

SANGFOR_AD_6.4_四层虚拟服务 基本配置指导书



深信服科技有限公司

文档编号	AD_CONF_03_09	审核	huangbing
修订记录			
版本	时间	修订内容	
6.4	2016年7月		

目 录

1	介绍.....	3
1.1	文档说明.....	3
1.2	读者对象.....	3
1.3	缩写和约定.....	3
1.4	使用反馈.....	3
2	功能简介.....	3
3	应用场景.....	3
4	配置思路.....	5
5	配置方式及截图.....	6
5.1	路由模式.....	6
5.2	旁路模式.....	9
6	注意事项.....	14

1 介绍

1.1 文档说明

本文档深信服公司及其许可者版权所有，并保留一切权利。未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式出版传播。

由于产品版本升级或其他原因，本手册内容有可能变更。深信服保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，深信服尽全力在本手册中提供准确的信息，但是并不确保手册内容完全没有错误。

1.2 读者对象

本配置指导文档主要适用于如下工程师：

- ✓ 网络或应用管理人员
- ✓ 现场技术支持与维护人员
- ✓ 负责网络配置和维护的网络管理员

1.3 使用反馈

如果您在使用过程中发现本资料的任何问题，欢迎及时反馈给我们，可以通过反馈到深信服技术社区：bbs.sangfor.com.cn

感谢您的支持与反馈，我们将会做的更好！

2 功能简介

内外网用户访问AD 进行服务器负载均衡；向外发布应用服务，实现负载均衡，减轻单台服务器的压力；

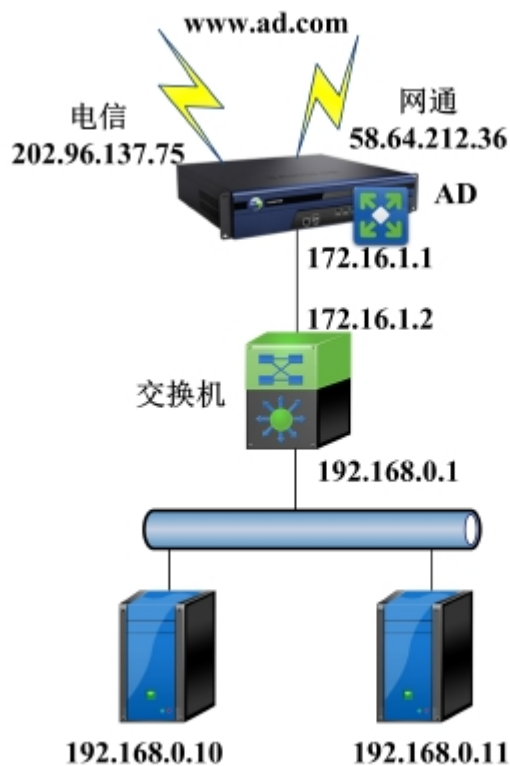
3 应用场景

AD配置虚拟服务有两种应用场景

1.路由模式

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服务，IP 地址分别是192.168.0.10 和192.168.0.11。

网络拓扑如下：

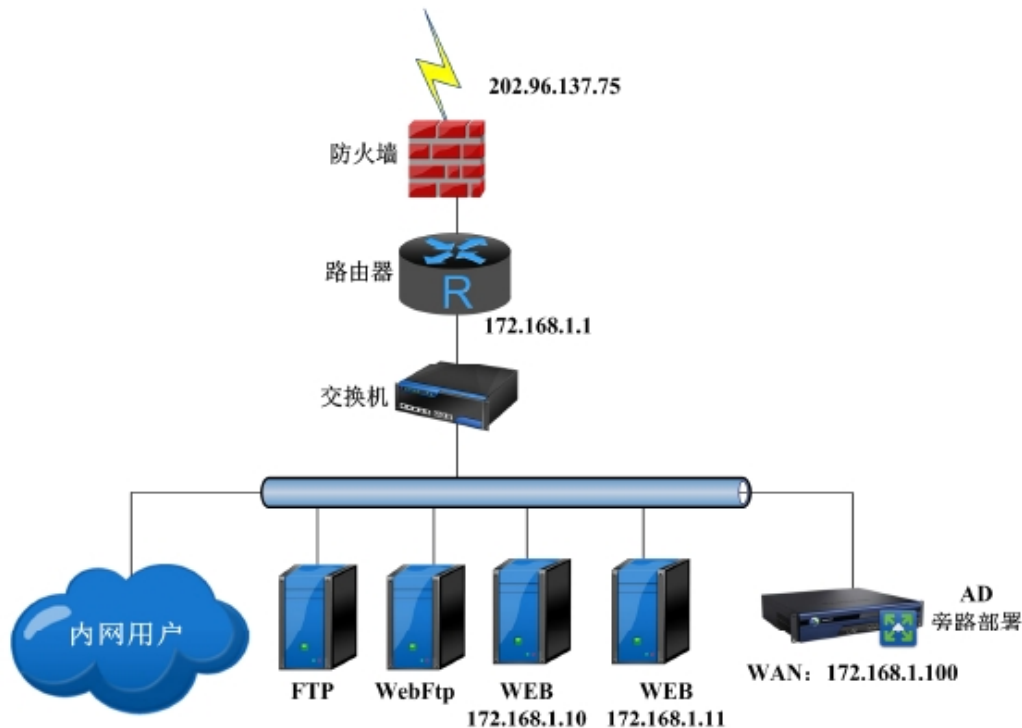


2.旁路模式

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

网络拓扑如下：



4 配置思路

1. 【应用负载】-【服务】，新建服务，此处的配置一般情况与WEB服务器提供服务的端口一致。
2. 【应用负载】-【会话保持】，新建会话保持，本案例使用sourceip会话保持。
3. 【应用负载】-【IP组】，新建一个IP组，加入WAN口线路的IP地址。
4. 【应用负载】-【节点监视器】，新建用于检查服务器健康状态的监视器。AD设备默认已经新建好 ping和connect监视。
5. 【应用负载】-【节点池】，新建节点池，添加两个服务器ip。
6. 【应用负载】-【虚拟服务】，新建一个虚拟服务，将服务、IP组、节点池关联起来即可。

5 配置方式及截图

5.1 路由模式

第一步：网络配置略；

第二步：在『应用负载』→『服务』页面，新建一个tcp服务，设置好服务类型和服务端口，界面如图所示：



系统导航菜单

- 系统概况
- 报表配置
- 公共对象
- 数据中心
- 应用负载
 - 服务
 - IP组
 - 会话保持
 - 节点监视器
 - 节点池
- 智能DNS
- 路由配置
- 网络配置

服务

新建

属性

名称: tcp

类型: TCP

端口: 80

端口列表

添加 删除

取消 完成

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: 应用发布

IP组

已选择

- 电信 202.96.137.75
- 网通 58.64.212.36

待选

(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』→『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

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

节点状态监视器

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

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

192.168.0.10:80/1
192.168.0.11:80/1

当前已配置2/500个节点

取消

完成

第五步：在『应用负载』→『虚拟服务』页面，，新建一个四层虚拟服务，关联上设置好的各个选项，配置虚拟服务页面如下图：

系统导航菜单

▸ 系统概况

▸ 报表配置

▸ 公共对象

▸ 数据中心

▾ 应用负载

▸ 节点监视器

▸ 节点池

▸ SSL

▸ 策略

▸ 虚拟服务

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

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 --

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

5.2 旁路模式

第一步：网络配置略。

第二步：在『应用负载』→『服务』页面，新建一个tcp服务，设置好服务类型和服务端口；界面如图所示：

The top screenshot shows the 'Service' configuration page. On the left is a 'System Navigation Menu' with options like 'System Overview', 'Report Configuration', 'Public Objects', 'Data Center', 'Application Load', 'IP Group', 'Session Persistence', 'Node Monitor', 'Node Pool', 'Smart DNS', 'Route Configuration', and 'Network Configuration'. The 'Application Load' section is expanded, showing 'Service', 'IP Group', 'Session Persistence', 'Node Monitor', and 'Node Pool'. The 'Service' sub-section is selected. The main area is titled 'Service' and contains a 'List of service types that can be created'. Under 'Please select service type', 'TCP' is selected with a radio button. Other options include UDP, HTTP, HTTPS (based on SSL protocol), SSL (encapsulating ordinary TCP's SSL, usable for other secure smtp, pop3), Radius, DNS, FTP, MYSQL, and ORACLE. At the bottom are 'Cancel' and 'Next Step' buttons.

The bottom screenshot shows the 'New Service' dialog box. It has a 'Name' field with 'tcp', a 'Type' dropdown set to 'TCP', and a 'Port' field with '80'. There are 'Add' and 'Delete' buttons next to the port field. A note indicates the port range is 1~65535. At the bottom are 'Cancel' and 'Finish' buttons.

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：

The screenshot shows the '新建' (New) dialog for an 'IP组' (IP Group). The '名称' (Name) field contains '旁路IP组'. Under the 'IP组' (IP Group) section, there is a list of '已选择' (Selected) items: '旁路WAN口' and '202.96.137.75'. To the right is a '待选' (Waiting Selection) area. Below the list, it says '(最多可以添加32个IP)' (Up to 32 IPs can be added). A checkbox labeled '显示WAN口IP对应的互联网IP' is checked. At the bottom are '取消' (Cancel) and '完成' (Finish) buttons.

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：

节点池

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

节点状态监视器

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

至少1个常规监视器通过

恢复时间

0秒

温暖时间

0秒

所有节点繁忙后强制调度

☐ 启用 ☒ 禁用

节点

节点列表

起始地址

结束地址

端口

权重1

172.16.1.10:80/1
172.16.1.11:80/1

添加

删除

当前已配置2/500个节点

取消

完成

第五步：在『应用负载』→『虚拟服务』页面，新建一个四层虚拟服务，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 the Sangfor system navigation menu on the left, with '应用负载' (Application Load Balancing) expanded and '虚拟服务' (Virtual Service) selected. The main content area is titled '虚拟服务' (Virtual Service) and '新建虚拟服务' (New Virtual Service). Under '选择负载模式' (Select Load Mode), the '四层模式' (Layer 4 Mode) radio button is selected. At the bottom, there are '取消' (Cancel) and '下一步' (Next Step) buttons.

The screenshot shows the '属性' (Properties) and '配置' (Configuration) sections of the Virtual Service configuration page. The '属性' section includes fields for '名称' (Name) and '状态' (Status), with '启用' (Enable) selected. The '配置' section includes fields for '负载模式' (Load Mode) set to '七层' (Layer 7), '服务' (Service) set to 'http', 'IP 组' (IP Group) set to '-- 请选择 --', and '调度方式' (Scheduling Method) set to '每一个请求' (Every Request). The '前置策略' (Pre-Strategy) section shows a list of strategies with navigation buttons. Below this, a note states '(可以配置0~100个前置策略)' (Can configure 0~100 pre-strategies). The '默认节点池' (Default Node Pool) is set to '-- 请选择 --', '优化策略' (Optimization Strategy) is set to '-- 未启用 --', 'TCP策略' (TCP Strategy) is set to '七层虚拟服务TCP策略', 'Qos策略' (QoS Strategy) is set to '-- 未启用 --', and 'SNAT地址集' (SNAT Address Set) is set to '自动SNAT'.

第六步：勾选启用自动SNAT，这一步在旁路部署模式下一般都需要选择，主要是解决节点池服务器回包时候也会到达AD来，当然如果节点池服务器的网关就是AD设备，则可以不用启用自动SNAT。

6 注意事项

路由模式下注意：

1. 需要在『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）。

单臂模式下注意：

1. 会话保持不能选择cookie，因为cookie属于应用层属性。
2. 启用自动SNAT可以解决节点池服务器到AD之间的回包路由问题，当然服务器可以将数据都转发到AD，则可以不用启用自动SNAT。