脚本漏洞	cms漏洞	高	启用
15090274	Joomla Multi Calendar组件跨站脚本漏洞	cms漏洞	高	启用
15090273	Joomla 2.5 远程授权漏洞	cms漏洞	高	启用
15090272	Joomla 3.2 SQL注入漏洞	cms漏洞	高	启用
15090271	Joomla 3.2 HTML注入漏洞	cms漏洞	高	启用
15090270	Joomla Simple File List 组件本地文件包含漏洞	cms漏洞	高	启用
15090269	Joomla Jetloader 组件本地文件包含漏洞	cms漏洞	高	启用
15090268	Joomla JoomTouch 组件本地文件包含漏洞	cms漏洞	高	启用
15090267	Drupal v6 OpenID模块认证绕过漏洞	cms漏洞	高	启用
15090266	Drupal v6 上传模块多个权限许可和访问控制漏洞	cms漏洞	高	启用
15090265	Drupal v6 OpenID模块用户认证绕过漏洞	cms漏洞	高	启用

启用按钮可以用于启用该漏洞识别。

禁用按钮可以用于禁用该漏洞识别。

立即更新按钮可以用于在线更新漏洞识别库。

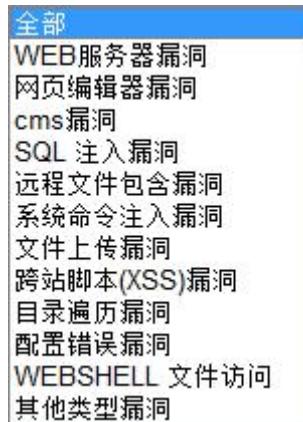
点击**离线升级**按钮可以用于在没有公网环境漏洞识别库的手动更新。升级文件需要联系深信服客户人员获取，售后电话：400-630-6430.



当前版本用于显示漏洞识别库当前的版本信息。

可以通过『类别』自定义选择查看漏洞识别库类型。目前共分为WEB服务器漏洞、网页编辑器漏洞、cms漏洞、SQL注入漏洞、远程文件包含漏洞、系统命令注入漏洞、文件上传漏洞、跨站脚本（XSS）漏洞、目录遍历漏洞、配置错误漏洞、WEBSHELL文件访问、

其他类型漏洞 12 种不同的类型，加上弱密码的识别。



可以通过『查找』输入关键字查看漏洞识别。

可以通过点击漏洞名称查看漏洞详细信息，自定义是否启用。



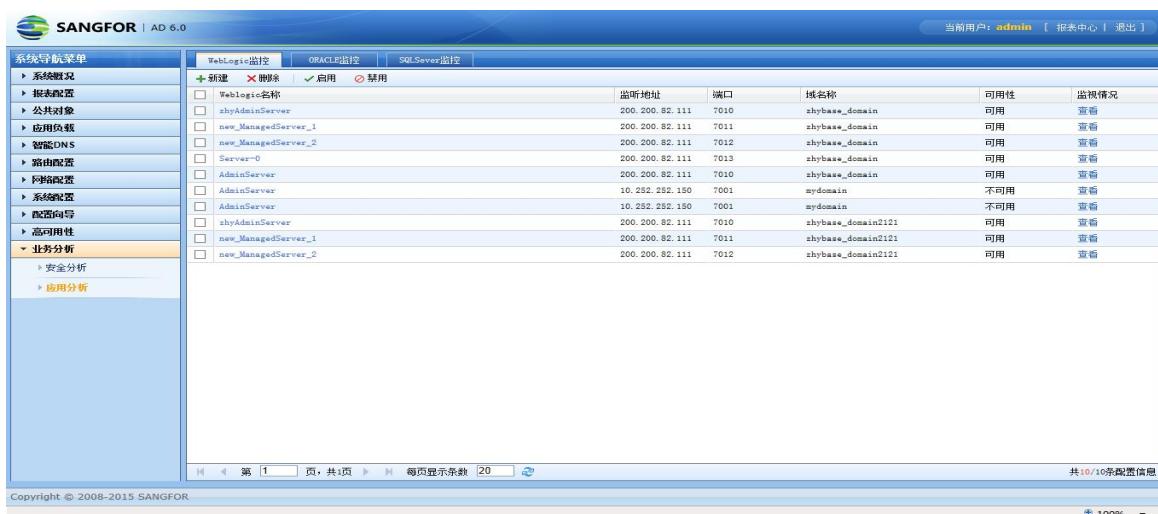
规则ID: 15090265
状态: 启用 禁用
漏洞名称: Drupal v6 OpenID 模块用户认证绕过漏洞
漏洞描述: 当前被发现风险的主机正在运行 Drupal v6 版本，这个版本 OpenID 模块由于没有检查 openid.response_nonce 值的重用违反了 OpenID 2.0 协议，远程攻击者可以利用 OpenID 供应商提供的断言绕过认证。
攻击影响: 攻击者利用此漏洞可以获取敏感信息。
严重等级: 高
参考信息: CVE-2010-3685
42388
解决方案: 升级到 Drupal 最新版本。
* 推荐部署深信服下一代防火墙

14.2. 应用分析

『应用分析』用于配置『WeLogic 监控』、『ORACLE 监控』，『SQLServer 监控』等功能。帮助体现 AD 对客户业务的监控，帮助客户分析业务状态，改进应用发布质量。

WEBUI 路径：『业务分析』→『应用分析』。

界面如下图所示：



当前用户: admin [报表中心 | 退出]

WebLogic监控	ORACLE监控	SQLServer监控																																																							
<input checked="" type="checkbox"/> 新建 <input type="checkbox"/> 脱机 <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 <input type="checkbox"/> WebLogic名称 <input type="checkbox"/> zhyAdminServer <input type="checkbox"/> new_ManagedServer_1 <input type="checkbox"/> new_ManagedServer_2 <input type="checkbox"/> Server-0 <input type="checkbox"/> AdminServer <input type="checkbox"/> AdminServer <input type="checkbox"/> zhyAdminServer <input type="checkbox"/> new_ManagedServer_1 <input type="checkbox"/> new_ManagedServer_2		<table border="1"> <thead> <tr> <th>监听地址</th> <th>端口</th> <th>域名</th> <th>可用性</th> <th>监视情况</th> </tr> </thead> <tbody> <tr> <td>200.200.82.111</td> <td>7010</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7011</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7012</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7013</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7010</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>10.252.252.180</td> <td>7001</td> <td>mydomain</td> <td>不可用</td> <td>查看</td> </tr> <tr> <td>10.252.252.180</td> <td>7001</td> <td>mydomain</td> <td>不可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7010</td> <td>zhybase_domain2121</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7011</td> <td>zhybase_domain2121</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7012</td> <td>zhybase_domain2121</td> <td>可用</td> <td>查看</td> </tr> </tbody> </table>	监听地址	端口	域名	可用性	监视情况	200.200.82.111	7010	zhybase_domain	可用	查看	200.200.82.111	7011	zhybase_domain	可用	查看	200.200.82.111	7012	zhybase_domain	可用	查看	200.200.82.111	7013	zhybase_domain	可用	查看	200.200.82.111	7010	zhybase_domain	可用	查看	10.252.252.180	7001	mydomain	不可用	查看	10.252.252.180	7001	mydomain	不可用	查看	200.200.82.111	7010	zhybase_domain2121	可用	查看	200.200.82.111	7011	zhybase_domain2121	可用	查看	200.200.82.111	7012	zhybase_domain2121	可用	查看
监听地址	端口	域名	可用性	监视情况																																																					
200.200.82.111	7010	zhybase_domain	可用	查看																																																					
200.200.82.111	7011	zhybase_domain	可用	查看																																																					
200.200.82.111	7012	zhybase_domain	可用	查看																																																					
200.200.82.111	7013	zhybase_domain	可用	查看																																																					
200.200.82.111	7010	zhybase_domain	可用	查看																																																					
10.252.252.180	7001	mydomain	不可用	查看																																																					
10.252.252.180	7001	mydomain	不可用	查看																																																					
200.200.82.111	7010	zhybase_domain2121	可用	查看																																																					
200.200.82.111	7011	zhybase_domain2121	可用	查看																																																					
200.200.82.111	7012	zhybase_domain2121	可用	查看																																																					

Copyright © 2008-2015 SANGFOR

共10/10条配置信息

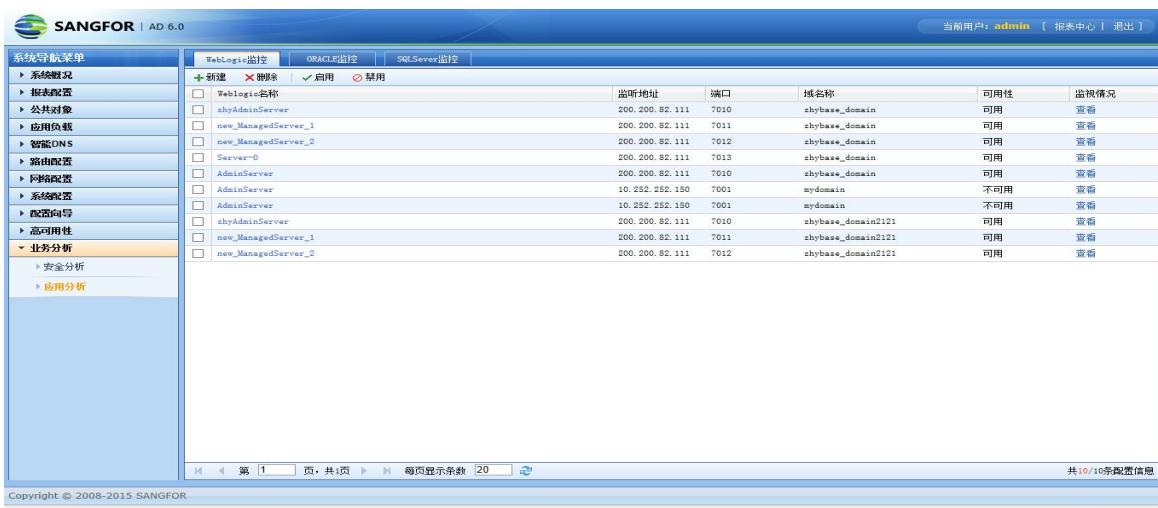
100%

14.2.1. WeLogic 监控

WEBUI 路径：『业务分析』→『应用分析』→『WeLogic 监控』。

『WeLogic 监控』用于配置需要监控的 Weblogic 应用服务器。

界面如下图所示：



当前用户: admin [报表中心 | 退出]

WebLogic监控	ORACLE监控	SQLServer监控																																																							
<input checked="" type="checkbox"/> 新建 <input type="checkbox"/> 脱机 <input checked="" type="radio"/> 启用 <input type="radio"/> 禁用 <input type="checkbox"/> WebLogic名称 <input type="checkbox"/> zhyAdminServer <input type="checkbox"/> new_ManagedServer_1 <input type="checkbox"/> new_ManagedServer_2 <input type="checkbox"/> Server-0 <input type="checkbox"/> AdminServer <input type="checkbox"/> AdminServer <input type="checkbox"/> zhyAdminServer <input type="checkbox"/> new_ManagedServer_1 <input type="checkbox"/> new_ManagedServer_2		<table border="1"> <thead> <tr> <th>监听地址</th> <th>端口</th> <th>域名</th> <th>可用性</th> <th>监视情况</th> </tr> </thead> <tbody> <tr> <td>200.200.82.111</td> <td>7010</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7011</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7012</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7013</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7010</td> <td>zhybase_domain</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>10.252.252.180</td> <td>7001</td> <td>mydomain</td> <td>不可用</td> <td>查看</td> </tr> <tr> <td>10.252.252.180</td> <td>7001</td> <td>mydomain</td> <td>不可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7010</td> <td>zhybase_domain2121</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7011</td> <td>zhybase_domain2121</td> <td>可用</td> <td>查看</td> </tr> <tr> <td>200.200.82.111</td> <td>7012</td> <td>zhybase_domain2121</td> <td>可用</td> <td>查看</td> </tr> </tbody> </table>	监听地址	端口	域名	可用性	监视情况	200.200.82.111	7010	zhybase_domain	可用	查看	200.200.82.111	7011	zhybase_domain	可用	查看	200.200.82.111	7012	zhybase_domain	可用	查看	200.200.82.111	7013	zhybase_domain	可用	查看	200.200.82.111	7010	zhybase_domain	可用	查看	10.252.252.180	7001	mydomain	不可用	查看	10.252.252.180	7001	mydomain	不可用	查看	200.200.82.111	7010	zhybase_domain2121	可用	查看	200.200.82.111	7011	zhybase_domain2121	可用	查看	200.200.82.111	7012	zhybase_domain2121	可用	查看
监听地址	端口	域名	可用性	监视情况																																																					
200.200.82.111	7010	zhybase_domain	可用	查看																																																					
200.200.82.111	7011	zhybase_domain	可用	查看																																																					
200.200.82.111	7012	zhybase_domain	可用	查看																																																					
200.200.82.111	7013	zhybase_domain	可用	查看																																																					
200.200.82.111	7010	zhybase_domain	可用	查看																																																					
10.252.252.180	7001	mydomain	不可用	查看																																																					
10.252.252.180	7001	mydomain	不可用	查看																																																					
200.200.82.111	7010	zhybase_domain2121	可用	查看																																																					
200.200.82.111	7011	zhybase_domain2121	可用	查看																																																					
200.200.82.111	7012	zhybase_domain2121	可用	查看																																																					

Copyright © 2008-2015 SANGFOR

共10/10条配置信息

100%

启用按钮可以用于启用 Weblogic 监控。

禁用按钮可以用于禁用 Weblogic 监控。

删除按钮可以用于删除 Weblogic 监控。

新建按钮可以用于新建 Weblogic 监控。

点击**新建**按钮，将会弹出 Weblogic 监控编辑界面，如下图所示：



The screenshot shows a configuration dialog for WebLogic monitoring. At the top, there are three tabs: 'WebLogic监控' (selected), 'ORACLE监控', and 'SQLServer监控'. Below the tabs, the word '新建' (New) is displayed. The main area is divided into two sections: '属性' (Properties) and '高级选项' (Advanced Options). In the '属性' section, there are four input fields: '连接地址' (Address) with placeholder '(管理主机的IP或域名)', '端口' (Port) set to '7001', '用户名' (Username) set to 'admin', and '密码' (Password) represented by four asterisks. In the '高级选项' section, there are three settings: '查询周期' (Query Period) set to '2 分钟' (2 minutes), '并行查询数' (Parallel Query Count) set to '2 个' (2 items), and a '监控模式' (Monitoring Mode) switch between '分散模式' (Decentralized mode) and '集中模式' (Centralized mode), which is currently set to '分散模式'. At the bottom of the dialog are two buttons: '取消' (Cancel) and '下一步' (Next).

『连接地址』：填写需要监控的 Weblogic 的 IP 或域名。

『端口』：填写 Weblogic 的访问端口。

『用户名和密码』：填写连接 Weblogic 的正确的用户名和密码，任意权限的用户名和密码均可。

『查询周期』：查询周期设置的时间越短，对服务器的影响越大。

『并行查询数』：并行查询数越大，查询越快，建议保持两个或两个以上的并行查询数。

『监控模式』：可选择分散模式或集中模式。选择分散模式时，AD 设备将直接访问域中各受到管理的服务器进行查询；选择集中模式时，AD 设备监控域中所有受管理的服务器信息均需通过管理服务器进行查询。建议使用分散模式，这样查询速度会比较快，对管理服务器的性能影响较小。

编辑完成后，点击**下一步**进行服务器的连接，连接成功后，可以在点击**查看**进行查看Weblogic服务器的运行状态和性能详情。

The screenshot displays two main sections of the Sangfor Cloud management interface:

Top Section (Performance Details):

- 会话 (Sessions):** WebLogic 响应时间: 3 ms, 会话数: 0.
- 应用 (Application):** 应用部署总数: 10, 健康应用部署数: 10, 健康度: -; Web 应用数: 9, Servlet 总个数: 108.
- JDBC (JDBC):** 最繁忙数据源: 当前连接数: 0, 连接池使用率: 0%.
- 数据库 (Database):** 数据源总数: 0, 等待连接数: 0.

Bottom Section (Performance Analysis):

- 概况 (Overview):** 显示了可用性图表（18:00 - 12:00）和响应时间图表（16:00 - 12:00）。
- 性能分析列表 (Performance Analysis List):** 包含了 JVM, 执行队列, JDBC, 应用部署, WEB 应用, EJB 应用, JTA, JMS 等项。

取消按钮可以用于取消本次配置。

14.2.2. ORACLE 监控

WEBUI 路径：『业务分析』→『应用分析』→『ORACLE 监控』。

『ORACLE 监控』用于配置需要监控的 ORACLE 应用服务器。

界面如下图所示：



数据连接名	用户	可用性	监视情况
200.200.83.85/orcl	sys	可用	查看
192.200.243.11:1522/orcl	sys	不可用	查看
192.200.243.12:1522/orcl	sys	不可用	查看
192.200.243.101:ad1	sys	可用	查看
192.200.243.14:1522/orcl	sys	不可用	查看
192.200.243.13:1522/orcl	sys	不可用	查看
192.200.243.185:1522/orcl	sys	不可用	查看
192.200.243.186:1522/orcl	sys	不可用	查看
192.200.243.102:ad1	sys	可用	查看
192.200.243.192:1522/orcl	sys	不可用	查看

启用按钮可以用于启用 ORACLE 监控。

禁用按钮可以用于禁用 ORACLE 监控。

删除按钮可以用于删除 ORACLE 监控。

新建按钮可以用于新建 ORACLE 监控。

点击**新建**按钮，将会弹出 ORACLE 监控编辑界面，如下图所示：

WebLogic监控 | ORACLE监控 | SQLServer监控

新建

属性

连接字符串 (格式为:IP/实例名或IP:端口/实例名)

用户名

密码

高级选项

查询周期 分钟

并行查询数 个

操作

『连接字符串』：填写需要监视的 Oracle 数据库的 IP，端口和实例名。填写格式为：IP:端口/实例名或 IP/实例名，如果数据库使用默认的 1521 端口，也可以这样填写：IP/实例名。

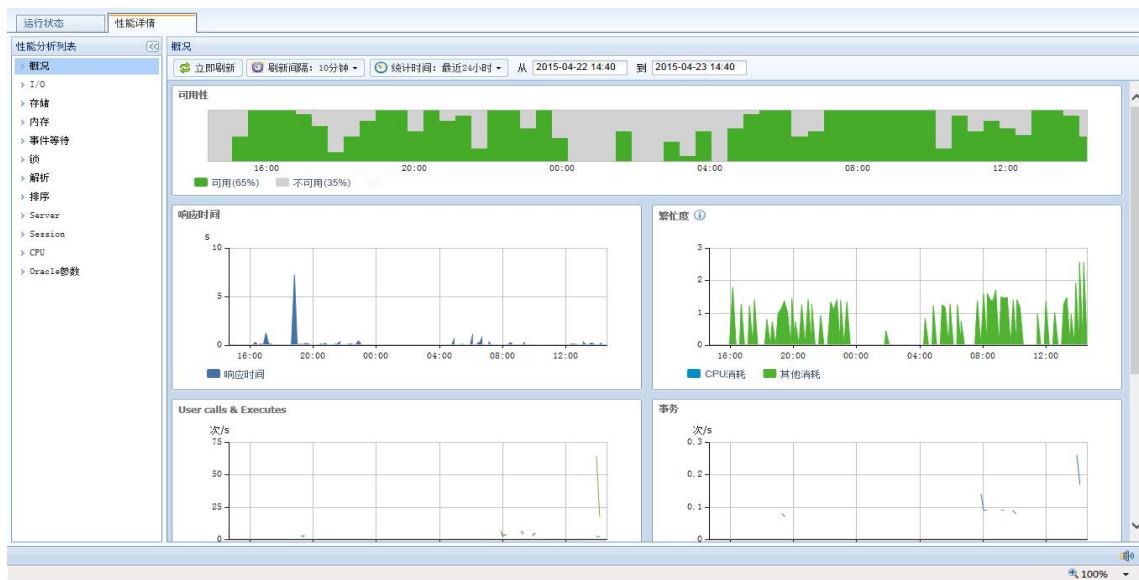
『用户名和密码』：填写连接 Oracle 数据库的用户名和密码，必须具有动态视图和表的查询权限，即 connect select_catalog_role 和 connect 权限。

『查询周期』：查询周期设置的时间越短，对服务器的影响越大。

『并行查询数』：并行查询数越大，查询越快，建议保持两个或两个以上的并行查询数。

编辑完成后，点击 **完成** 进行请求，请求成功后，可以在点击 **查看** 进行查看 ORACLE 服务器的运行状态和性能详情。





取消按钮可以用于取消本次配置。

14.2.3. SQLServer 监控

WEBUI 路径：『业务分析』→『应用分析』→『SQLServer 监控』。

『SQLServer 监控』用于配置需要监控的 SQLServer 应用服务器。

界面如下图所示：

The screenshot shows a configuration table for SQL Server monitoring:

数据库连接名	用户	可用性	监视情况
191.200.243.11:1433/MSSQLSERVER	sa	可用	查看
191.200.243.12:1433/MSSQLSERVER	sa	可用	查看
191.200.243.13:1433/MSSQLSERVER	sa	可用	查看
191.200.243.14:1433/MSSQLSERVER	sa	可用	查看
191.200.243.15:1433/MSSQLSERVER	sa	可用	查看
191.200.243.16:1433/MSSQLSERVER	sa	可用	查看
191.200.243.17:1433/MSSQLSERVER	sa	可用	查看
191.200.243.18:1433/MSSQLSERVER	sa	可用	查看
191.200.243.19:1433/MSSQLSERVER	sa	可用	查看
191.200.243.20:1433/MSSQLSERVER	sa	可用	查看

启用按钮可以用于启用 SQLServer 监控。

禁用按钮可以用于禁用 SQLServer 监控。

删除按钮可以用于删除 SQLServer 监控。

新建按钮可以用于新建 SQLServer 监控。

点击**新建**按钮，将会弹出 SQLServer 监控编辑界面，如下图所示：

WebLogic 监控 | ORACLE 监控 | SQLServer 监控

新建

属性

连接字符串 (格式为:IP或IP:端口)

状态 启用 禁用

用户名

密码

高级选项

查询周期 分钟

并行查询数 个

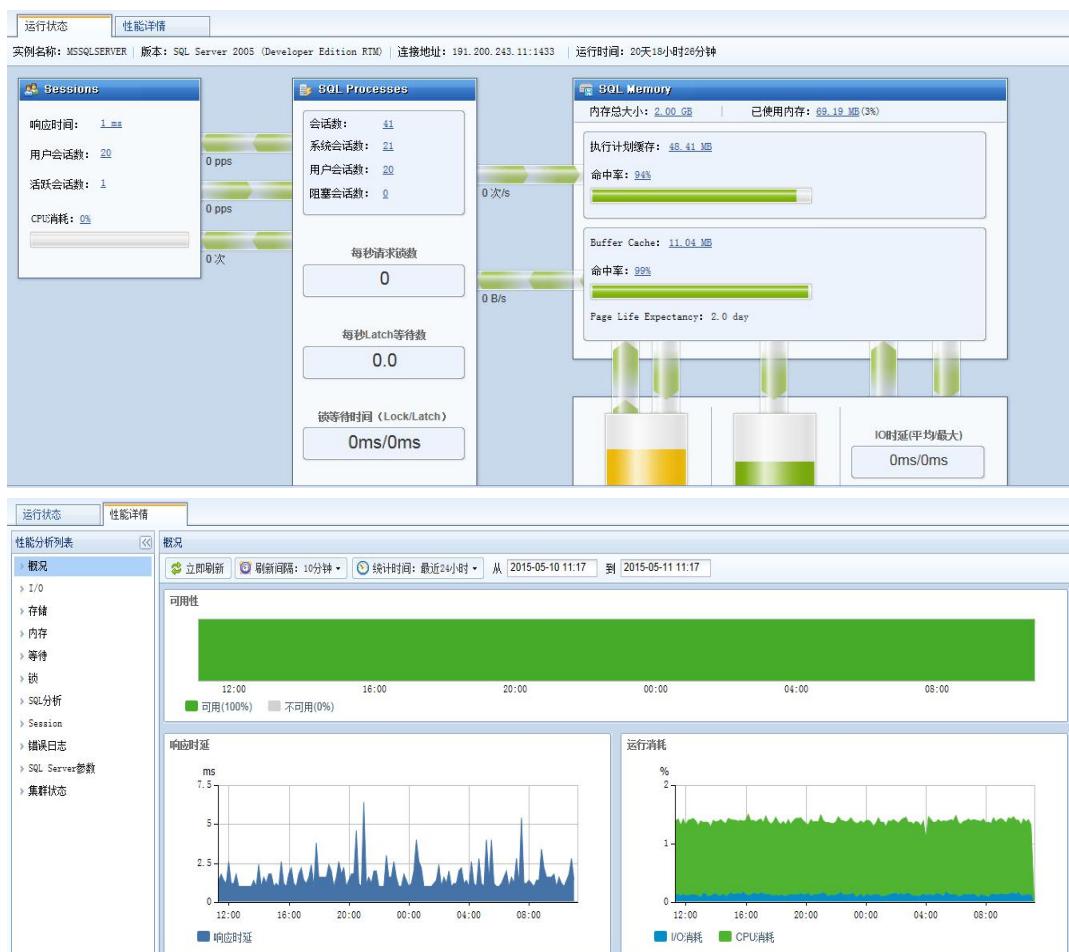
『连接字符串』：填写需要监视的 SQL Server 数据库的 IP，端口。填写格式为：IP:端口或只填 IP，如果数据库使用默认的 1433 端口，则可以只填写 IP。

『用户名和密码』：填写连接 SQL Server 数据库的用户名，必须拥有系统管理员权限，即该用户必须是 sysadmin 角色成员。

『查询周期』：查询周期设置的时间越短，对服务器的影响越大。

『并行查询数』：并行查询数越大，查询越快，建议保持两个或两个以上的并行查询数。

编辑完成后，点击 **完成** 进行测试连接数据库，测试连接成功后，可以在点击 **查看** 进行查看 SQL Server 服务器的运行状态和性能详情。



取消按钮可以用于取消本次配置。

第 15 章 增值服务

15.1. 增值服务导航

通过增值服务导航可以快速跳转深信服社区，进行发帖求助、在线咨询等服务；帮助管理员激活设备。



15.1.1. 激活信息

新购买设备，初次登录设备控制台，会提示一下页面。



如果您是首次激活：输入您的手机号，点击获取验证码，勾选接受深信服隐私权保护声明，点击立即激活。成功激活后，您的设备在服务期内将享受完整的售后服务。

隐私权保护声明

深信服公司（下称“深信服”）非常重视个人信息的保护，在使用深信服提供的产品和服务之前，请您（下称“用户”）务必仔细阅读并充分理解《隐私权保护声明》（下称“本声明”）。一旦用户选择使用，即表示认可并接受本声明所有内容。

本声明解释了用户个人隐私信息收集和使用的有关情况，本声明适用于深信服的所有相关产品和服务。

1. 用户在使用深信服提供的产品和服务时，可能需要提供一些必要的能够对用户进行个人辨识以及个人通信的信息，包括但不限于用户真实姓名、手机号码、所在地理位置信息等。如果用户无法提供此类信息，可能无法使用对应服务或在使用过程中受到限制。同时，为了运营和改善深信服的产品和服务，深信服可能会公开收集使用或向第三方提供用户对产品的操作状态以及使用习惯等信息和其他一切个人隐私信息范围内的普通信息，以改善用户体验。

2. 一般情况下，用户可随时浏览、修改自己提交的信息，但出于安全性和身份识别的考虑，用户可能无法修改注册时提供的初始注册信息及其验证信息。

3. 保护用户个人信息是深信服的一贯制度，深信服将会采取合理的措施保护用户个人信息。深信服未经用户同意，不向任何第三方公开、透露用户个人隐私信息。但以下特定情形造成的用户个人隐私信息泄露由用户自行承担：

- (1) 深信服根据法律法规规定或有机构的指示提供给用户的个人隐私信息；
- (2) 由于用户将其用户名和密码告知他人或与他人共用注册帐户与密码等非深信服原因导致的任何个人隐私信息的泄漏；
- (3) 用户自行向第三方公开其个人隐私信息；
- (4) 用户与深信服及合作单位之间就用户个人隐私信息的使用公开达成约定，深信服因此向合作单位公开用户个人隐私信息；
- (5) 任何由于黑客攻击、电脑病毒侵入及其他不可抗力事件导致用户个人隐私信息的泄露。

4. 深信服郑重提醒用户注意本声明中免除深信服责任的条款，请用户仔细阅读，自主考虑风险。

以上各项条款内容的最终解释权及修改权归深信服所有。

如果您以前激活过：切换到已验证手机号激活页面，直接输入已验证的手机号码，勾选接受深信服隐私权保护声明，点击立即激活，成功激活后，您的设备在服务期内将享受完整的售后服务。



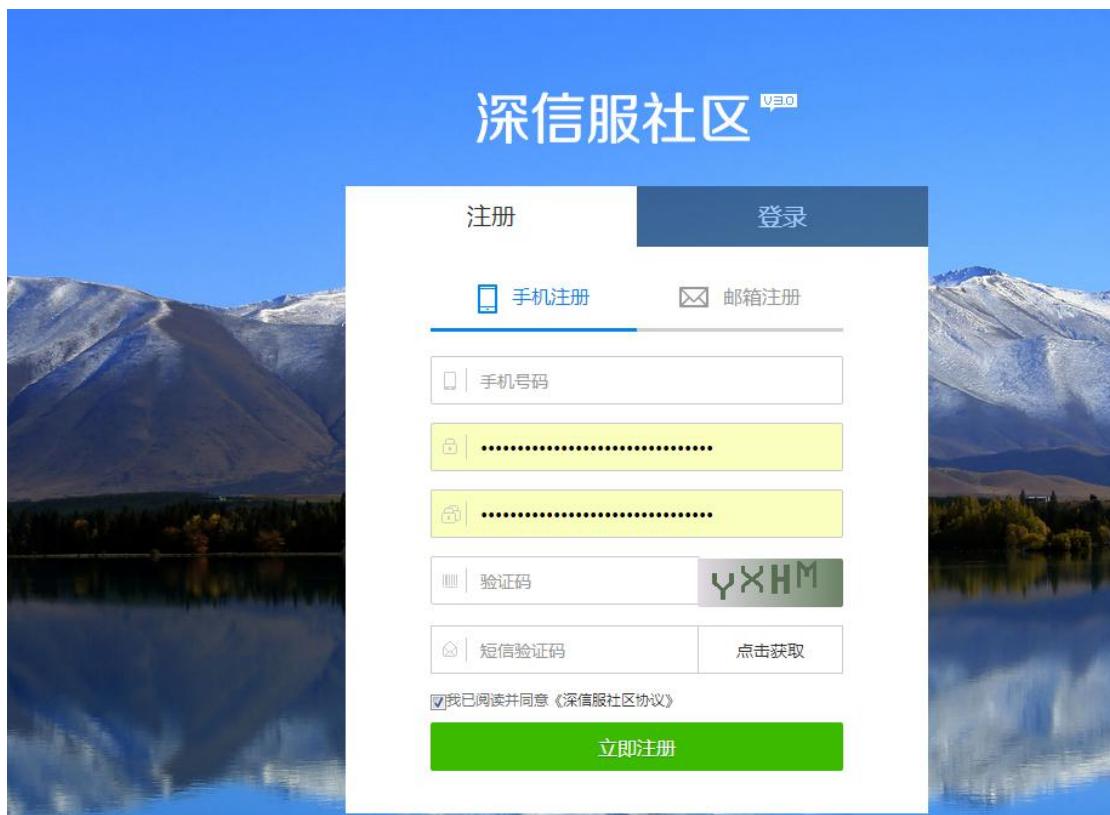
完成激活后，可以点击  admin，确认管理员激活信息正确无误。



15.1.2. 发帖求助&在线咨询

深信服社区（bbs.sangfor.com.cn）是深信服公司向用户提供的以深信服产品为核心，与渠道伙伴和企业员工进行讨论、交流的平台。

点击『发帖求助』，会在浏览器新页面自动跳转到深信服社区登录系统。输入注册后的手机号码和密码，就可以进入社区。



15.1.3. 社区疑问&资料搜索

设备使用过程中遇到疑问，可以根据关键词在搜索栏进行检索。

举例：检索关键字 AD + 升级 

回车后页面自动跳转到相关关键字检索结果页面。

深信服社区 

资讯 论坛 版块 资料库 活动 自助服务 登录 | 注册 | 找回密码

综合 用户

全部 资料 帖子 版块筛选：应用交付 ▾ 排序：综合排序 ▾

AD 6.2版本 业务正常，LAN口地址ping不通 

AD 升级 到 6.2 版本后，发现 LAN口地址 ping 不通，但是业务数据还能正常转发。用 LAN 口地址也不能管理到设备，只能使用默认的 0 口管理设备。重启后还是这样，搞不清楚是怎么回事。
... 从 5...

 | 应用交付 | 133 3

AD 版本更新日志

AD 5.4 —、新增和改进功能 1、SSL卸载支持TLS1.1、TLS1.2协议 2、SSL卸载支持国密算法 3、服务器过载保护 4、支持Radius、**AD**域外部认证 5、全球地址段，增加“导出”...

 | 应用交付 | 92 0

AD 5.6 从 5.6版本升级到 6.2版本，升级完成后重启需要多久啊

AD 5.6 从 5.6 版本 **升级** 到 6.2 版本，**升级** 完成后重启需要多久啊？**升级** 完成后过了好久都还没有启动起来

 | 应用交付 | 128 2

AD-1800恢复出厂设置显示升级失败，(bakcfgsh execute fail) 

我这里有一台**AD-1800** 登陆控制台界面显示502错误，无法进入控制台界面打算恢复出厂设置设备的版本是4.8，下载4.8的**升级**包进行刷时在开始备份配置时提示(bakcfgsh execute f...

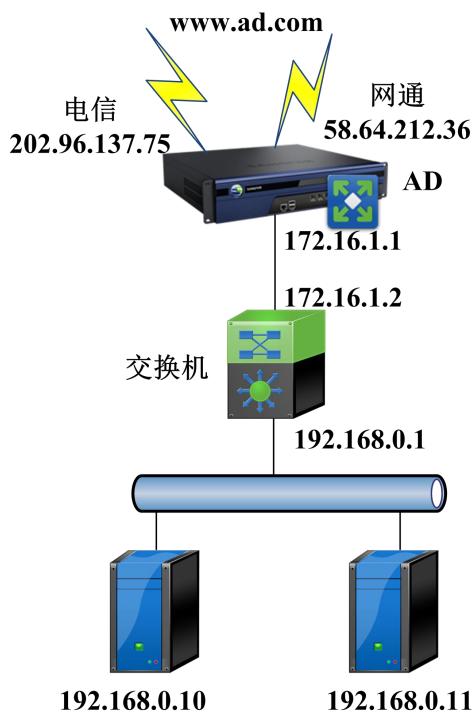
第 16 章 案例集

16.1. 部署配置案例

16.1.1. 路由模式部署案例

路由模式优点：可以实现链路负载和服务器负载，使用 AD 的全部功能。

部署案例网络拓扑：



AD 以路由模式进行部署，同时作为网关代理内网上网，有两条外网线路分别是电信线路和网通线路，IP 分别为 202.96.137.75 和 58.64.212.36，并且这两个 IP 对应同一个域名 www.ad.com；AD 内网接口 IP 为 172.16.1.1；三层交换机接在 AD 下面，和 AD 相连的接口 IP 为 172.16.1.2，和内网相连的接口 IP 为 192.168.0.1；内网有两台服务器提供相同的 WEB 服务，IP 地址分别是 192.168.0.10 和 192.168.0.11。

网络需求：使用 AD 实现外网链路负载，并对两台 WEB 服务器进行应用负载。

案例详细配置步骤：

第一步：在『网络配置』→『网络接口』页面，新增内网接口 LAN，界面如下图所示：



选择 LAN，点击 **下一步**，界面如下图所示：



第二步：在『网络配置』→『网络接口』页面，新增外网接口 WAN，建立电信接口，
界面如下图所示：



选择 WAN，点击 **下一步**，界面如下图所示：

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

新建WAN口

属性

名称	电信
网络接口	NET2
类别	WAN
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

网络地址配置

地址列表

起始IP	
结束IP	
掩码/前缀	202.96.137.75/24

当前已配置1/512个地址

网关

202.96.137.78

对应互联网IP

起始IP :	
结束IP :	

当前已配置0/512个地址

线路带宽

上行带宽	100 Mbps	上行带宽繁忙比例	99 %
下行带宽	100 Mbps	下行带宽繁忙比例	99 %

健康检查

监视器状态	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
插拔网线检测	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用

第三步：在『网络配置』→『网络接口』页面，新增外网接口 WAN，建立网通接口，界面如下图所示：



选择 WAN，点击 下一步，界面如下图所示：

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

新建/编辑

属性

名称: 网通
网络接口: NET3
类别: WAN
状态: 启用 禁用

网络地址配置

地址列表
起始IP: _____
结束IP: _____
掩码/前缀: 58.64.212.36/24
添加 | 删除

当前已配置1/512个地址
58.64.212.38
起始IP: _____
结束IP: _____
添加 | 删除

当前已配置0/512个地址

线路带宽

上行带宽: 100 Mbps 上行带宽繁忙比例: 99 %
下行带宽: 100 Mbps 下行带宽繁忙比例: 99 %

健康检查

监视器状态: 启用 禁用
插拔网线检测: 启用 禁用

取消 | 更新

第四步：网络接口配置完成；界面如下图所示：

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

网口连接实时状态

名称	网络接口	IP地址	上行带宽	下行带宽	类别
内网接口	NET1	172.16.1.1	100.00Mbps	100.00Mbps	LAN
电信	NET2	202.98.137.75	100.00Mbps	100.00Mbps	WAN
网通	NET3	58.64.212.36	100.00Mbps	100.00Mbps	WAN

第五步：在『网络配置』→『源地址转换』页面，设置代理内网上网；

设置内网通过电信线路上网，界面如下图所示：



源地址转换 SNAT地址集 源地址转换关联组 帮助信息

新建 属性 >> 高级配置视图

名称: 电信NAT

状态: 启用 禁用

类型: IPv4 IPv6

配置

出接口: 指定网口 WAN1

代理网段:

代理所有IPV4地址

代理指定网段 - 源IP地址属于如下设置的网段才可以经过NAT源地址转换

转换源IP地址为:

使用网口地址

使用指定地址

起始地址: 202.96.137.75

结束地址: 202.96.137.75

转换策略:

源IP和目的IP哈希

源IP哈希

取消 完成

设置内网通过网通线路上网，界面如下图所示：



源地址转换 SNAT地址集 源地址转换关联组 帮助信息

新建 属性 >> 高级配置视图

名称: 网通NAT

状态: 启用 禁用

类型: IPv4 IPv6

配置

出接口: 指定网口 WAN2

代理网段:

代理所有IPV4地址

代理指定网段 - 源IP地址属于如下设置的网段才可以经过NAT源地址转换

转换源IP地址为:

使用网口地址

使用指定地址

起始地址: 58.64.212.36

结束地址: 58.64.212.36

转换策略:

源IP和目的IP哈希

源IP哈希

取消 完成

点击**完成**按钮，保存配置。

代理上网设置完成后，界面如下图所示：



名称	出接口	子网网段	操作
电信NAT	电信	全部	  
网通NAT	网通	全部	  

第六步：在『路由配置』→『静态路由』页面，添加到服务器的系统路由（回包路由），界面如下图所示：



静态路由

新建

属性

网络号	192.168.0.0
掩码/前缀	255.255.255.0
网关	172.16.1.2
支持重分发	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用

取消 完成

第七步：在『应用负载』→『服务』页面，新建一个服务，设置好服务类型和服务端口，由于AD设备默认已经有HTTP服务，因此这一步骤可省略。

第八步：在『应用负载』→『IP组』页面，新建一个IP组，将外网IP添加到这个IP组，界面如下图所示：

IP组

新建

属性

名称：应用发布

IP组：

已选择：

- 电信 202.96.137.75
- 网通 58.64.212.36

(最多可以添加32个IP)

显示WAN口IP对应的互联网IP

取消 完成

第九步：在『应用负载』→『节点池』页面，新建一个节点池，将服务器的IP地址添加到节点池中，设置好节点监视器，会话保持方式（设备默认不存在任何会话保持方式，若需要根据会话保持调度节点，可以在这之前配置好会话保持方式），节点选择策略选轮询等，配置如下图：

节点池

帮助信息

新建

配置

名称：web

节点选择策略：轮询

会话保持：none

备用会话保持：none

已选择：

- 常规监视器 ping

节点状态监视器

待选：

- 常规监视器
- ping6
- connect_tcp
- connect_udp
- http
- ftp
- pop3
- smtp

节点有效条件：至少 1 个常规监视器通过

恢复时间：0 秒

温暖时间：0 秒

节点池繁忙处理策略： 强制调度 排队等待 调度失败

连接数统计： 全状态统计 ESTABLISHED状态统计

节点

节点列表	起始地址	结束地址
	端口	权重
	192.168.0.10:80/1	1
	192.168.0.11:80/1	

当前已配置2/500个节点

[添加](#) [删除](#)

[取消](#) [完成](#)

第十步：在『应用负载』→『虚拟服务』页面，，新建一个七层虚拟服务，关联上设置好的各个选项，配置虚拟服务页面如下图：

虚拟服务

新建虚拟服务

选择负载模式

四层模式
 七层模式

[取消](#) [下一步](#)

虚拟服务 | 虚拟服务关联组

新建

属性

名称:

状态: 启用 禁用

配置

负载模式: 七层

服务: http

IP 组: --请选择--

调度方式: 首个请求 每一个请求

前置策略: (可以配置0~100个前置策略)

默认节点池: --请选择--

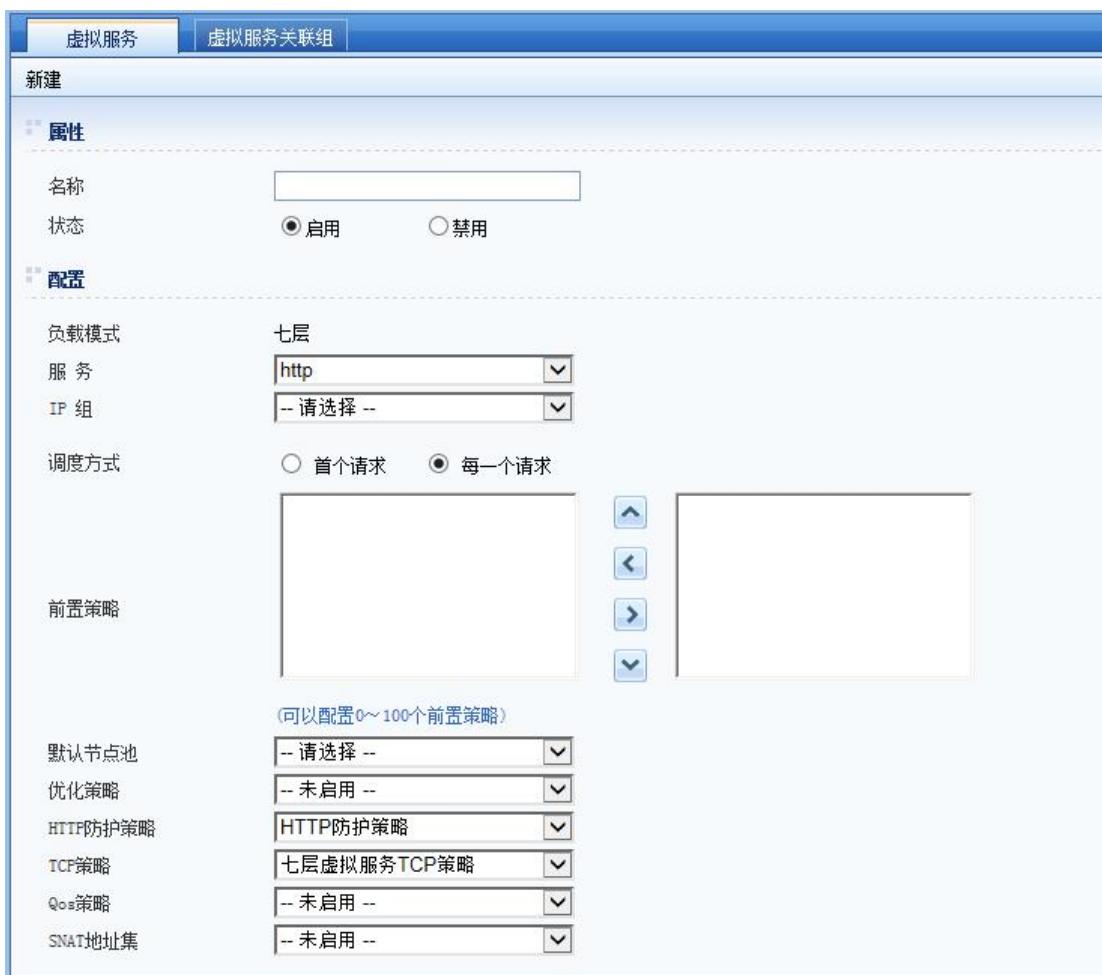
优化策略: --未启用--

HTTP防护策略: HTTP防护策略

TCP策略: 七层虚拟服务TCP策略

QoS策略: --未启用--

SNAT地址集: --未启用--



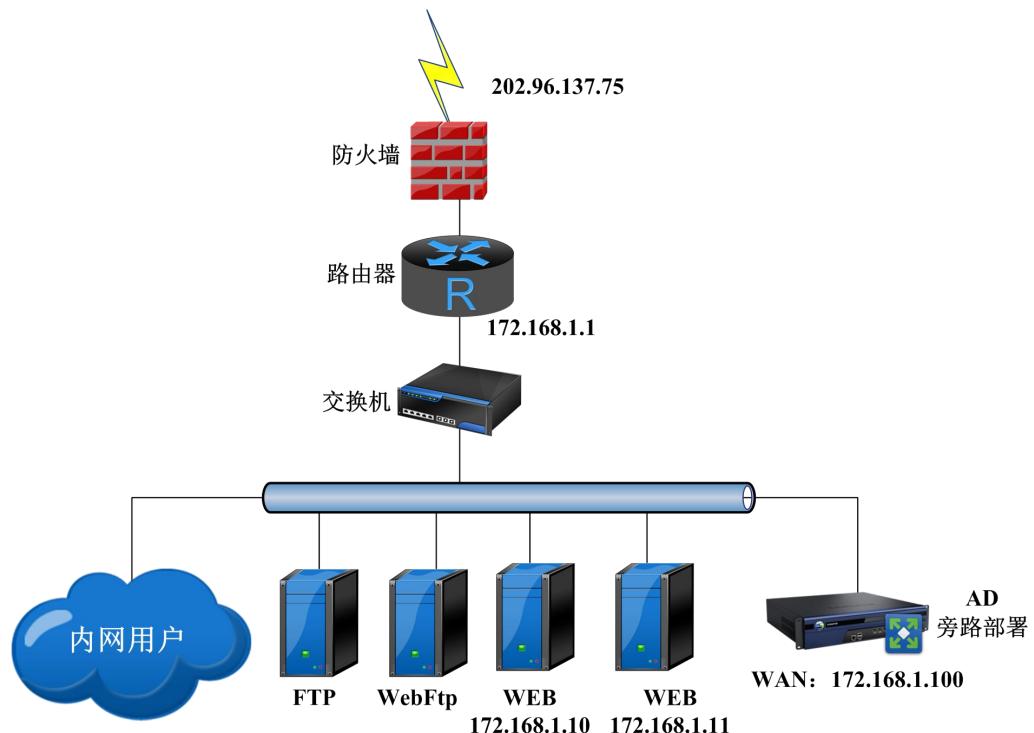
16.1.2. 旁路模式部署案例

旁路模式：通过单口收发数据，来实现原本需要多对接口共同作用实现的业务功能。

旁路模式优点：无需更改原网络拓扑结构，直接加入设备进行配置即可。

旁路模式主要功能：内网用户访问 AD 进行服务器负载均衡；向外发布应用服务，实现负载均衡；支持智能 DNS 的入站链路负载。

旁路模式部署案例网络拓扑：



防火墙 IP 为 202.96.137.75，代理内网上网；中间路由器，内网接口 IP 为 172.168.1.1；二层交换机连接内网各个设备；AD 旁路模式部署，IP 地址为 172.168.1.100；内网有两台服务器提供相同的 WEB 服务，IP 地址分别是 172.168.1.10 和 172.168.1.11。

网络需求：使用 AD 对两台 WEB 服务器进行应用负载。

案例网络配置注意事项：

- 1、AD WAN 口与服务器相同网段。
- 2、AD 网关和服务器相同，指向前置路由设备
- 3、出口防火墙做对应应用的端口映射到 AD WAN 口

案例详细配置步骤：

第一步：在『网络配置』→『网络接口』页面，新增外网接口 WAN，建立旁路 WAN 接口，界面如下图所示：

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

新建WAN口

属性

名称	旁路WAN口
网络接口	NET1
类别	WAN
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

网络地址配置

地址列表

起始IP	
结束IP	
掩码/前缀	172.16.1.100/24

当前已配置1/512个地址

网关

172.16.1.1

对应互联网IP

起始IP :	
结束IP :	202.96.137.75

当前已配置1/512个地址

添加 **删除**

线路带宽

上行带宽	100 Mbps	上行带宽繁忙比例	80 %
下行带宽	100 Mbps	下行带宽繁忙比例	80 %

健康检查

监视器状态	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用	
网关ARP检查	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用	
有效监视器	ping		
监视主机	<input type="text"/> ping/202.96.137.1		
<input type="button" value="添加"/> <input type="button" value="删除"/>			

插拔网线检测 启用 禁用

第二步：在『应用负载』→『服务』页面，新建一个服务，设置好服务类型和服务端口，由于 AD 设备默认已经有 HTTP 服务，因此这一步骤可省略。

第三步：在『应用负载』→『IP 组』页面，新建一个 IP 组，将外网 IP 添加到这个 IP 组，界面如下图所示：

IP组

新建

属性

名称	旁路IP组				
IP组	<table border="1"><tr><td>已选择</td><td>旁路WAN口 202.96.137.75</td></tr><tr><td>待选</td><td></td></tr></table>	已选择	旁路WAN口 202.96.137.75	待选	
已选择	旁路WAN口 202.96.137.75				
待选					

(最多可以添加32个IP)

显示WAN口IP对应的互联网IP

第四步：在『应用负载』→『节点池』页面，新建一个节点池，界面如下图所示：

新建

配置

名称	旁路节点池
节点选择策略	轮询
会话保持	none
备用会话保持	none

已选择

常规监视器
ping

待选

常规监视器
ping6
connect_tcp
connect_udp
http
ftp
pop3
smtp

节点有效条件

全部

恢复时间

0	秒
---	---

温暖时间

0	秒
---	---

节点池繁忙处理策略

强制调度 排队等待 调度失败

连接数统计

全状态统计 ESTABLISHED状态统计

节点

节点列表

起始地址	结束地址
端口	权重
172.16.1.10:80/1	1
172.16.1.11:80/1	

添加 删除

第五步：在『应用负载』→『节点池』页面，，新建一个七层虚拟服务，关联上设置好的各个选项，配置虚拟服务页面如下图：

虚拟服务

新建虚拟服务

选择负载模式

四层模式 七层模式

取消 下一步

虚拟服务 | 虚拟服务关联组

新建

属性

名称

状态 启用 禁用

配置

负载模式 七层

服务 http

IP 组 --请选择--

调度方式 首个请求 每一个请求

前置策略

(可以配置0~100个前置策略)

默认节点池 --请选择--

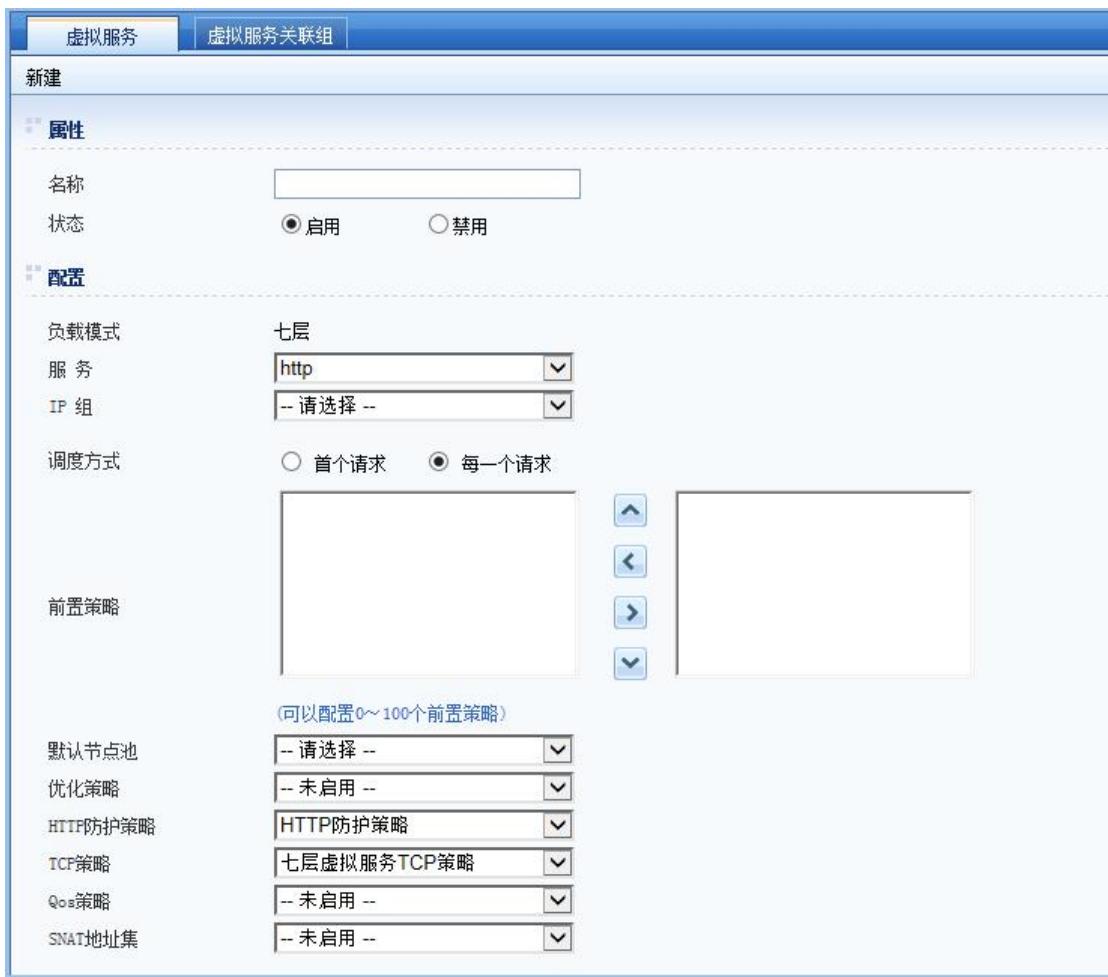
优化策略 --未启用--

HTTP防护策略 HTTP防护策略

TCP策略 七层虚拟服务TCP策略

QoS策略 --未启用--

SNAT地址集 --未启用--



第六步：勾选启用自动 SNAT，这一步在旁路部署模式下必选。

点击完成按钮，保存配置。

第七步：配置完成。



旁路模式部署只需要保证 WAN 口能与内网服务器通信即可，WAN 口与服务器不在一个网段也可以。

16.2. 服务器负载配置案例

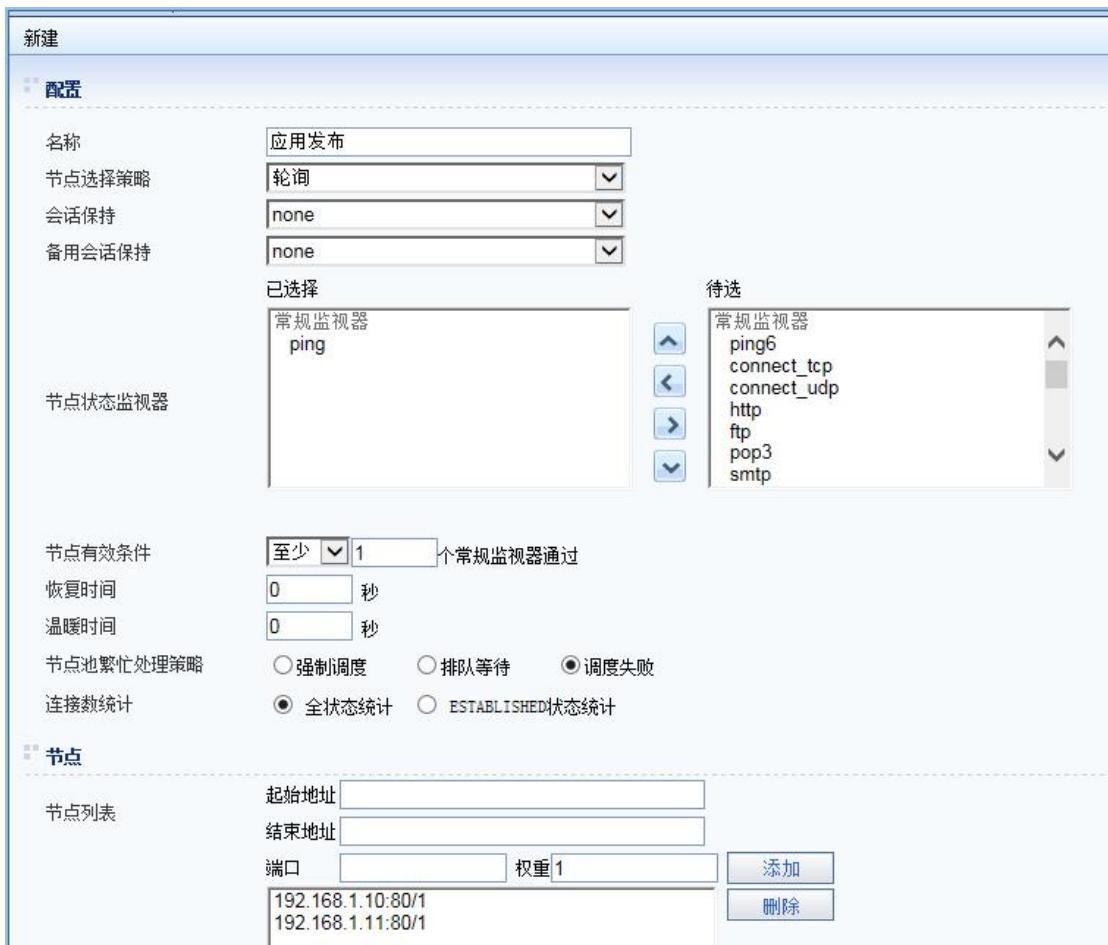
需求：某客户部署 AD 设备于网络的出口处，客户内网有两台 WEB 服务器，访问端口为 TCP 80，需要实现服务器的轮询负载。

配置步骤：

第一步：参考第7章7.1服务，新建一个服务，设置好服务类型和服务端口，由于AD设备默认已经有HTTP服务，因此这一步骤可省略。

第二步：新建一个IP组，将外网IP添加到这个IP组，详细配置请参考6.2IP组。

第三步：参考6.5节点池，新建一个节点池，将服务器的IP地址添加到节点池中，设置好节点监视器，会话保持方式（设备默认不存在任何会话保持方式，若需要根据会话保持调度节点，可以在这之前配置好会话保持方式），节点选择策略选轮询等，配置如下图：



第四步：参考6.8虚拟服务，新建一个虚拟服务，关联上设置好的各个选项，配置虚拟服务页面如下图：

虚拟服务 虚拟服务关联组

新建

属性

名称

状态 启用 禁用

配置

负载模式 七层

服务

IP 组

调度方式 首个请求 每一个请求

前置策略

(可以配置0~100个前置策略)

默认节点池

优化策略

HTTP防护策略

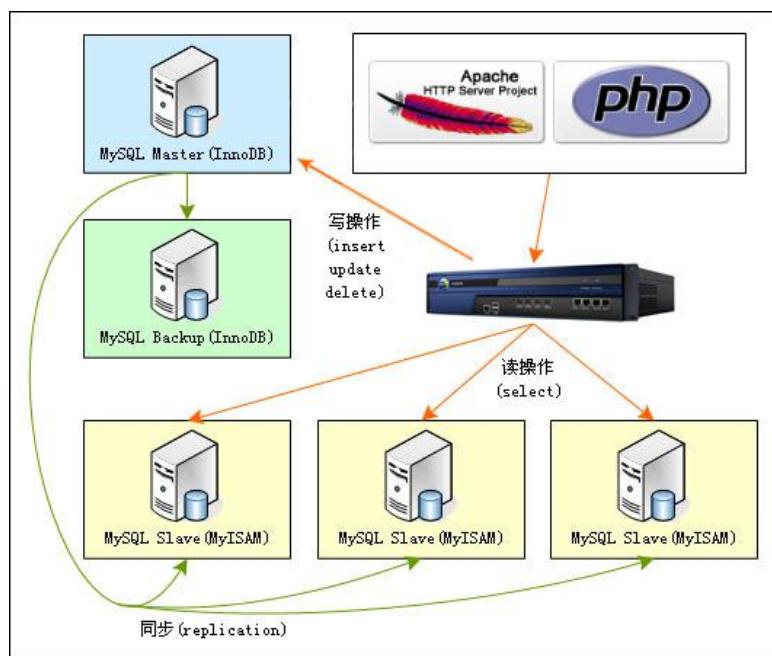
TCP策略

QoS策略

SNAT地址集

16.3. MySQL 数据库负载配置案例

需求背景：数据库服务场景，一主多备，服务器版本需要 5.0~5.6 包括 5.0 和 5.6。认证方式为 MySQL 的默认认证方式。AD6.3 增加对数据库负载的功能，此功能主要用来提高用户服务器的吞吐并发。用户只需要增加设备而不需要更改自身应用层的架构就可以实现数据库的负载，达到吞吐和并发的提升。



配置步骤：

AD 的管理 IP: 10.252.252.68

数据库主机 IP: 10.250.66.12

数据库主机 IP: 10.250.66.13

第一步：配置写节点监视器

温馨提示：在填写发送内容时，请尽量使用不耗损性能、数据量小的可执行的SQL语句

属性

名称	master
类型	MYSQL

基本配置

间隔时间	10 秒
超时时间	60 秒
尝试次数	3
监视地址	*
监视端口	* * default
用户名	root
密码	*****
数据库名	test
开启测试日志	<input type="radio"/> 是 <input checked="" type="radio"/> 否

附加配置

检测对象	查询结果集
	select 1
发送内容	
结果定位	1 行 1 列
接收内容必须包含	1

数据库配置检测

服务器地址: 10.250.66.12
 服务器端口: 3306

检测结果:
 结果: 节点有效

返回

第二步：配置写节点池

配置

名称	master
节点选择策略	轮询
会话保持	none
备用会话保持	none

已选择

常规监视器
master

待选

mssql
mysql
https
connect_ssl
slave
智能监视器
tcp_RST
tcp_zero_win

节点有效条件 全部

恢复时间 0 秒

温暖时间 0 秒

节点池繁忙处理策略 强制调度 排队等待 调度失败 (radio)

连接数统计 全状态统计 ESTABLISHED状态统计 (radio)

节点

节点列表

起始地址	结束地址
端口	权重
10.250.66.12:3306/1	1

添加 删除

当前已配置 1 / 498 个节点

第三步：配置读节点监视器

节点监视器

温馨提示：在填写发送内容时，请尽量使用不耗损性能、数据量小的可执行的SQL语句

属性

名称: slave
类型: MYSQL

基本配置

间隔时间: 10 秒
超时时间: 60 秒
尝试次数: 3
监视地址: *
监视端口: * * default
用户名: root
密码: *****
数据库名: test
开启调试日志: 是 否

附加配置

检测对象: 同步状态
show slave status;
发送内容:

开启同步超时检查: 是 否

数据库配置检测

服务器地址: 10.250.66.13
服务器端口: 3306 检测

检测结果: 结果: 节点失效
原因: 查询结果为空

返回

数据库配置检测 取消 完成

第四步：配置备机节点池

节点池

新建

配置

名称	slave
节点选择策略	轮询
会话保持	none
备用会话保持	none
已选择	常规监视器 slave
待选	mssql mysql https connect_ssl master 智能监视器 tcp_RST tcp_zero_win

节点状态监视器

节点有效条件 全部

恢复时间 0 秒

温暖时间 0 秒

节点池繁忙处理策略 强制调度 (radio) 排队等待 (radio) 调度失败 (radio)

连接数统计 全状态统计 (radio) ESTABLISHED状态统计 (radio)

节点

节点列表

起始地址	10.250.66.12
结束地址	
端口	3306 权重1
添加	
删除	

当前已配置0/498个节点

完成

第五步：配置 wan 口和 lan 口

	名称	网络接口	IP地址	上行带宽	下行带宽	类别
<input type="checkbox"/>	10.250.66.89	NET1	10.250.66.89			LAN
<input type="checkbox"/>	10.250.67.89	NET2	10.250.67.89	111Kbps	111Kbps	WAN

第六步：创建对外发布 vip

+ 新建 **- 删除**

<input type="checkbox"/>	名称	IP地址
<input type="checkbox"/>	vip	10.250.67.89

第七步：配置虚拟服务

新建

属性

名称: mysql
状态: 启用 禁用

配置

负载模式: 七层
服务: mysql
IP 组: vip
读写分离 [帮助文档]: 启用 禁用
读节点池: master
写节点池: slave
数据库用户列表:
帐号:
密码:
root/**********
admin/**********
guest/**********
添加
删除
当前已配置 3/100 个用户

TCP策略: 七层虚拟服务TCP策略
QoS策略: --未启用--
SNAT地址集: 自动SNAT

高级配置

MySQL连接池: 启用 禁用
连接池大小: 1024
老化时间: 60 秒
源IP掩码: 0.0.0.0

取消 完成

第八步：利用前置调度策略读写分离。

前置调度策略 | 优化策略 | HTTP改写策略 | TCP策略 | SSL策略 | URL下载速度控制 | QoS

新建

属性

名称: strategy

关联属性

服务: mysql
源IP范围: 所有地址
高级条件匹配:

字段: SQL语句
条件: 包含 select
属性: 区分大小写 条件取反

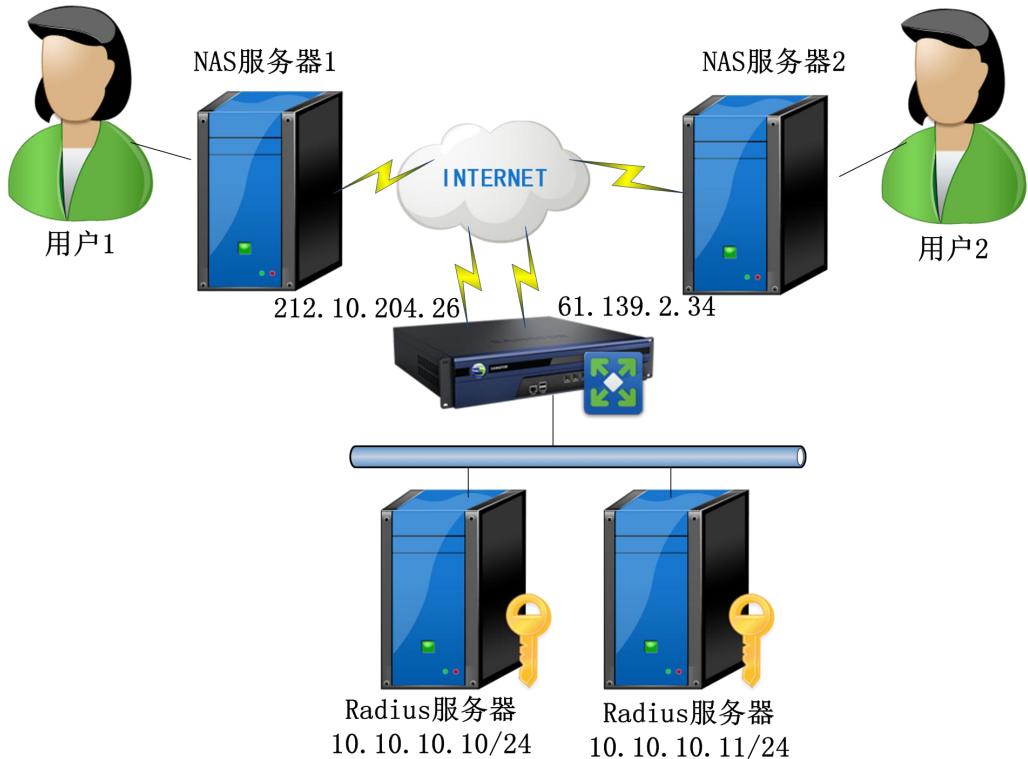
SQL匹配 SQL语句 包含 select aa 添加 删除

动作: 调度节点池
调度节点池: slave
失败动作: 匹配下一条

取消 完成

16.4. Radius 服务器负载配置案例

需求背景: 客户那边有多台 Radius 服务器, 用户做认证时, 请求先发给 NAS, 再由 NAS 发给 Radius 服务器。AD 设备根据请求中的 NAS-IP-ADDRESS 做会话保持, 要求 NAS-IP-ADDRESS 为 IP1 的请求分配到节点 1, NAS-IP-ADDRESS 为 IP2 的请求分配到节点 2。



配置步骤：

第一步：在『应用负载』→『服务』页面，新建一个 Radius 认证服务，设置好服务类型和服务端口，由于 AD 设备默认已经有 radius_auth 服务，因此这一步骤可省略。

服务			
<input type="button" value="+ 新建"/>	<input type="button" value="X 删除"/>		
<input type="checkbox"/>	名称	类型	端 口
	http	HTTP	80
	smtp	TCP	25
	pop3	TCP	110
	dns	DNS	53
	https	HTTPS	443
	ssl	SSL	443
	imap_ssl	SSL	993
	smtp_ssl	SSL	465
	pop3_ssl	SSL	995
	<u>radius_auth</u>	RADIUS	1812
	<u>radius_acct</u>	RADIUS	1813

第二步：在『应用负载』→『IP 组』页面，新建一个 IP 组，将外网 IP 添加到这个 IP 组，配置如下图：

IP组

新建

属性

名称 外网IP组

IP组 已选择

待选

电信 212.10.204.26
网通 61.139.2.34

(最多可以添加32个IP)

显示WAN口IP对应的互联网IP

取消 完成

第三步：在『应用负载』→『会话保持』页面，新建会话保持方式，配置 Radius 会话保持，配置如下图：

会话保持

新建

属性

名称

类型 Radius

配置

属性ID User-Name 1
超时时间 1 天
优先于繁忙 启用 禁用

取消 完成

第四步：在『应用负载』→『节点池』页面，新建一个节点池，将服务器的 IP 地址添加到节点池中，设置好节点监视器，会话保持方式，节点选择策略选轮询等，配置如下图：

节点池

新建

配置

名称:

节点选择策略: 轮询

会话保持: none

备用会话保持: none

已选择: 节点状态监视器

待选: 常规监视器
ping
ping6
connect_tcp
connect_udp
http
ftp
pop3

节点有效条件: 至少 1 个常规监视器通过

恢复时间: 0 秒

温暖时间: 0 秒

节点池繁忙处理策略: 强制调度 () 排队等待 () 调度失败 (checked)

连接数统计: 全状态统计 (checked) ESTABLISHED状态统计

节点

节点列表: 起始地址
结束地址
端口 权重 添加 删除

当前已配置 0/500 个节点

取消 完成

第五步：在『应用负载』→『虚拟服务』页面，新建一个虚拟服务，关联上设置好的各个选项，配置虚拟服务页面如下图：

虚拟服务 | 虚拟服务关联组

新建

属性

名称:

状态: 启用 禁用

配置

负载模式: 七层

服务: radius_auth

IP 组: --请选择--

前置策略: (可以配置0~100个前置策略)

默认节点池: --请选择--

QoS策略: --未启用--

SNAT地址集: --未启用--



若需配置Radius计费负载，请按上述配置步骤再配置一个radius_acct虚拟服务，在配置时，请注意需要配置相同的会话保持方法并调度到同一个节点池。

16.5. 传输客户端 IP 至后台服务器配置案例

需求：AD 旁路模式部署，内网有两台 WEB 服务器，访问端口为 TCP 80，需要实现服务器的轮询负载，并且对客户端的访问进行优化，同时要求 WEB 服务器获得真实的客户端源地址。

配置步骤：

第一步：参考第 7 章 7.1 服务，新建一个服务，设置好服务类型和服务端口，由于 AD 设备默认已经有 HTTP 服务，因此这一步骤可省略。

第二步：新建一个 IP 组，将外网 IP 添加到这个 IP 组，详细配置请参考 6.2 IP 组。

第三步：参考 6.5 节点池，新建一个节点池，将服务器的 IP 地址添加到节点池中，设置好节点监视器，节点选择策略选轮询，配置如下图：

The screenshot shows the 'Node Pool' configuration page. In the 'Configuration' tab, the 'Selection Strategy' is set to 'Round Robin'. Under 'Monitors', there is a list of monitors: ping, ping6, connect_tcp, connect_udp, http, ftp, and pop3. The 'Effective Condition' is set to 'At least 1 monitor passes'. The 'Recovery Time' and 'Warmup Time' are both set to 0 seconds. Under 'Load Balancing Strategy', 'Round Robin' is selected. The 'Connection Statistics' section shows 'Full Status Statistics' is selected. In the 'Nodes' tab, there is a table for adding nodes with columns for 'Start Address', 'End Address', 'Port', 'Weight', 'Add', and 'Delete'. It also displays the message 'Currently configured 0/500 nodes'. At the bottom are 'Cancel' and 'Finish' buttons.

第四步：参考 6.7.2 优化策略，新建一个优化策略，启用传输客户端 IP 至后台服务器，并进行相关配置，配置优化策略界面如下图所示：

前置调度策略 | 优化策略 | **HTTP改写策略** | HTTP防护策略 | TCP策略 | SSL策略 | URL下载速度控制 | QoS策略

新建

属性

名称 (长度限制为1~63字符，且不能包含`| " , : % < > / \`特殊字符)

HTTP连接池

状态 启用 禁用

HTTP缓存

状态 启用 禁用

HTTP压缩

状态 启用 禁用

其他

传输客户端IP至后台服务器 启用 禁用

使用HTTP头部携带的IP连接服务器 启用 禁用

取消 **完成**

第五步：参考 6.8 虚拟服务，新建一个虚拟服务，关联上设置好的各个选项，配置虚拟服务页面如下图：

虚拟服务 | 虚拟服务关联组 | 新建

属性

名称:
状态: 启用 禁用

配置

负载模式: 七层
服务: http
IP 组: --请选择--
调度方式: 首个请求 每一个请求

前置策略:
(可以配置0~100个前置策略)

默认节点池: --请选择--
优化策略: --未启用--
HTTP防护策略: HTTP防护策略
TCP策略: 七层虚拟服务TCP策略
QoS策略: --未启用--
SNAT地址集: --未启用--

16.6. 入站前置调度策略案例

需求：内网有两台 web 服务器 A 和 B 提供同一域名服务，访问端口为 TCP 80，域名是 sangfor.com，需要实现服务器的轮询负载，服务器 A 的性能比 B 强。有一个特殊的 IP 地址 202.96.130.36 需要一直调度到服务器 A 上来访问。

配置步骤：

第一步：参考第 7 章 7.1 服务，新建一个服务，设置好服务类型和服务端口，由于 AD 设备默认已经有 HTTP 服务，因此这一步骤可省略。

第二步：新建一个 IP 组，将外网 IP 添加到这个 IP 组，详细配置请参考第 7 章 7.2 IP 组。

第三步：参考 6.5 节点池，新建一个节点池，将服务器的 IP 地址添加到节点池中，设置好节点监视器，会话保持方式，节点选择策略选轮询，配置如下图：

节点池

新建

配置

名称:

节点选择策略: 轮询

会话保持: none

备用会话保持: none

已选择:

节点状态监视器:

待选:

常规监视器

ping

ping6

connect_tcp

connect_udp

http

ftp

pop3

节点有效条件: 至少 1 个常规监视器通过

恢复时间: 0 秒

温暖时间: 0 秒

节点池繁忙处理策略:

○ 强制调度 ○ 排队等待 调度失败

连接数统计:

全状态统计 ESTABLISHED 状态统计

节点

节点列表:

起始地址:

结束地址:

端口: 权重: 1

添加

删除

当前已配置 0 / 500 个节点

取消 完成

第四步：参考 6.5 节点池，再新建一个节点池，将服务器 A 的 IP 地址添加到节点池中，设置好节点监视器，节点选择策略选轮询，配置如下图：

节点池

新建

配置

名称:

节点选择策略: 轮询

会话保持: none

备用会话保持: none

已选择:

待选: 常规监视器
ping
ping6
connect_tcp
connect_udp
http
ftp
pop3

节点状态监视器:

节点有效条件: 至少 1 个常规监视器通过

恢复时间: 0 秒

温暖时间: 0 秒

节点池繁忙处理策略: 强制调度 排队等待 调度失败

连接数统计: 全状态统计 ESTABLISHED状态统计

节点

节点列表: 起始地址
结束地址
端口 权重 添加 删除

当前已配置 0/500 个节点

取消 完成

第五步：参考 6.7.1 前置调度策略，新建一个前置调度策略，选择服务，源 IP 范围，高级条件可不设置，调度节点池为第四步中配置的优先调用的节点，失败动作设置为匹配下一条。

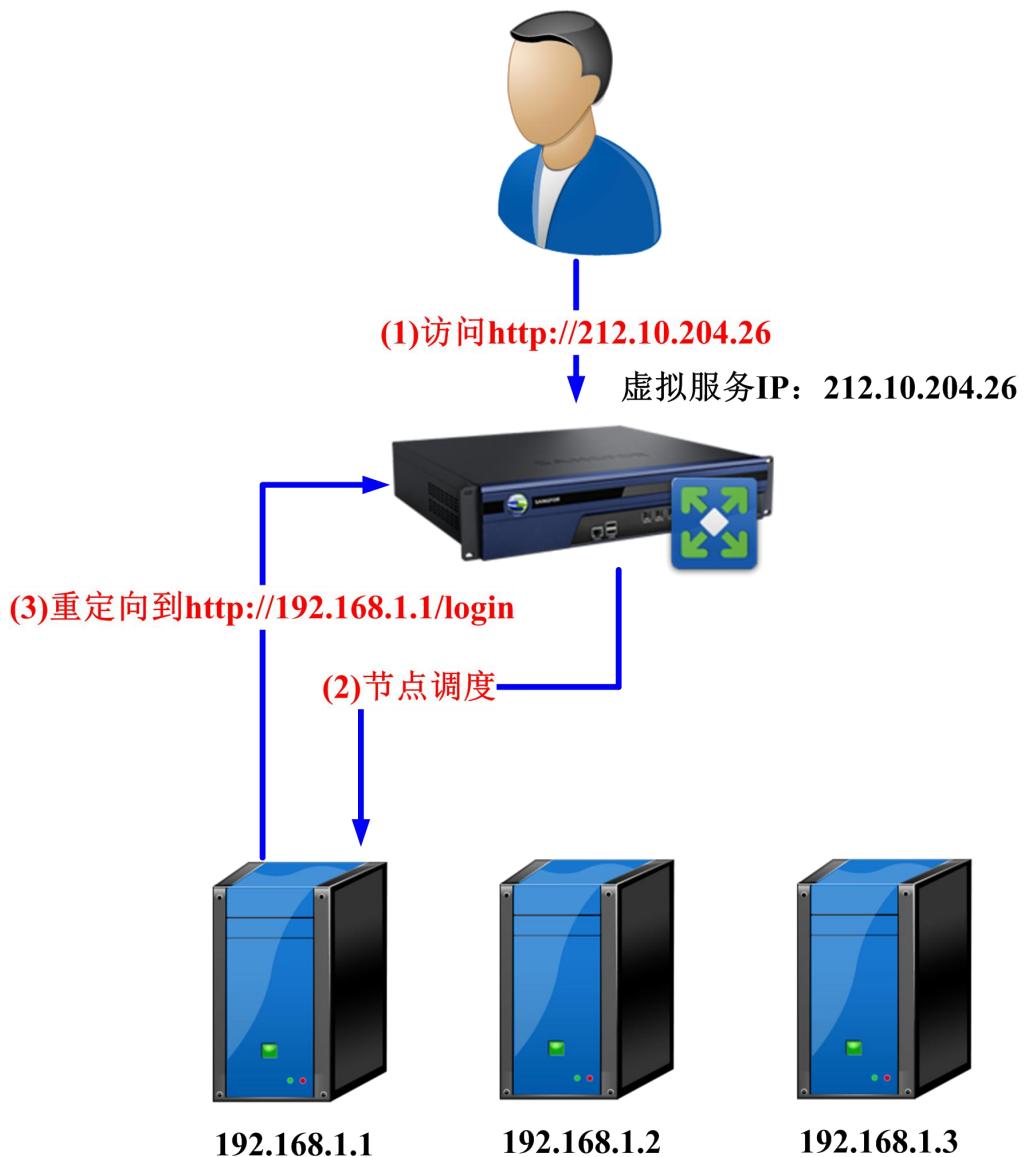
The screenshot shows a configuration interface for Sangfor Cloud. At the top, there is a navigation bar with tabs: 前置调度策略 (Frontend Load Balancing Policy), 优化策略 (Optimization Policy), HTTP改写策略 (HTTP Rewrite Policy), HTTP防护策略 (HTTP Protection Policy), TCP策略 (TCP Policy), SSL策略 (SSL Policy), URL下载速度控制 (URL Download Speed Control), and QoS策略 (QoS Policy). The current tab is "HTTP改写策略". Below the navigation bar, there is a sub-menu for "新建" (New) and a section titled "属性" (Properties) with a "名称" (Name) input field. Under "关联属性" (Associated Properties), there are dropdown menus for "服务" (Service), "源IP范围" (Source IP Range), "调度节点池" (Scheduling Node Pool), and "失败动作" (Failure Action). At the bottom of the dialog are two buttons: "取消" (Cancel) and "完成" (Finish).

第六步：参考 6.8 虚拟服务，新建一个七层虚拟服务，关联上设置好的各个选项，配置虚拟服务页面如下图：

The screenshot shows a configuration interface for Sangfor Cloud. At the top, there is a navigation bar with tabs: 虚拟服务 (Virtual Service), 优化策略 (Optimization Policy), HTTP改写策略 (HTTP Rewrite Policy), HTTP防护策略 (HTTP Protection Policy), TCP策略 (TCP Policy), SSL策略 (SSL Policy), URL下载速度控制 (URL Download Speed Control), and QoS策略 (QoS Policy). The current tab is "虚拟服务". Below the navigation bar, there is a sub-menu for "新建" (New) and a section titled "属性" (Properties) with a "名称" (Name) input field and a note about character length and restrictions. There is also a radio button for "启用" (Enable). Under "配置" (Configuration), there is a section for "负载模式" (Load Mode) set to "七层" (Layer 7), and dropdown menus for "服务" (Service) and "IP 组" (IP Group). Below this is a "前置策略" (Pre-Route Policy) section with a list area and move buttons. At the bottom, there are dropdown menus for "默认节点池" (Default Node Pool), "QoS策略" (QoS Policy), and "SNAT地址集" (SNAT Address Set).

16.7. HTTP 头部改写配置案例

用户那边有多台 HTTP 服务器提供 WEB 服务，用 AD 设备实现服务器负载。当客户端访问网站根目录的时候 (<http://212.10.204.26>)，后台服务器会重定向到节点 IP 的 local 目录下 (<http://192.168.1.1/login/>)，就会造成客户端无法访问。需要通过 AD 设备修改后台服务器的 HTTP 应答的头部，将后台服务器重定向的内容“<http://192.168.1.1/login/>”改成“<http://212.10.204.26/login>”并让用户后续的访问仍然调度到 192.168.1.1，则要通过配置 HTTP 头部改写功能来实现。



配置步骤：

第一步：在『应用负载』→『服务』页面，新建一个 http 服务，步骤省略。

服务			
	名称	类型	端口
	http	HTTP	80
	smtp	TCP	25
	pop3	TCP	110
	dns	DNS	53
	https	HTTPS	443
	ssl	SSL	443
	imap_ssl	SSL	993
	smtp_ssl	SSL	465
	pop3_ssl	SSL	995
	<u>radius_auth</u>	RADIUS	1812
	<u>radius_acct</u>	RADIUS	1813

第二步：在『应用负载』→『IP组』页面，新建一个IP组，将外网IP添加到这个IP组，配置如下图：



The screenshot shows the 'IP组' (IP Group) configuration page. A new group is being created with the name 'HTTP头部改写'. In the '已选择' (Selected) section, the IP address '212.10.204.26' is listed under the '电信' (Telecommunications) provider. In the '待选' (Available) section, the IP address '61.139.2.34' is listed under the '网通' (China Telecom) provider. There are arrows between the two sections to move selected IPs. A note at the bottom left says '(最多可以添加32个IP)' (Up to 32 IPs can be added). A checked checkbox at the bottom right says '显示WAN口IP对应的互联网IP' (Show WAN port IP corresponding to the Internet IP). At the bottom are '取消' (Cancel) and '完成' (Finish) buttons.

第三步：在『应用负载』→『会话保持』页面，新建会话保持方式，配置会话保持，配置如下图：

会话保持

编辑

普通属性

名称: SourceIP (长度限制为1~63字符, 且不能包含& | " ' , : % < > / \ 特殊字符)

类型: SourceIP

超时时间: 1 天

配置

IPv4掩码: 24

IPv6前缀: 96

优先于繁忙: 启用 禁用

取消 完成

第四步：在『应用负载』→『节点池』页面，新建一个节点池，将服务器的 IP 地址添加到节点池中，设置好节点监视器，会话保持方式，节点选择策略选轮询等，配置如下图：

节点池

新建

配置

名称: (长度限制为1~63字符, 且不能包含& | " ' , : % < > / \ 特殊字符)

节点选择策略: 轮询

会话保持: none

备用会话保持: none

已选择: 待选

常规监视器: ping, ping6, connect_tcp, connect_udp, http, ftp, pop3

节点状态监视器:

节点有效条件: 至少 1 个常规监视器通过

恢复时间: 0 秒

温暖时间: 0 秒

节点池繁忙处理策略: 强制调度 排队等待 调度失败

连接数统计: 全状态统计 ESTABLISHED状态统计

第五步：在『应用负载』→『策略』→『HTTP 头部改写』页面，新建一个应答改写策略，关联上设置好的各个选项，配置 HTTP 头部改写策略页面如下图：

前置调度策略 | 优化策略 | HTTP改写策略 | TCP策略 | SSL策略 | URL下载速度控制 | QoS策略

新建

属性

名称: HTTP应答改写
类型: 应答改写

关联属性

源IP范围: 所有地址
高级条件匹配:
请求行 应答行 请求头部 应答头部
字段: URI
条件: 等于 /
属性: 区分大小写 条件取反
请求行 URI 等于 / aa

动作: 改写头部
头部名称: location
匹配内容: *
改写内容: http://212.10.204.26/login (长度限制为0~255个字符)
变量编码方式: 原文

第六步：在『应用负载』→『策略』→『前置调度策略』页面，新建一个前置调度策略，关联上设置好的各个选项，配置前置调度策略页面如下图：

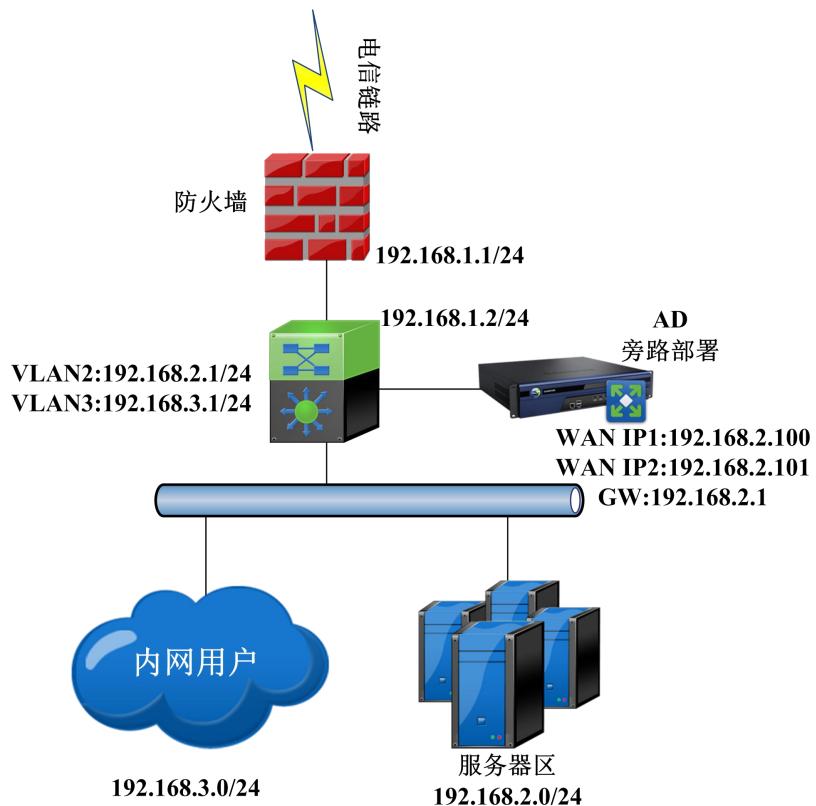


第七步：在『应用负载』→『虚拟服务』页面，新建一个七层虚拟服务，关联上设置好的各个选项，配置虚拟服务页面如下图：



16.8. 三角传输配置案例

某客户拓扑如下，客户需要实现 WEB 服务器负载，但是不在 AD 设备做 SNAT 功能，让服务器回包经过三层交换机直接返回给客户端，不经过 AD 设备。以便减轻 AD 设备的压力。



配置方法：

第一步：参考 6.1 服务，新建一个 TCP 服务，设置好服务类型和服务端口。

服务

编辑

属性

名称: (长度限制为1~63字符, 且

类型: TCP

端口:

端口列表:

第二步：新建一个 IP 组，将外网 IP(192.168.2.100)添加到这个 IP 组，详细配置请参考 6.2 IP 组。

第三步：参考 6.5 节点池，新建一个节点池，将服务器的 IP 地址添加到节点池中，设置好节点监视器，节点选择策略选加权轮询，配置如下图：

节点池

新建

配置

名称:

节点选择策略: 轮询

会话保持: none

备用会话保持: none

已选择:

节点状态监视器:

待选: 常规监视器
ping
ping6
connect_tcp
connect_udp
http
ftp
pop3

节点有效条件: 至少 个常规监视器通过

恢复时间: 0 秒

温暖时间: 0 秒

节点池繁忙处理策略: 强制调度 排队等待 调度失败

连接数统计: 全状态统计 ESTABLISHED状态统计

节点

节点列表: 起始地址
结束地址
端口 权重

当前已配置0/500个节点

取消 完成

第四步：新建虚拟服务，并且启用三角传输功能，界面如下：

属性

名称

状态 启用 禁用

配置

负载模式 四层

服务

IP 组

前置策略 

(可以配置0~100个前置策略)

默认节点池

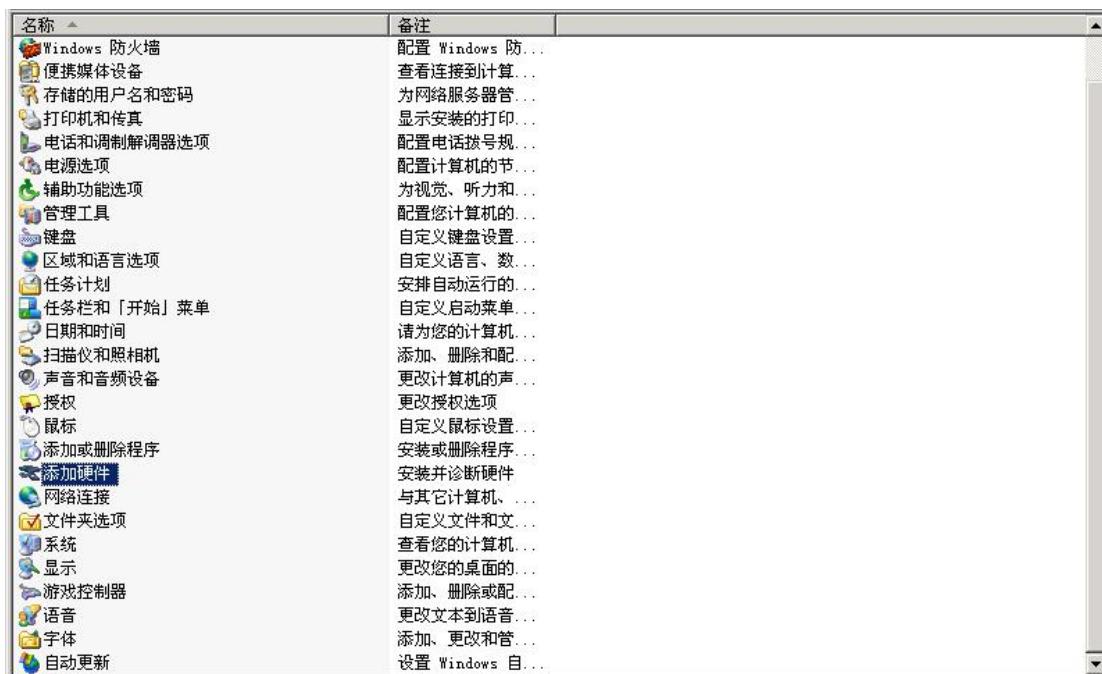
QoS策略

SNAT地址集

三角传输 启用 禁用

第五步：在两台服务器上添加 Loopback Adapter 虚拟网卡，并且设置网卡 IP 地址为虚拟服务 IP 组的 IP 地址，本案例中设置为 192.168.2.100，界面如下：

首先进入服务器的控制面板，双击添加硬件：



添加硬件向导



欢迎使用添加硬件向导

这个向导帮助您：

- 安装软件来支持添加到计算机的硬件。
- 解决您的硬件问题。

 **如果硬件带安装 CD，建议您单击“取消”，关闭这个向导，用制造商的 CD 来安装这个硬件。**

要继续，请单击“下一步”。

< 上一步(B) **下一步(N) >**

取消

添加硬件向导

硬件是否已连接？

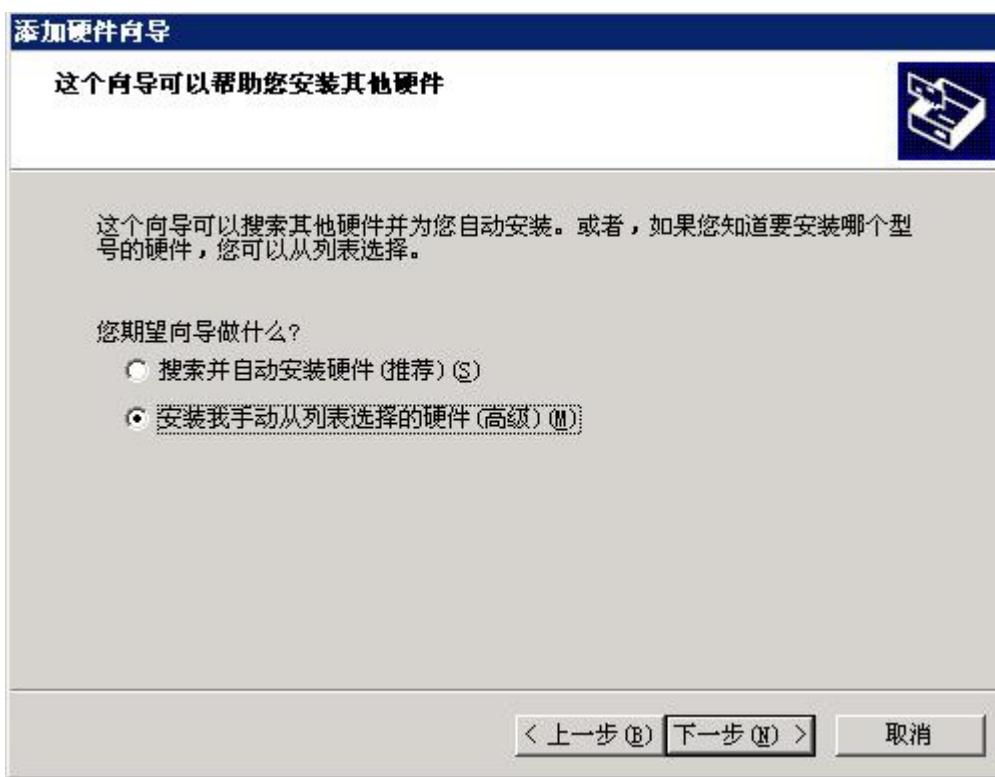
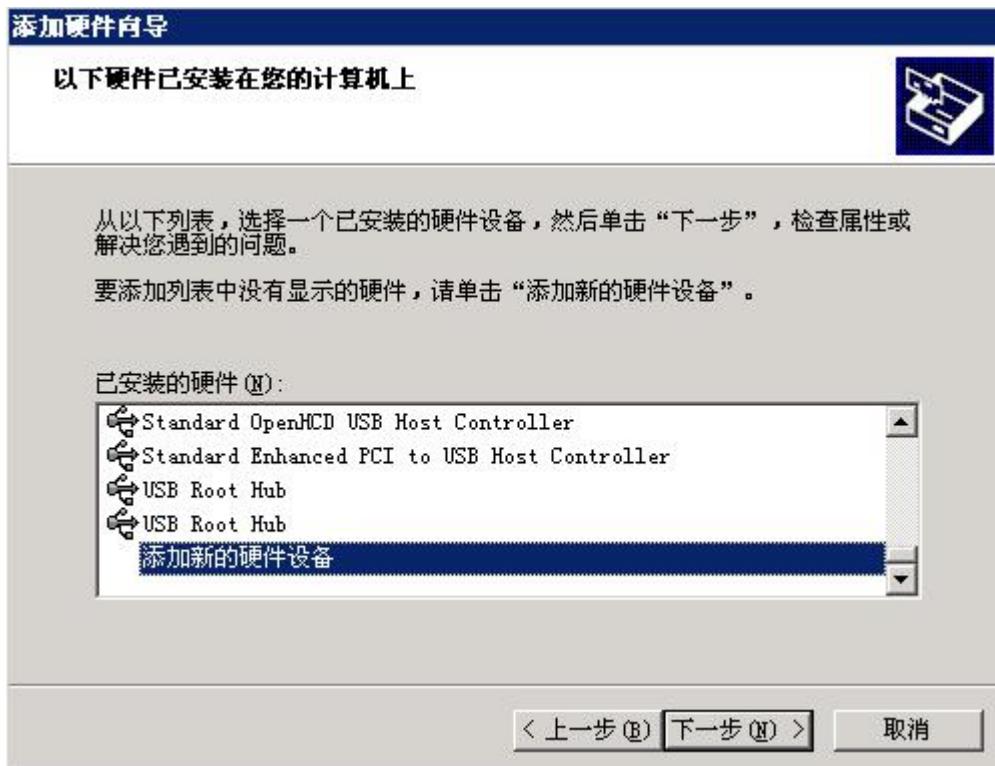


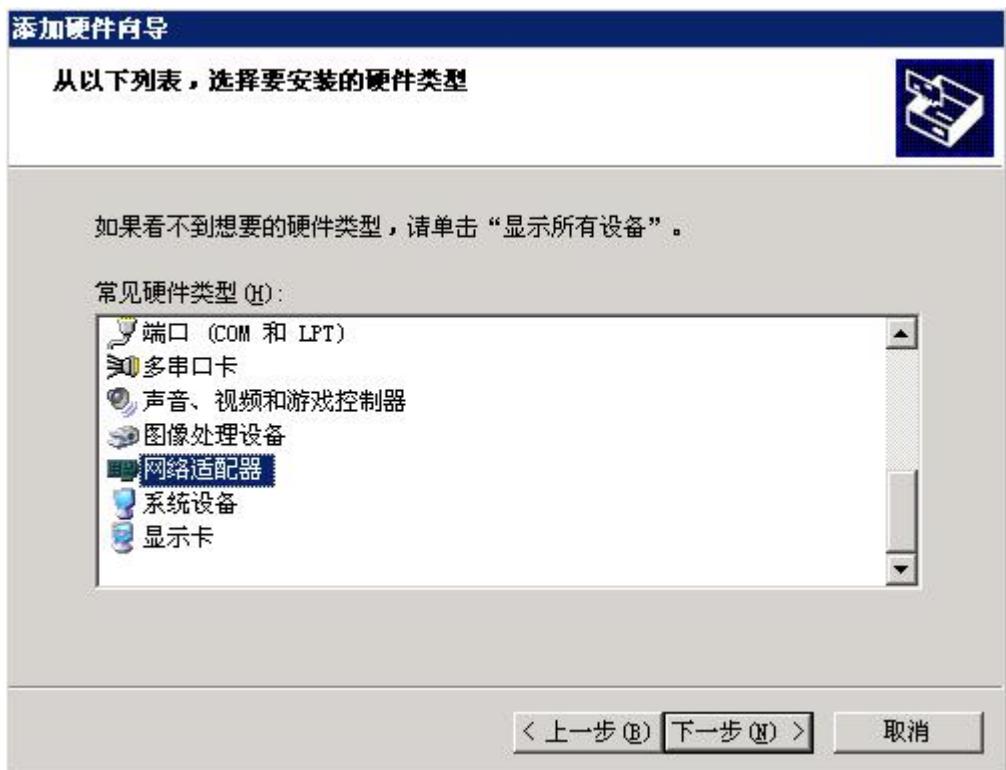
您是否已将这个硬件跟计算机连接？

- 是，硬件已连接好 (I)
 否，尚未添加硬件 (N)

< 上一步(B) **下一步(N) >**

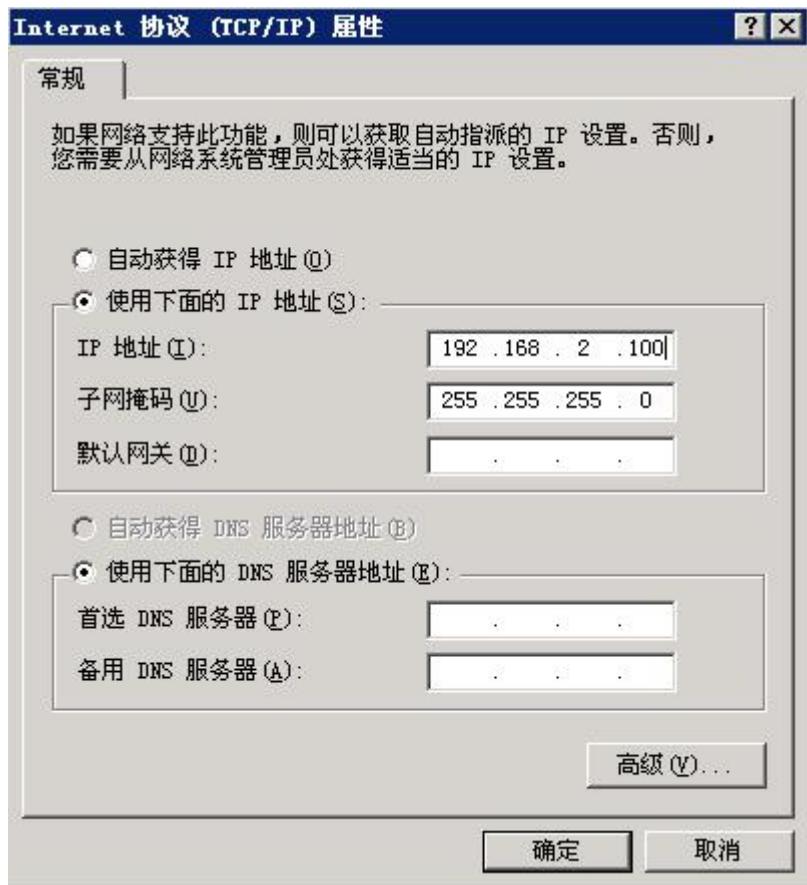
取消







添加成功之后在网上邻居找到该网卡，修改 IP 地址即可，界面如下：



第六步：配置完成。



1. 该案例中如果启用了三角传输又针对所有源 IP 做了 SNAT（代理上网），则不能实现三角传输功能，服务器回包还是会经过 AD 设备。
2. 旁路模式部署需要 WAN 口设置多 IP，第一个 IP 不能是虚拟服务发布的 IP，否则节点监视器无法监视节点。因为三角传输发布的虚拟服务的 IP 是服务器上 loopback IP，如果 AD 设备以这个 loopback IP 发给服务器时，服务器无法回包给 AD。

16.9. SSL 策略配置案例

需求：设备路由模式部署，服务器提供 HTTP 服务，需要实现客户端访问服务的时候，后台 AD 建立 https 通道，实现加密公网传输数据的需求，同时对客户端的认证做会话保持。

配置步骤：

第一步：新建一个服务类型为 https 的服务，详细配置步骤请参照 6.1 服务，设置 https 页面如下图。



第二步：新建一个 IP 组，将外网 IP 添加到这个 IP 组，详细配置请参照 6.2 IP 组。

第三步：新建一个服务器证书，详细配置请参照 6.6.1 服务器证书。

第四步：新建一个节点池，将服务器的 IP 地址添加到节点池中，详细配置请参照 6.5 节点池。

第五步：新建一个 SSL 策略，详细配置请参照 6.7.5 SSL 策略。配置截图如下所示：

属性

名称

配置

RSA服务器证书

国密服务器证书 (签名证书)

国密服务器证书 (加密证书)

启用协议 SSL3.0 TLS1.0 TLS1.1 TLS1.2 国密1.1

已选择 (选择ECDH算法必须启用客户端认证)

待选

SSL_RSA_WITH_NULL_MD5
SSL_RSA_WITH_NULL_SHA
TLS1_TXT_ECC_SM2_WITH_SM4_128_CBC_SM3
TLS1_TXT_ECDHE_SM2_WITH_SM4_128_CBC_SM3

加密算法

TLS_RSA_WITH_AES_256_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_DES_CBC_SHA

会话复用 启用 禁用

缓存会话数量 2000

缓存超时时间 1800 秒

客户端认证 启用 禁用

认证失败默认规则 -

认证失败默认规则 拒绝 -
SSL协议版本未启用 拒绝 -

SSL策略失败规则

第六步：新建一个虚拟服务，详细配置步骤请参照 6.8 虚拟服务，关联上设置好的各个选项，配置虚拟服务页面如下图：

虚拟服务 虚拟服务关联组

新建

属性

名称:

状态: 启用 禁用

配置

负载模式: 七层

服务: https

IP 组: --请选择--

调度方式: 首个请求 每一个请求

前置策略:

(可以配置0~100个前置策略)

默认节点池: --请选择--

优化策略: --未启用--

HTTP防护策略: HTTP防护策略

TCP策略: 七层虚拟服务TCP策略

QoS策略: --未启用--

SNAT地址集: --未启用--

16.10. 智能路由配置案例

某客户以路由模式将 SANGFOR AD 设备部署在网络出口处，外网两条链路，链路 1 是电信线路，链路 2 是网通线路，需要实现内网上网，访问的目标地址是电信的数据走电信线路，访问的目标地址是网通的数据走网通线路，如果访问目标地址既不是电信的也不是网通的，则动态探测目的地址，选择较快的线路。

配置步骤如下：

第一步：设置电信数据走电信线路，新建一个智能路由策略，设置好目的 IP 地址和使用链路范围，配置如下图：

智能路由 出站高级配置 路由测试

新建

属性

名称: (长度为1~63个字符, 且不能包含& () + | ^ ~ , : % < > / \ 特殊字符)

状态: 启用 禁用

配置

源IP地址: 所有IP
目的IP地址: 所有IP
TOS: 0

协议条件: 所有协议 指定类型 TCP

已选择:
待选: wan4

使用链路范围

生效时间: 全天
链路选择策略: 无

链路繁忙保护: 启用 禁用
链路调度失败的默认动作: 四配下一条 丢弃

第二步：设置网通数据走网通线路，新建一个智能路由策略，设置好目的 IP 地址和使用链路范围，配置如下图：

智能路由 出站高级配置 路由测试

新建

属性

名称: (长度为1~63个字符, 且不能包含& () + | ^ ~ , : % < > / \ 特殊字符)

状态: 启用 禁用

配置

源IP地址: 所有IP
目的IP地址: 所有IP
TOS: 0

协议条件: 所有协议 指定类型 TCP

已选择:
待选: wan4

使用链路范围

生效时间: 全天
链路选择策略: 无

链路繁忙保护: 启用 禁用
链路调度失败的默认动作: 四配下一条 丢弃

第三步：设置非电信和非网通的数据，新建一个智能路由策略，设置好目的IP地址和使用链路范围，配置如下图：



The screenshot shows the 'Intelligent Routing' configuration interface. The top navigation bar includes tabs for 'Intelligent Routing' (selected), 'Advanced Outbound Policy', and 'Route Test'. Below the tabs, there's a 'New' button and a 'Properties' section. The 'Properties' section contains fields for 'Name' (with a note about character length and special characters), 'Status' (set to 'Enabled'), and a 'Configuration' section. In the 'Configuration' section, 'Source IP Address' is set to 'All IP Addresses', 'Destination IP Address' is set to 'All IP Addresses', 'TOS' is set to '0', and 'Protocol Condition' is set to 'All Protocols'. There's also a 'Link Range Usage' section where 'wan4' is listed under 'Selected' (indicated by a right-pointing arrow). Other settings include 'Effective Time' (set to 'All Day'), 'Route Selection Strategy' (set to 'None'), 'Link Congestion Protection' (set to 'Enabled'), and 'Route Failure Default Action' (set to 'Match Next'). At the bottom are 'Cancel' and 'Finish' buttons.

配置完成，可以看到智能路由配置页面如下：

智能路由 | 出站高级配置 | 路由测试 |

+ 新建 | - 删 除 | 启用 | 禁用 |  导入 |  导出 | 

<input type="checkbox"/>	名称	源IP	目的IP	协议	使用链路	生效时间	操作
<input type="checkbox"/>	电信走电信	所有	电信	ALL	电信	全天	  
<input type="checkbox"/>	网通走网通	所有	联通(原网通)	ALL	网通	全天	  
<input type="checkbox"/>	动态探测	所有	所有	ALL	电信,网通	全天	  
	Default	所有	所有	ALL	电信,网通	全天	 

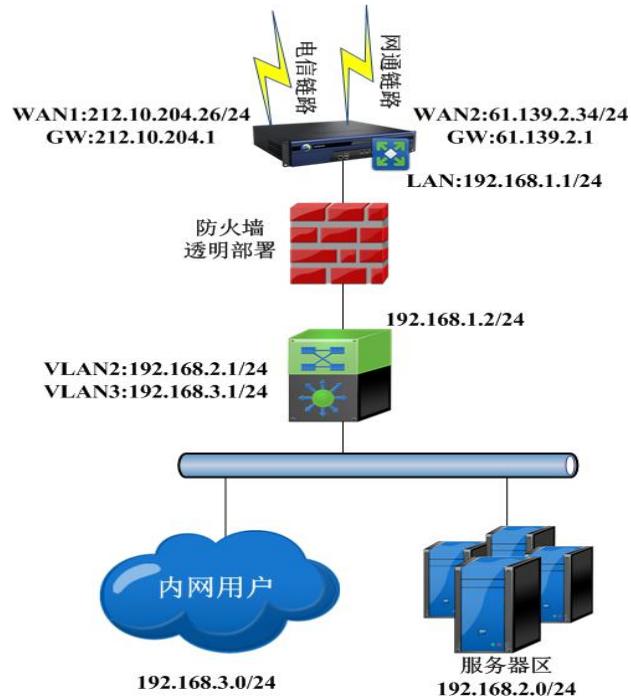
第 1 页, 共1页 | 每页显示条数 20 | 

共 4 / 100 条配置信息

16.11. 智能 DNS 案例

16.11.1. 单站点智能 DNS 链路负载

某客户以路由模式将 SANGFOR AD 设备部署在网络出口处，外网两条链路，链路 1 是电信线路(212.10.204.26)，链路 2 是网通线路(61.139.2.34)，内网服务器区（192.168.2.0）接交换机，外网通过 www.sangfor.com 访问，需要实现外网通过域名访问 WEB 服务器时，当客户端是电信的时候访问电信地址，当客户端是网通的时候访问网通地址，如果两者都不是，则通过动态探测的方式选择一条更快的链路。客户网络拓扑图如下：



准备工作：在公网域名服务商服务器上申请两个 DNS 记录：NS 记录：
 www.sangfor.com—>ns1.sangfor.com； A 记录： ns1.sangfor.com—>212.10.204.26(或
 61.139.2.34)

配置步骤如下：

第一步：基础网络配置，设置好、网络接口的信息，详细配置请参考 9.1 网络接口。

第二步：在『应用负载』→『服务』页面，新建一个服务，设置好服务类型和服务端口：

服务

新建

属性

名称: web服务器

类型: HTTP

端口: 80

添加

删除

端口列表

取消 完成



第三步：在『应用负载』→『IP组』页面，新建一个IP组，选择外网发布的两个IP：

IP组

属性

名称: 外网IP组

地址类型: IPv4

IP组: 已选择

待选:

电信 212.10.204.26
网通 61.139.2.34

(最多可以添加32个IP)

显示WAN口IP对应的互联网IP

取消 完成



第四步：在『应用负载』→『会话保持』页面，新建会话保持方式，这里假设客户希望根据Cookie名称作会话保持：

会话保持

编辑

普通属性

名称	cookie	(长度限制为1~63字符，且不能包含* " " , : % < > / \ 特殊字符)
类型	Cookie	
保持方式	插入	
Cookie名称	insert_cookie	
Cookie作用域	域名:	
	路径:	/
会话Cookie	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
HttpOnly	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用

配置

优先于繁忙	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
-------	-------------------------------------	--------------------------

取消 **完成**

第五步：在『应用负载』→『节点池』页面，新建一个节点池，将服务器的IP地址添加到节点池中：

节点池

新建

配置

名称	输入框
节点选择策略	轮询
会话保持	none
备用会话保持	none
已选择	待选
节点状态监视器	常规监视器 ping ping6 connect_tcp connect_udp http ftp pop3
节点有效条件	至少 1 个常规监视器通过
恢复时间	0 秒
温暖时间	0 秒
节点池繁忙处理策略	<input type="radio"/> 强制调度 <input type="radio"/> 排队等待 <input checked="" type="radio"/> 调度失败
连接数统计	<input checked="" type="radio"/> 全状态统计 <input type="radio"/> ESTABLISHED状态统计

节点

节点列表

起始地址	<input type="text"/>
结束地址	<input type="text"/>
端口	<input type="text"/> 权重 <input type="text" value="1"/>
<input type="button" value="添加"/> <input type="button" value="删除"/>	

当前已配置0/500个节点

第六步：在『应用负载』→『虚拟服务』页面，新建一个七层负载模式的虚拟服务，选择定义好的服务、节点池、IP 组：

虚拟服务

新建

属性

名称 (长度为1~63字符，且不能包含& | " ' , : % < > / \ 特殊字符)

状态 启用 禁用

配置

负载模式 七层

服务

IP 组

前置策略

(可以配置0~100个前置策略)

默认节点池

QoS策略

SNAT地址集

第七步：在『智能 DNS』→『DNS 服务器』页面，添加 DNS 服务器的监听地址：

DNS服务器

更新DNS服务器配置

普通属性

状态 启用 禁用

DNS服务器属性

已选择 监听地址：212.10.204.26, 61.139.2.34

待选

不添加监听IP将使DNS配置失效！

DNS端口：53

不存在的域名处理： 不回应 拒绝 代理

DNS探测属性

探测超时时间：2 秒

探测结果缓存时间：10800 秒

探测方法：DNS反向查询

更新

第八步：在『智能 DNS』→『虚拟 IP 池』→『本地虚拟 IP 池』页面，新建一个本地虚拟 IP 池，添加需要发布的外网 IP，并设置好首选策略为静态就近性，备选策略为动态就近性：

本地虚拟IP池 | 全局虚拟IP池

新建

普通属性

名称: web发布IP
状态: 启用 禁用
类型: IPv4 IPv6

策略配置

主动监视器: 已选择 ping; 待选 ping6, connect_tcp, connect_udp, http, ftp, pop3, smtp, imap
虚拟IP有效条件: 至少 1 个监视器通过
繁忙保护: 启用 禁用
首选策略: 静态就近性
备选策略: 动态就近性

IP池

虚拟IP列表: 地址 [] 端口 [] 协议 [TCP] 权值 [1] 添加
[61.139.2.34:80/1 TCP
212.10.204.26:80/1 TCP]
[localhost
Radius虚拟服务
212.10.204.26:1812/1 UDP
61.139.2.34:1812/1 UDP
传输客户端IP至后台服务器
212.10.204.26:80/1 TCP
三角传输
212.10.204.26:25/1 TCP]

第九步：在『智能 DNS』→『DNS 映射』→『本地 DNS 映射』页面，新建一个本地 DNS 映射，添加需要解析的域名，选择我们要发布的虚拟 IP 池：

本地DNS映射 全局DNS映射

新建

普通属性

名称:
状态: 启用 禁用
类型: IPv4 IPv6

策略配置

域名列表:

选择策略: 静态就近性

会话保持: 启用 禁用
会话超时时间: 300 秒
TTL: 60 秒

已选择:

待选:

虚拟IP池列表:

第十步：在『智能 DNS』→『LDNS 集合』→『本地 LDNS 集合』页面，新建两个本地 LDNS 集合，一个添加电信的地址段，另一个添加网通的地址段：

本地LDNS集合 全局LDNS集合

新建

属性

名称

地址集

地址类型

地址段

当前已配置181/10000个地址范围

本地LDNS集合 全局LDNS集合

新建

属性

名称 网通LDNS

地址集

地址类型 ISP地址段

地址段 联通（原网通）

1.24.0.0-1.31.255.255
1.56.0.0-1.63.255.255
1.188.0.0-1.191.255.255
27.8.0.0-27.15.255.255
27.36.0.0-27.47.255.255
27.98.224.0-27.98.255.255
27.192.0.0-27.223.255.255
58.16.0.0-58.23.255.255

添加

当前已配置 179 / 10000 个地址范围

删除

取消 完成

第十一步：在『智能 DNS』→『静态就近性』→『虚拟 IP 池级别』页面，新建两个静态就近性策略，分别对应的策略是：访问 www.sangfor.com 域名时，当 LDNS 是电信 LDNS 时，返回 212.10.204.26；当 LDNS 是网通 LDNS 时，返回 61.139.2.34：

新建

属性

配置范围 本地 全局

状态 启用 禁用

虚拟IP池 web发布IP

LDNS集合 电信LDNS

已选择列表 212.10.204.26

池内IP < >

可选择列表 61.139.2.34

取消 完成



16.11.2. 分布式部署智能 DNS 链路负载

某客户在广州、北京、西安各有一台 WEB 服务器作为门户网站，外网通过 www.sangfor.com 访问，并且外网都是电信、网通双线路，如下图所示：



现在需要达到以下目的：

1. 华北、东北的用户请求调度到“北京 AD”，并通过相同运营商的线路访问服务器，其他运营商的用户则通过动态检测最快的线路接入。
2. 西北、西南的用户请求调度到“西安 AD”，并通过相同运营商的线路访问服务器，其他运营商的用户则通过动态检测最快的线路接入。
3. 华中、华南的用户请求调度到“广州 AD”，并通过相同运营商的线路访问服务器，其他运营商的用户则通过动态检测最快的线路接入。
4. 其他地区的用户请求调度到“北京 AD”，并通过相同运营商的线路访问服务器，其他运营商的用户则通过动态检测最快的线路接入。

现在以“广州 AD”为配置实例，链路 1 是电信线路(212.10.204.26)，链路 2 是网通线路(61.139.2.34)，内网 WEB 服务器（192.168.1.2）接内网交换机。

准备工作：在公网域名服务商服务器上申请两个 DNS 记录：NS 记录：
www.sangfor.com—>ns1.sangfor.com； A 记录： ns1.sangfor.com—>212.10.204.26(或 61.139.2.34)

配置步骤如下：

第一步：在『应用负载』→『服务』页面，新建一个服务，设置好服务类型和服务端口：

服务

新建

属性

名称: web服务器

类型: HTTP

端口: 80

添加

删除

端口列表

取消 完成



第二步：在『应用负载』→『IP组』页面，新建一个IP组，选择外网发布的两个IP：

IP组

属性

名称: 外网IP组

地址类型: IPv4

IP组: 已选择

待选:

电信 212.10.204.26
网通 61.139.2.34

(最多可以添加32个IP)

显示WAN口IP对应的互联网IP

取消 完成



第三步：在『应用负载』→『节点池』页面，新建一个节点池，将服务器的IP地址添加到节点池中：

节点池

新建

配置

名称:

节点选择策略: 轮询

会话保持: none

备用会话保持: none

已选择: 节点状态监视器

待选: 常规监视器
ping
ping6
connect_tcp
connect_udp
http
ftp
pop3

节点有效条件: 至少 个常规监视器通过

恢复时间: 0 秒

温暖时间: 0 秒

节点池繁忙处理策略: 强制调度 () 排队等待 () 调度失败 (checked)

连接数统计: 全状态统计 (checked) ESTABLISHED状态统计

节点

节点列表: 起始地址
结束地址
端口 权重
 添加
 删除

当前已配置 0/500 个节点

取消 完成

第四步：在『应用负载』→『虚拟服务』页面，新建一个七层负载模式的虚拟服务，选择定义好的服务、节点池、IP 组：

虚拟服务

新建

属性

名称 (长度为1~63字符，且不能包含& | " ' , : % < > / \ 特殊字符)

状态 启用 禁用

配置

负载模式 七层

服务

IP 组

前置策略

(可以配置0~100个前置策略)

默认节点池

Qos策略

SNAT地址集

↑ ↓ ← →

第五步：在『公共对象』→『IP 地址集』→『用户地域』页面，新建用户地域，添加上华北/东北、西北/西南、华中/华南以及所有地域的地域地址段，如下图：

ISP地址段 | 全球地址段 | 用户地域 | 自动更新 | 帮助信息

编辑

属性

名称 华北 东北

描述

配置

地域选择 亚太 - 选择国家 - - 选择省市 - 添加

亚太/China/河南省
亚太/China/山西省
亚太/China/北京市
亚太/China/天津市
亚太/China/内蒙古自治区
亚太/China/黑龙江省
亚太/China/吉林省
亚太/China/辽宁省

删除

地址范围 [] - [] 添加

1.12.0.0-1.15.255.255
1.24.0.0-1.31.255.255
1.56.0.0-1.63.255.255
1.68.0.0-1.71.255.255
1.88.0.0-1.93.255.255
1.180.0.0-1.183.255.255
1.188.0.0-1.199.255.255
1.202.0.0-1.203.255.255

当前已配置497/10000个地址范围

删除

ISP地址段 | 全球地址段 | **用户地域** | 自动更新 | 帮助信息

新建

属性

名称 西北 西南

描述

配置

地域选择 亚太 ▾ China ▾ 湖北省 ▾ **添加**

亚太/China/甘肃省
亚太/China/宁夏回族自治区
亚太/China/青海省
亚太/China/新疆维吾尔自治区
亚太/China/陕西省
亚太/China/四川省
亚太/China/重庆市
亚太/China/贵州省

地址范围

27.224.0.0-27.227.255.255
59.76.0.0-59.76.41.255
60.13.0.0-60.13.63.255
60.164.0.0-60.165.255.255
61.134.64.0-61.134.95.255
61.159.64.0-61.159.127.255
61.178.0.0-61.178.255.255
115.85.192.0-115.85.255.255

当前已配置**282**/10000个地址范围

删除

ISP地址段 全球地址段 **用户地域** 自动更新 [帮助信息](#)

新建

属性

名称: 华中 华南

描述:

配置

地域选择: 亚太 ▾ China ▾ 澳门特别行政区 ▾ [添加](#)

亚太/China/湖北省
亚太/China/湖南省
亚太/China/广西壮族自治区
亚太/China/广东省
亚太/China/海南省
亚太/China/香港特别行政区
亚太/China/澳门特别行政区

[删除](#)

地址范围: - [添加](#)

27.16.0.0-27.31.255.255
58.19.0.0-58.19.255.255
58.48.0.0-58.55.255.255
59.68.0.0-59.68.63.255
59.68.80.0-59.68.233.255
59.172.0.0-59.175.255.255
61.45.128.0-61.45.191.255
61.136.128.0-61.136.255.255

当前已配置**269**/10000个地址范围

[删除](#)

ISP地址段 全球地址段 **用户地域** 自动更新 ? 帮助信息

新建

属性

名称: 所有地域
描述:

配置

地域选择: 亚太 - 选择国家 - 选择省市 -
添加

地址范围: [] - [] 添加
0.0.0.0-255.255.255.255

当前已配置 1/10000 个地址范围
删除



第六步：在『应用负载』→『节点监视器』页面，新建一个监视器，定义为 CONNECT

80:

节点监视器

新建

属性

名称	CONNECT 80
类型	CONNECT (TCP)

基本配置

间隔时间	5	秒
超时时间	2	秒
尝试次数	3	
监视地址	*	
监视端口	80	http
调试	<input type="radio"/> 是	<input checked="" type="radio"/> 否

附加配置

回应内容的最大长度	2048 字节	
发送内容	<input type="text"/>	
接收内容必须包含	<input type="text"/>	
断开之前发送的内容	<input type="text"/>	
启用十六进制模式	<input type="radio"/> 是	<input checked="" type="radio"/> 否

第七步：在『智能 DNS』→『DNS 服务器』页面，添加 DNS 服务器的监听地址：

DNS服务器

更新DNS服务器配置

普通属性

状态 启用 禁用

DNS服务器属性

已选择 待选

212.10.204.26
61.139.2.34

监听地址

不添加监听IP将使DNS配置失效！

DNS端口 53

不存在的域名处理 不回应 拒绝 代理

DNS探测属性

探测超时时间 2 秒

探测结果缓存时间 10800 秒

探测方法 DNS反向查询

更新

第八步：在『智能 DNS』→『站点集合』页面，新建三个站点，分别定义为本地站点、北京 AD、西安 AD，并定义好通讯 IP 地址和端口：

站点集合

新建

普通属性

站点名称：本地站点
地理位置：广州

站点通讯配置

地址列表

已选择：212.10.204.26
61.139.2.34

待选：电信
网通

通讯端口：558
同步角色：Server
同步公差：5 秒
通信加密密钥：
再次输入密钥：

取消 完成

站点集合 帮助信息

新建

普通属性

站点名称

站点通讯配置

地址列表

220.181.220.14
61.48.20.10

通讯端口

站点集合 帮助信息

新建

普通属性

站点名称

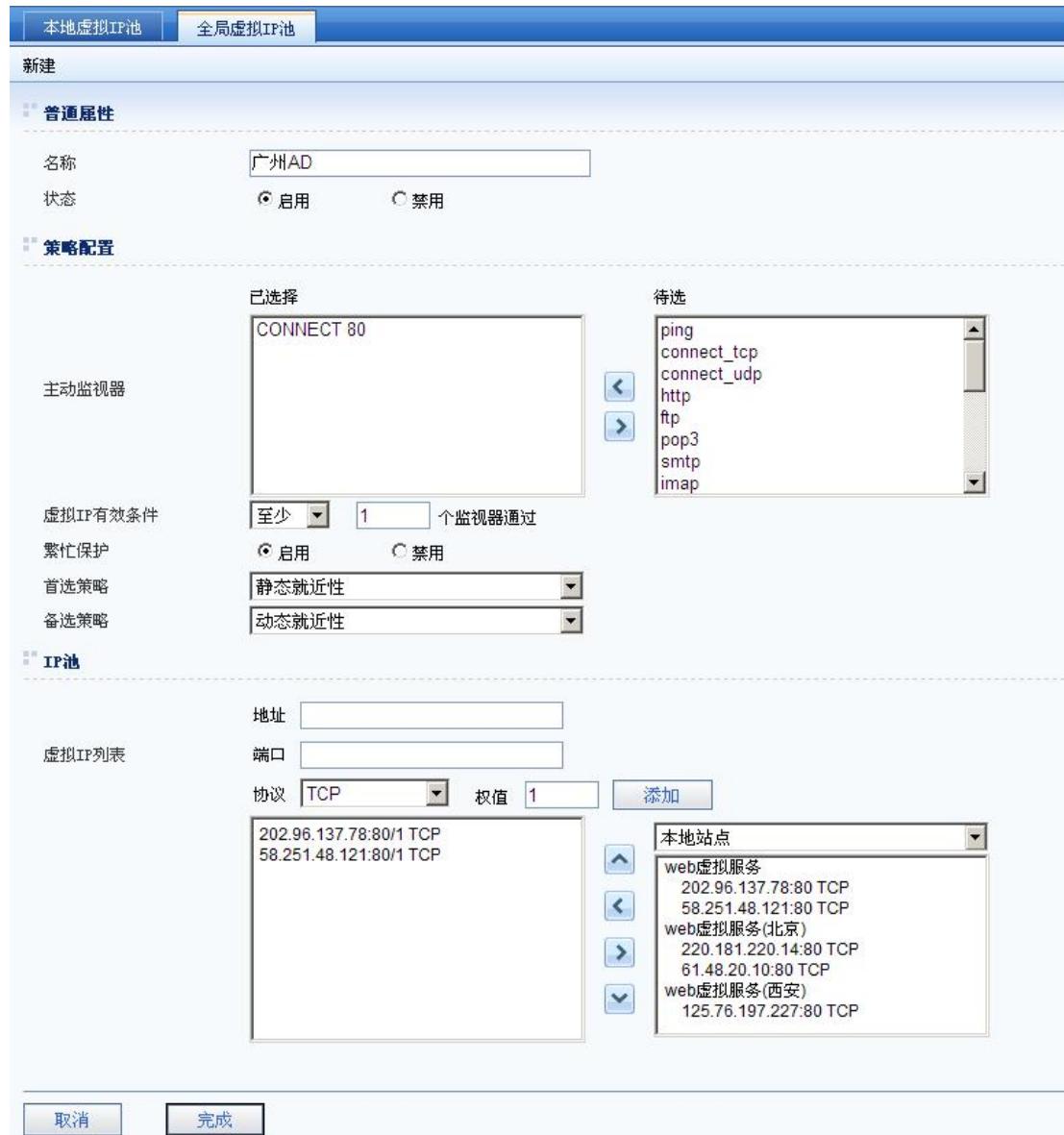
站点通讯配置

地址列表

125.76.197.227
60.161.63.20

通讯端口

第九步：在『智能 DNS』→『虚拟 IP 池』→『全局虚拟 IP 池』页面，新建三个虚拟 IP 池，分别定义为广州 AD、北京 AD、西安 AD，并定义好发布的 IP 和端口：



虚拟 IP 列表选择广州 AD 发布的 IP 和端口，其中，web 虚拟服务（北京）和 web 虚拟服务（西安）分别是从北京 AD 和西安 AD 读取过来的北京 AD 和西安 AD 发布的 IP 和端口。

选择 web 虚拟服务（北京）发布的 IP 和端口，并配置监视器监视说发布服务和端口是否可用。

本地虚拟IP池 全局虚拟IP池

新建

普通属性

名称: 北京AD
状态: 启用 禁用

策略配置

已选择: CONNECT 80
主动监视器

待选: ping, connect_tcp, connect_udp, http, ftp, pop3, smtp, imap

虚拟IP有效条件: 至少 1 个监视器通过
繁忙保护: 启用 禁用
首选策略: 静态就近性
备选策略: 动态就近性

IP池

虚拟IP列表: 地址: [] 端口: [] 协议: TCP 权值: 1 添加

本地站点: web虚拟服务 202.96.137.78:80 TCP
58.251.48.121:80 TCP
web虚拟服务(北京) 220.181.220.14:80 TCP
61.48.20.10:80 TCP
web虚拟服务(西安) 125.76.197.227:80 TCP

取消 完成

选择 web 虚拟服务（西安）发布的 IP 和端口，并配置监视器监视该发布服务和端口是否可用。

本地虚拟IP池 全局虚拟IP池

新建

普通属性

名称: 西安AD
状态: 启用 禁用

策略配置

已选择: CONNECT 80
主动监视器

待选: ping, connect_tcp, connect_udp, http, ftp, pop3, smtp, imap

虚拟IP有效条件: 至少 1 个监视器通过
繁忙保护: 启用 禁用
首选策略: 静态就近性
备选策略: 动态就近性

IP池

虚拟IP列表: 地址: [输入框], 端口: [输入框], 协议: TCP, 权值: 1, 添加

本地站点: 125.76.197.227:80/1 TCP, 61.161.63.20:80/1 TCP

本地站点: web虚拟服务, 202.96.137.78:80 TCP, 58.251.48.121:80 TCP, web虚拟服务(北京), 220.181.220.14:80 TCP, 61.48.20.10:80 TCP, web虚拟服务(西安), 125.76.197.227:80 TCP

取消 完成

第十步：在『智能 DNS』→『DNS 映射』→『全局 DNS 映射』页面，新建一个 DNS 映射：

本地DNS映射 全局DNS映射 帮助信息

新建

普通属性

名称: www.sangfor.com
状态: 启用 禁用

策略配置

域名列表: www.sangfor.com

选择策略: 静态就近性
会话保持: 启用 禁用
会话超时时间: 300 秒
TTL: 60 秒

虚拟IP池列表: 广州AD, 北京AD, 西安AD

已选择列表: 广州AD, 北京AD, 西安AD

可选择列表:

第十一步：在『智能 DNS』→『LDNS 集合』→『全局 LDNS 集合』页面，新建五个 LDNS 集合，分别定义为华北东北、西北西南、华中华南、所有地域、电信、网通：

本地LDNS集合 全局LDNS集合 ? 帮助信息

新建

属性

名称 华北东北

地址集

地址类型 用户地域

地址段 华北 东北

1.12.0.0-1.15.255.255
1.24.0.0-1.31.255.255
1.56.0.0-1.63.255.255
1.68.0.0-1.71.255.255
1.88.0.0-1.93.255.255
1.180.0.0-1.183.255.255
1.188.0.0-1.199.255.255
1.202.0.0-1.203.255.255

当前已配置 497 / 10000 个地址范围

操作

取消 完成

本地LDNS集合 全局LDNS集合 ? 帮助信息

新建

属性

名称 西北西南

地址集

地址类型 用户地域

地址段 西北 西南

1.48.0.0-1.49.255.255
1.204.0.0-1.207.255.255
27.8.0.0-27.31.255.255
27.98.224.0-27.98.255.255
27.144.0.0-27.144.255.255
27.224.0.0-27.227.255.255
58.16.0.0-58.16.255.255
58.17.128.0-58.17.255.255

当前已配置 234 / 10000 个地址范围

操作

取消 完成

本地LDNS集合 全局LDNS集合 帮助信息

新建

属性

名称

地址集

地址类型 添加

地址段

当前已配置 237/10000个地址范围

删除

取消 完成

本地LDNS集合 全局LDNS集合 帮助信息

新建

属性

名称

地址集

地址类型 添加

地址段

当前已配置 1/10000个地址范围

删除

取消 完成

本地LDNS集合 全局LDNS集合 ? 帮助信息

新建

属性

名称

地址集

地址类型 添加

地址段

当前已配置 184/10000 个地址范围

本地LDNS集合 全局LDNS集合 ? 帮助信息

新建

属性

名称

地址集

地址类型 添加

地址段

当前已配置 179/10000 个地址范围

第十二步：在『智能 DNS』→『静态就近性』→『DNS 映射级别』页面，新建三个策略，分别定义为华北东北→北京 AD、西北西南→西安 AD、华中华南→广州 AD、所有地域→北京 AD：



DNS映射级别 虚拟IP池级别

新建

属性

状态 启用 禁用

配置范围 本地 全局

DNS映射: www.sangfor.com

LDNS集合: 华中华南

虚拟IP池: 广州AD

取消 **完成**

DNS映射级别 虚拟IP池级别

新建

属性

状态 启用 禁用

配置范围 本地 全局

DNS映射: www.sangfor.com

LDNS集合: 所有地域

虚拟IP池: 北京AD

取消 **完成**

第十三步：在『智能 DNS』→『静态就近性』→『虚拟 IP 池级别』页面，新建六个策略，分别定义为当 DNS 映射的一级调度方法调度到某虚拟 IP 池时，根据运营商来判断返回相应的 IP 地址给用户：

新建

属性

配置范围

 本地 全局

状态

 启用 禁用

虚拟IP池

广州AD

LDNS集合

电信

已选择列表

可选择列表

池内IP

202.96.137.78

58.251.48.121



取消

完成

新建

属性

配置范围

 本地 全局

状态

 启用 禁用

虚拟IP池

广州AD

LDNS集合

网通

已选择列表

可选择列表

池内IP

58.251.48.121

202.96.137.78



取消

完成

新建

属性

配置范围

 本地 全局

状态

 启用 禁用

虚拟IP池

北京AD

LDNS集合

电信

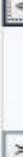
已选择列表

可选择列表

220.181.220.14

61.48.20.10

池内IP



取消

完成

新建

属性

配置范围

 本地 全局

状态

 启用 禁用

虚拟IP池

北京AD

LDNS集合

网通

已选择列表

可选择列表

61.48.20.10

220.181.220.14

池内IP



取消

完成

新建

属性

配置范围 本地 全局

状态 启用 禁用

虚拟IP池: 西安AD

LDNS集合: 电信

已选择列表 可选择列表

池内IP: 125.76.197.227 < 61.161.63.20 >

取消 完成

新建

属性

配置范围 本地 全局

状态 启用 禁用

虚拟IP池: 西安AD

LDNS集合: 网通

已选择列表 可选择列表

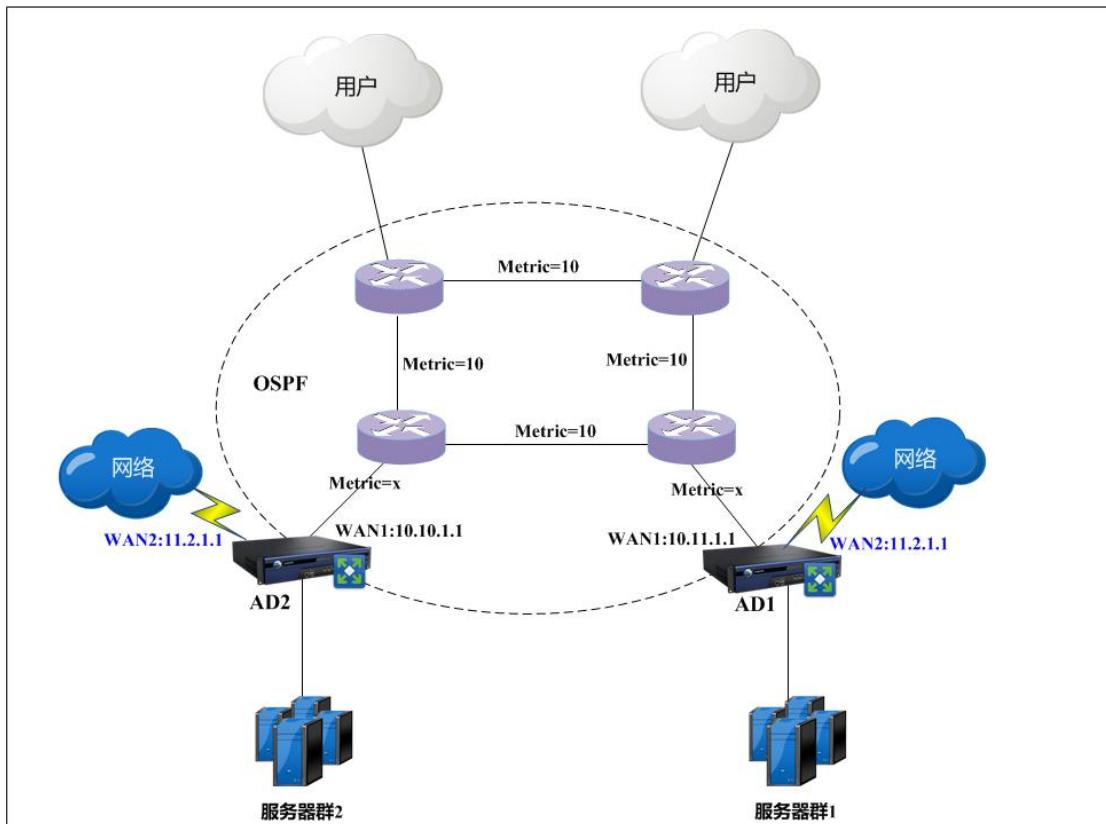
池内IP: 61.161.63.20 < 125.76.197.227 >

取消 完成

16.12. IP-Anycast 配置案例

某客户拓扑如下，客户网络中有两个服务器群，服务器群 1 与服务器群 2，两个服务器

群均提供相同的服务，两台 AD 设备均启用了 OSPF 部署到网络中，并且虚拟服务配置好了，AD1 发布虚拟服务的 IP 组为 11.2.1.1，AD2 发布虚拟服务的 IP 组为 11.2.1.1。现在客户要求用户区域访问虚拟服务的时候实现自动计算最优链路访问到服务器群 1 或者服务器群 2；同时实现冗余备份，当某台 AD 设备的虚拟服务不可用时，用户自动访问到另外一个 AD 设备的虚拟服务。



配置步骤:

第一步：配置虚拟服务，参考服务器负载配置案例，本案例中两台 AD 设备的虚拟服务配置如下图：

AD1 设备的虚拟服务配置

虚拟服务					
+ 新建		X 删除		✓ 启用	✗ 禁用
□	名称	负载模式	服务	IP组	前置策略
□	服务器群1	七层	http	服务器群1	服务器群1

AD2 设备的虚拟服务配置

虚拟服务					
		新建		删除	
		启用		禁用	
名称	负载模式	服务	IP组	前置策略	默认节点池
服务器群2	七层	http	服务器群2		服务器群2

第二步：启用 OSPF，OSPF 详细设置请参考 OSPF 章节，此处不一一截图说明。要使用 IP-Anycast 功能必须启用 OSPF 重分发，Metric-Type 可以选择 Metric-Type1 指定一个值（一般为 0 就可以），也可以选择 Metric-Type2 为默认值，精确就近原则访问时请使用 Metric-Type1，界面如下：

AD1 设备的 OSPF 设置：

全局配置 | 接口配置 | 邻居关系表

全局配置

基本配置

路由器ID: 1
OSPF状态: 启用 禁用

路由重分发配置

默认路由强制重分发: 启用 禁用
静态路由重分发: 启用 禁用
RIP路由重分发: 启用 禁用
Metric-type: Type-1 Type-2
Metric-value: 0

区域配置

区域ID: 1
接受自治系统外部路由: 启用 禁用

运行网段

运行网段: IP地址: []
掩码/前缀: []
[添加] [删除]
10.10.1.0/24

当前已配置1/16个运行网段

更新

AD2 设备的 OSPF 设置:

全局配置 | 接口配置 | 邻居关系表

全局配置

基本配置

路由器ID: 2
OSPF状态: 启用 禁用

路由重分发配置

默认路由强制重分发: 启用 禁用
静态路由重分发: 启用 禁用
RIP路由重分发: 启用 禁用
Metric-type: Type-1 Type-2
Metric-value: 0

区域配置

区域ID: 1
接受自治系统外部路由: 启用 禁用

运行网段

运行网段: IP地址: []
掩码/前缀: []
10.11.1.0/24 []
[添加] [删除]

当前已配置1/16个运行网段

更新

第三步：配置 IP-Anycast，本案例配置如下：

AD1 设备的 IP-Anycast 设置：

IP Anycast

新建IP Anycast

属性

名称: 1
状态: 启用 禁用

配置

虚拟服务: 服务器群1
虚拟IP: 已选择 11.2.1.1
网关: 10.11.1.1

待选

取消 完成

AD2 设备的 IP-Anycast 设置:

IP Anycast

新建IP Anycast

属性

名称: 1
状态: 启用 禁用

配置

虚拟服务: 服务器群2
虚拟IP: 已选择 11.2.1.1
网关: 10.10.1.1

待选

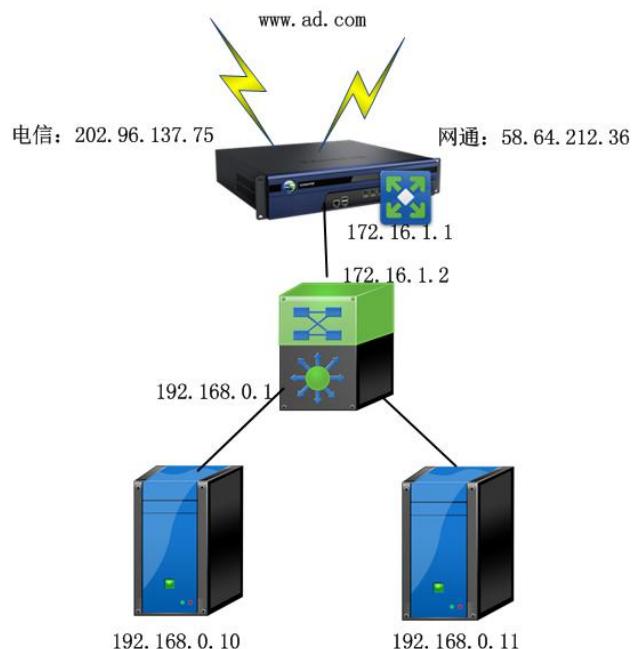
取消 完成

第四步：配置完成。配置完成后，路由器会根据 Metric 值来计算到达两台设备 11.2.1.1

这个 IP 地址的最优路径，用户访问的时候，则路由器根据选择的最优路径转发到对应的 AD 设备。如果 AD1 设备的虚拟服务不可用，则 AD1 设备会向 OSPF 区域通告删除本设备的该路由，于是用户访问到 AD2 设备的虚拟 IP。

16.13. DNS 代理案例

某客户网络拓扑图如下，AD 以路由模式进行部署，同时作为网关代理内网上网，有两条外网线路分别是电信线路和网通线路，IP 分别为 202.96.137.75 和 58.64.212.36，并且这两个 IP 对应同一个域名 www.ad.com；AD 内网接口 IP 为 172.16.1.1；三层交换机接在 AD 下面，和 AD 相连的接口 IP 为 172.16.1.2，和内网相连的接口 IP 为 192.168.0.1；内网电脑使用的网段是 192.168.0.0/24；有两台服务器提供相同的 WEB 服务，IP 地址分别是 192.168.0.10 和 192.168.0.11。客户希望实现 AD 设备可以进行解析域名，并代理内网 PC 转发 DNS 请求。



配置步骤如下：

第一步：『网络配置』→『DNS 代理』，添加电信接口 DNS 服务器。界面如下图所示：

DNS代理 前置调度策略 内网DNS记录 HOSTS

网关DNS设置

DNS服务器列表

网口：	-请选择网络接口-
IP地址：	<input type="text"/>
权值：	<input type="text"/>
WAN1/223.5.5.1	
<input type="button" value="添加"/>	
<input type="button" value="删除"/>	
(设备本机发出的域名解析请求仅使用最前面的三个DNS服务器)	

DNS透明代理

启用DNS代理 启用 禁用

IPv4监听地址

监听端口

缓存 启用 禁用

并发查询 启用 禁用

第二步：『网络配置』→『DNS 代理』，添加网通接口 DNS 服务器。界面如下图所示：

DNS代理 前置调度策略 内网DNS记录 HOSTS

网关DNS设置

DNS服务器列表	网口： <input type="text" value="-请选择网络接口-"/>
	IP地址： <input type="text"/>
	权值： <input type="text"/>
	<input type="button" value="添加"/>
	<input type="button" value="删除"/>
	<input type="button" value="↑"/>
	<input type="button" value="↓"/>
	WAN1/223.5.5.1

(设备本机发出的域名解析请求仅使用最前面的三个DNS服务器)

DNS透明代理

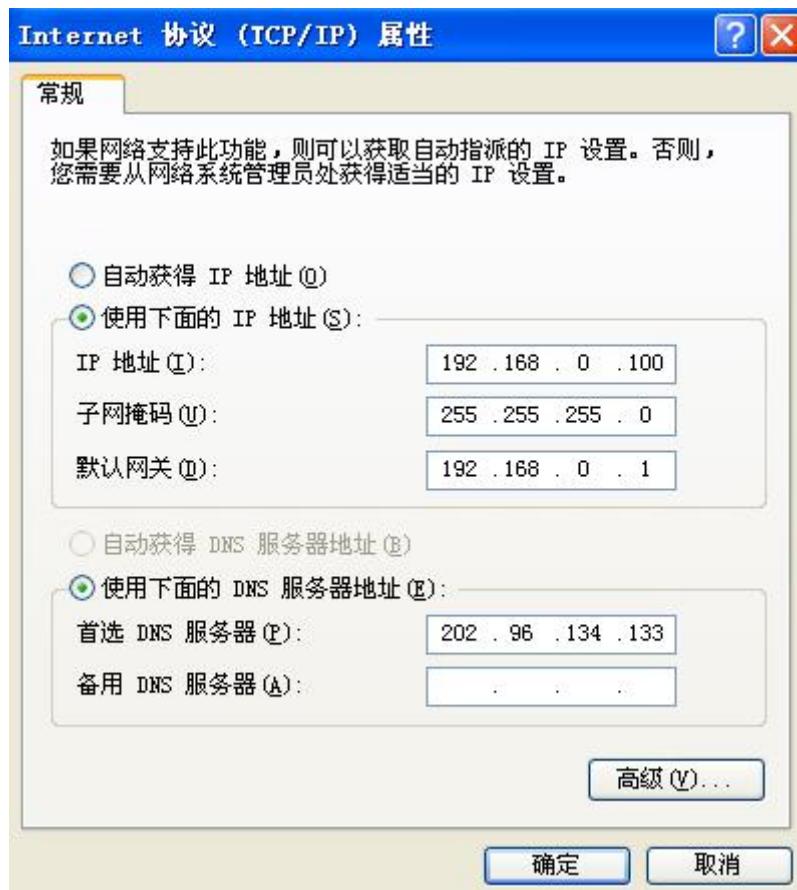
启用DNS代理	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
IPv4监听地址	<input type="text"/>	
监听端口	<input type="text" value="5353"/>	
缓存	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
并发查询	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用

第三步：『网络配置』→『DNS 代理』，启用 DNS 代理。界面如下图所示：

DNS透明代理

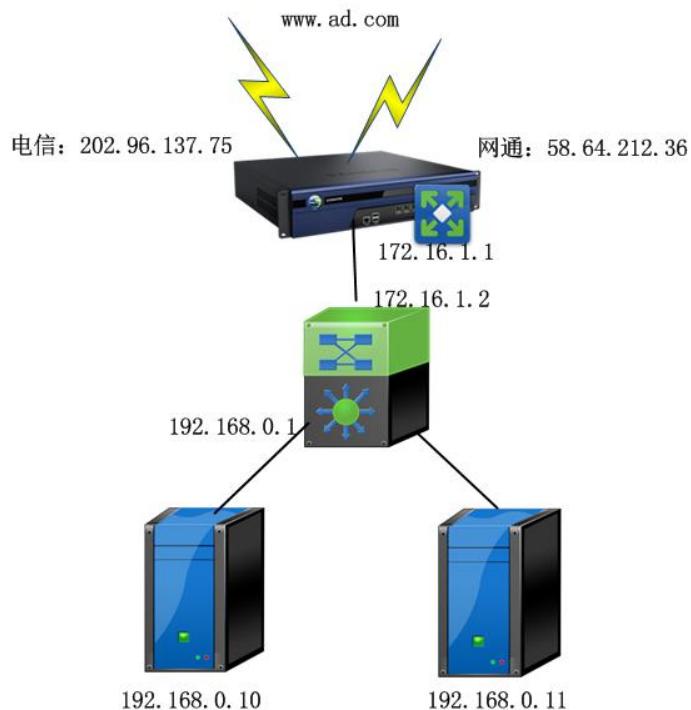
启用DNS代理	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
IPv4监听地址	<input type="text"/>	
监听端口	<input type="text" value="5353"/>	
缓存	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
并发查询	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用
选择策略	<input type="text" value="轮询"/>	
代理目标范围	<input type="text" value="全部DNS请求"/>	
代理内网网段	<input checked="" type="radio"/> 所有网段	<input type="radio"/> 部分网段
监视域名	<input type="text" value="www.baidu.com"/>	
	<input type="button" value="添加"/>	<input type="button" value="删除"/>
前置调度策略	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
链路繁忙保护	<input type="radio"/> 启用	<input checked="" type="radio"/> 禁用

第四步：在内网 PC 上配置 DNS 服务器地址。界面如下图所示：



16.14. 出站前置调度策略案例

某客户网络拓扑图如下，AD 以路由模式进行部署，同时作为网关代理内网上网，有两条外网线路分别是电信线路和网通线路，IP 分别为 202.96.137.75 和 58.64.212.36，并且这两个 IP 对应同一个域名 www.ad.com；AD 内网接口 IP 为 172.16.1.1；三层交换机接在 AD 下面，和 AD 相连的接口 IP 为 172.16.1.2，和内网相连的接口 IP 为 192.168.0.1；内网电脑使用的网段是 192.168.0.0/24；有两台服务器提供相同的 WEB 服务，IP 地址分别是 192.168.0.10 和 192.168.0.11。客户希望实现 AD 设备可以进行域名解析，并代理内网 PC 转发 DNS 请求，其中电脑 192.168.0.100 只从电信线路解析域名 www.sina.com.cn。



配置步骤如下：

第一步：『网络配置』→『DNS 代理』，添加电信接口 DNS 服务器。界面如下图所示：

DNS代理 前置调度策略 内网DNS记录 HOSTS 帮助信息

网关DNS设置

网口: 电信

DNS服务器列表

IP地址:

权值: 添加

电信/202.96.134.133/1

(设备本机发出的域名解析请求仅使用最前面的三个DNS服务器)

删除

DHS透明代理

启用DNS代理 启用 禁用

第二步：『网络配置』→『DNS 代理』，添加网通接口 DNS 服务器。界面如下图所示：



DNS代理 前置调度策略 内网DNS记录 HOSTS 帮助信息

网关DNS设置

DNS服务器列表

网口: 网通

IP地址:

权值: 添加

电信/202.96.134.133/1
网通/210.51.176.1/1

(设备本机发出的域名解析请求仅使用最前面的三个DNS服务器)

删除

DNS透明代理

启用DNS代理 启用 禁用

第三步：『网络配置』→『DNS 代理』，启用 DNS 代理。界面如下图所示：



DNS透明代理

启用DNS代理 启用 禁用

IPv4监听地址

监听端口 5353

缓存 启用 禁用

并发查询 启用 禁用

选择策略 轮询

代理目标范围 全部DNS请求

代理内网网段 所有网段 部分网段

监视域名 www.baidu.com

前置调度策略 启用 禁用

链路繁忙保护 启用 禁用

更新

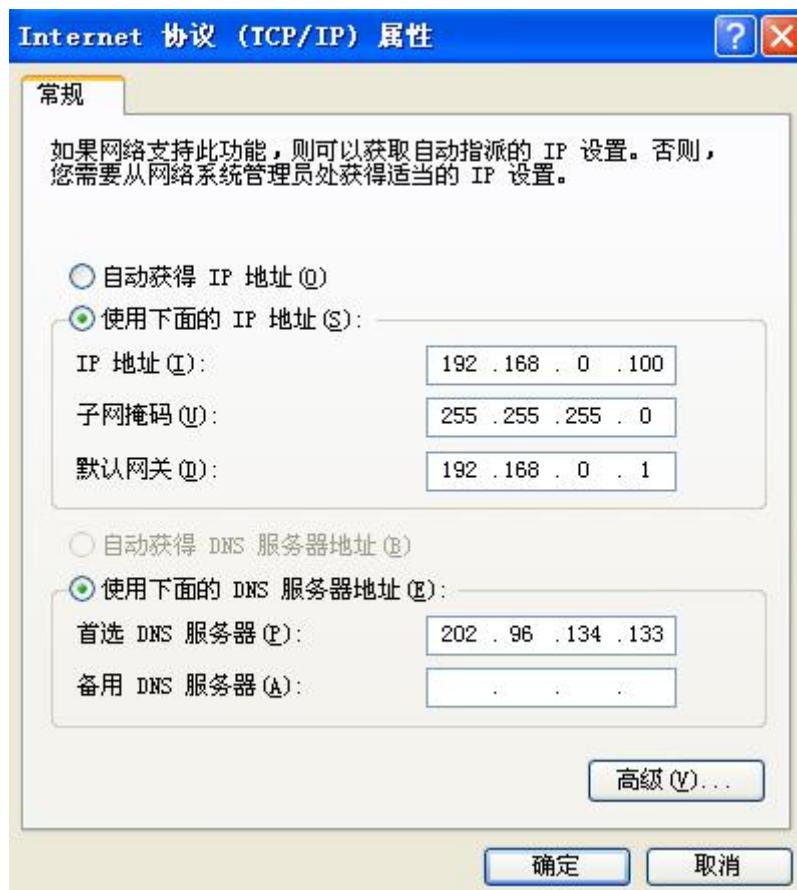
第四步：『网络配置』→『DNS 代理』→『前置调度策略』，设置前置调度策略，电

电脑 192.168.0.100 只能从电信线路解析域名 www.sina.com.cn。界面如下图所示：



The screenshot shows the 'DNS代理' (DNS Proxy) section of the Sangfor management interface. A new policy is being created under the '前置调度策略' (Pre-positioned Load Balancing Strategy) tab. The '普通属性' (General Properties) section includes a name '前置调度策略', status set to '启用' (Enabled), and an IP range '192.168.0.100 - 192.168.0.100'. The '域名' (Domain Name) field contains 'www.sina.com.cn'. The '策略配置' (Policy Configuration) section shows '内网用户' (Intranet User) set to 'IP地址段' (IP Range). Below this, two servers are listed: '电信/202.96.134.133' in the '已选择' (Selected) list and '网通/210.51.137.71' in the '待选' (Available) list. Under 'DNS服务器' (DNS Server), the '链路繁忙保护' (Link Busy Protection) is disabled ('禁用'), and the '失效动作' (Failure Action) is set to '匹配下一条策略' (Match Next Rule). At the bottom are '取消' (Cancel) and '完成' (Finish) buttons.

第五步：在内网 PC 上配置 DNS 服务器地址。界面如下图所示：



16.15. ACL 配置案例

某客户路由模式部署 AD 设备于网络出口处，客户希望禁止 GRE 封装的数据包（协议号为 47）访问内部的 192.168.2.0 网段的服务器。

配置步骤如下：

第一步：『网络配置』→『ACL 配置』→『基本 ACL 控制』，匹配数据包的五元组，禁止放通协议号为 47，目的 IP 为 192.168.2.0 网段的数据。界面如下图所示：

基本ACL控制 | 高级ACL控制 | 帮助信息

新建基本ACL

属性

名称: 禁止GRE
状态: 启用 禁用

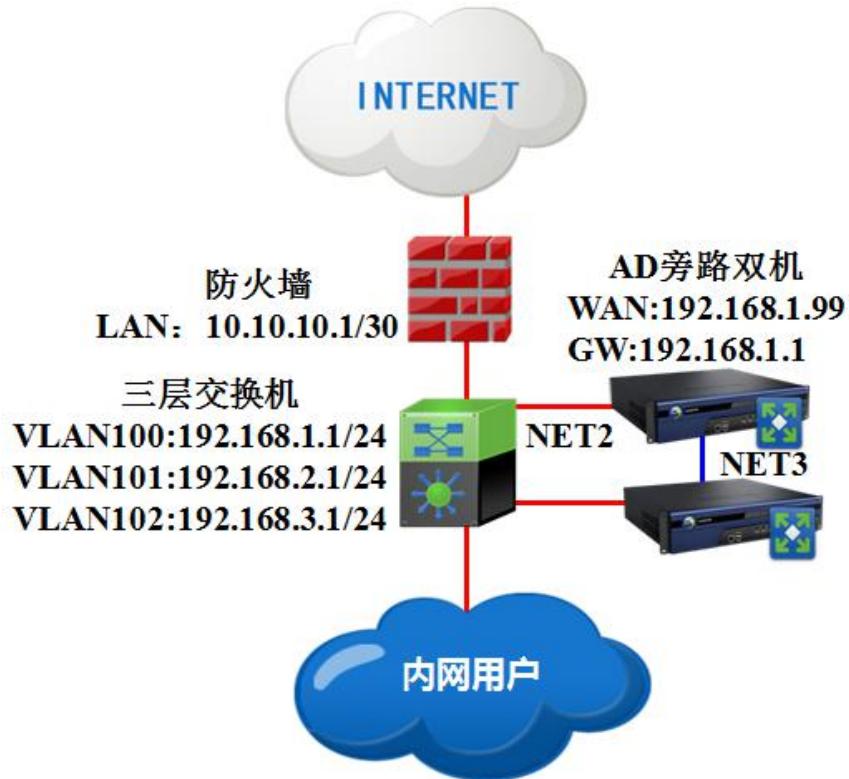
规则配置

协议: 自定义
协议号: 47
指定入接口: ALL
源IP地址: 单个IP
IP地址:
目的IP地址: IP范围
IP范围: 起始IP: 192.168.2.0
结束IP: 192.168.2.254
动作: 允许 拒绝

取消 完成

16.16. 主备双机配置案例

某客户拓扑如下，客户需要旁路模式部署实现服务器负载，并且实现双机热备功能，当某一个设备出现故障后，切换到另外一台AD设备工作。



双机配置上架规范：

第一步：配置一台主机 A（需要配置基础网络配置、虚拟服务、双机维护），并且确保该主机部署到网络中虚拟服务等工作正常。

第二步：配置另外一台主机 B（仅配置双机维护）并且将该主机关机，接主机 B 的双机口（通信介质选择的网口）到主机 A 对应接口。

第三步：主机 B 开机。

第四步：主机 B 开机后，主机 B 成为备机，主机 A 会将配置同步至主机 B。主机 B 的 ALARM 灯一直闪烁，说明工作正常。

第五步：将主机 A 关机或者通过拔线检测，查看 AD 是否切换，应用是否正常。正常的话则双机工作正常。配置完成。

下面介绍本案例中 AD 设备双机维护的配置方法：

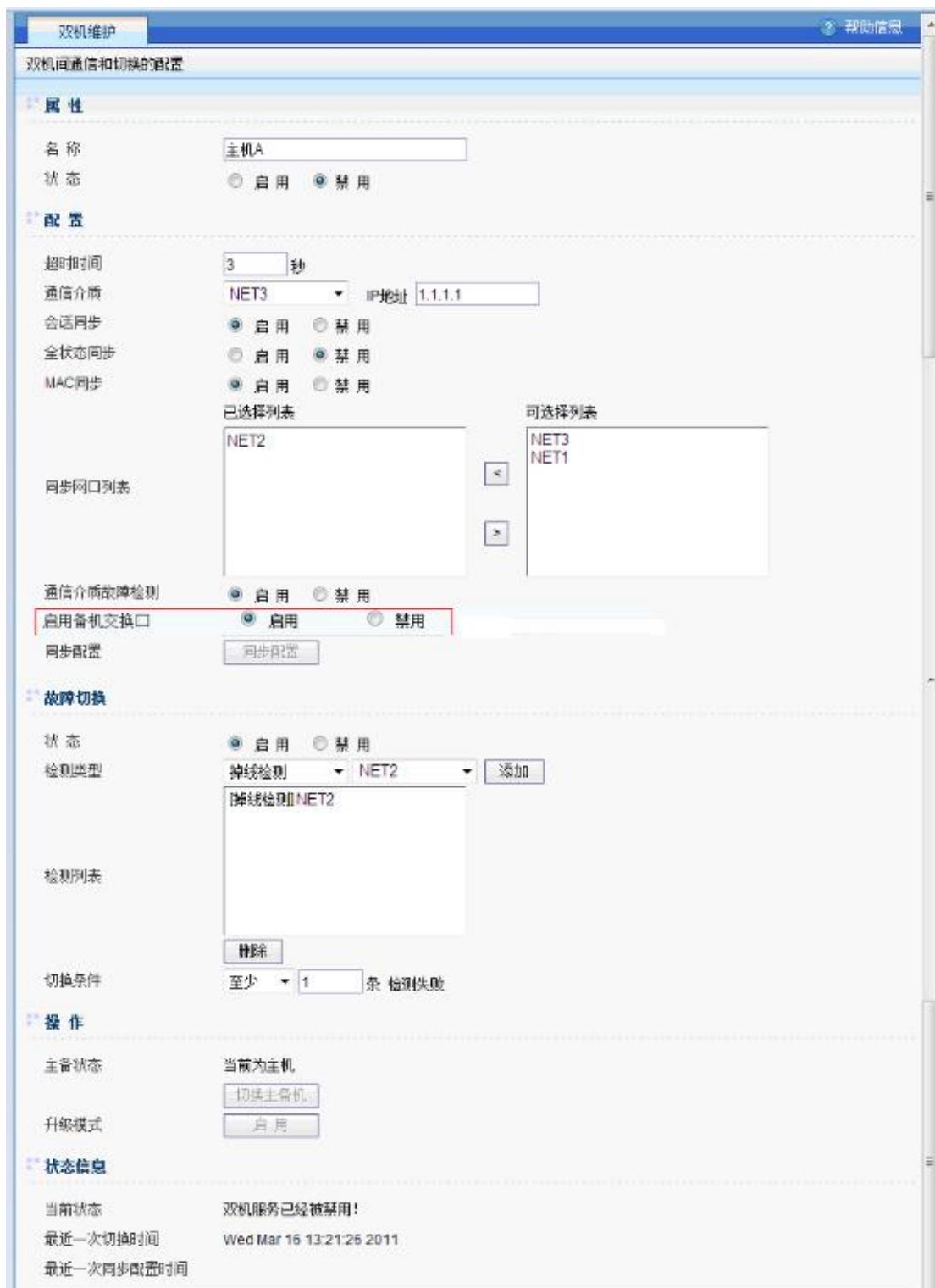
第一步：任意选取一台 AD 设备为主机 A，配置好网络配置，虚拟服务等基本信息，并且保证内网通过 AD 设备访问虚拟服务正常。详细配置方法请参考网络配置和应用负载章节。

第二步：进入主机 A 的高可用性配置页面，模式选择主备模式，界面如下：

The screenshot shows the Sangfor system navigation menu on the left, with 'High Availability' selected. The main window displays the 'Mode' configuration page. Under 'Select Mode', the 'Master-Slave Mode' radio button is selected. A detailed description states: 'This mode connects two devices to build a master-slave deployment. One device acts as the master, providing services, while the other acts as the slave, not providing services. When the master fails, the slave will switch to become the master to take over the original master's services.' Below this is a 'Finish' button. To the right, a diagram shows two servers connected by a 'Heartbeat Line'. The left server is labeled 'Master' and the right one is labeled 'Slave'. A note at the bottom says: 'This mode supports all functions of a single device.'

第三步：进入主机 A 双机维护配置界面，定义名称为主机 A，选择通信介绍为 NET3，并且设置 IP 地址为 1.1.1.1。启用会话同步，禁用全状态同步（全状态同步为三角传输时需

要启用）。启用 MAC 同步。通信介质故障检测选择 NET2 接口。界面如下：



第四步：进入主机 B 的高可用性配置页面，模式选择主备模式。

系统导航菜单

- › 系统概况
- › 报表配置
- › 公共对象
- › 应用负载
- › 智能DNS
- › 路由配置
- › 网络配置
- › 系统配置
- › 配置向导
- ▼ 高可用性
 - › 模式
 - › 集群
 - › 成员管理
 - › 应用组管理

模式

模式

选择模式

主备模式

高可用集群模式

高性能集群模式

该模式将两台设备快速构建成主备机部署方式，一台设备作为主机，提供服务，另一台设备作为备机，不提供服务。当主机发生故障时，备机切换为主机，接替原主机的服务。

完成

该模式支持单台设备的所有功能。



第五步：进入主机 B 的双机维护配置界面，定义名称为主机 B，选择通信介绍为 NET3，并且设置 IP 地址为 1.1.1.2。启用会话同步，禁用全状态同步（全状态同步为三角传输时需要启用）。启用 MAC 同步。通信介质故障检测选择 NET2 接口。界面配置如下：



第六步：主机 B 关机，并且将 NET3 口与主机 A 的 NET3 口对接。

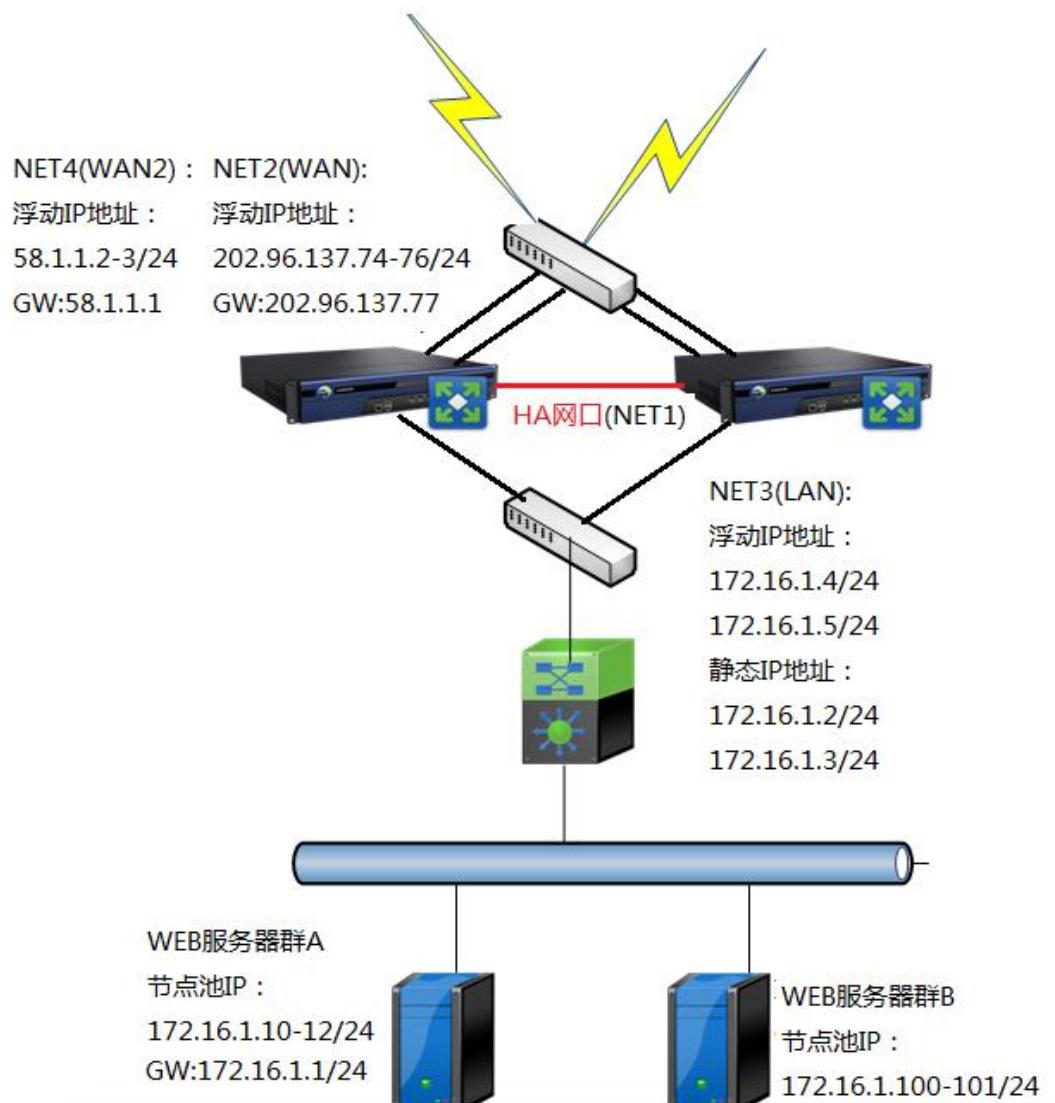
第七步：主机 B 开机，主机 B 成为备机，主机 A 会将配置同步至主机 B。主机 B 的 ALARM 灯一直闪烁，说明工作正常。

第八步：将主机 A 关机或者通过拔线检测，查看 AD 是否切换，应用是否正常。正常

的话则双机工作正常。配置完成。

16.17. 集群部署配置案例

某客户拓扑如下，路由模式部署实现服务器负载，两台 AD 设备组成集群，内网有两个 WEB 服务器群，正常情况下，公网用户通过链路负载访问 WEB 服务器群 A 和 WEB 服务器群 B，希望实现访问 WEB 服务器 A 时，主机 A 设备做主控；访问 WEB 服务器群 B 时，主机 B 设备做主控；当其中一个设备出现故障后，该应用的所有流量自动切换到另外一台 AD 设备。



集群配置上架规范：

第一步：配置一台主机 A（创建集群）。

第二步：创建集群成功后，登陆集群控制中心进行配置。（基础网络配置，SNAT 和 DNAT 设置，虚拟服务，应用组管理）

第三步：将两台设备的 HA 网口用交叉线直连，或者连接到同一个交换机上。需要注意两台设备均需要使用相同的网口作为 HA 网口。

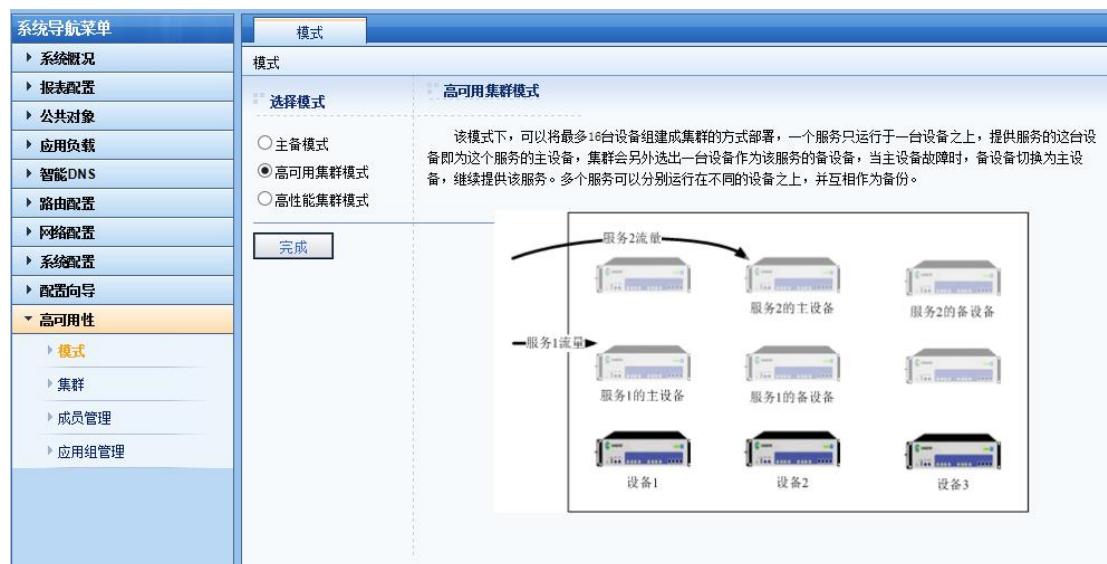
第四步：配置另外一台主机 B（加入集群）。

第五步：登陆集群控制中心，成员管理中添加 B 设备。查看两台设备是否在线，B 设备在线后会自动同步配置。

第六步：将主机 A 关机或者通过拔线检测，查看应用访问是否正常。正常的话则集群工作正常，配置完成。

下面介绍本案例中集群的配置方法：

第一步：任意选取一台 AD 设备为主机 A， 创建集群。



系统导航菜单

- ▶ 系统概况
- ▶ 报表配置
- ▶ 公共对象
- ▶ 应用负载
- ▶ 智能DNS
- ▶ 路由配置
- ▶ 网络配置
- ▶ 系统配置
- ▶ 配置向导
- ▼ 高可用性
 - ▶ 模式
 - ▶ **集群**
 - ▶ 成员管理
 - ▶ 应用组管理

集群维护

集群维护

设备集群状态

状态	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用
动作	<input type="radio"/> 加入集群	<input checked="" type="radio"/> 创建集群

本地设备配置

设备管理IP	10.252.252.74/24
HA网口	NET1
IP地址	10.0.0.1
掩码	255.255.255.0
密钥	*****
再次输入密钥	*****

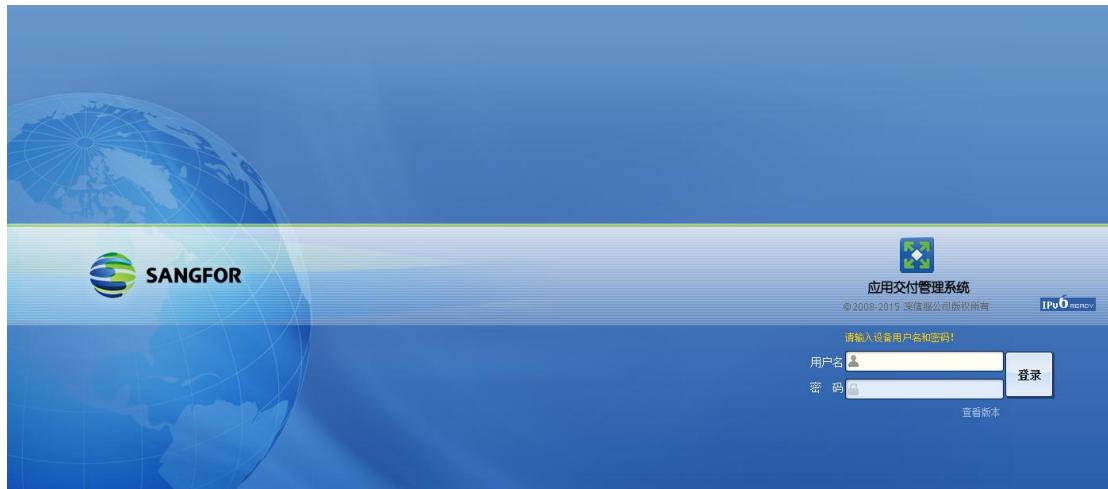
集群配置

集群名称	sangfor
集群管理IP	10.252.252.77
子网掩码	24

>>高级配置

更新

第二步：登陆集群控制中心，用户名密码默认为“cluster”和“cluster”：



第三步：基础网络配置。『网络配置』→『网络接口』页面，新增内网接口 LAN，如下图所示：



点击下一步，设置 LAN 口的静态 IP 地址和浮动 IP 地址，开启 LAN 口的健康检查：

网络接口 | 交换网口 | 端口聚合 | VLAN子接口 | 接口模式

编辑LAN口

属性

名称	LAN
网络接口	NET3
类别	LAN (IPv4)
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

网络地址配置

静态IP地址列表

起始IP	
结束IP	
掩码	
生效设备	A
172.16.1.2/24 [A]	
添加	
删除	

当前生效设备已配置1个静态IP

浮动IP地址列表

起始IP	
结束IP	
掩码	
172.16.1.4/24	
172.16.1.5/24	
添加	
删除	

当前已配置3/512个地址，其中静态IP为1个，浮动IP为2个

健康检查

健康状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
插拔网线检测	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
ARP检查	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

取消 **完成**

静态 IP 用于跟节点池通信，获取节点池的健康状态。网口的静态 IP 不是必须要配置的，只要确保每台设备都能获取到节点池的健康状态即可。如果节点池在设备的 LAN 口方向，那么只需要在 LAN 口设置静态 IP，WAN 口的静态 IP 无需设置。

此时 B 设备未加入集群，无法为主机 B 设置对应的静态 IP 地址，需等 B 设置加入集群后，再修改网口配置，设置主机 B 的静态 IP。

浮动 IP 地址则在各个设备间浮动，如果有多个虚拟服务要分开做策略，每个虚拟服务至少要有一个浮动 IP 地址对应。

第四步：『网络配置』→『网络接口』页面，新增内网接口 WAN，如下图所示：



点击下一步，设置 WAN 口浮动 IP 地址，网关等，如下图所示：

新建WAN口

属性

名称	WAN
网络接口	NET2
类别	WAN
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

网络地址配置

静态IP地址列表

起始IP	
结束IP	
掩码	
生效设备	A
添加	
删除	

当前生效设备已配置0个静态IP

浮动IP地址列表

起始IP	
结束IP	
掩码/前缀	
添加	
删除	

202.96.137.74/24
202.96.137.75/24
202.96.137.76/24

当前已配置3/512个地址，其中静态IP为0个，浮动IP为3个

网关

202.96.137.77

第五步：设置应用负载。『应用负载』→『服务』页面，设置HTTP服务端口，如下图：

服务

新建

属性

名称: WEB

类型: HTTP

端口: 8080

端口列表:

取消 完成

This screenshot shows the 'Service' configuration interface. It displays a new service named 'WEB' of type 'HTTP' on port 8080. The interface includes fields for name, type, and port, along with a list of ports and buttons for canceling or saving the configuration.

『应用负载』→『IP组』页面，设置IP组，如下图：

IP组

编辑

属性

名称: WEB服务群A

地址类型: IPv4

IP地址:

已选择: WAN (202.96.137.74), WAN2 (58.1.1.2)

待选: WAN (202.96.137.75, 202.96.137.76), WAN2 (58.1.1.3)

(最多可以添加32个IP)

显示WAN口IP对应的互联网IP

取消 完成

This screenshot shows the 'IP Group' configuration interface. It displays the creation of a new IP group named 'WEB服务群A'. The interface includes fields for name, address type, and IP addresses, along with lists for selected and available IP addresses. A checkbox for displaying WAN port IP corresponding to the Internet IP is also present.

IP组

新建

属性

名称: WEB服务器群B

IP地址:

已选择: WAN
WAN1
202.96.137.76
WAN2
58.1.1.3

待选: WAN
202.96.137.74
202.96.137.75
WAN2
58.1.1.2

(最多可以添加32个IP)

显示WAN口IP对应的互联网IP

取消 完成

『应用负载』→『节点池』页面，设置节点池：

新建

配置

名称: WEB服务器群A

节点选择策略: 轮询

会话保持: none

备用会话保持: none

已选择: 常规监视器
http

待选: 常规监视器
ping
ping6
connect_tcp
connect_udp
ftp
pop3
smtp

节点有效条件: 至少 1 个常规监视器通过

恢复时间: 0 秒

温暖时间: 0 秒

节点池繁忙处理策略: 强制调度
排队等待
调度失败
全状态统计
ESTABLISHED状态统计

节点

节点列表: 起始地址
结束地址
端口 权重
172.16.1.10:80/1
172.16.1.11:80/1
172.16.1.12:80/1

添加
删除

新建

配置

名称	WEB服务器群B
节点选择策略	加权最少连接
会话保持	none
备用会话保持	none
已选择	常规监视器 http ping
待选	常规监视器 ping6 connect_tcp connect_udp ftp pop3 smtp imap
节点有效条件	至少 1 个常规监视器通过
恢复时间	0 秒
温暖时间	0 秒
节点池繁忙处理策略	<input type="radio"/> 强制调度 <input type="radio"/> 排队等待 <input checked="" type="radio"/> 调度失败
连接数统计	<input checked="" type="radio"/> 全状态统计 <input type="radio"/> ESTABLISHED状态统计
节点	节点列表
起始地址	[输入框]
结束地址	[输入框] (起始地址必须小于或等于结束地址，如果只添加一个节点，填写起始地址即可)
端口	[输入框] 权重[1]
	[添加] [删除]
	172.16.1.100:8080/1 172.16.1.101:8080/1

『应用负载』→『虚拟服务』页面，设置虚拟服务：

虚拟服务 | 虚拟服务关联组

编辑

属性

名称: WEB服务器群A
状态: 启用 禁用
所属虚拟服务关联组: 虚拟服务关联组_4

配置

负载模式: 七层
服务: http
IP 组: WEB服务群A
调度方式: 首个请求 每一个请求

前置策略: (可以配置0~100个前置策略)

默认节点池: WEB服务器群A
优化策略: --未启用--
空闲超时时间: 600 秒
自动SNAT: 启用 禁用
TCP单边加速: 启用 禁用
强制关闭连接: 启用 禁用

URL流量控制和统计

URL流量统计: 启用 禁用
URL下载速度控制: --未启用--

带宽控制

链路带宽控制: 启用 禁用
用户带宽控制: 启用 禁用

取消 完成

虚拟服务 虚拟服务关联组

新建

属性

名称: WEB服务器群B
状态: 启用 禁用

配置

负载模式: 七层
服务: WEB
IP 组: WEB服务器群B
调度方式: 首个请求 每一个请求

前置策略 (可以配置0~100个前置策略)

默认节点池: WEB服务器群B
优化策略: -未启用-
空闲超时时间: 600 秒
自动SNAT: 启用 禁用
TCP单边加速: 启用 禁用
强制关闭连接: 启用 禁用

URL流量控制和统计

URL流量统计: 启用 禁用
URL下载速度控制: -未启用-

带宽控制

链路带宽控制: 启用 禁用
用户带宽控制: 启用 禁用

操作

取消 完成

配置完虚拟服务后，可看到自动生成了虚拟服务关联组，如下图所示：



名称	虚拟服务
Virtual Service Group_4	WEB服务器群A/
Virtual Service Group_5	WEB服务器群B/

第六步：将两台设备的 HA 网口（NET1）用交叉线直连或者连接到同一个交换机上。

需要注意两台设备均需要使用相同的网口作为 HA 网口。

第七步：配置另外一台主机 B 加入集群。登陆 B 设备的控制台页面，『高可用性』→

『集群』页面：



第七步：登陆集群控制中心，『高可用性』→『成员管理』页面添加主机 B 设备：

新建设备

新建设备

属性

名称 B

配置

设备管理IP 10.252.252.75

设备信息

HA口IP 未知

取消 完成

在集群控制中心的成员管理页面，添加完 B 设备后，首先能看到 B 设备是故障状态，提示配置不一致正在同步；当主机 B 设备的配置同步完后，则可看到两台设备是在线状态，说明两台设备成功组成了集群，如下图所示：

成员管理						
操作		名称	管理IP	角色	健康状态	管理状态
<input type="checkbox"/>	+添加	A	10.252.252.74	主控	在线	启用
<input type="checkbox"/>	-删除	B	10.252.252.75	备控	在线	启用

第八步：在集群控制中心编辑 LAN 口的网络接口配置，添加 B 设备对应的静态 IP 地址：

网络接口 交换网口 端口聚合 VLAN子接口 接口模式

编辑LAN口

属性

名称	LAN
网络接口	NET3
类别	LAN (IPv4)
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

网络地址配置

静态IP地址列表	起始IP	
	结束IP	
	掩码	
	生效设备	B
		<input type="button" value="添加"/>
	172.16.1.3/24 [B]	<input type="button" value="删除"/>

当前生效设备已配置1个静态IP

第九步：在集群控制中心设置应用组，『高可用性』→『应用组管理』：

属性

名称	<input type="text" value="WEB服务器组A"/> (长度限制为1~63字符, 且不能包含& " : % < > / \ :)
会话同步	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
默认设备	<input type="text" value="A"/>
抢占模式	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
故障检测	链路 <input type="text" value="请选择关联链路"/> LAN <input type="button" value="添加"/> <input type="button" value="删除"/>

>>高级配置

应用组权重	<input type="text" value="20"/>
虚拟MAC	链路 <input type="text" value="请选择关联链路"/> 虚拟MAC <input type="text" value="LAN 00:01:2a:3c:e5:c4"/> LAN 00:01:2a:3c:e5:c4 <input type="button" value="添加"/> <input type="button" value="删除"/>

应用组关联信息

已选择	待选
虚拟服务关联组 虚拟服务关联组_4 浮动IP 172.16.1.4/24	Default 虚拟服务关联组 虚拟服务关联组_5 浮动IP 172.16.1.5/24 202.96.137.75/24
<input type="button" value="<"/> <input type="button" value=">"/>	

完成

『会话同步』开启会话同步，主控设备发生切换时，已经建立的连接不会中断。

『默认设备』则主控设备。

『抢占模式』若开启抢占模式，如果主控设备恢复后重新加入集群，则继续充当主控。

如果不开启抢占模式，主控设备恢复后重新加入集群，则充当备控的角色。

『故障检测链路』设置应用组检测的链路，如果检测到链路故障，则发生切换。

『应用组权重』设置该应用组的权值，集群控制中心会根据每台设备上的应用组权值之和选举主控和备控设备。

『虚拟 MAC』设置对应链路的虚拟 MAC 地址，当发生切换时，相邻交换机和路由器设备无需刷新 MAC 地址，提高切换的效率。

『应用组关联信息』设置虚拟服务关联组，浮动 IP，SNAT 和 DNAT 的相关信息。包含了相同的 IP 组或者节点池的虚拟服务，使用了相同 IP 的 NAT 组以及浮动 IP，当应用组

生效设备故障时自动切换到其他设备。 应用组为集群最小的切换单元。

新建应用组

新建应用组

属性

名称	WEB服务器群B
会话同步	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
默认设备	B
抢占模式	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
故障检测	链路 LAN
<input type="button" value="添加"/> <input type="button" value="删除"/>	

>>高级配置

应用组权重	20						
虚拟MAC	链路 LAN						
<table border="0"> <tr> <td>虚拟MAC</td> <td>00-11-11-11-11-11</td> </tr> <tr> <td colspan="2">LAN 00:11:11:11:11:11</td> </tr> <tr> <td colspan="2" style="text-align: right;"> <input type="button" value="添加"/> <input type="button" value="删除"/> </td> </tr> </table>		虚拟MAC	00-11-11-11-11-11	LAN 00:11:11:11:11:11		<input type="button" value="添加"/> <input type="button" value="删除"/>	
虚拟MAC	00-11-11-11-11-11						
LAN 00:11:11:11:11:11							
<input type="button" value="添加"/> <input type="button" value="删除"/>							

应用组关联信息

<p>已选择</p> <p>虚拟服务关联组 虚拟服务关联组_5 浮动IP 172.16.1.5/24</p>	<p>待选</p> <p>浮动IP 202.96.137.75/24</p>
--	---

应用组管理

+ 新建 **X 删除** 刷新时间间隔: 5秒

名称	默认设备	生效设备	备份设备	会话同步状态	切换
Default	A	B		同步完成	
WEB服务器组A	A	A	B	同步完成	
WEB服务器群B	B	B	A	同步完成	

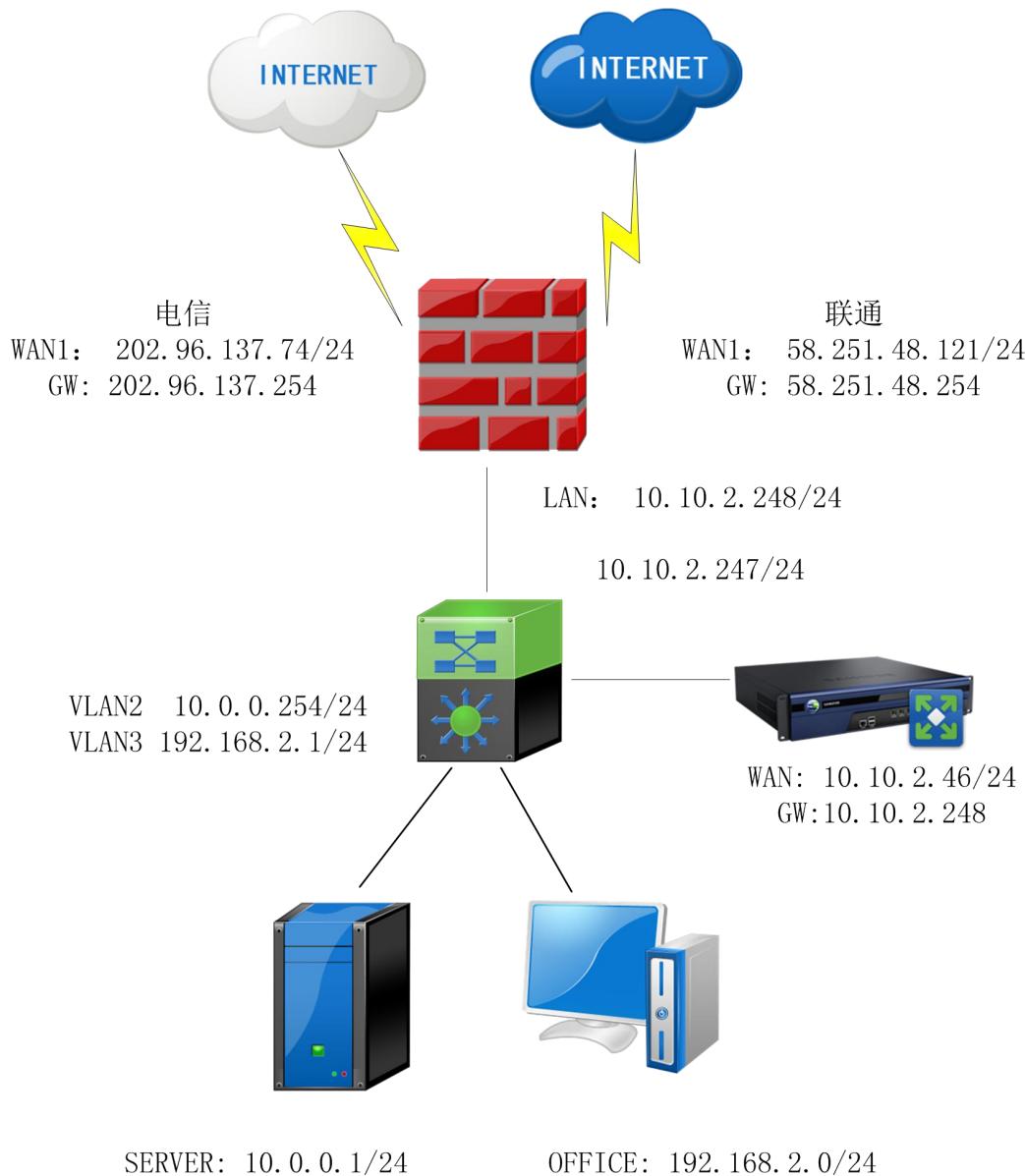


说明：高可用集群模式和高性能集群模式界面配置大致相同，案例为高可用集群模式

情景，高性能集群模式配置参考 12.3.2。

16.18. 虚拟链路健康检查案例

某客户外网有电信、网通两条链路，外网用户都是通过两条链路的 IP 来访问服务器的，内网有一台服务器，提供 http 服务（80 端口）。AD 设备单臂模式部署，客户提出需要实现入站链路负载，同时需要检查外网线路运营商网关是否正常，如果发现电信或联通的 ISP 链路出现异常，则不会将故障链路的 IP 地址解析给用户，确保在这种情况下用户仍然能够正常访问。



准备工作：在公网域名服务商服务器上申请两个 DNS 记录：NS 记录：
 www.sangfor.com—>ns1.sangfor.com； A 记录： ns1.sangfor.com—>202.96.137.74(或
 58.251.48.121)

配置步骤如下：

第一步：设置网络接口 WAN 口，绑定电信的地址，如下图所示：

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

编辑WAN口

属性

名称	wan1
网络接口	NET1
类别	WAN (IPv4)
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

网络地址配置

地址列表	起始IP	结束IP	掩码/前缀	添加	删除
			10.10.2.46/24		
当前已配置1/512个地址					

网关

线路带宽

上行带宽	1000000	Kbps	上行带宽繁忙比例	80	%
下行带宽	1000000	Kbps	下行带宽繁忙比例	80	%

第二步：定义 IP 组，添加 WAN 口 IP。

IP组

编辑

属性

名称	IP-GROUP
地址类型	IPv4
IP组	已选择
wan1	
10.10.2.46	
(最多可以添加32个IP)	
<input checked="" type="checkbox"/> 显示WAN口IP对应的互联网IP	

取消 完成

第三步：配置节点监视器，监视网关是否正常：【应用负载】 - 【节点监视器】，新建节点监视器，此处以 ping 为例，联通线路同样配置即可。

节点监视器

编辑

属性

名称	ping电信网关
类型	ICMP

配置

间隔时间	5	秒
超时时间	2	秒
尝试次数	3	
监视地址	202.96.137.254	
调试	<input type="radio"/> 是	<input checked="" type="radio"/> 否

取消 完成

第四步：配置 DNS 服务器

DNS服务器

更新DNS服务器配置

普通属性

状态 启用 禁用

DNS服务器属性

已选择 **10.10.2.46**

待选

监听地址

不添加监听IP将使DNS配置失效！

DNS端口 **53**

不存在的域名处理 不回应 拒绝 代理

DNS探测属性

探测超时时间 **2** 秒

探测结果缓存时间 **10800** 秒

探测方法 **DNS反向查询** ▾

更新

第五步：定义虚拟 IP 池，以电信为例，联通地址同样配置即可：

本地虚拟IP池

新建

普通属性

名称: 电信
状态: 启用 禁用
类型: IPv4 IPv6

策略配置

主动监视器: 已选择 ping, 待选 ping6, connect_tcp, connect_udp, http, ftp, pop3, smtp, imap
虚拟IP有效条件: 至少 1 个监视器通过
繁忙保护: 启用 禁用
首选策略: 轮询
备选策略: 加权轮询

IP池

地址: 202.96.137.74
端口: 80
协议: TCP
权值: 1
添加: 202.96.137.74:80/1 TCP
(最多配置64个地址)

取消 完成

完成后，再次编辑刚刚新建的本地虚拟 IP 池，并点击**编辑虚拟 IP**，如下图所示：

本地虚拟IP池

编辑

普通属性

名称	电信
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6

策略配置

主动监视器

已选择	ping
-----	------

待选

ping6
connect_tcp
connect_udp
http
ftp
pop3
smtp
imap

虚拟IP有效条件

至少 1 个监视器通过

繁忙保护

启用 禁用

首选策略

静态就近性

备选策略

动态就近性

虚拟IP

虚拟IP列表

编辑虚拟IP

出现如下虚拟 IP 的编辑页面：

虚拟IP

+ 新建 X 删除 | 返回

地 址	权 值	协 议
61.139.2.34:80	1	TCP
212.10.204.26:80	1	TCP
202.96.137.74:80	1	TCP

点击虚拟 IP 池中的 IP 202.96.137.74:80，『监视器类型』选择“独立”，『虚拟 IP 监视器』选择“ping 电信网关”

虚拟IP

编辑

普通属性

IP地址	202.96.137.74
端口	80
协议	TCP
权值	1

虚拟IP健康检查

监视器类型 继承 独立

已选择 **ping电信网关**

虚拟IP监视器

虚拟IP有效条件 至少 个监视器通过

待选 **ssl3.0**
snmp
dns
radius_auth
radius_acct
oracle
mssql
mysql

取消

第六步：配置 DNS 映射：

本地DNS映射

新建

普通属性

名称	vnet
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6

策略配置

域名列表

www.vnet.cn	<input type="button" value="添加"/> <input type="button" value="删除"/>
-------------	--

选择策略 静态就近性

会话保持 启用 禁用

会话超时时间 300 秒

TTL 60 秒



第七步：新建并配置本地 LDNS 集合，选择电信的 ISP 地址段，联通同样配置即可，如下图所示：



第八步：配置 DNS 映射级别，如下图所示：

DNS映射级别 | 虚拟IP池级别

新建

属性

配置范围	<input checked="" type="radio"/> 本地 <input type="radio"/> 全局
DNS映射	vnet
LDNS集合	电信
虚拟IP池	电信

取消 完成

DNS映射级别 | 虚拟IP池级别

新建

属性

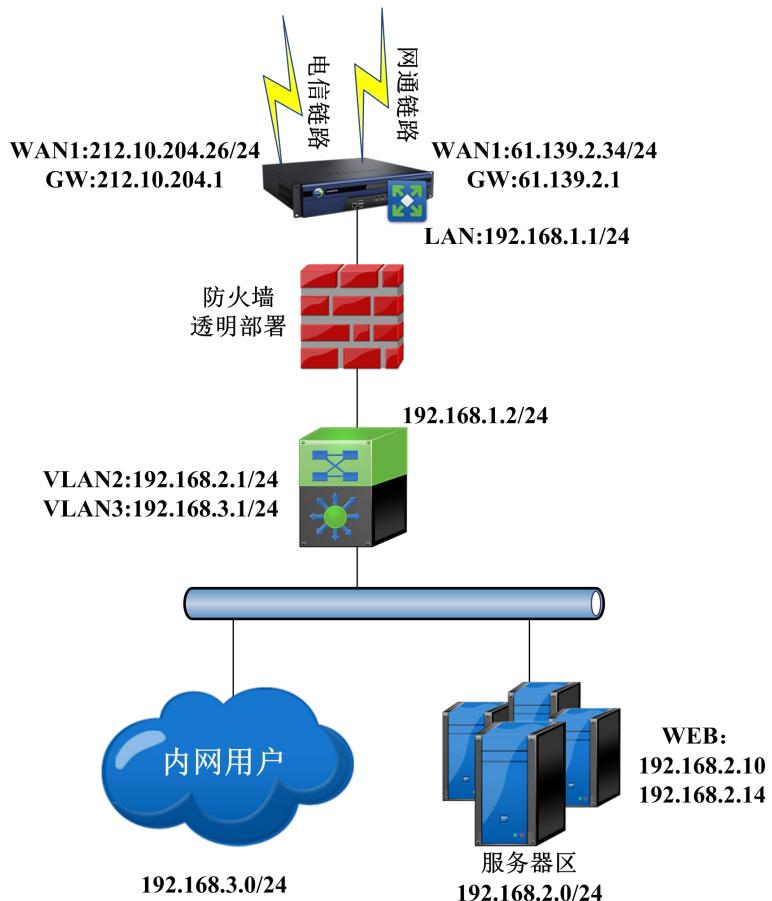
配置范围	<input checked="" type="radio"/> 本地 <input type="radio"/> 全局
DNS映射	vnet
LDNS集合	联通
虚拟IP池	联通

取消 完成

第九步：配置节点池、虚拟服务，配置步骤省略。

16.19. 综合案例

某客户拓扑如下，客户有两条公网链路，网通 100M 和电信 100M，AD 设备部署在网络出口处。客户内网有两台服务器提供 WEB 网站服务，该服务使用 80 端口，并且统一用域名 `www.sangfor.com` 访问，该域名用 A 记录指向 `212.10.204.26`，客户希望实现网通用户访问该域名时走网通线路接进来，电信用户访问该域名时走电信线路接进来，其他运营商自动选择最快链路访问，与此同时还能够实现 `200.100.100.0/24` 网段的用户访问 `192.168.2.10` 这台服务器，其余用户对服务器的访问进行服务器负载。内网用户上网的数据实现自动选路功能。



准备工作：在公网域名服务商服务器上申请两个 DNS 记录：NS 记录：
 www.sangfor.com—>ns1.sangfor.com； A 记录： ns1.sangfor.com—>212.10.204.26(或
 61.139.2.34)。

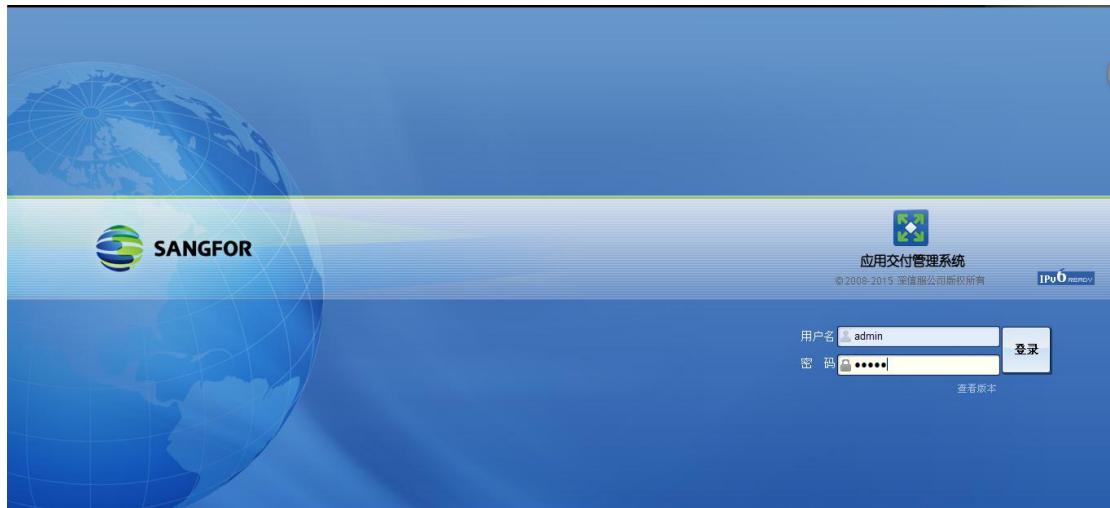
配置以及上架方法：

上架前配置：

第一步：首先将设备开机，用网线接设备的 MANAGE 口，将电脑网卡的 IP 配置成 10.252.252.100，界面如下：



第二步：打开 IE 浏览器，输入 <https://10.252.252.252>，即可到登录界面，输入设备出厂默认的账号密码 admin/admin，界面如下：



第三步：进入『网络配置』→『网络接口』，建立内网口。界面如下：

网络接口 交换网口 端口聚合 VLAN 接口模式

选择类别

LAN
 WAN

取消 **下一步**

网络接口 交换网口 端口聚合 VLAN子接口 接口模式

编辑LAN口

属性

名称：内网接口
网络接口：NET1
类别：LAN (IPv4)
状态： 启用 禁用

网络地址配置

地址列表 起始IP：
结束IP：
掩码/前缀： **添加** **删除**
192.168.1.1/24

当前已配置1/512个地址

健康检查

健康状态： 启用 禁用

取消 **更新**

第四步：进入『网络配置』→『网络接口』，建立电信接口。界面如下：

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

选择类别

LAN
 WAN

取消 **下一步**

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

新建WAN口

属性

名称: 电信
网络接口: NET2
类别: WAN
状态: 启用 禁用

网络地址配置

地址列表

起始IP	结束IP	掩码/前缀	操作
			添加
212.10.204.26/24			删除

当前已配置1/512个地址

网关: 202.10.204.1
对应互联网IP
起始IP:
结束IP:
添加
删除

网络带宽

上行带宽	100000	Kbps	上行带宽繁忙比例	80	%
下行带宽	100000	Kbps	下行带宽繁忙比例	80	%

健康检查

监视器状态 启用 禁用

网关ARP检查 启用 禁用

有效监视器

监视主机

插拔网线检测 启用 禁用

第六步：进入『网络配置』→『网络接口』，建立网通接口。界面如下：

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

选择类别

LAN WAN

网络接口 | 交换网口 | 端口聚合 | VLAN | 接口模式

新建WAN口

属性

名称	网通
网络接口	NET3
类别	WAN
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

网络地址配置

地址列表

起始IP	
结束IP	
掩码/前缀	<input type="button" value="添加"/>
61.139.2.34/24	<input type="button" value="删除"/>

当前已配置 1 / 512 个地址

网关

61.139.2.1

对应互联网IP

起始IP:	
结束IP:	<input type="button" value="添加"/> <input type="button" value="删除"/>

第七步：进入『线路带宽』→『健康检查』，建立到达内网的静态路由。界面如下：

The screenshot shows the Sangfor Cloud interface for network configuration. It includes sections for 'Bandwidth Settings' (with up and down bandwidth limits of 100000 Kbps) and 'Health Check' (with monitoring status set to 'Enabled'). A dropdown menu under 'Health Check' lists 'ping' and 'ping/61.139.2.1'. There is also a 'Ping' button and 'Add' and 'Delete' buttons. At the bottom, there is a 'Line Detection' section with 'Enabled' selected. Buttons for 'Cancel' and 'Update' are at the bottom.

第七步：进入『路由配置』→『静态路由』，建立到达内网的静态路由。界面如下：

The screenshot shows the Sangfor Cloud interface for route configuration. It is titled 'Static Route' and has a 'New' tab selected. Under 'Properties', it shows a 'Network Number' of 192.168.0.0, a 'Mask' of 255.255.0.0, and a 'Gateway' of 192.168.1.2. The 'Forwarding' option is set to 'Disabled'. Buttons for 'Cancel' and 'Finish' are at the bottom.

第八步：本案例中还需要 AD 设备代理内网用户和服务器上网，所以还需要设置代理上网。进入『网络配置』→『源地址转换』，界面如下：

源地址转换

新建

属性

名称

状态 启用 禁用

配置

出接口 指定网口

代理网段 代理所有IP地址
 代理指定网段 - 源IP地址属于如下设置的网段才可以经过NAT源地址转换

转换源IP地址为 使用网口地址
 使用指定地址

转换策略 源IP和目的IP哈希
 源IP哈希

源地址转换

新建

属性

名称

状态 启用 禁用

配置

出接口 指定网口

代理网段 代理所有IP地址
 代理指定网段 - 源IP地址属于如下设置的网段才可以经过NAT源地址转换

转换源IP地址为 使用网口地址
 使用指定地址

转换策略 源IP和目的IP哈希
 源IP哈希

源地址转换			
操作		搜索	
+新建	×删除	启用	禁用
<input type="checkbox"/>	名称	出接口	子网网段
<input type="checkbox"/>	代理上网-网通	网通	全部
<input type="checkbox"/>	代理上网-电信	电信	全部

第九步：进入『网络配置』→『DNS 代理』，配置 DNS 代理，添加电信和网通两条线路的 DNS 服务器 IP 地址，界面如下：

DNS代理 前置调度策略 内网DNS记录 HOSTS

网关DNS设置

DNS服务器列表

网口： 网通

IP地址：

权值： 添加

电信/218.2.135.1/1
网通/221.6.96.1/1

(设备本机发出的域名解析请求仅使用最前面的三个DNS服务器)

删除



DNS透明代理

启用DNS代理	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
IPv4监听地址	<input type="text"/>
监听端口	<input type="text"/> 5353
缓存	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
并发查询	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
选择策略	<input type="button" value="轮询"/> <input type="button" value=""/>
代理目标范围	<input type="button" value="全部DNS请求"/> <input type="button" value=""/>
代理内网网段	<input checked="" type="radio"/> 所有网段 <input type="radio"/> 部分网段
监视域名	<input type="text"/> www.163.com
	<input type="button" value="添加"/> <input type="button" value="删除"/>
前置调度策略	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
链路繁忙保护	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用

第十步：进入『路由配置』→『智能路由』，配置智能路由，设备默认有一条根据加权最小流量进行链路选择的匹配策略。此时，配置内网用户访问公网网通服务器时走网通线路，访问电信服务器时走电信线路的策略，界面如下：

智能路由 出站高级配置 路由测试

新建

属性

名称: 电信走电信
状态: 启用 禁用

配置

源IP地址: 所有IP
目的IP地址: ISP地址段
ISP地址段: 电信
TOS: 0

协议条件: 所有协议 指定类型 TCP

已选择列表: 电信
可选择列表: 网通

使用链路范围

生效时间: 全天
链路选择策略: 无
链路繁忙保护: 启用 禁用
链路调度失败的默认动作: 匹配下一条规则 丢弃

取消 完成

新建

属性

名称	网通走网通
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用

配置

源IP地址	所有IP
目的IP地址	ISP地址段
ISP地址段	联通（原网通）
TOS	0
协议条件	<input checked="" type="radio"/> 所有协议 <input type="radio"/> 指定类型 TCP
已选择列表	网通
可选择列表	电信
使用链路范围	
生效时间	全天
链路选择策略	无
链路繁忙保护	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
链路调度失败的默认动作	<input checked="" type="radio"/> 匹配下一条规则 <input type="radio"/> 丢弃

取消 **完成**

智能路由							
出站高级配置 路由测试							
+新建 X删除 <input checked="" type="checkbox"/> 启用 <input type="checkbox"/> 禁用 <input type="checkbox"/> 导入 <input type="checkbox"/> 导出 <input type="checkbox"/> 配置向导							
名 称	源IP	目的IP	协 议	使 用 链 路	生 效 时 间	操 作	
电信走电信	所有	电信	ALL	电信	全天		
网通走网通	所有	联通（原网通）	ALL	网通	全天		
Default	所有	所有	ALL	电信 网通	全天		

以上步骤配置完成，即可将设备按照拓扑中的接线方式上架。上架后正常则进行服务器负载以及链路负载相关配置

服务器负载与链路负载配置：

第一步：在『应用负载』→『服务』页面，新建一个 web 服务，设置好服务类型和服务端口：

服务

新建

属性

名称: web服务器

类型: HTTP

端口: 80

端口列表

添加

删除

取消 完成

第二步：在『应用负载』→『IP组』页面，新建一个IP组，选择外网发布的两个IP：

IP组

属性

名称: 外网IP组

地址类型: IPv4

IP组: 已选择

待选:

电信 212.10.204.26
网通 61.139.2.34

(最多可以添加32个IP)

显示WAN口IP对应的互联网IP

取消 完成

第三步：在『应用负载』→『会话保持』页面，新建会话保持方式，这里假设客户希望根据Cookie名称作会话保持：

会话保持

编辑

普通属性

名称	cookie
类型	Cookie
保持方式	插入
Cookie名称	_umta
Cookie作用域	域名: [] 路径: [/]
会话Cookie	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
HttpOnly	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
超时时间	86400 秒

配置

优先于繁忙	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
-------	--

取消 完成

第四步：在『应用负载』→『节点池』页面，新建两个节点池，一个节点池只包含192.168.2.10这台服务器，用于前置策略的调度，另一个节点池包含所有的服务器IP，用于服务器的负载均衡调度：

节点池

新建

配置

名称:

节点选择策略: 轮询

会话保持: none

备用会话保持: none

已选择: 节点状态监视器

待选: 常规监视器
ping
ping6
connect_tcp
connect_udp
http
ftp
pop3

节点有效条件: 至少 1 个常规监视器通过

恢复时间: 0 秒

温暖时间: 0 秒

节点池繁忙处理策略: 强制调度 () 排队等待 () 调度失败 (checked)

连接数统计: 全状态统计 (checked) ESTABLISHED状态统计

节点

节点列表: 起始地址
结束地址
端口 权重 添加 删除

当前已配置 0/500 个节点

取消 完成

第五步：在『应用负载』→『策略』→『前置调度策略』页面，新建一个前置调度策略，让 200.100.100.0/24 网段的用户能够始终调度到 192.168.2.10 这台服务器上：

前置调度策略 | 优化策略 | HTTP改写 | SSL策略 | URL下载速度控制

新建

属性

名称: 10服务器前置策略

关联属性

服务: web服务器
源IP范围: 子网
子网: 网络号: 200.100.100.0
掩码: 24

高级条件匹配:

请求行 请求头部
字段: VERSION
条件: HTTP/1.0

请求行	VERSION	等于	HTTP/1.0	aa	添加
					删除

动作: 调度节点池
调度节点池: 10服务器

失败动作: 匹配下一条 丢弃

[取消](#) [完成](#)

第六步：在『应用负载』→『虚拟服务』页面，新建一个七层负载模式的虚拟服务，选择定义好的服务、节点池、IP组以及前置调度策略：

虚拟服务

新建

属性

名称:

状态: 启用 禁用

配置

负载模式: 七层

服务: -请选择-

IP 组: -请选择-

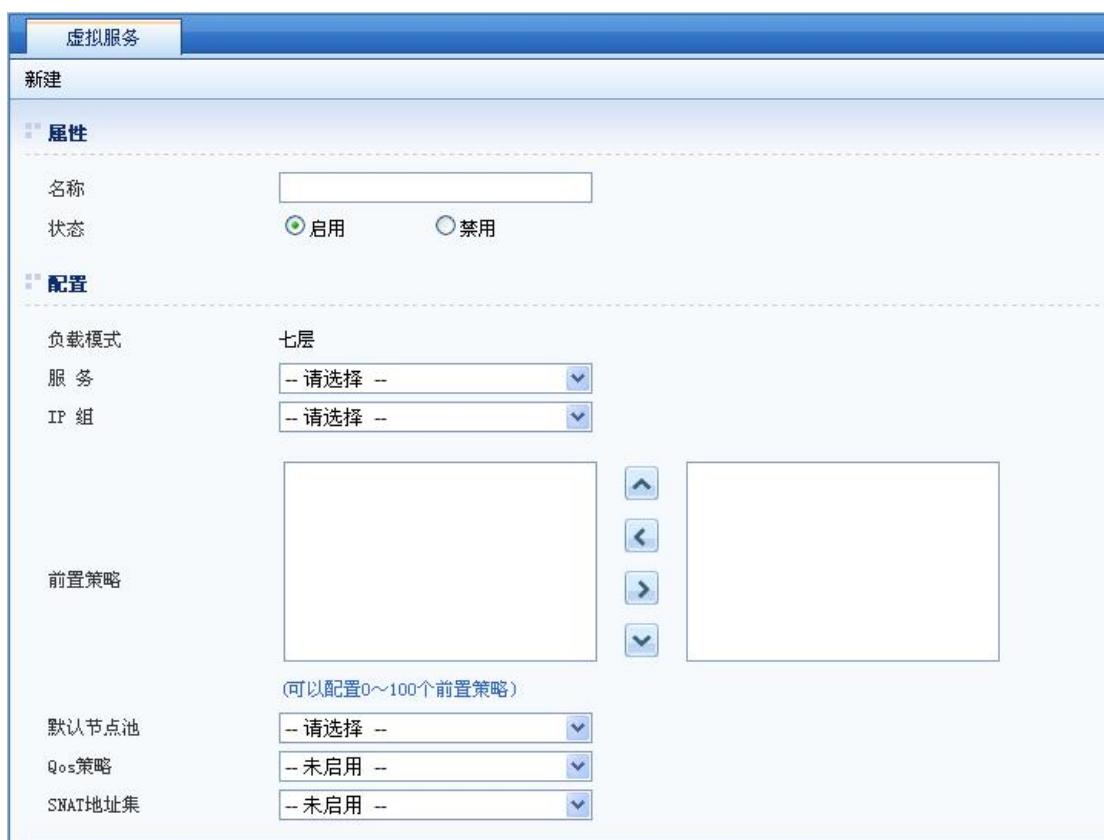
前置策略:

(可以配置0~100个前置策略)

默认节点池: -请选择-

QoS策略: -未启用-

SNAT地址集: -未启用-



第七步：在『智能 DNS』→『虚拟 IP 池』→『本地虚拟 IP 池』页面，新建一个本地虚拟 IP 池，添加需要发布的外网 IP，并设置好首选策略为静态就近性，备选策略为动态就近性：

本地虚拟IP池 全局虚拟IP池

新建

普通属性

名称:

状态: 启用 禁用

类型: IPv4 IPv6

策略配置

主动监视器: 已选择 待选: ping, ping6, connect_tcp, connect_udp, http, ftp, pop3, smtp

繁忙保护: 启用 禁用

首选策略: 轮询

备选策略: 加权轮询

IP池



第八步：在『智能 DNS』→『DNS 映射』→『本地 DNS 映射』页面，新建一个本地 DNS 映射，添加需要解析的域名，选择我们要发布的虚拟 IP 池：



第九步：在『智能 DNS』→『LDNS 集合』→『本地 LDNS 集合』页面，新建两个本地 LDNS 集合，一个添加电信的地址段，另一个添加网通的地址段：

本地LDNS集合 全局LDNS集合

新建

属性

名称 电信LDNS

地址集

地址类型 ISP地址段 添加

地址段 电信

1.48.0.0-1.49.255.255
1.180.0.0-1.183.255.255
1.192.0.0-1.199.255.255
1.202.0.0-1.207.255.255
27.16.0.0-27.31.255.255
27.128.0.0-27.129.255.255
27.148.0.0-27.159.255.255
27.184.0.0-27.191.255.255

当前已配置 181/10000 个地址范围

删除

取消 完成

本地LDNS集合 全局LDNS集合

新建

属性

名称 网通 LDNS

地址集

地址类型 ISP地址段

地址段 联通（原网通）

1.24.0.0-1.31.255.255
1.56.0.0-1.63.255.255
1.188.0.0-1.191.255.255
27.8.0.0-27.15.255.255
27.36.0.0-27.47.255.255
27.98.224.0-27.98.255.255
27.192.0.0-27.223.255.255
58.16.0.0-58.23.255.255

当前已配置 179/10000 个地址范围

删除

取消 完成

第十步：在『智能 DNS』→『静态就近性』→『虚拟 IP 池级别』页面，新建两个静态就近性策略，分别对应的策略是：访问 www.sangfor.com 域名时，当 LDNS 是电信 LDNS 时，返回 212.10.204.26；当 LDNS 是网通 LDNS 时，返回 61.139.2.34：

新建

属性

配置范围 本地 全局

状态 启用 禁用

虚拟IP池 web发布IP

LDNS集合 电信 LDNS

已选择列表 212.10.204.26

池内IP < >

可选择列表 61.139.2.34

取消 完成

新建

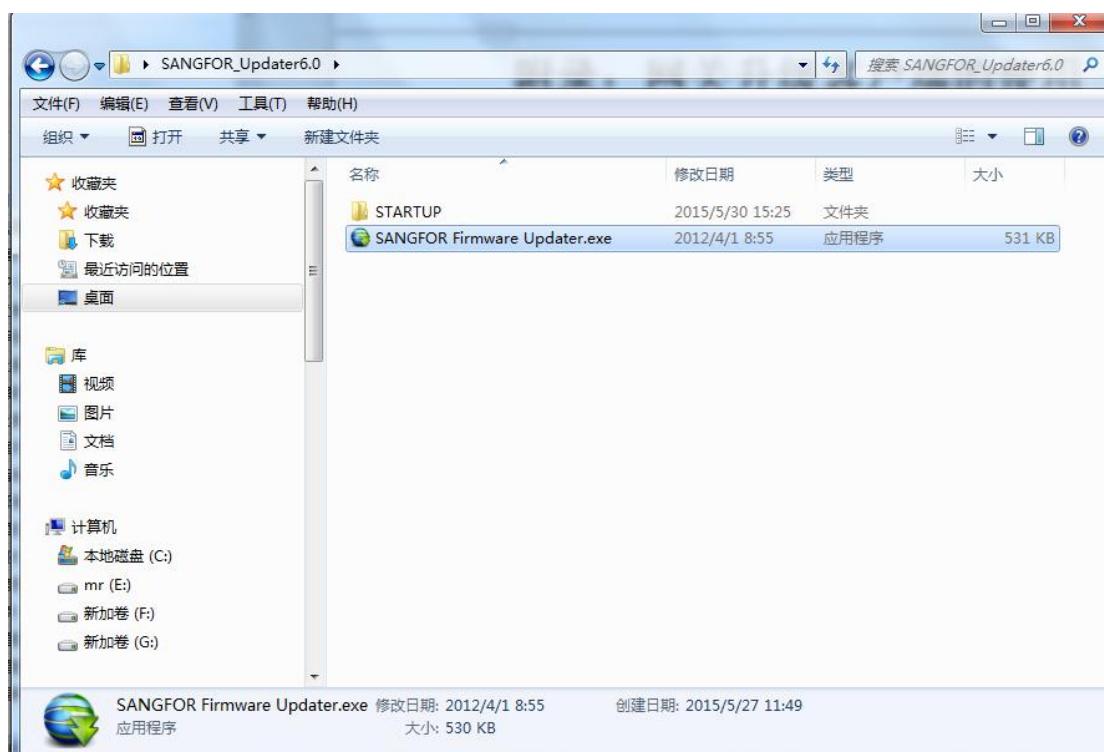
属性

配置范围	<input checked="" type="radio"/> 本地	<input type="radio"/> 全局						
状态	<input checked="" type="radio"/> 启用	<input type="radio"/> 禁用						
虚拟IP池	web发布IP							
LDNS集合	网通LDNS							
池内IP	<table border="1"><tr><td>已选择列表</td><td>可选择列表</td></tr><tr><td>61.139.2.34</td><td>212.10.204.26</td></tr><tr><td><input type="button" value="<"/></td><td><input type="button" value=">"/></td></tr></table>		已选择列表	可选择列表	61.139.2.34	212.10.204.26	<input type="button" value="<"/>	<input type="button" value=">"/>
已选择列表	可选择列表							
61.139.2.34	212.10.204.26							
<input type="button" value="<"/>	<input type="button" value=">"/>							

第十一步：配置完成。

附录：网关升级客户端的使用

网关升级系统与恢复系统可用于对设备进行内核版本升级和备份恢复设备配置。在设备出现致命错误时，也可通过网关恢复系统把设备恢复到出厂状态。同时，网关恢复系统还可用于检查系统网口工作状态，路由等配置信息，更改网口工作模式等。界面如下：



双击 SANGFOR Firmware Updater，界面如下所示：



输入 AD 设备的 IP 地址，管理员密码则是控制台 admin 用户对应的密码，默认是 admin，
点击 **连接**：



『在线升级』将连接到 SANGFOR 的公网服务器，获取新版本信息，直接从公网下载

升级包升级。请慎用在线升级方式，一般升级包都比较大，在线升级可能出现升级包下载不完全的情况，导致升级出现异常。

『从本地加载升级包』选择本地的升级包升级。升级之前，系统会自动备份设备的配置。

同时按下 Ctrl+Shift+F10，调出如下技术支持工具：



技术支持工具有『升级』、『备份』、『时间』、『命令』、『修改密码』和『帮助』几个菜单，下面分别介绍它们的功能。

『升级』：包括恢复出厂配置，恢复出厂配置仅网络部分，查看软件升级过期时间和升级历史记录。如下图：



『恢复出厂设置』：只有登录硬件设备成功后，才可用。

用于将硬件设备的核心 Firmware 恢复设备出厂配置，这些操作涉及设备的核心文件的更新，还可能涉及序列号的更换等。请不要自行操作，如需要升级，请在深信服技术支持工程师的指导下进行操作。

『恢复出厂设置仅网络部分』：将 AD 管理口的 IP 地址恢复为 10.252.252.252/24。SANGFOR AD 设备必须使用 sangfor update 6.0 版本恢复默认网络，建议电脑与 AD 设备的管理口直连，所需密码为控制台 admin 的密码，恢复默认网络后，管理口 IP 地址将被恢复为 10.252.252.252/24。

『查看软件升级过期时间』：检测当前网关是否处于升级服务有效期内。若不在升级服务有效期内，则不能升级，需要购买相应授权才能升级。

『升级历史记录』：可查看当前设备的升级记录。



1. 设备只能从低版本升级到高版本，而且一般不能跨版本升级。

2. 恢复出厂设置具有一定的风险，如需升级请联系深信服科技客户服务部。

『备份』：包括『备份配置』、『恢复备份配置』选项，如下图：



『备份配置』：将设备现有的配置信息进行备份。

『恢复备份配置』：将以前备份过的配置信息恢复到设备中。

『时间』：包括查看当前时间和获取公网时间。如下图所示：



『命令』：包括『Ping』、『查看路由表』、『查看 ARP 表』、『查看网络配置』等选项。如下图：



『Ping』：登录设备后，从设备往外网 ping，以验证设备是否和外网连通。

『查看路由表』：查看设备本机的路由表。

『查看 ARP 表』：查看设备本机的 ARP 表。

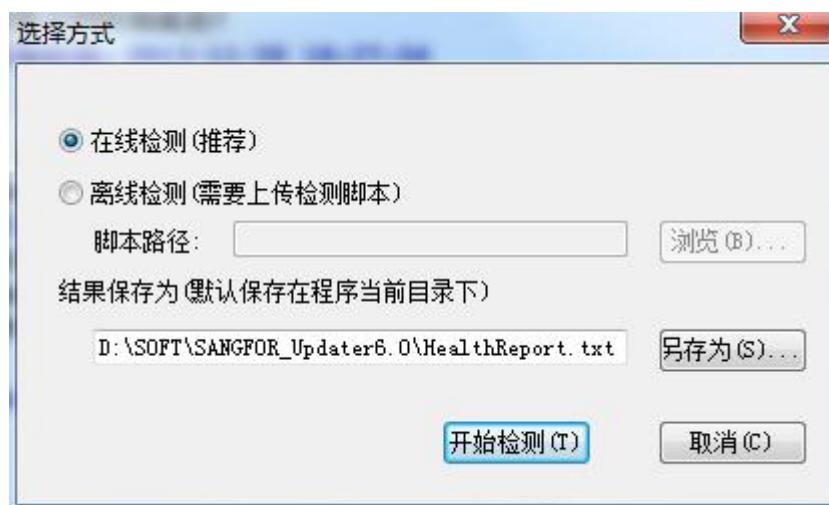
『查看网络配置』：查看设备本机的网络配置，包括接口 IP 配置等。

『查看网口工作模式』：查看设备网口的工作模式，可选择对应网卡。

『设置网口工作模式』：设置设备某个网口的工作模式。

『交换网卡物理位置』：用来交换网卡。

『设备健康状态检查』：可通过在线或者离线的方式检测设备的健康状态，如下图所示：



『修改密码』：修改升级客户端连入设备的密码。该密码如果修改，请妥善保管，若该密码丢失，需返厂重置。



『帮助』包括公网首页的链接，技术支持论坛的链接和查看当前网关升级客户端的版本信息。



警告：请谨慎进行网卡交换的操作，网卡被交换后，可能导致序列号失效。

产品升级步骤

- 1、下载升级包，并保存到本地
- 2、打开网关升级客户端，连接到设备
- 3、选择『从本地加载升级包』，加载下载到本地的升级包升级。
- 4、设备提示升级成功并自动重启



警告：升级硬件的 Firmware 核心，请在我们的技术支持工程师指导下进行。