SANGFOR AD6.6

User Manual



Nov 2017

Content

Declaration 9
Preface 10
About This Manual 10
Document Conventions 11
Graphic Interface Conventions 11
Symbol Conventions 12
Technical Support 12
Acknowledgments 12

Chapter 1 Knowing Your ADC 13

1.1 Operating Environment 13
1.2 Product Appearance 13
1.3 Deployment and Management 14
1.4 Connecting ADC 14

Chapter 2 Initial Login to Admin Console 17

2.1 Initial Login to Admin Console 17
Logging in to Admin Console 17
2.2 Viewing Status and Logs 18

Chapter 3 System Status Overview 20

3.1 System status 20
3.1.1 System Status 20
3.1.2 Resource Usage 21
3.1.3 Network Throughput 21
3.1.4 Connections 22
3.1.5 SSL Transactions per Second(TPS) 24
3.1.6 HTTP Transactions per second(TPS) 25
3.2 Virtual service 25
3.2.1 Virtual service 25
3.3.2 Caching 26
3.3.3 Cache Query 27
3.3.4 Cache Misses 28
3.3.5 URL Access Count 28
3.3.6 URL Access Traffic 29
3.4 Intelligent DNS 29
3.4.1 Realtime Queries 29
3.4.2 Queries By Domain 30
3.4.3 DNS Queries By Protocol 30
3.4.4 LDNS 31
3.4.5 LDNS Cache Miss 31
3.5 Anti-DDoS 31

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

3.5.1 L7 DDoS Attacks..... 31
3.5.2 L7 DDoS Attacks Statistics..... 32
3.6 Links..... 33
3.6.1 WAN Links..... 33
3.6.2 Virtual Service Link Status..... 33
3.7.1 Node Pools..... 34
3.7.2 Nodes..... 35
3.7.3 Scheduling..... 36
3.8 Interface..... 36
3.9 DNS Proxy..... 36
3.10 Virtual IP Pool..... 37
3.11 Dynamic Routing..... 37
3.12 Logs..... 37
3.12.1 System Logs..... 37
3.12.2 Operation Logs..... 38
3.12.3 SSL Logs..... 40
3.13 Debug Logs..... 40

Chapter 4 Report Generation and Subscription..... 42

4.1 Report..... 42
4.1.1 Report Generation..... 42
4.1.2 Report Subscription..... 43
4.2 Report Center..... 47
4.2.1 Report Center..... 47
4.2.2 Report Cleanup..... 48
4.3 Report Center..... 49
4.3.1 Link Statistics..... 49
4.3.2 Node Statistics..... 54
4.3.3 Virtual Service..... 59
4.3.4 Policy-Based Routing..... 61
4.3.5 Intelligent DNS..... 63
4.3.6 Cluster Status..... 68

Chapter 5 Objects..... 71

5.1 Local IP Group..... 71
5.2 Configuring IP Group..... 72
5.2.1 ISP IP Group..... 72
5.2.2 Continent IP Group..... 73
5.2.3 Region IP Group..... 77
5.2.4 Auto Update of Region IP Ranges..... 78
5.3 Configuring Schedule..... 79
5.4 Script Rules..... 81
5.5 Custom web page..... 83

Chapter 6 Data Center..... 86

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

6.1 Overview 86
6.2 DataCenter 86
6.3 Local Appliances 87

Chapter 7 Load Balancing 89

7.1 Configuring Service 89
7.2 WAN Link 91
7.3 Session Persistence 92
7.3.1 Source IP Session Persistence 92
7.3.2 Cookie Session Persistence 93
7.3.3 HTTP Header Session Persistence 95
7.3.4 RADIUS Session Persistence 96
7.3.5 SSL Session ID 97
7.4 Node Monitor 97
7.4.1 ICMP Monitor 98
7.4.2 ICMPv6 Monitor 99
7.4.3 Connect(TCP) Monitor 100
7.4.4 Connect(UDP) 102
7.4.5 HTTP Monitor 103
7.4.6 FTP Monitor 103
7.4.7 HTTPS Monitor 104
7.4.8 Connect(SSL) Monitor 105
7.4.9 SNMP Monitor 107
7.4.10 DNS Monitor 108
7.4.11 RADIUS Monitor 108
7.4.12 TCP Partially Open Connection Monitor 110
7.4.13 TCP Passive Monitor 110
7.4.14 HTTP Passive Monitor 111
7.4.15 Complex Monitor 112
7.4.16 MYSQL Monitor 113
7.4.17 LDAP Monitor 115
7.4.18 External Monitor 116
7.5 Node Pool 117
7.6 SSL 122
7.6.1 Generating SSL Certificate 122
7.6.2 CA Certificate 126
7.6.3 CRL 126
7.6 Policy 129
7.6.1 Scheduling Policy 129
7.6.2 Acceleration Policy 137
7.6.3 HTTP Rewriting Policy 141
7.6.4 TCP Policy 152
7.6.5 SSL Offload 154
7.6.6 Encryption Policy 158

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

7.6.7 Download Control 159
7.6.8 QoS Policy 161
7.7 Virtual Service 163
7.7.1 Virtual Service 163
7.7.2 Virtual Service Delivery Group 167

Chapter 8 Intelligent DNS 169

8.1 DNS Server 169
8.2 DNS Records 171
8.2.1 Local DNS Record 171
8.2.2 Configuring Global DNS Record 177
8.3 Virtual IP Pool 177
8.3.1 Local IP Pool 177
8.3.2 Global Virtual IP Pool 181
8.4 DNS Mapping 182
8.4.1 Local DNS Mapping 182
8.4.2 Global DNS Mapping 183
8.5 LDNS 184
8.5.2 Remote Site LDNS 185
8.6 Static Proximity 186
8.6.1 DNS Mapping Based Static Proximity 186
8.6.2 Configuring Global DNS Mapping 187
8.7 Backup/Restore 188
8.7.1 Taking Configuration Snapshot 188
Configuration Snapshots. 188
8.7.2 Synchronizing Configuration to Other Sites 189

Chapter 9 Routing 190

9.1 Policy-Based Routing 190
9.1.1 Policy-Based Routing 191
9.1.2 Outbound Options 192
9.1.3 Route Troubleshooting 193
9.2 Static Route 194
9.3 Virtual Route 195
9.4 IP Anycast 197
9.5 RIP 198
9.5.1 General Settings 198
9.5.2 RIP Interface 199
9.6 OSPF 200
9.6.1 General Settings 201
9.6.2 OSPF Interface 203
9.6.3 Neighbors 204

Chapter 10 Network 206

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

10.1 Interface..... 206
10.1.1 Physical Interface..... 206
10.1.2 Layer 2 Interface..... 213
10.1.3 Aggregate Interface..... 217
10.1.4 VLAN Interface..... 220
10.1.5 Link Mode..... 222
10.2 Creating Link Monitor..... 222
10.3 Source NAT..... 225
10.3.1 Source NAT..... 225
10.3.2 SNAT Address Pool..... 229
10.3.3 SNAT Associations..... 229
10.4 Destination NAT..... 230
10.5 DNS Proxy..... 233
10.5.1 DNS Proxy..... 233
10.5.2 Scheduling Policy..... 236
10.5.3 Internal DNS Records..... 237
10.5.4 HOSTS..... 241
10.6 Security..... 242
10.6.1 Attack Prevention..... 242
10.6.2 ARP/ND Protection..... 243
10.6.3 ARP Proxy..... 245
10.6.4 Advanced Options..... 246
10.7 ACL..... 247
10.7.1 Basic ACL..... 247
10.7.2 Advance ACL..... 249

Chapter 11 System..... 251

11.1 General Settings..... 251
11.1.1 Device..... 251
11.1.2 Date/Time..... 253
11.1.3 Backup/Restore..... 253
11.1.4 Shut Down..... 255
11.1.5 WebConsole..... 255
11.2 Licensing..... 256
11.3 Administrators..... 258
11.3.1 Administrators..... 258
11.3.2 Roles..... 259
11.3.3 Log In With External Account..... 262
11.4 SMTP Server..... 263
11.5 SNMP..... 264
11.5.1 SNMP (V1, V2C)..... 265
11.5.2 SNMP (V3)..... 266
11.5.3 Traps(V1)..... 267
11.6 Alarm Options..... 268

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

11.6.1 Email Alarm..... 268
11.6.2 SMS Alarm..... 269
11.6.3 SNMP Trap Alarm..... 272
11.7 Logging Options..... 273
11.7.1 HTTP Logs..... 273
11.7.2 Syslog Servers..... 275
11.7.3 NAT Log Server..... 276
11.8 System Update..... 277
11.8.1 System Update..... 277
11.8.2 System Rollback..... 278
11.8.3 Update and Privacy..... 279
11.8.4 Proxy Options..... 280

Chapter 12 Wizard..... 281

12.1 Load Balancing Wizard..... 281
12.2 Routing Wizard..... 281

Chapter 13 High Availability..... 284

13.1 HA Mode..... 284
13.2 Active-standby..... 285
13.3 Cluster..... 288
13.3.1 High-availability Cluster..... 288

Chapter 14 Cases Study..... 295

14.1 Deployment and Configuration..... 295
14.1.1 Scenario 1: Deploying Device in Route Mode..... 295
14.1.2 Scenario 2: Deploying Device in Bypass Mode..... 304
14.2 Server Load Balancing..... 310
14.3 MySQL Database Load balance..... 312
14.4 Radius Server Load Balance..... 318
14.5 Get Client IP..... 322
14.6 Inbound Scheduling Policy..... 325
14.7 HTTP Rewriting Case..... 329
14.8 Direct Route mode（DR mode）..... 335
14.9 SSL Policy..... 341
14.10 Policy-Based Routing..... 344
14.11 Intelligent DNS..... 347
14.11.1 Scenario 3: Single Site Intelligent DNS..... 347
14.11.2 Scenario 4: Distributed Intelligent DNS..... 354
14.12 IP-Anycast..... 376
14.13 DNS Proxy..... 380
14.14 Outbound Scheduling Policy..... 384
14.15 ACL..... 388
14.16 High Availability..... 389

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

14.17 Cluster Deployment..... 394
14.18 Virtual Link Health Detection..... 403
14.19 Comprehensive Case..... 413

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Declaration

Copyright © 2017 Sangfor Technologies Co., Ltd. All rights reserved.

No part of the contents of this document shall be extracted, reproduced or transmitted in any form or by any means without prior written permission of SANGFOR.

SINFOR, SANGFOR and the Sangfor logo  are the trademarks or registered trademarks of Sangfor Inc. All other trademarks used or mentioned herein belong to their respective owners.

This manual shall only be used as usage guide, and no statement, information, or suggestion in it shall be considered as implied or express warranty of any kind, unless otherwise stated. This manual is subject to change without notice. To obtain the latest version of this manual, please contact the Customer Service of Sangfor.

Preface

About This Manual

This Application Delivery Controller (ADC) User Manual includes the following chapters:

Chapter	Description
Chapter 1 Knowing Your Sangfor Device	The product appearance, features and performance parameters of ADC, wiring and cautions before installation
Chapter 2 Initial Login to Admin Console	The configuration steps required when administrator accesses the Web administrator console of ADC for the first time
Chapter 3 System Status Overview	The system status overview of SANGFOR ADC products.
Chapter 4 Report Generation and Subscription	The ADC report for IT manager.
Chapter 5 Objects	IT manager can specify objects in this chapter, like IP group, time schedule, domain.
Chapter 6 Data Center	All data for statistics been stored in data center ,It manager can view device or service here.
Chapter 7 Load balancing	Server load balance, IT manager can deliver service here.
Chapter 8 Intelligent DNS	ADC realize inbound load balance via intelligent DNS.
Chapter 9 Routing	Policy-based routing, static route, dynamic routing.
Chapter 10 Network	Basic network setting.
Chapter 11 System	General setting, license , administrator and so on.
Chapter 12 Wizard	A configuration guider for IT manager.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 13 High Available	The high available configuration for ADC, it improve business availability.
Chapter 14 Case Study	Case study

Document Conventions

Graphic Interface Conventions

This user manual uses the following typographical conventions for special terms and instructions:

Convention	Meaning	Example
boldface	Page title,parameter, Menu/submenu, Button, key press, link, other highlighted keyword or item	Page/tab name example: Navigate to **System** > **Users** to enter the **User** page. Parameter example: **IP Address:** Specifies the IP address that you want to reserve for certain computer Menus/submenus example: Log in to the Web administrator console and go to **System** > **Network** > **Deployment**. Button example: Click the **Save** button to save the settings. Key press example: Press **Enter** key to enter the admin console. Link example: Once the certificate signing request is generated, click the **Download** link to download the request. Highlighted keyword/item example: The username and password are **admin** by default.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

italics	Directory,URL	**Website:***http://www.sangfor.com*
>	Multilevel menu and submenu	Log in to the Web administrator console and go to **System** > **Network** > **Deployment**.
""	Prompt,quotation	The prompt box shows that " You have saved the configuration successfully ,and the configuration has changed . It is required to reboot DLAN to validate the service, do you want to operate this right now?"

Symbol Conventions

This manual also adopts the following symbols to indicate the parts which need special attention to be paid during the operation:

Convention	Meaning	Description
	Caution	Indicates actions that could cause setting error, loss of data or damage to the device
	Warning	Indicates actions that could cause injury to human body
	Note	Indicates helpful suggestion or supplementary information

Technical Support

- **User Support Email :** tech.support@sangfor.com
- **Technical support Tel:** +60 12711 7129 (7511)
- **Website:** *http://www.sangfor.com*

Acknowledgments

Thanks for using our product and user manual. If you have any suggestion about the product or user manual, please provide feedback to us through phone call or email. Your suggestion will be much appreciated.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 1 Knowing Your ADC

This chapter introduces the Application Delivery Controller(ADC) and the way of connecting ADC. After proper hardware deployment and installation, you can configure and debug the system.

1.1 Operating Environment

- Voltage input: 110V/230V
- Temperature: 0-45°C
- Humidity: 5%-90%

To ensure endurance and stability of the ADC, please ensure the following:

- The power supply is well grounded
- Dustproof measures are taken
- Working environment is well ventilated
- Indoor temperature is kept stable

This product conforms to the requirements on environment protection. The placement, usage and discard of the product should comply with the relevant national laws and regulations of the country where it is applied.

1.2 Product Appearance



Above is the front panel of AD-1600. The interfaces from left to right are described in the following table:

Interface	Description
CONSOLE	Network interface used for high availability (HA) feature or used by device supplier to debug system.
MANAGE	Ethernet port, used for manage device, orange LED on the left side indicates link status, while green LED on the right side indicates data traffic.
NET1	Ethernet port, orange LED on the left side indicates link status, while green LED on the right side indicates data traffic.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

NET2	Ethernet port, orange LED on the left side indicates link status, while green LED on right side indicates data traffic.
NET3	Ethernet port, orange LED on the left side indicates link status, while green LED on the right side indicates data traffic.
POWER	Power LED
ALARM	Alarm LED (keeps on during startup)



The picture above is just for reference. The actual product you purchased and received may vary.

1.3 Deployment and Management

You need a computer before deploying the gateway and ensure the web browsers supports IE, firefox and chrome landing work well. Connect the computer to the SANGFOR AD in the same LAN and configure the device over the network

1.4 Connecting ADC

After deploying the Application Delivery Controller (ADC) in your network (for details, please refer to 9. 1 interface), follow the instructions below to connect the ADC.

1. Plug the power cable into the power interface on the rear panel of the device. Attach and turn on power supply, and then watch the LEDs on the front panel of the ADC.

   When the device starts up, **ALARM** LED will turn on and keep on for 1 to 2 minutes, then turn off; **POWER** LED (in green) will turn on; connection status LEDs (in orange) next to **NET 1** and **NET2** interface will also turn on.

   After successful bootup, **POWER** LED (in green), connection status LEDs (in orange) **NET 1** and **NET2** interface will stay on. If data are being transferred through a port, the data traffic LED (in green, beside connection status LED) will blink.

   If **ALARM** LED stays on always, please switch off the power supply and reboot the device. If **ALARM** LED still keeps on after reboot, contact Customer Service.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

If the corresponding LED indicates normal working status, turn off and unplug the power supply, and perform the following steps.

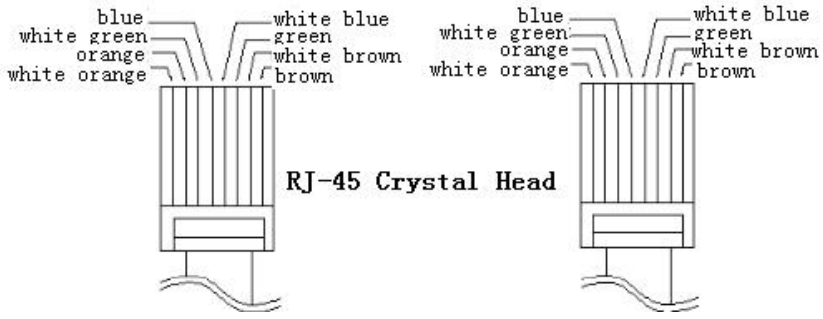
2. Use RJ-45 straight-through Ethernet cable to connect the defined **LAN** interface to the internal network.
3. Use RJ-45 Ethernet crossover cable to connect the defined **WAN** interface to the external network, (i. e. , router, optical fiber transceiver or ADSL Modem for external network).



- WAN interface on the ADC does not support ADSL dial up.
- Multi-Link AD device support several Internet lines. At this point, the network port defined as WAN2 port, is connected to the second Internet access device, the network port defined as WAN3 port, is connected to the third Internet access device and so on.
- Use crossover cable to connect WAN interface to the router for external network.
- Use straight-through cable to connect LAN interface to switch in the internal network.

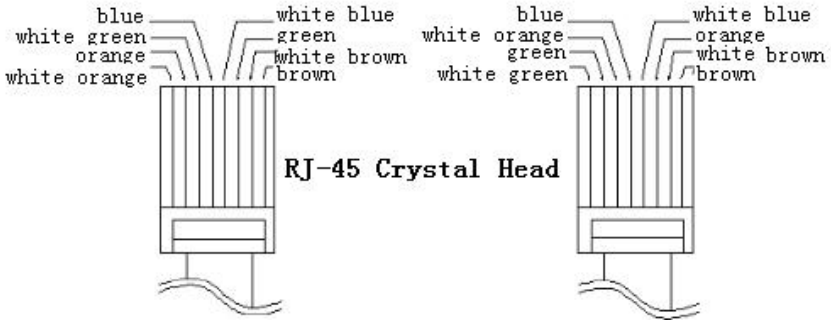
In case session cannot be established but the corresponding LED indicates normal working status, please check whether the right type of cables are being used. The differences between straight-through cable and crossover cable are shown in the figures on the following page.

1. Wire Sequence of Straight-through Cable



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

2. Wire Sequence of Crossover Cable



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 2 Initial Login to Admin Console

2.1 Initial Login to Admin Console

Application Delivery Controller (ADC) provides Web-based administration. The initial URL for Web administrator console access is https://10.252.252.252.

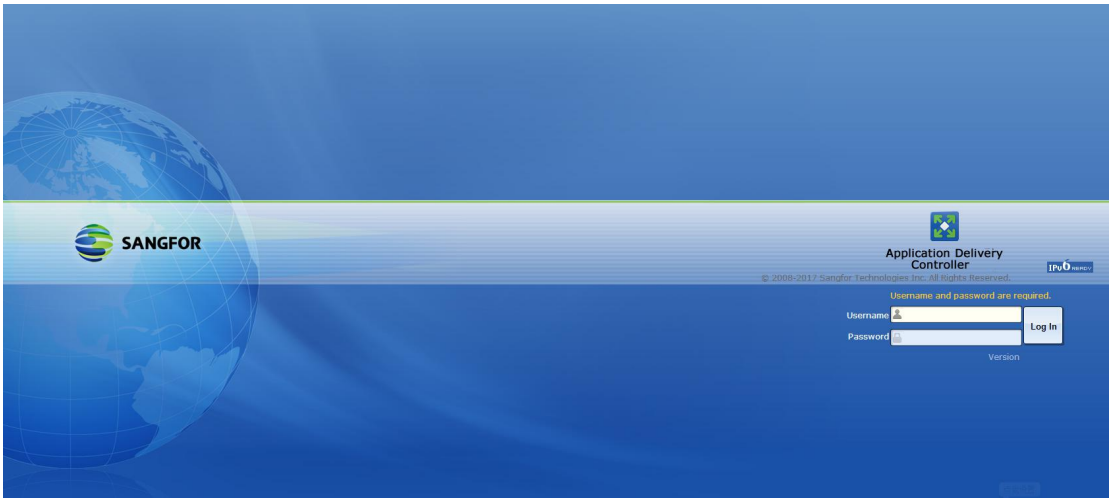
Before logging in to administrator console of ADC, please ensure the following:

- Deploy a computer in the subnet where the ADC resides.
- Connect the PC's network interface card (NIC) and **LAN** interface of ADC to a same layer-2 switch, or connect the PC's NIC to **LAN** interface directly with a network cable.
- Ensure IE browser is installed on the PC. Non-IE browsers Opera, Firefox, Safari and Chrome are not supported.

Logging in to Admin Console

1. Turn on the PC and the ADC. Add an IP address on the PC, an IP address that resides in the network segment **10.252.252.X** (for instance, 10.252.252.100), and type the default landing IP, port of gateway and https://10.252.252.252 in the web browsers supports IE, firefox and chrome landing, as shown below:

2. Open the IE browser and enter the URL address (https://10.252.252.252) into the address bar. Press **Enter** key to visit the login page to Web administrator console, as shown below:



3. Enter the administrator username and password and click the **Log In** button. The default administrator username is **admin** (case-insensitive) and password is **admin** (case-sensitive).

4. For version information of the software, click on **Version** below the textboxes.



Before configuring any **NET** port, connect the **MANAGE** interface to your internal network with a network cable and then log in to the Web administrator console. Only the **NET** port is configured in **Network** > **Interface** > **Physical Interface**, can you access the network port to connect to SANGFOR. (For details, refer to 9. 1 interface)

MANAGE interface has two IP address when the ADC is shipped from factory, **10.252.252.252** and **10.254.254.254**.

2.2 Viewing Status and Logs

On login to the Web administrator console, you can see the following function modules, namely, **Status**, **Report**, **Objects**, **Load Balancing**, **Intelligent DNS**, **Routing**, **Network**, **System** and **Wizard**.





During configuration, if there is an **OK**, **Save** or **Save and Apply** button on the web page, click it to save or apply the settings. This will not be illustrated again in the subsequent parts in this user manual.

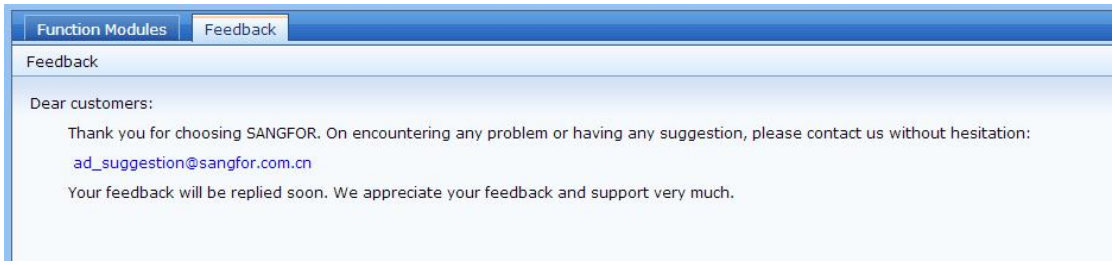
On the **Welcome** page, there are two modules, Function Modules and Feedback. There is also alarm notification and you may follow the instructions to view details.

Function Modules enable you to know corresponding modules quickly.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



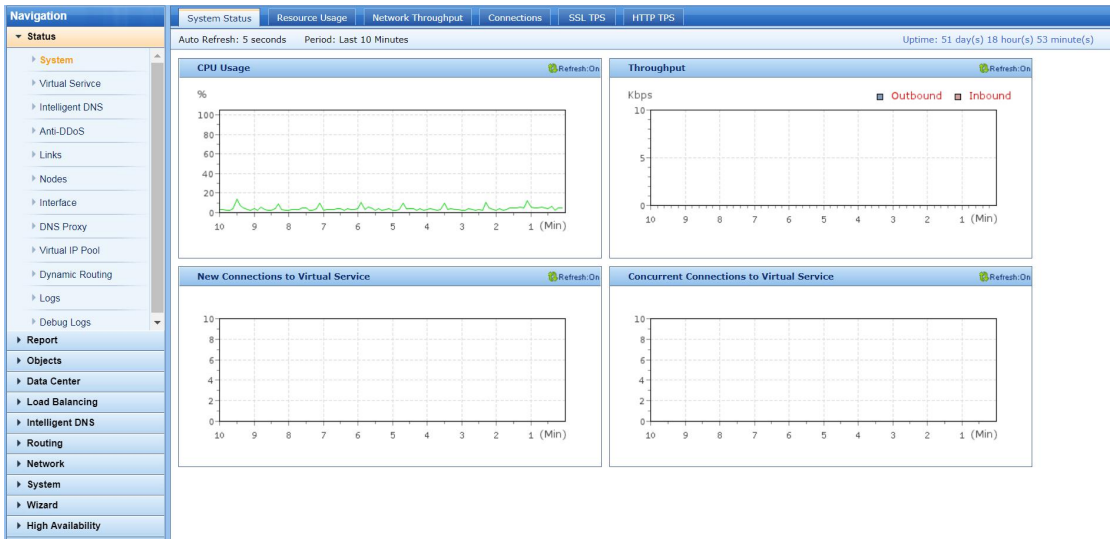
Feedback module enables you to offer valuable advice and suggestions to Sangfor.



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 3 System Status Overview

Status includes status of system, virtual services, links and servers, etc. The contents are including **System, Virtual Service, Intelligent DNS, Anti-DDos, Links, Nodes, Interface, DNS Proxy, Virtual IP Pool, Dynamic Routing, Logs** and **Debug Logs** as shown in the following figure:



3.1 System status

In **Status > System**, there are six tabs, **System Status, Resource Usage, network Throughput, Connections, SSL TPS** and **HTTP TPS**, and you can check the executable time on the top right corner of the surface.

3.1.1 System Status

In **Status > System > System Status** last 10 minutes CPU usage , throughput, new connections to virtual service, concurrent connections to virtual service will be displayed.

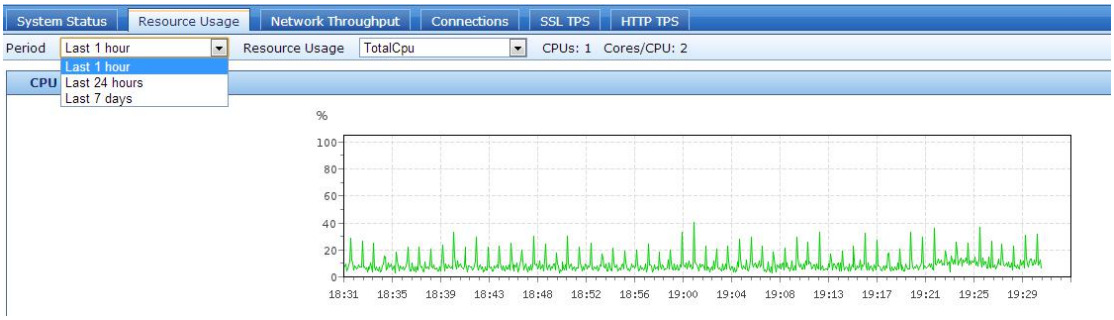
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Click **Refresh**: **On** on the upper right corner to disable automatic refresh.

3.1.2 Resource Usage

In **Status** > **System** > **Resource Usage**, CPU usage and memory usage of ADC can be displayed. As for CPU usage, both single CPU usage and total CPU usage can be displayed.

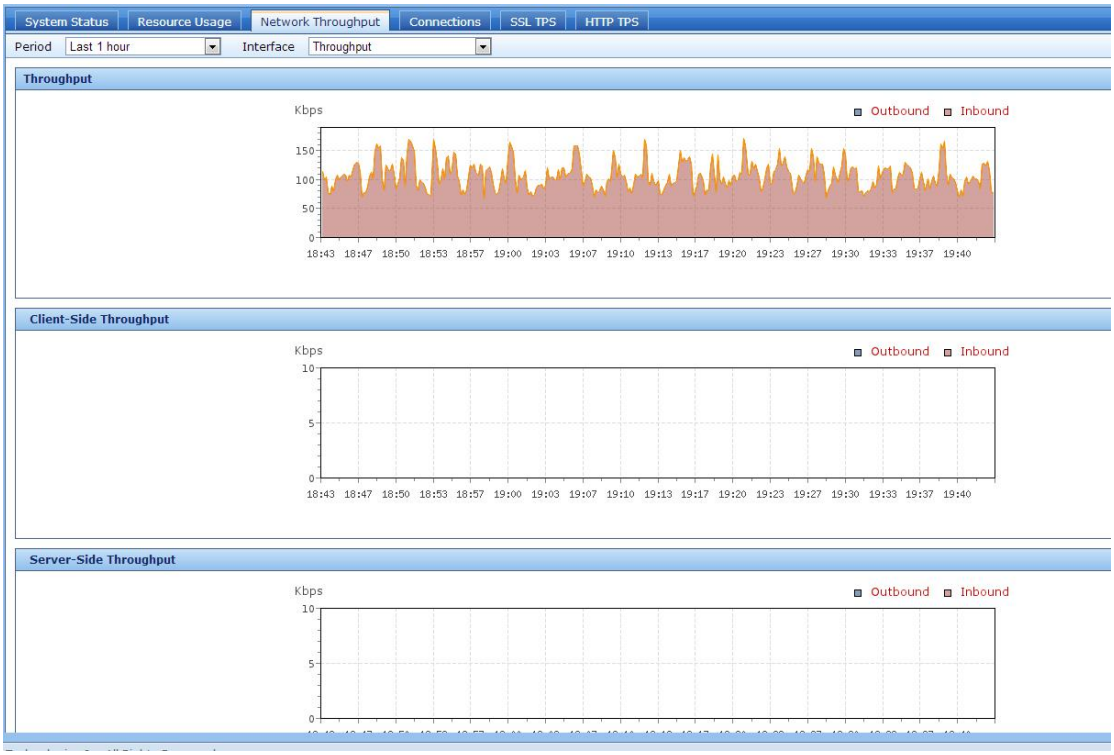


By default, data during the past 10 minutes are refreshed every five seconds. You can click on **Refresh: On** to disable automatic refresh and select period, **Last 1 hour**, **Last 24 hours** or **Last 7 days** on the enlarged tab.

3.1.3 Network Throughput

In **Status** > **System** > **Network Throughput**, this page is used to show real-time network outbound and inbound traffic, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Period: You can select **Last 1 hour**, **Last 24 hours**, or **Last 7 days** to display throughput within different periods of time.

You can view throughput of all interfaces and throughput on specific WAN interfaces.

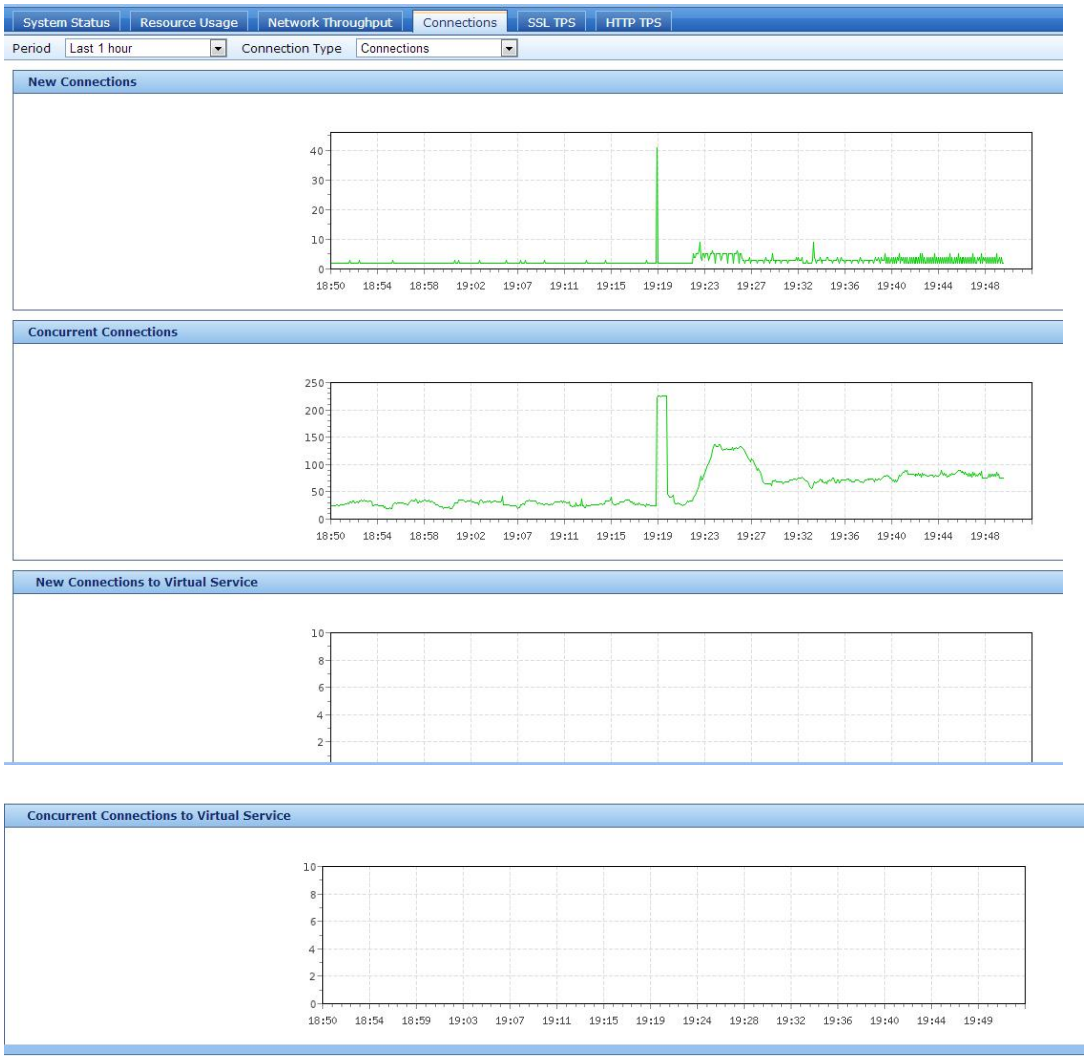
Refresh: Once enabled, data will be automatically refreshed every five seconds.

3.1.4 Connections

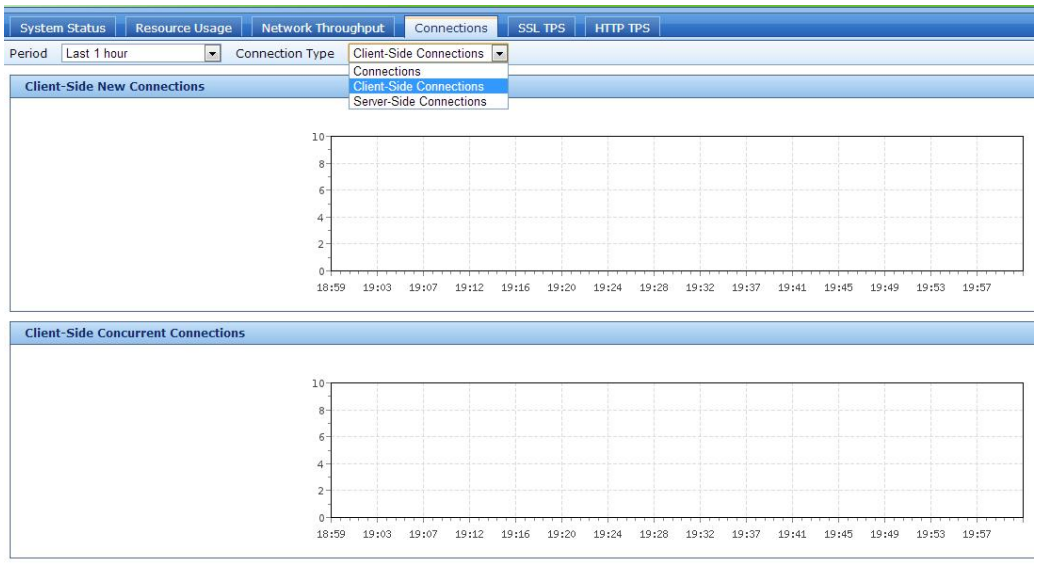
In **Status** > **System** > **Connections**, You can view total connections, client-side connections and server-side connections. If **Connections** is selected for **Connection Type,** you may view **New Connections**, **Concurrent Connections**, **New Connections to Virtual Service** and **Concurrent Connections to Virtual Service**.

Device connections include system connections, system concurrent connections, virtual service new connections and virtual service concurrent connections.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

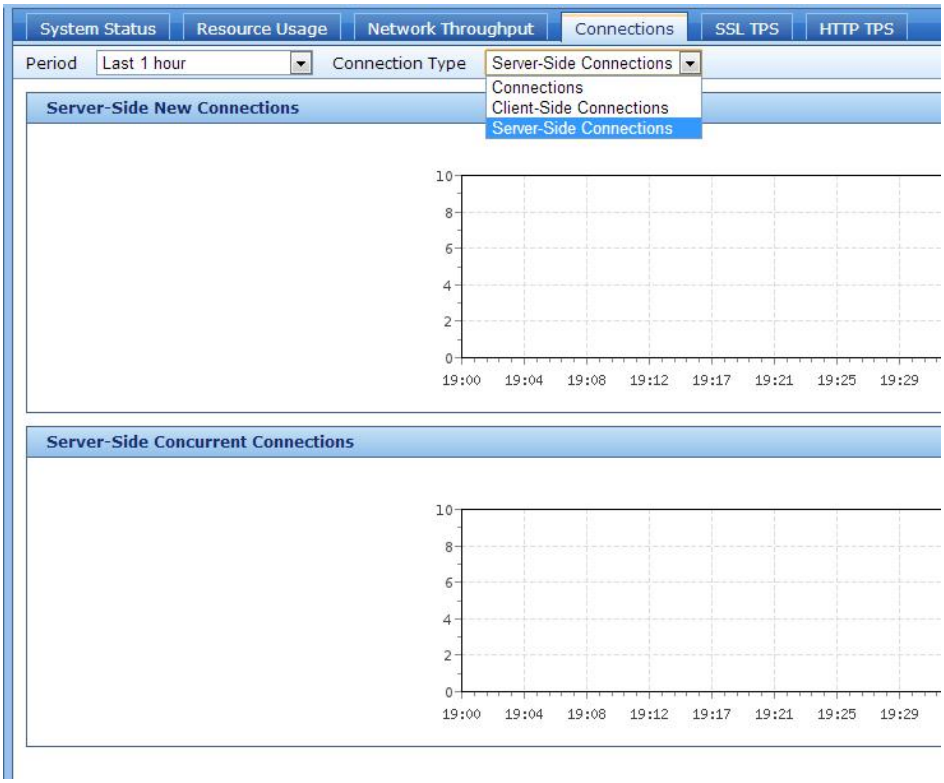


Client-Side Connections include **Client-Side New Connections** and **Client-Side Concurrent Connections.**



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

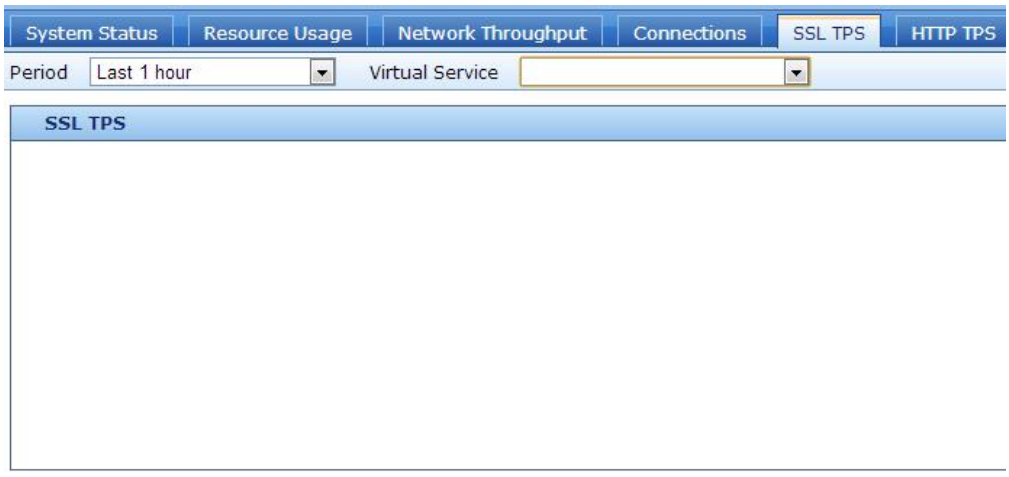
Server-Side Connections include **Server-Side New Connections** and **Server-Side Concurrent Connections**.



Period: You can select **Last 1 hour**, **Last 24 hours**, or **Last 7 days** to display connections within different periods of time.
Refresh: Once enabled, data will be automatically refreshed every five seconds. You cam click to disable auto refresh.

3.1.5 SSL Transactions per Second(TPS)

In **Status** > **System** > **SSL TPS**, you can view SSL connections, as shown below:



Period: You can select **Last 1 hour**, **Last 24 hours**, or **Last 7 days** to display SSL connections

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

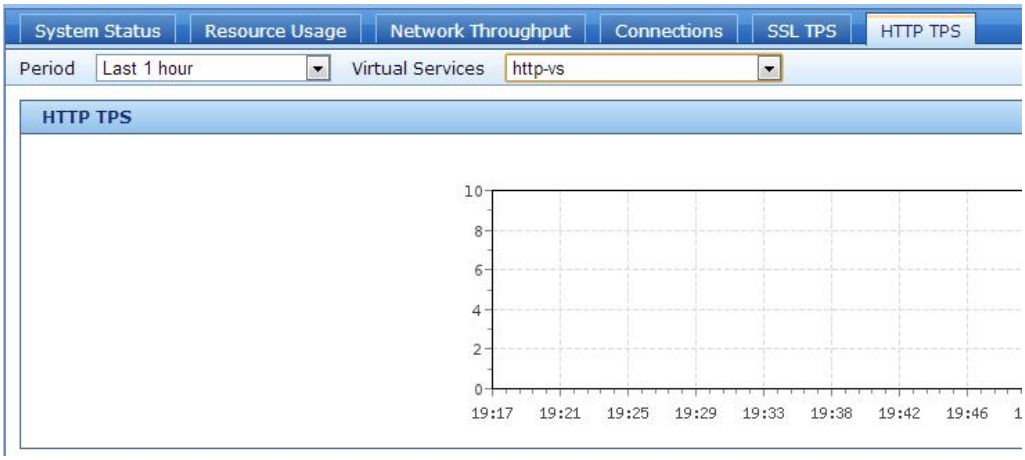
within different periods of time.

Virtual Service: You can select different virtual services.

Refresh: Once enabled, data will be automatically refreshed every five seconds. You cam click to disable auto refresh.

3.1.6 HTTP Transactions per second(TPS)

In **Status** > **System** > **HTTP TPS**, you can view HTTP connections, as shown below:



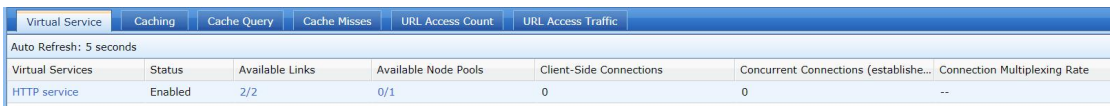
Period: You can select **Last 1 hour**, **Last 24 hours**, or **Last 7 days** to display data within different periods of time.

Virtual Service: You can select different virtual services.

Refresh: Once enabled, data will be automatically refreshed every five seconds. You cam click to disable auto refresh.

3.2 Virtual service

Virtual Service includes virtual service status, cache and traffic situation, etc. The contents include virtual service status, cache/traffic status, cache query, cache miss reason, URL counts and URL real-time traffic.

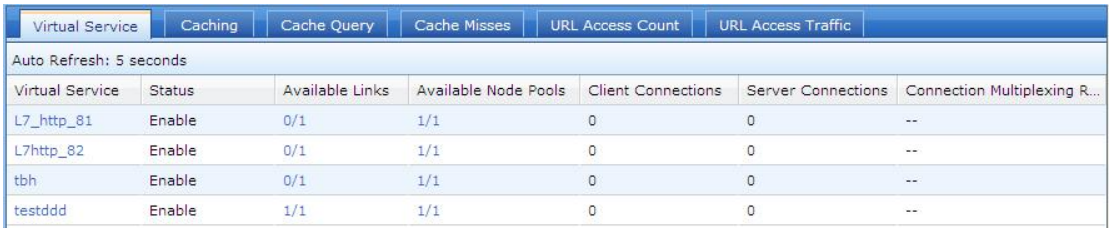


3.2.1 Virtual service

In **Status > Virtual Service** > **Virtual Service**, virtual service are usable link for virtual service,

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

usable node pool, client-side and server-side connections, the corresponding status can be selected in the list accordingly.



Click on the virtual service **name** in the list, you can edit the virtual service.

Status column shows the status of virtual service, **Enabled** or **Disabled**.

Available Links column shows the number of links associated with a virtual service and available links. Click on the number, you can enter another tab to view the detailed link status.

Available Node Pools column shows the number of nodes associated with a virtual service and available node pools. Click on the number, you can enter another tab to view the detailed pool status.

Client Connections column shows the number of connections from client side.

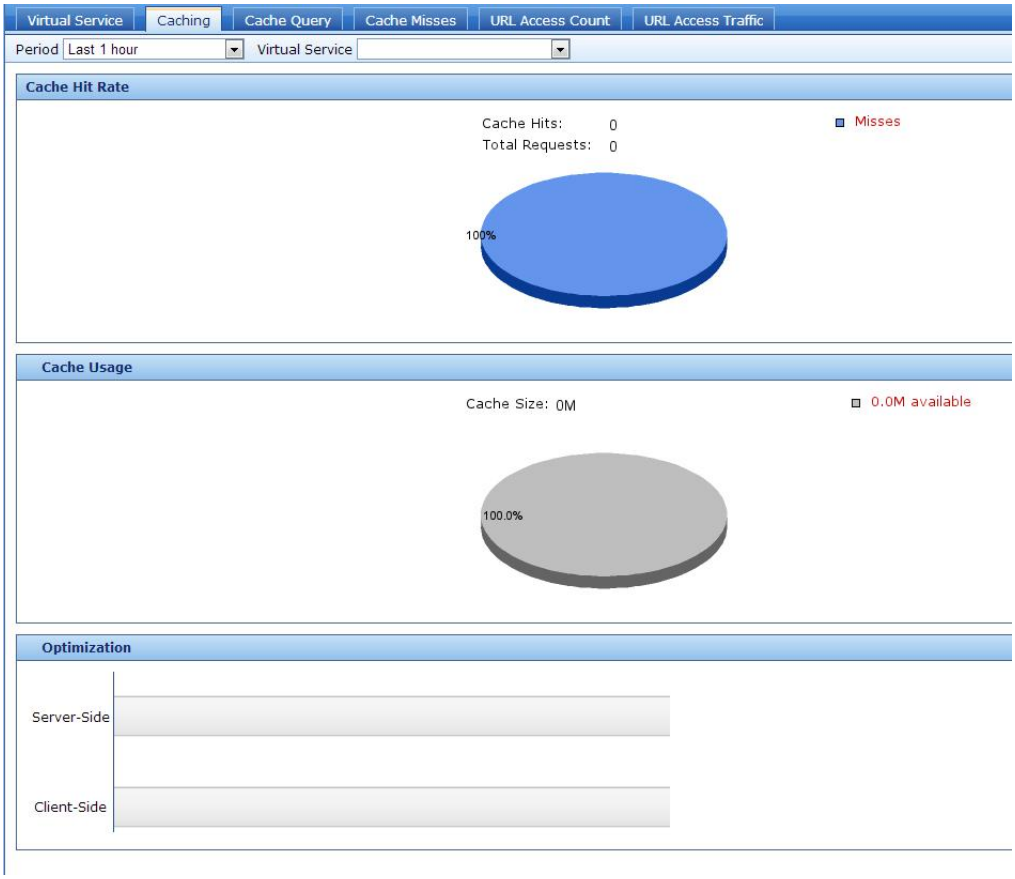
Server Connection column shows the number of connections to server side.

Connection Multiplexing Rate column shows the multiplexing information of connections to virtual service.

3.3.2 Caching

In **Status** > **Virtual Service > Caching**, you can view cache hits and misses, cache usage and optimization of specific virtual service during specified period, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Period options are **Last 1 hour**, **Last 24 hours** and **Last 7 days**

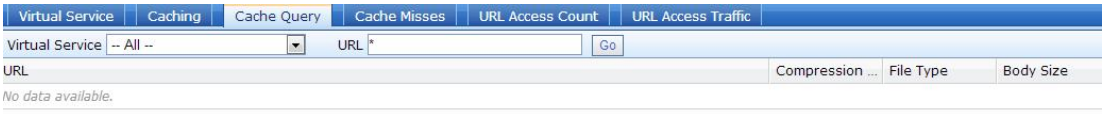
Select a virtual service to search for the caching statistics.

Click the **Traffic** recycle bin icon (at the right top of the screen) to clear the traffic data.

Click the **Cache** recycle bind icon (at the right top of the screen) to clear the cached data.

3.3.3 Cache Query

In **Status** > **Virtual Service > Cache Query**, you can search for URL of virtual service to check if it is cached on the ADC, as shown in the following figure:



Select a virtual service to search for the caching statistics.

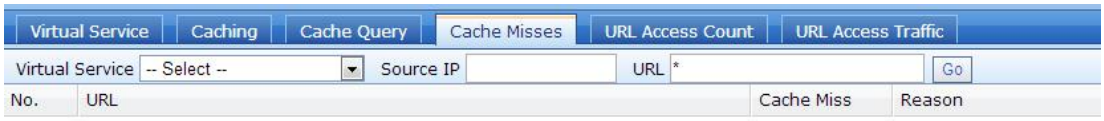
Enter a URL to search for the caching statistics. Wild cards supported.

Click **Go** to search for the caching statistics based on the criteria specified above. A maximum of 10000 entries will be displayed if available.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

3.3.4 Cache Misses

In **Status** > **Virtual Service > Cache Misses**, you can view number of caching failures of a URL during a specific period, and the cause of caching failures as well, as shown in the following figure:



Select a virtual service to search for the caching failures.

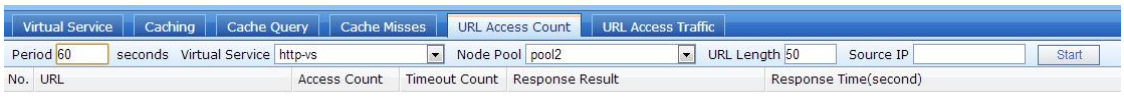
Select the source IP address of virtual service access.

Enter the URL to search for for the caching failures. Wild cards supported.

Click **Go** to search for the caching failures based on the criteria specified above.

3.3.5 URL Access Count

In **Status** > **Virtual Service > URL Access Count**, you can view the access information of the URL addresses provided by HTTP server in specific node pools of virtual service, as shown in the following figure:



Specify period to search for statistics during that period.

Select a virtual service to search for the data related to that virtual service.

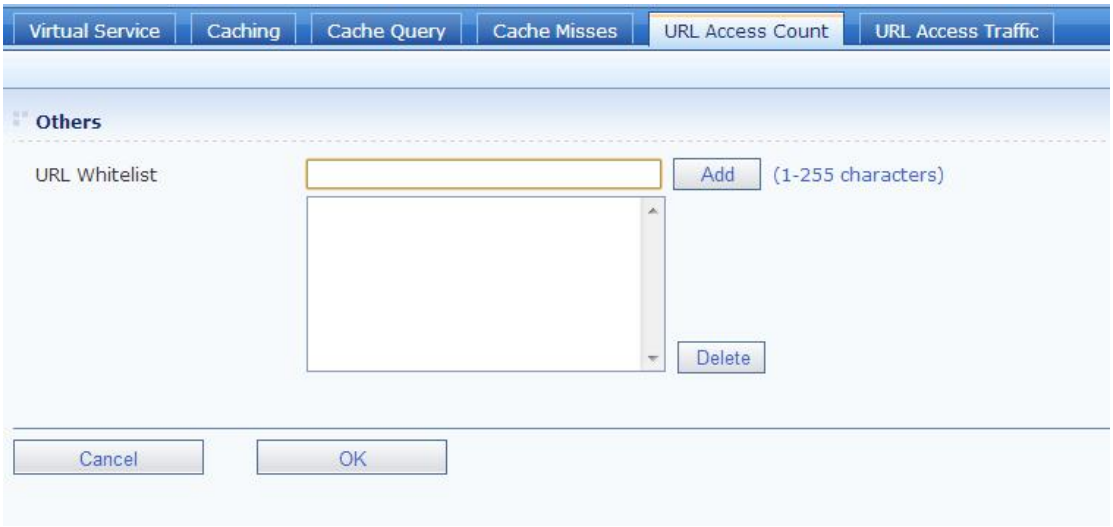
Select a node pool to search for the data related to that pool.

Specify the URL length so that only data of URL within the length are categorized into one URL entry.

Specify source IP to search for the data related to that source.

After setting the conditions, click **start** to statistic the number of accessing URLs. Click **Excluded**, you can add URLs to URL Whitelist where URL do not need to be counted, then click **OK** to save.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



3.3.6 URL Access Traffic

In **Status** > **Virtual Service > URL Access Traffic**, you can view the HTTP and HTTPS traffic information of access to virtual service URLs, as shown in the following figure:



Select a virtual service to search for the data related to that virtual service. Virtual service can be HTTPS or HTTP based. Click **Go** to start searching based on the criteria.

3.4 Intelligent DNS

In **Status** > **Intelligent DNS**, there are statistics related to DNS records, including real-time domain access, domain access history, DNS requests, LDNS and LDNS misses.

3.4.1 Realtime Queries

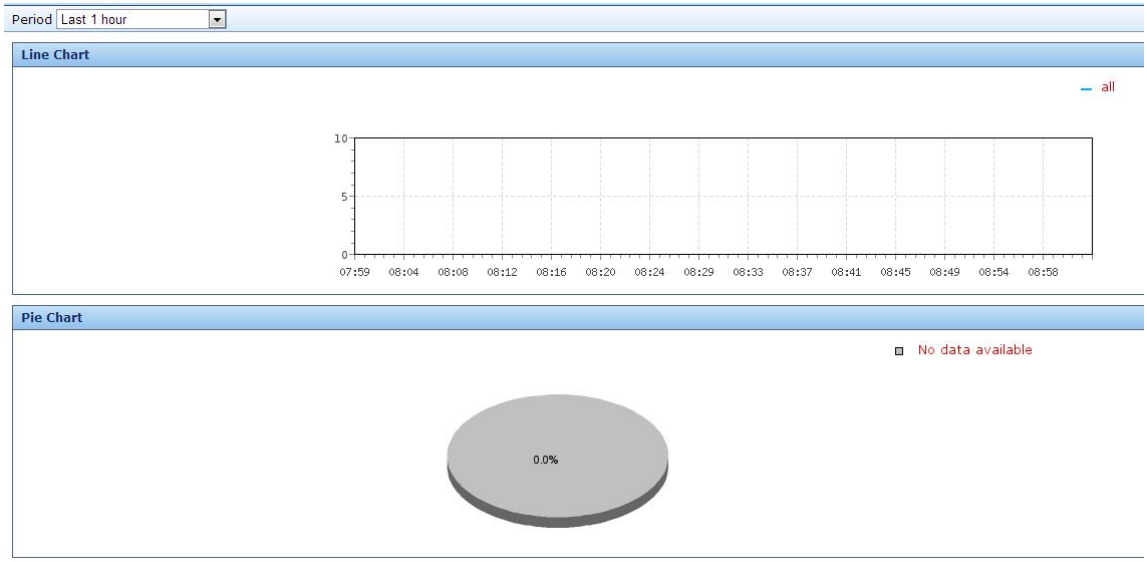
In **Status** > **Intelligent DNS** > **Realtime Queries**, you can view the total number of requests to each domain in one second, as shown in the following figure:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

3.4.2 Queries By Domain

In **Status** > **Intelligent DNS** > **Queries By Domain**, you can view the total number of requests to each domain in the past, as shown in the following figure:

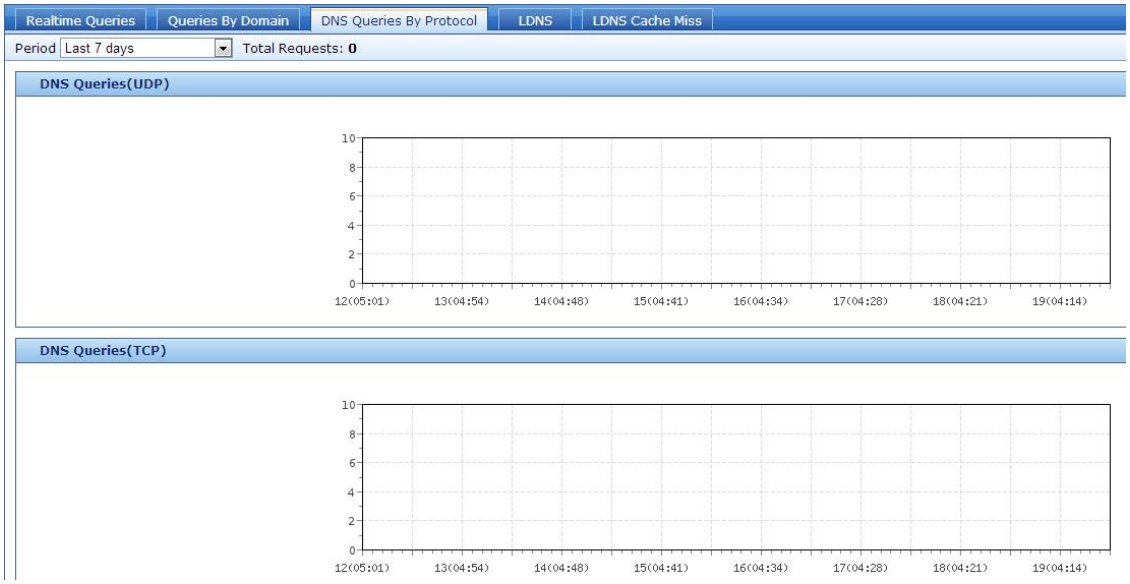


Select a period to show the data generated during that period, 1 hour, 24 hours or 7 days.

Select domain or All domains to show total request to a specific or all the domains in the past.

3.4.3 DNS Queries By Protocol

In **Status** > **Intelligent DNS** > **DNS Queries By Protocol**, you can view the total DNS requests, as shown in the following figure:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

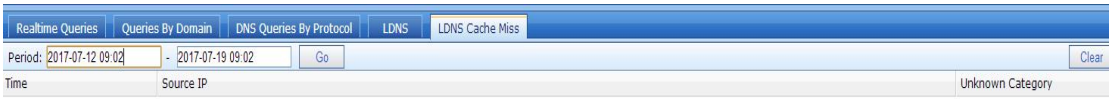
3.4.4 LDNS

In **Status** > **Intelligent DNS** > **LDNS**, you can view the LDNS source and access count of DNS request in one second, as shown in the figure below:



3.4.5 LDNS Cache Miss

In **Status** > **Intelligent DNS** > **LDNS Cache Misses**, you can view the LDNS records missing in the ISP address pool. You can view the data given that you have started the statements, as shown in the following figure :



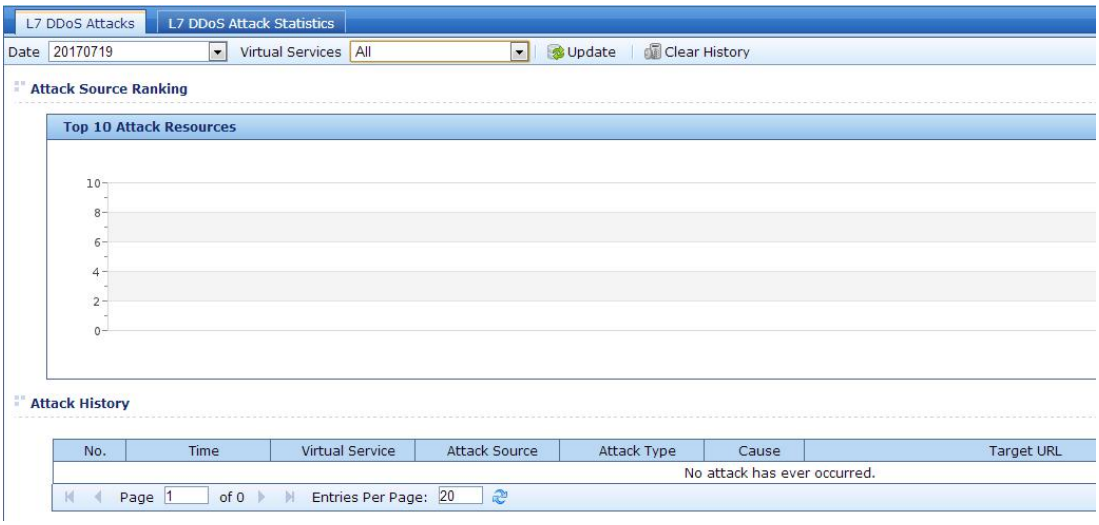
3.5 Anti-DDoS

In **Status > Anti-DDoS**, there are two modules, **L7 DDoS Attacks** and **L7 DDoS Attack Statistics**.

3.5.1 L7 DDoS Attacks

In **Status** > **Anti-DDoS > L7 DDoS Attacks**, you can view layer 7 DDoS attacks and view top 10 attack resources. In **Attack History,** attack details are displayed, including **Time, Virtual Service, Attack Source, Attack Type, Cause, Target URL, Attack Count and Action**. You can click the link under **Action** and you will be directed to corresponding policies, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



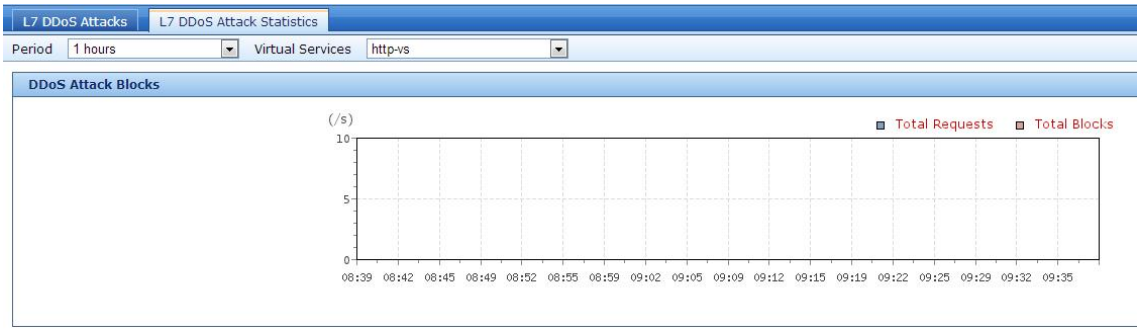
Date: You can specify a specific date within one week.
Virtual Service: You can select a specific virtual service.
Update: You can click **Update** to update data to the latest.
Clear History: You can click **Clear History** to remove all data of virtual service from the database.
Export Logs: You can click **Export Logs** to export logs for further analysis.

Action: When the record's virtual service takes default strategy, it will pop-up prompt to warn the user that modify default policy will affect all virtual services that take default policy, and options are add policy and edit default policy.

Prompt: If you select to edit default policy, it will jump to default HTTP defence policy edit page. You can fill in the deployment accordingly. Click OK, then pop-up prompt to confirm the modification.

3.5.2 L7 DDoS Attacks Statistics

In **Status** > **Anti-DDoS > L7 DDoS Attacks Statistics**, you can view DDoS attack blocks during specific period of time and configure relevant protection policies, as shown below:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Period: You can select a specific period of time to display data, options are **1 hour**, **Last 24 hours**, or **Last 7 days**,

Virtual Service: You can select a specific virtual service.
Refresh: Once enabled, data will be automatically refreshed every 5 seconds.

3.6 Links

3.6.1 WAN Links

In **Status** > **Links > WAN Links**, you can view the traffic on and status of WAN links, as shown in the following figure:



Auto Refresh indicates the interval that the link list refreshes automatically, every 5 seconds by default.

Name column shows the name of the WAN link. For how to configure a WAN interface, refer to Chapter 9. 1 the relevant description of interface

Outbound and **Inbound** columns show the transmission rate on the WAN link at real time.

Status of a WAN link may be **Normal**, **Busy**, **Down** or **Disabled**.

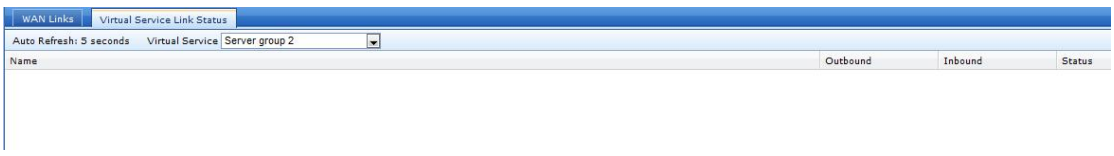
Busy means bandwidth usage of the link reaches the specified threshold. For the configuration of a WAN link, refer to the Chapter 9. 1 the setting of interface

Down means the WAN link is unavailable at present.

Disabled means the WAN link is disabled (see Chapter 9. 1 the setting of interface

3.6.2 Virtual Service Link Status

In **Status** > **Links > Virtual Service Link Status**, you can view the traffic on and status of the WAN links for virtual service access.



Auto Refresh indicates the interval that the link list refreshes automatically, every 5 seconds

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

by default.

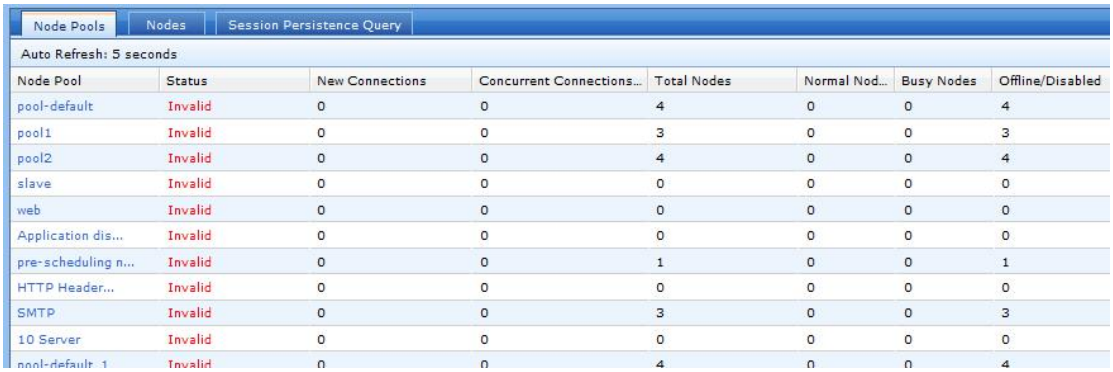
Select a virtual service to show the list of related WAN links. For how to configure a virtual service, refer to Chapter 3. 7. 8 the setting of virtual service

Outbound and **Inbound** column show the transmission rate of specified virtual service data on the WAN link at real time.

Status of WAN link for virtual service access may be **Normal**, **Busy** or **Down.**

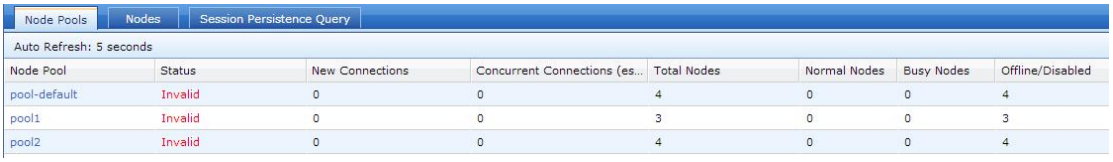
3.7 Nodes

In **Status** > **Nodes**, there are three modules, **Node Pools, Nodes**, and **Session Persistence Query**, as shown below:



3.7.1 Node Pools

In **Status** > **Nodes > Node Pools**, you can view status of nodes, number of active nodes and busy nodes in each pool.



Auto Refresh indicates the interval that the list refreshes automatically, every 5 seconds by default.

Status column shows the status of the node pool.
Total Nodes column shows the total number of nodes in the pool.
New Connections column shows new connections in the node pool.

Node Count column shows the number of nodes in the pool.

Concurrent Connections column shows the concurrent connections in this node pool.

Normal Nodes, Busy Nodes, Offline/Disabled columns show the number of nodes in the node pool in that status.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Normal means the node is available as normal.

Busy means the node has something wrong and triggered alert if SNMP-based node health monitor is in use, such as server CPU, memory or disk usage is beyond is the threshold.

If it shows '**Disabled**', the node is disabled by network administrator manually.

If it shows '**Disabled, system is shutting down..** ', the node does not allow new connections.

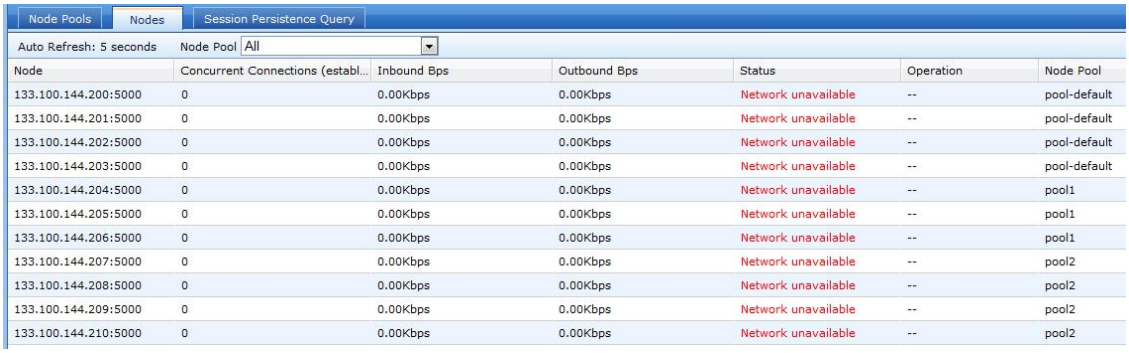
If it shows '**Disabled, shutdown is completed**', the node does not have any connection.

If it shows '**Normal, system powers on**', the node powers on and gradually allows new connections.

If it shows '**Network unavailable**', the node is unreachable.

3.7.2 Nodes

In **Status** > **Nodes > Nodes**, you can view the node status and number of connections to each node, as shown in the following figure:



Node	Concurrent Connections (establ...	Inbound Bps	Outbound Bps	Status	Operation	Node Pool
133.100.144.200:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool-default
133.100.144.201:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool-default
133.100.144.202:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool-default
133.100.144.203:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool-default
133.100.144.204:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool1
133.100.144.205:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool1
133.100.144.206:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool1
133.100.144.207:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool2
133.100.144.208:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool2
133.100.144.209:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool2
133.100.144.210:5000	0	0.00Kbps	0.00Kbps	Network unavailable	--	pool2

Auto Refresh indicates the interval that the list refreshes automatically, every 5 seconds by default.

Select a node pool to view the nodes in that pool.

Node column shows the IP address of the node.

Sessions column shows the number of connections to the node.

Outbound and **Inbound** columns show the rates at which the data is sent from and received by the node.

Normal, **Busy**, **Disabled** indicates the number of nodes in the node pool in that status.

Normal means the node is available as normal.

Busy means the node has something wrong and triggered alert if SNMP-based node health monitor is in use, such as server CPU, memory or disk usage is beyond is the threshold.

If it shows '**Disabled**', the node is disabled by network administrator manually.

If it shows '**Disabled, system is shutting down..** '' the node does not allow new connections.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

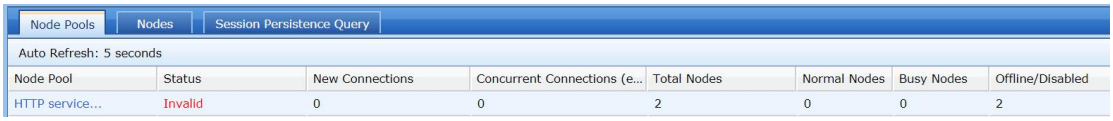
If it shows '**Disabled, shutdown is completed**', the node does not have any connection.

If it shows '**Normal, system powers on**', the node powers on and gradually allows new connections.

If it shows '**Network unavailable**', the node is unreachable.

3.7.3 Scheduling

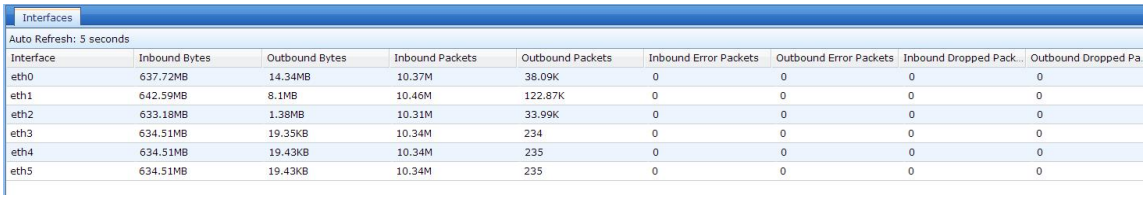
In **Status** > **Nodes > Scheduling**, you can view to which node the request from a user is forwarded.



Specify node pool and client IP address (IPv4 or IPv6 address), and click **Test** to search for the scheduling information.

3.8 Interface

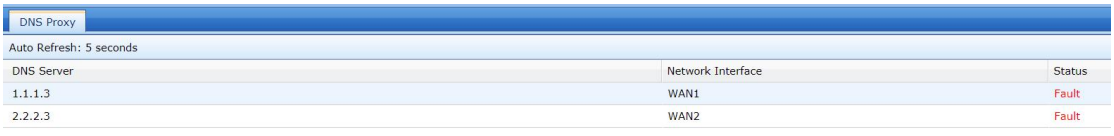
In **Status > Interface**, you can view status of interfaces, including Inbound Bytes, Outbound Bytes, Inbound Packets, Outbound Packets, etc, as shown below:



3.9 DNS Proxy

In **Status** > **DNS Proxy**, you can view the DNS service status, DNS status can be shown as long as you have enabled DNS proxy, refer to Chapter 9. 5 the relevant description of interface

as shown int he following figure:



Auto Refresh indicates the interval that the list refreshes automatically, every 5 seconds by

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

default.

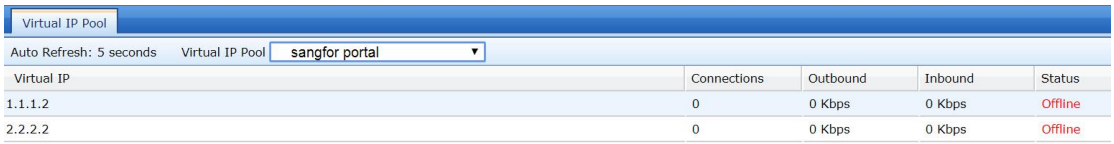
DNS Server column shows the IP address of the DNS server.

Interface column shows the interface on which DNS server is providing services.

Status column shows the status of DNS server.

3.10 Virtual IP Pool

In **Status** > **Virtual IP Pool**, you can view virtual IP pool information of intelligent DNS, as shown in the following figure:

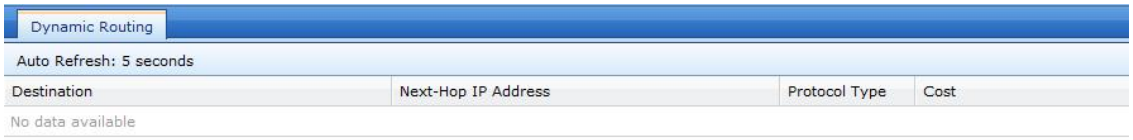


Auto Refresh indicates the interval that the list refreshes automatically, every 5 seconds by default.

Select a virtual IP pool to view information of the virtual IP address in the pool.

3.11 Dynamic Routing

In **Status** > **Dynamic Routing**, you can view the routes learned with RIP or OSPF, as shown in the following figure:



3.12 Logs

In **Status** > **Logs** contains error and operation event on this device. There are system logs, operation logs, SSL logs.

3.12.1 System Logs

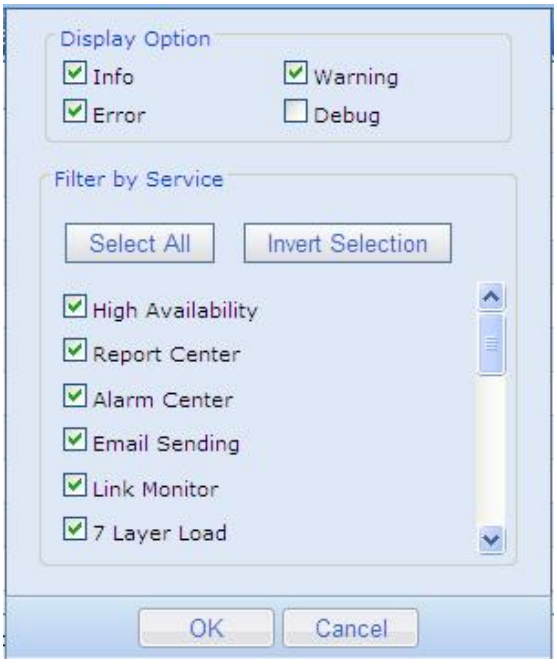
System Logs contains logs about the system itself, as shown in the figure above.

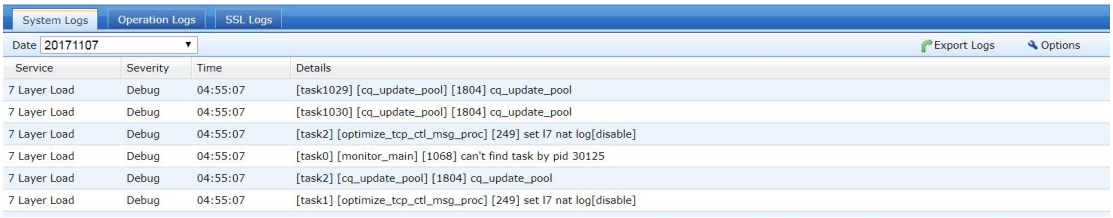
To view the logs generated on a specific day, select a date from the **Date** pull-down list.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

You can click **Export Logs** to export system logs, important back-end information, blackbox logs, etc.

To filter the types of logs you want to view, click **Options** and select the log and service type, as shown below:

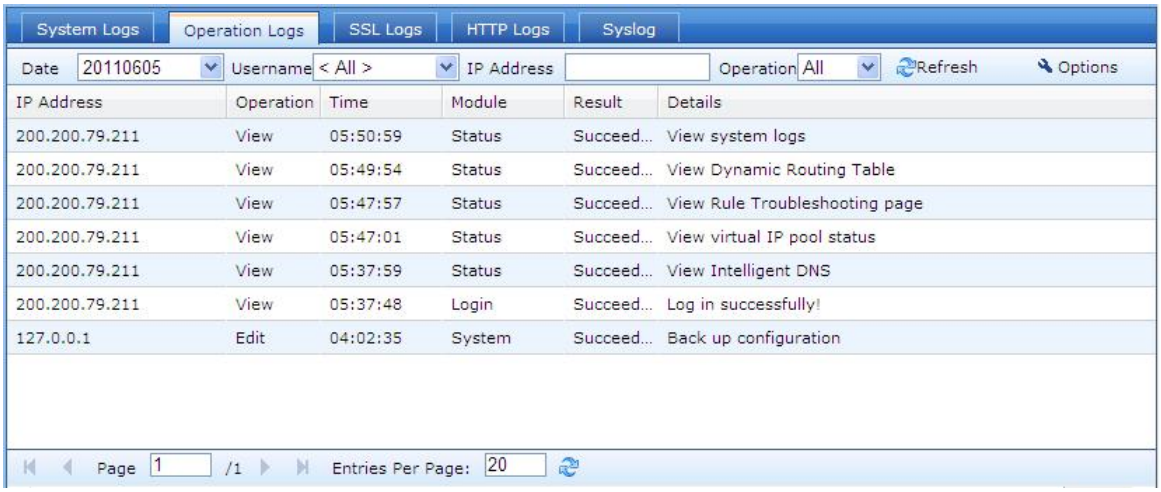




3.12.2 Operation Logs

Operation Logs contains logs that administrator operates on the system, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To view the logs generated on a specific day, select a date from the **Date** pull-down list.

To view the logs related to a specific administrator, select an account from **Username** pull-down list.

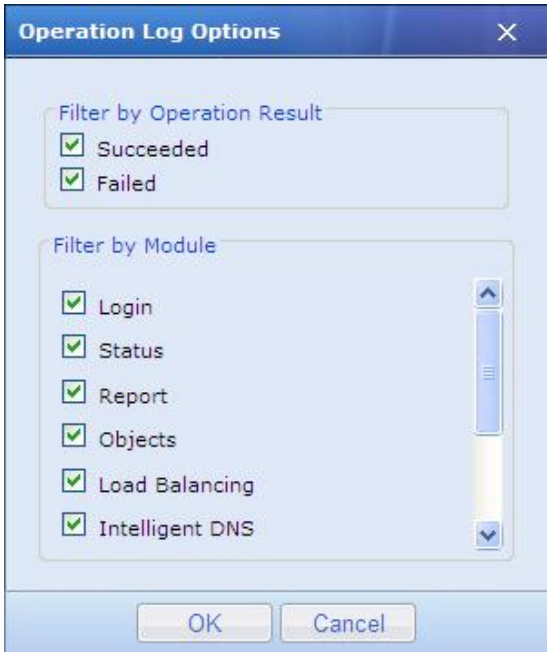
To view the logs related to a specific IP address, specify an **IP Address**.

To view logs related a specific operation, select an operation from the **Operation** pull-down list, Options are **All**, **View**, **Edit**, **Add**, **Delete**, **Update** and **Non-view**.

To export the logs generated on the selected date, click **Export**.

To refresh the page, click **Refresh**.

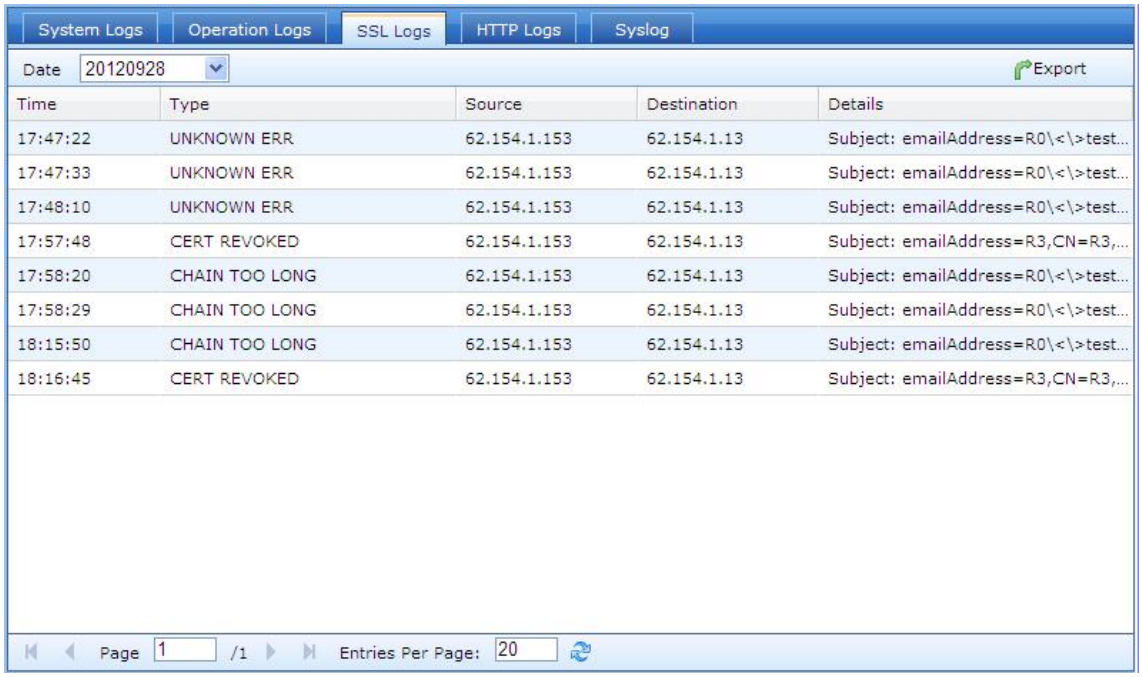
To filter the types of logs you want to view, click **Options** and select the log and service type, as shown below:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

3.12.3 SSL Logs

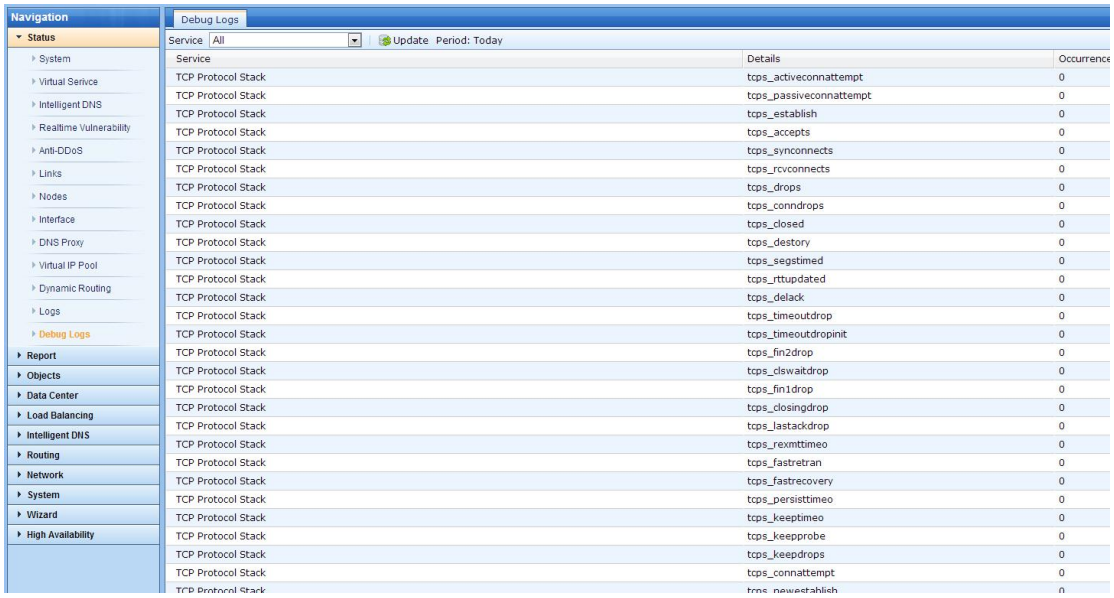
SSL Logs contains logs related to SSL based user authentication, as shown in the following figure:



3.13 Debug Logs

In **Status > Debug Logs > Debug Logs**, you can view debug logs for different services, including **TCP Protocol Stack, UDP Protocol Stack, SSL Protocol Stack, TCP Scheduling, HTTP Proxy,** etc., so as to help Sangfor technical support to do troubleshooting.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To refresh current data click **Update**.

To clear current data, click **Clear Logs**.

To export logs for detailed analysis, click **Export Logs**.

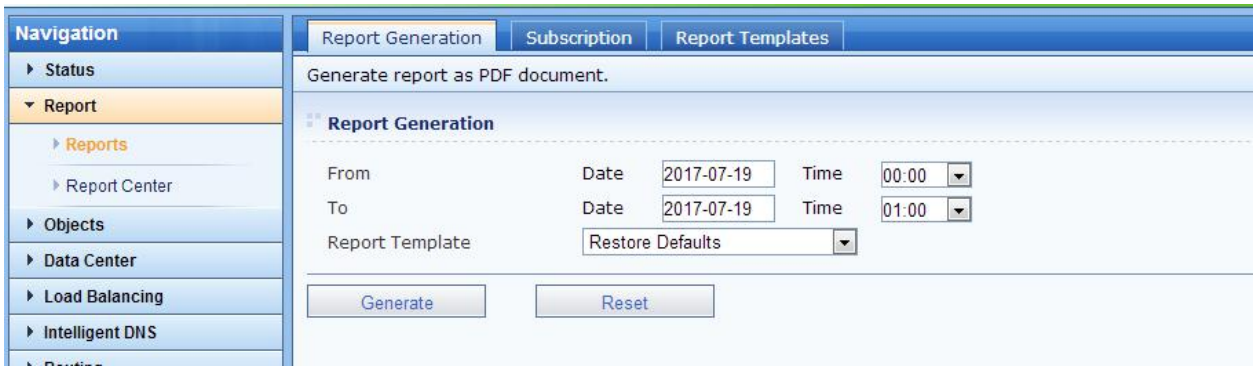
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 4 Report Generation and Subscription

4.1 Report

4.1.1 Report Generation

Navigate to **Report** > **Reports** > **Report Generation**, you can specify date range and report template to generate a report that contains specified statistics about the ADC, as shown in the figure below:



The following are the contents contained on the **Report Generation** tab:

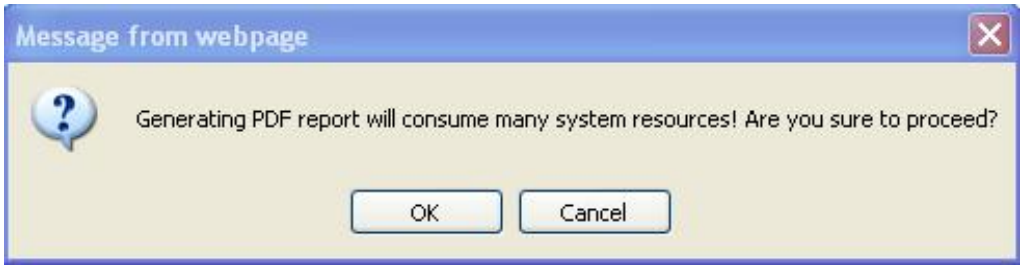
From: Specifies a start date and time to have the report contain data generated since that time point.

To: Specifies a end date and time to have the report contain data generated till that time point.

Report Template: Select a template based on which report is generated.

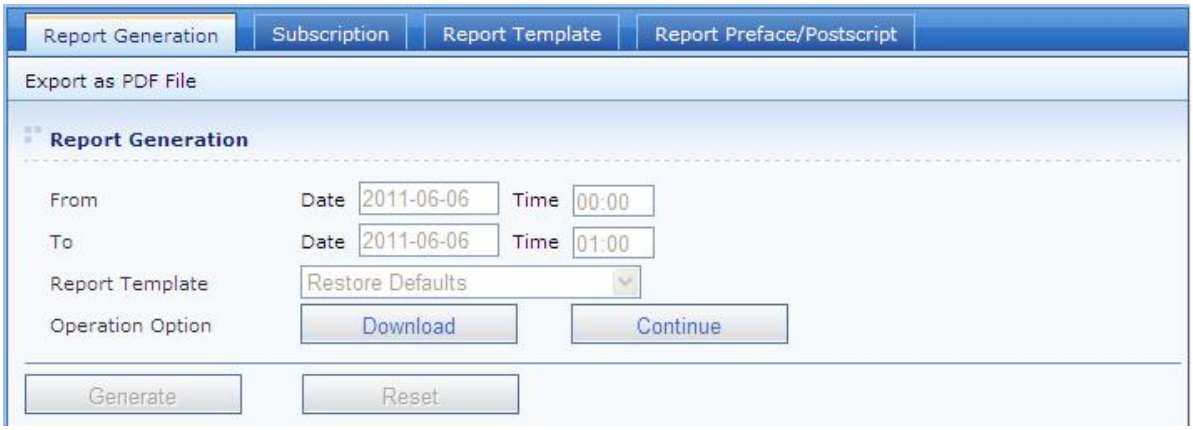
Reset: Click this button to restore the settings on this tab to defaults

Generate: Click this button to generate report based on the above criterial. Then the following dialog pops up:



Click **OK** to generate the report right now and go back to the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

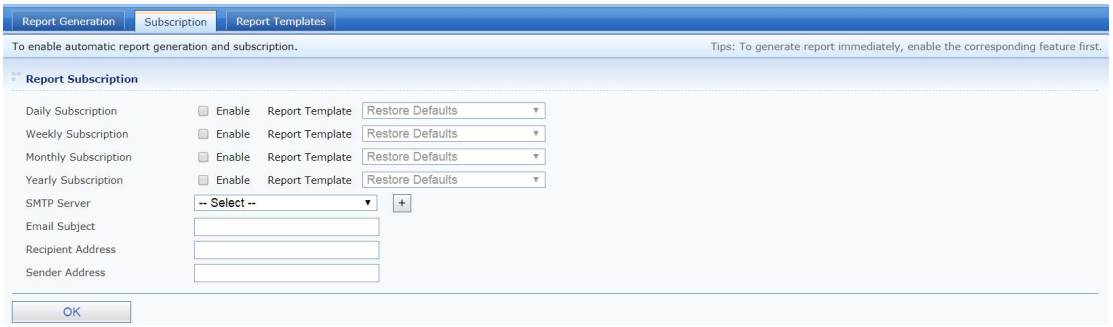


To save the report on the local computer, click **Download**.

To continue generating another report, click **Continue**.

4.1.2 Report Subscription

Navigate to **Report** > **Reports** > **Subscription**, you can have reports generated based on a report template and sent to specified email address on daily, weekly, monthly or yearly basis, as shown in the figure below:



Daily Subscription: Select **Enable** and specify a report template based on which report will be generated and sent to the specified email address, on daily basis.

Weekly Subscription: Select **Enable** and specify a report template based on which report will be generated and sent to the specified email address, on weekly basis.

Monthly Subscription: Select **Enable** and specify a report template based on which report will be generated and sent to the specified email address, on monthly basis.

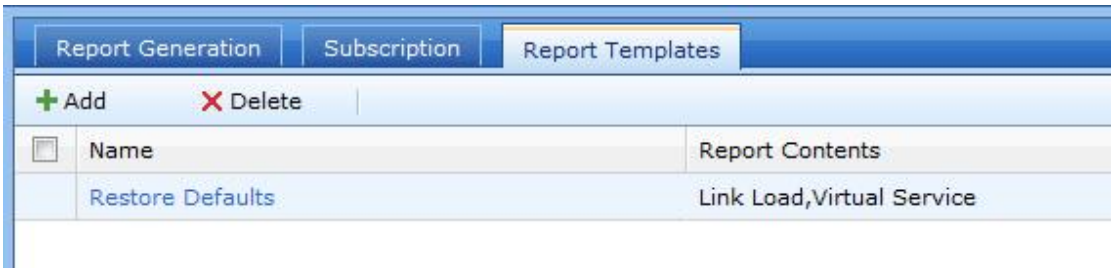
Yearly Subscription: Select **Enable** and specify a report template based on which report will be generated and sent to the specified email address, on yearly basis.

SMTP Server: Select or add a SMTP server to providing email delivery service. To add a SMTP server, click the plus icon and specify the basic information of the server, as shown in the Chapter 10. 4

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

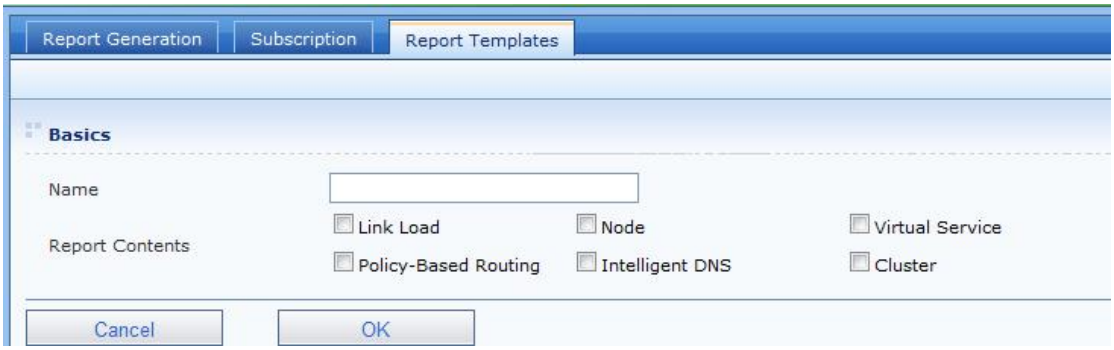
4.1.3 Report Templates

Navigate to **Report** > **Reports** > **Report Templates**, you can configure report template and select the specific contents contained in the report. Report generation and subscription are based on the selected report template.



To remove a template from the list, select the entry and click **Delete**.

To create a new template, click **Add** to enter the following page:

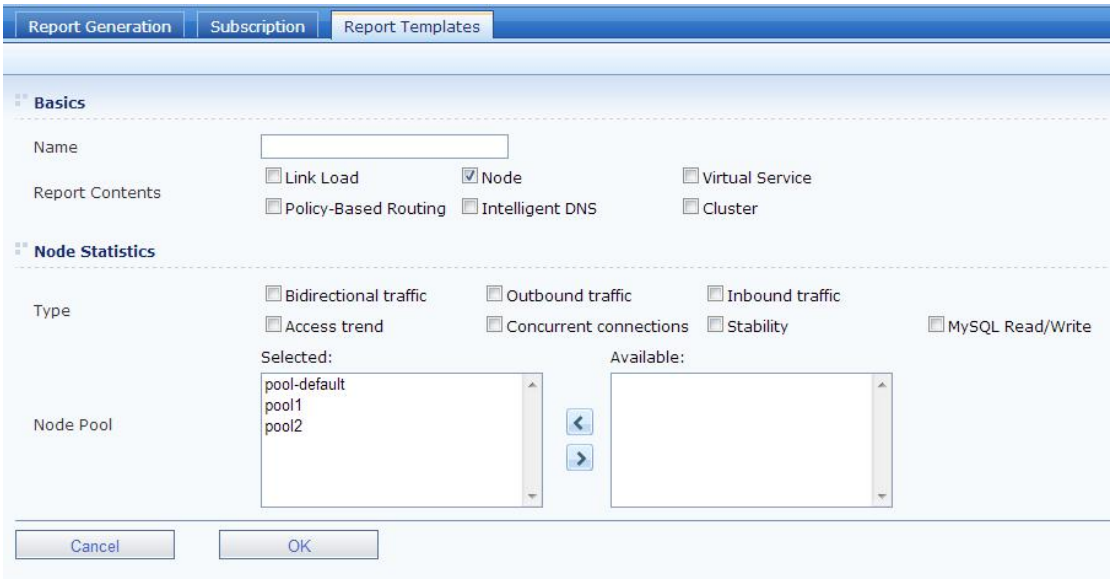


Name: Specifies name of the report template.

Report Contents: Select the contents you want the report contain, link load, node,virtual service policy-based routing intelligent DNS and cluster.

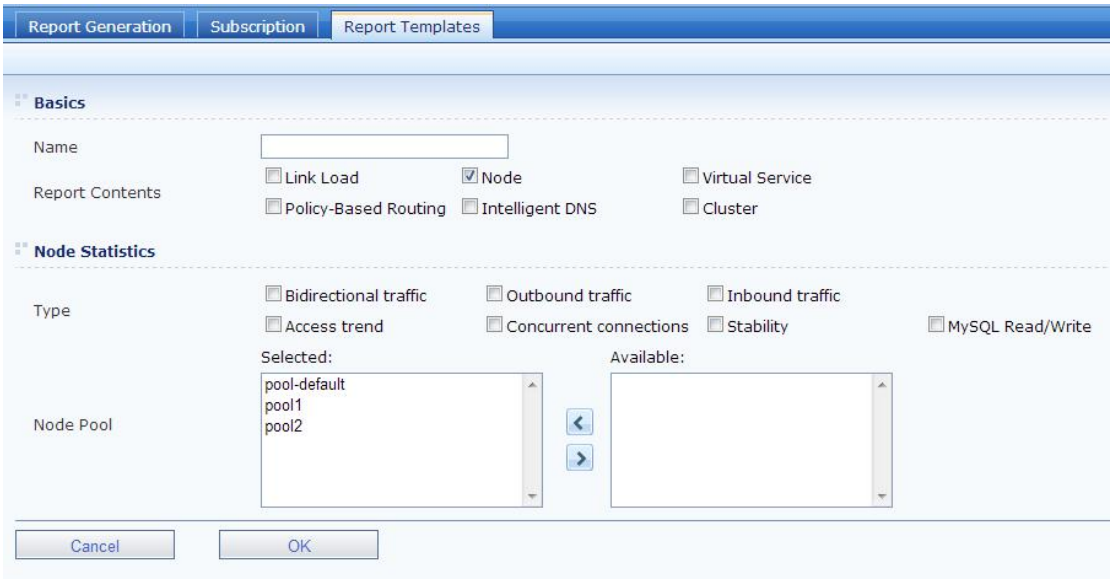
Link Load provides link load statistics of each link. You can specify the following fields to get report and know if specified links are evenly sharing the access requests.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Type: Options are **Bidirectional traffic， Outbound traffic， Inbound traffic, Access trend , Bandwidth utilization and Stability.**

Link: Select the links to have the report provide statistics about them.

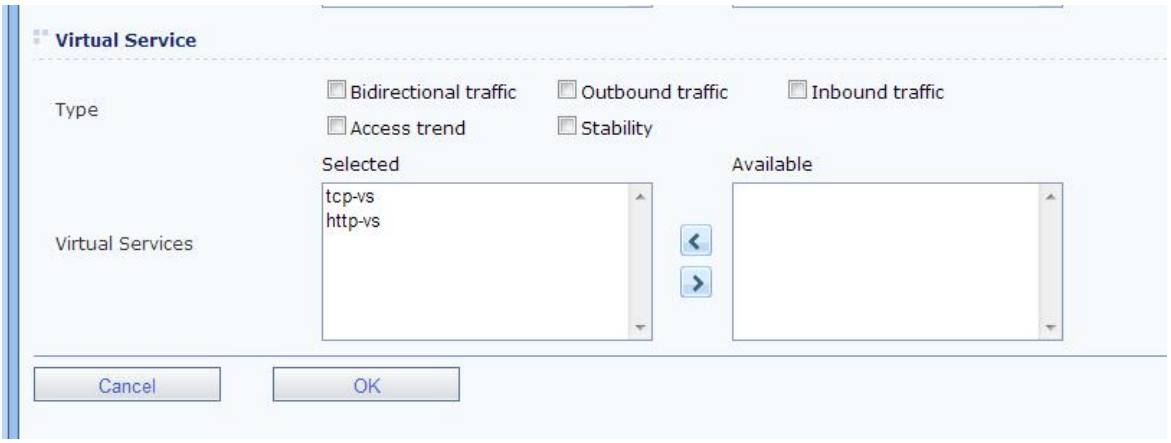


Node provides load statistics of each node You can specify the following fields to get report and know if specified nodes are evenly sharing the access requests.

Type: Options are **Bidirectional traffic, Outbound traffic, Inbound traffic, Access trend, Concurrent Connections, Stability** and **MySQL Read/Write**.
Node Pool: Select the nodes to have the report provide statistics about them.

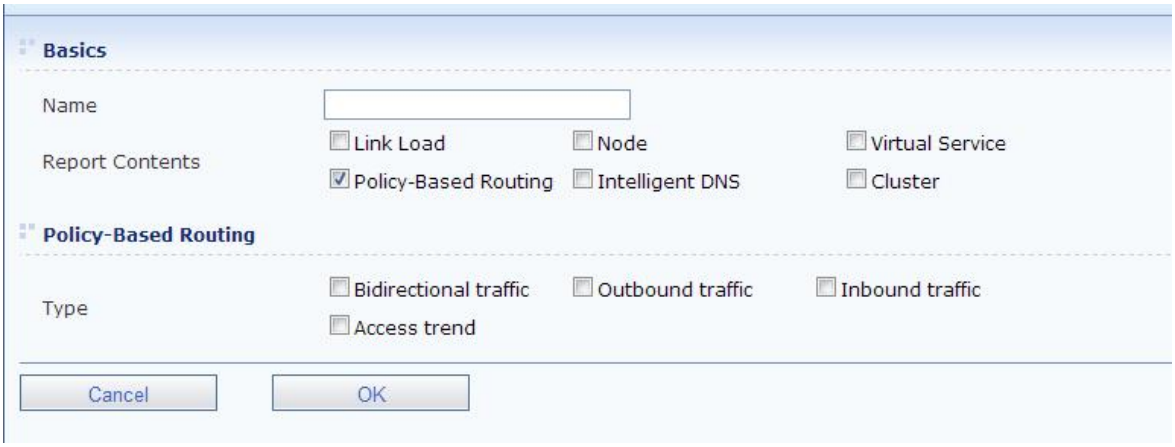
Virtual Services: Select to statistic each virtual service's load situations to judge whether all virtual service's load is balanced, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Type: Options are **Bidirectional traffic, outbound traffic, inbound traffic, Access trend** and **Stability**.
Virtual Services: Select to select the selected data in Virtual Services.

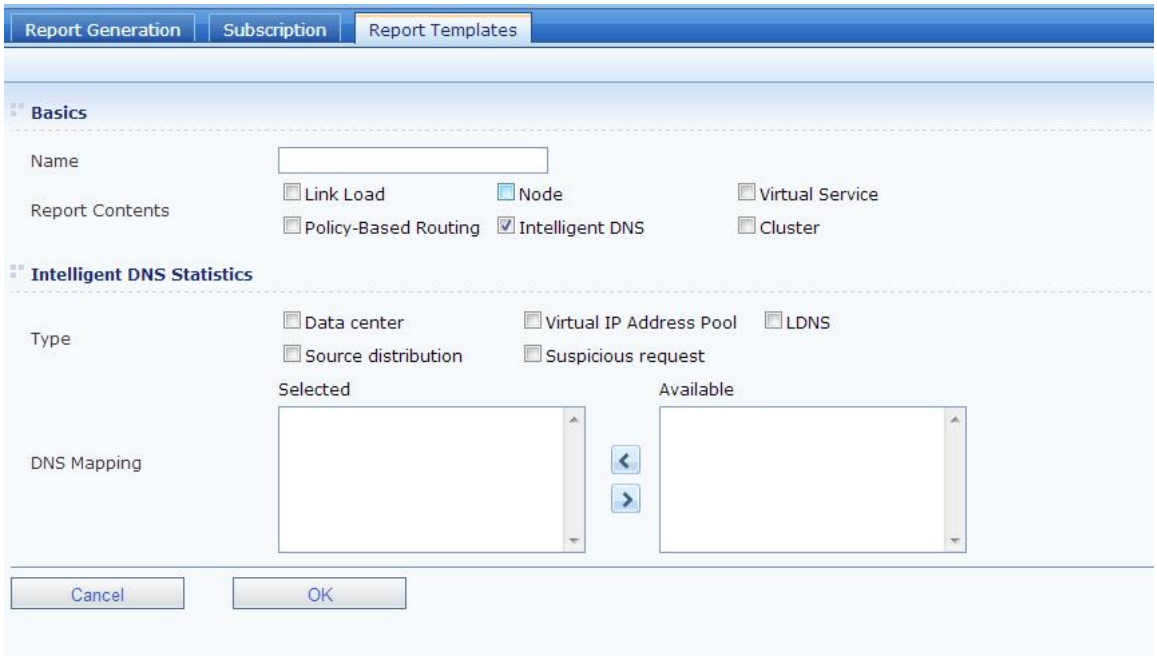
Policy-Based Routing: Select to deploy Policy-Based Routing Type and reports only generate those data in selected type.



Type: Options are Bidirectional traffic, Outbound traffic, Inbound traffic and Access trend.

Intelligent DNS provides statistics about intelligent DNS statistics.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

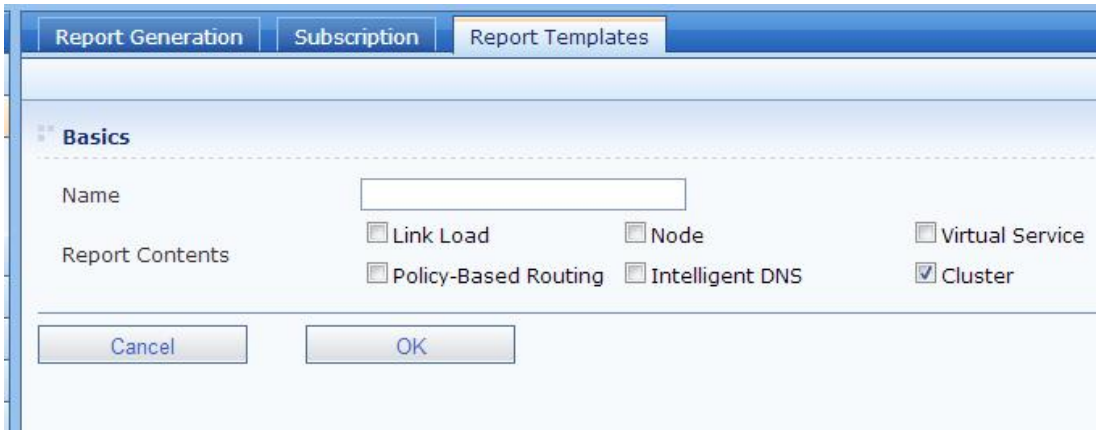


Type: Options are access including data center, virtual IP Address Pool, LDNS, Source distribution and suspicious request.

DNS Mapping: Select the DNS mapping to have the report contain data about the specified DNS mapping, i. e. , the first-level scheduling policy.

Click **OK** to save the settings, or **Cancel** to give up the changes.

Cluster: Select to configure the report whether to generate statistical data reports related with cluster.



4.2 Report Center

4.2.1 Report Center

To log in to report center and view various statistics (**Link Load, Node, Virtual Service,**

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Policy-Based Routing, Intelligent DNS and **Cluster**), go to **Report** > **Report Center**.

You can log in with the current administrator account or with another account, as shown in the following figure:



To enable report center and be able to log in to report center, select **Enabled**.

To log in to the report center with the current administrator account, click the **With the Current Account** button.

To log in to the report center with another account, click the **With Another Account** button, and you will enter the following page:



Type the username and password and click **Log In**.

4.2.2 Report Cleanup

To have report data removed automatically, go to **Report Cleanup** and specify the cleanup options.



The following are the contents contained on the **Report Cleanup** tab:

Response Time: Specifies the timeout for looking up data from sites.

Disk Usage Threshold: Specifies the upper limit of disk usage by report center.

Days Logs Will Be Kept: Specifies how many days the report data will be preserved. If disk usage reaches the threshold, data preserved for more than that will be removed.

OK: Click this button to save the settings on this tab.

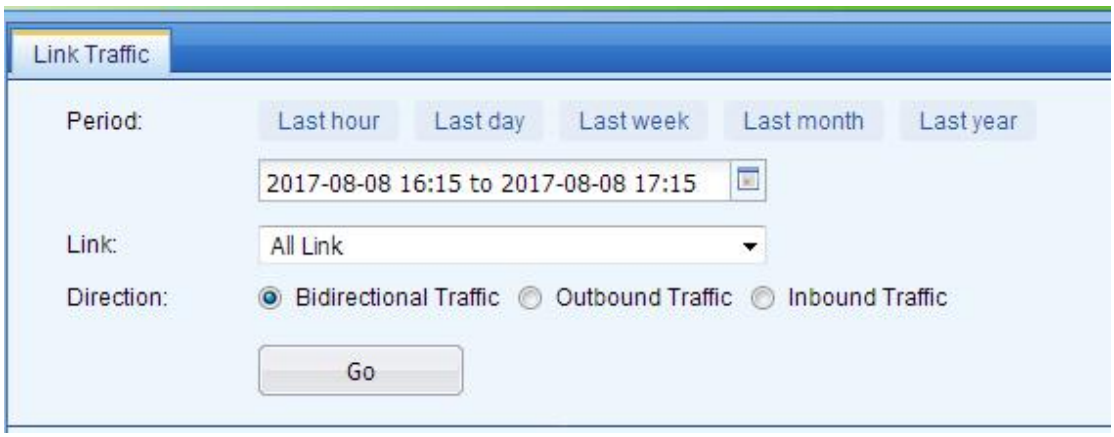
4.3 Report Center

4.3.1 Link Statistics

Link Traffic provides link statistics of each link. Specific contents are Link **Traffic**, **Access Trend**, **Bandwidth Utilization** and **Stability**.

Link Traffic indicates the traffic flowing through the ADC

1. Navigate to **Link Statistics** > **Link Traffic** as shown in the following figure:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Period: Click any of the buttons to view time type, **Last hour**, **Last day**, **Last week**, **Last month**, or **Last year** and specify the start and end date/time of the time range.

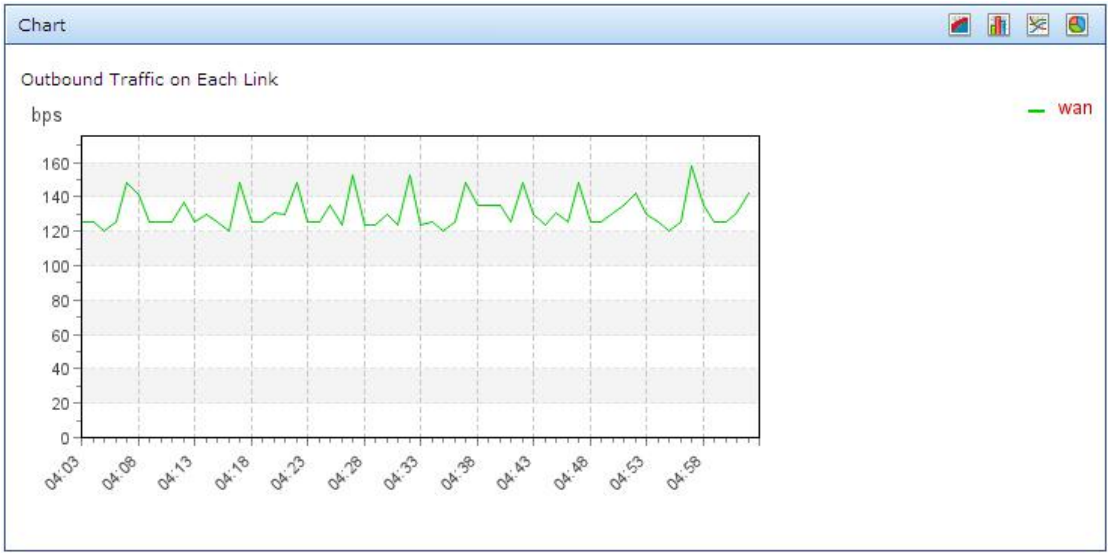
Link: Select all links or certain WAN link.

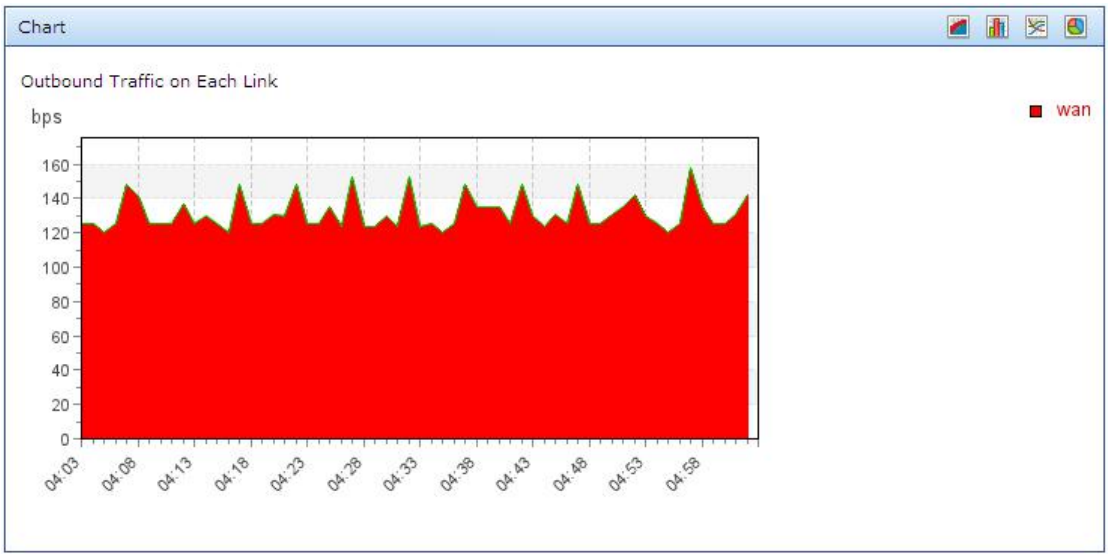
Direction: Specifies the traffic type, **Bidirectional Traffic**, **Outbound Traffic** or **Inbound Traffic**.

Go: Click the button to inquiry and generate results.

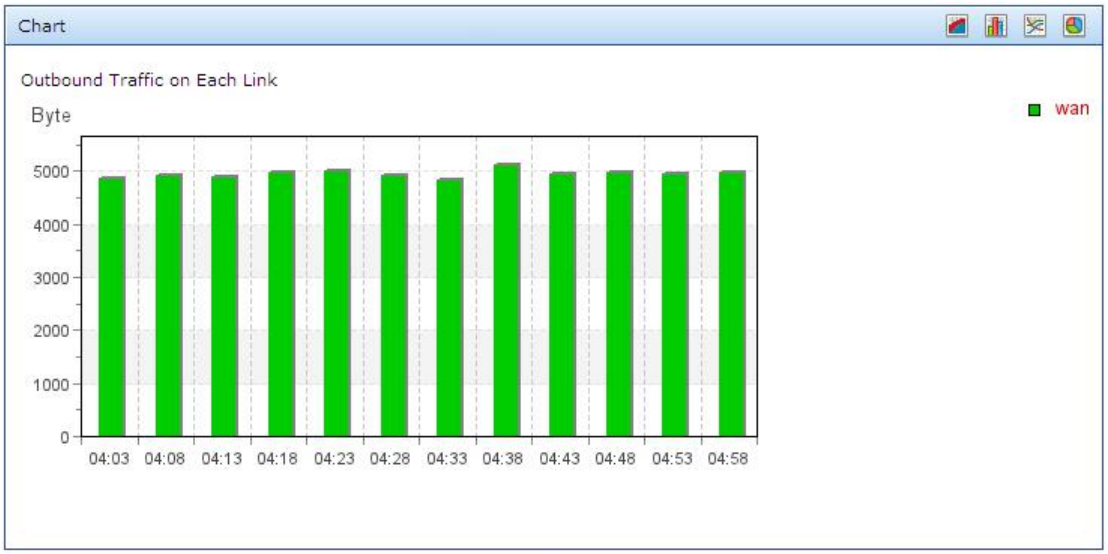
Export: Click the button to export and calculate out traffic chart based on the above criterial then save the statistics as PDF file.

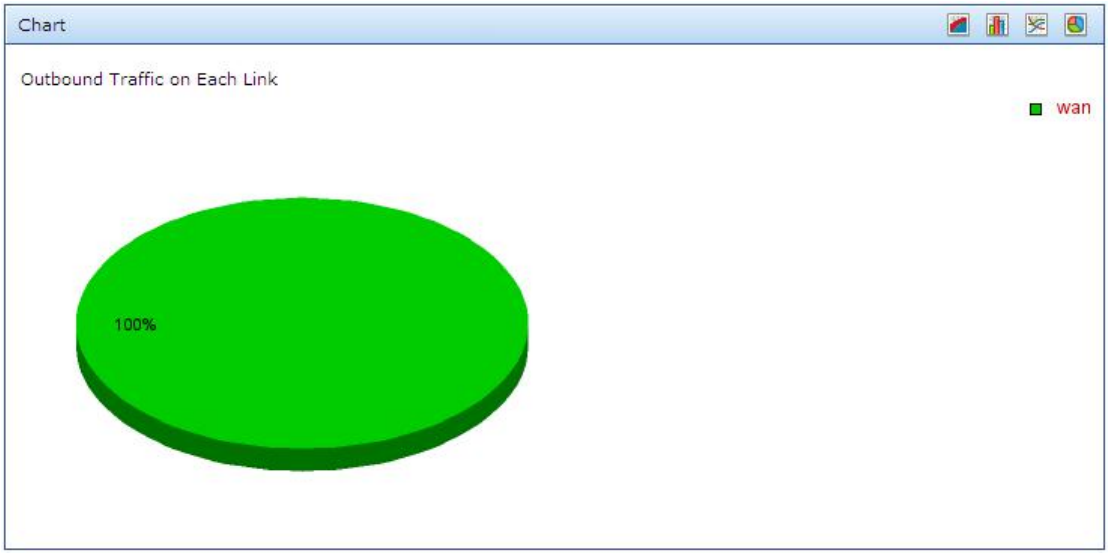
The following are the four types of charts presenting requested data, line chart, area chart, bar chart and pie chart respectively.





Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Table

Outbound Traffic on Each Link Byte, Time Unit(Minute)

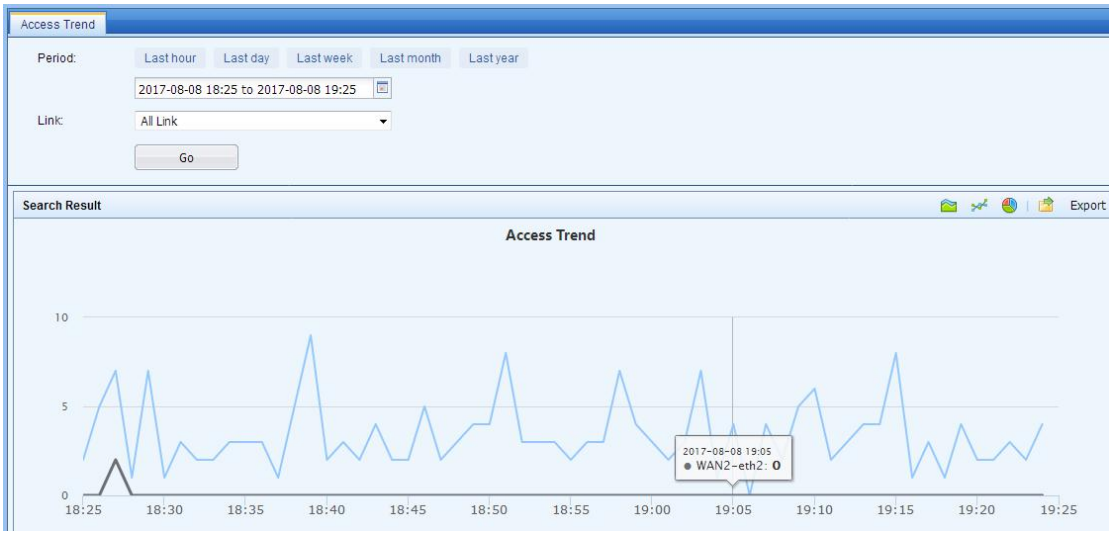
Time	wan	Total
04:03	4828	4828
04:08	4902	4902
04:13	4860	4860
04:18	4944	4944
04:23	4966	4966
04:28	4904	4904
04:33	4818	4818
04:38	5092	5092
04:43	4934	4934
04:48	4944	4944
04:53	4934	4934
04:58	4944	4944
Total	59070	59070

Access Trend

Access Trend indicates the number of accesses.

Below we take total traffic for example, to introduce how to get desired traffic statistics. Data query method is the same with other type of data.

Navigate to **Link Statistics** > **Access Trend**, as shown in the following figure:



Period: Click any of the buttons to view time type, **Last hour**, **Last day**, **Last week**, **Last month**, or **Last year** and specify the start and end date/time of the time range.

Link: Select all links or certain WAN link.

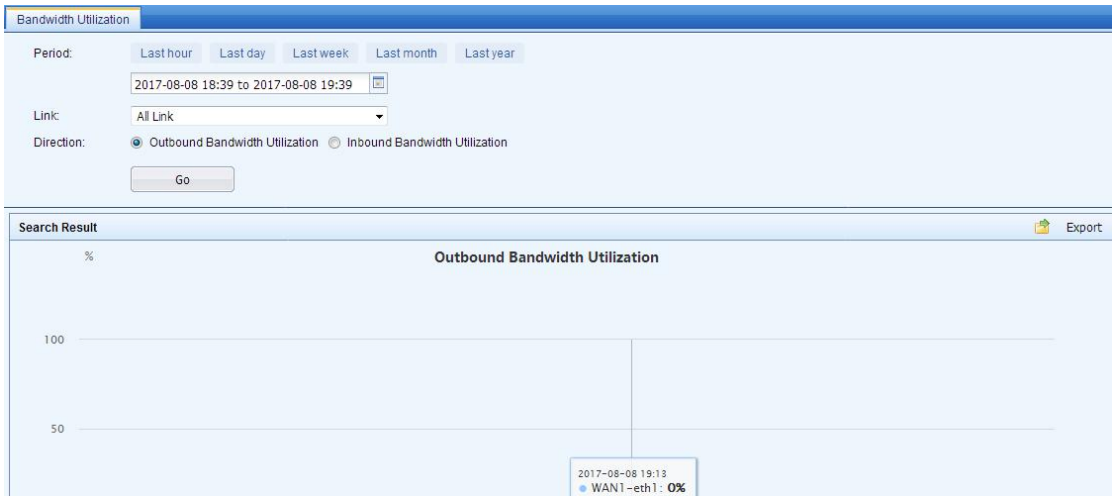
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Go: Click the button to inquiry and generate results.

Export: Click the button to export and calculate out access trend chart based on the above criterial then save the statistics as PDF file

Bandwidth Utilization

Bandwidth utilization is used to statistic bandwidth usage in links.

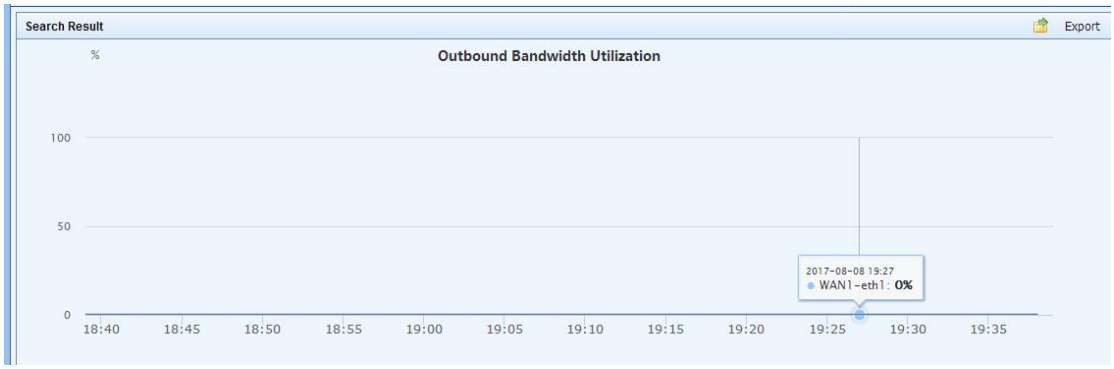


Period: Click any of the buttons to view time type, **Last hour**, **Last day**, **Last week**, **Last month** or **Last year** and specify the start and end date/time of the time range.

Link: Select all links or certain WAN link.

Direction: Specifies traffic direction, **Outbound Bandwidth Utilization** or **Inbound Bandwidth Utilization.**

Go: Click the button to inquiry and generate bandwidth utilization chart.

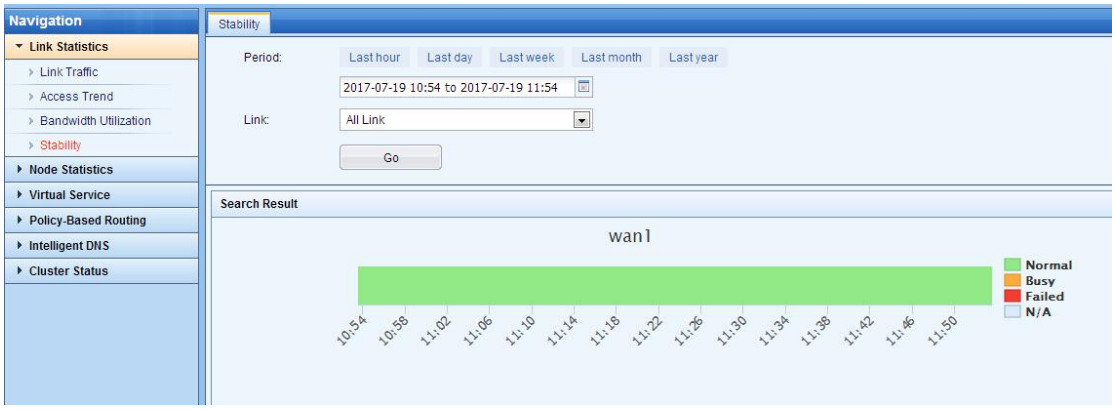


Export: Click the button to export and calculate out traffic chart based on the above criterial then save the statistics as PDF file.

Stability

Stability is used to statistic the stability of links, as shown in the following figure:

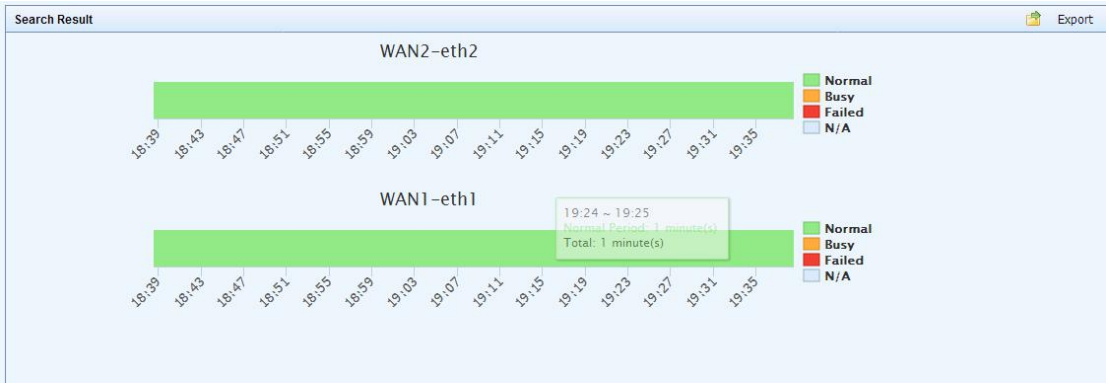
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

Link: Select all links or certain WAN link.

Go: Click the button to inquiry and generate link status chart.



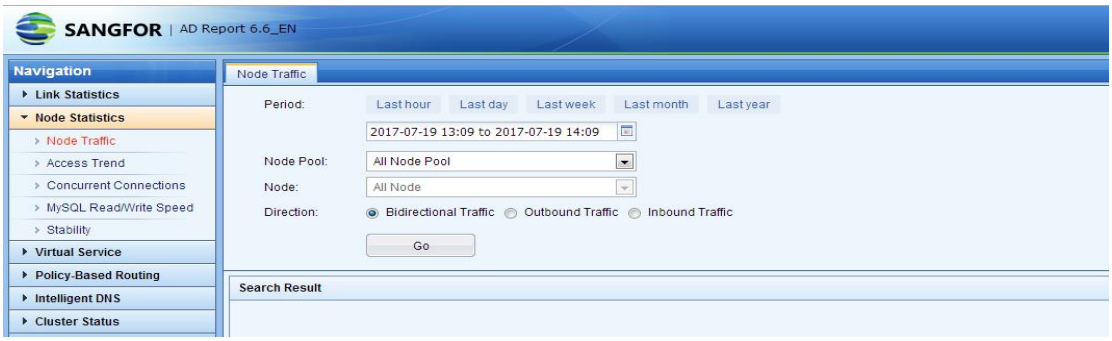
Go: Click the button to export and statistic status based on the above criterial then save the statistics as PDF file.

Export: Click the button to export and calculate out traffic chart based on the above criterial then save the statistics as PDF file.

4.3.2 Node Statistics

Node Traffic is used to statistic traffic information on specific node pool and node, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



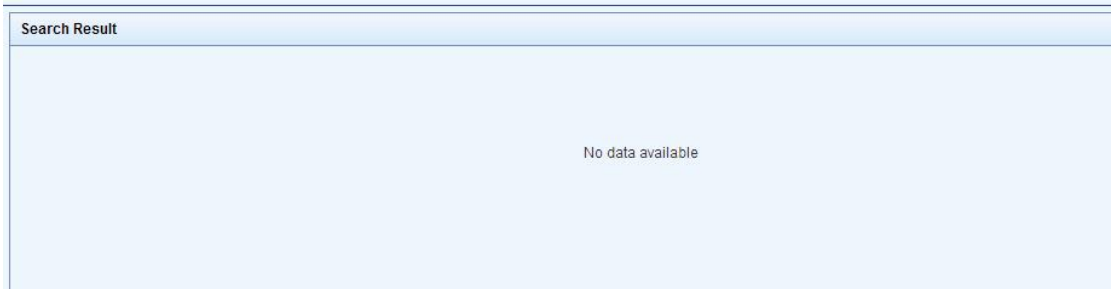
Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

Node Pool: Specify a specific node pool.

Node: Specify a specify node.

Direction: Click to specify the direction to statistic, including **Bidirectional Traffic, Outbound Traffi**c and **Inbound Traffic**.

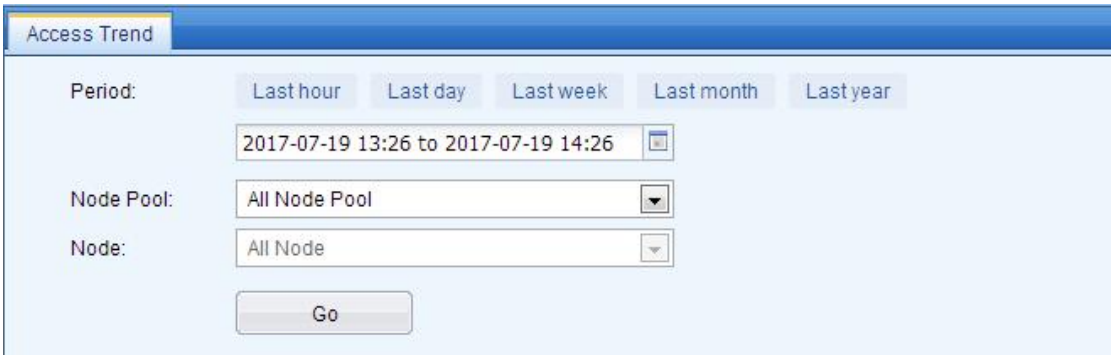
Go: Click the button to inquiry and generate results.



Export: Click the button to export the node traffic chart based on the above criterial then save the statistics as PDF file.

Access Trend

Access Trend is used to statistic access trend of specific node pool and node, as shown in the following figure:



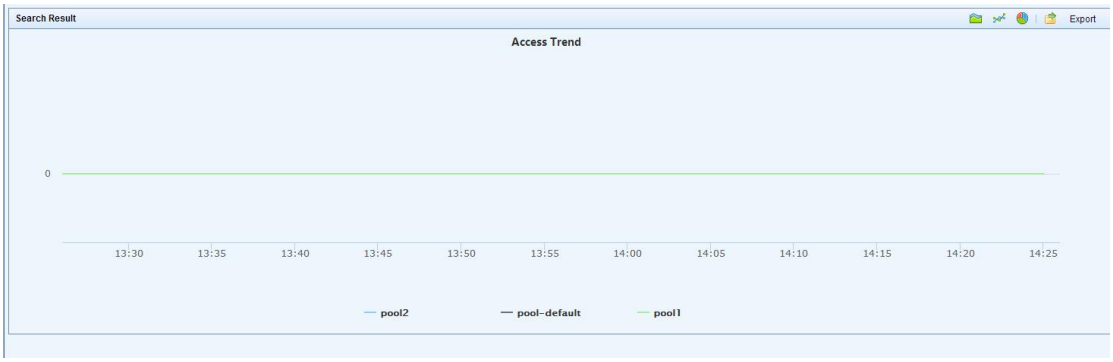
Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and.specify the start and end date/time of the time range.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Node Pool: Specify a specific node pool.

Node: Specify a specific node.

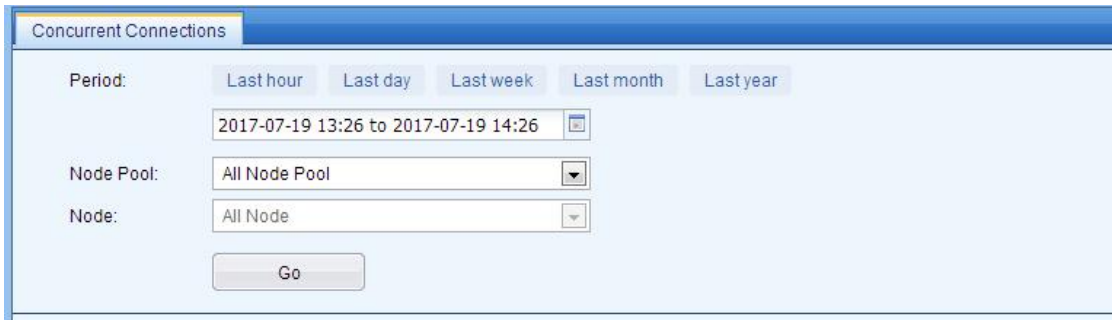
Go: Click the button to inquiry and generate results.



Export: Click the button to export the traffic access trend chart based on the above criterial then save the statistics as PDF file.

Concurrent Connections

Concurrent Connections is used to statistic concurrent connections of specific node pool and node, as shown in the following figure:



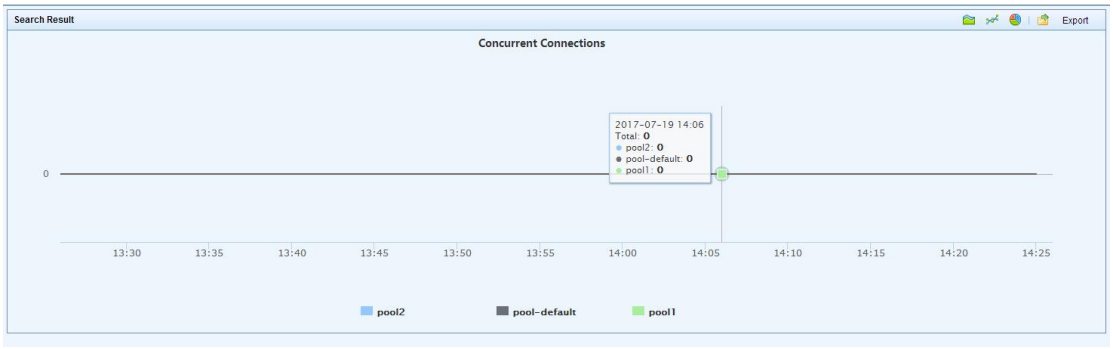
Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and.specify the start and end date/time of the time range.

Node Pool: Specify a specific node pool.

Node: Specify a specific node.

Go: Click the button to inquiry and generate results.

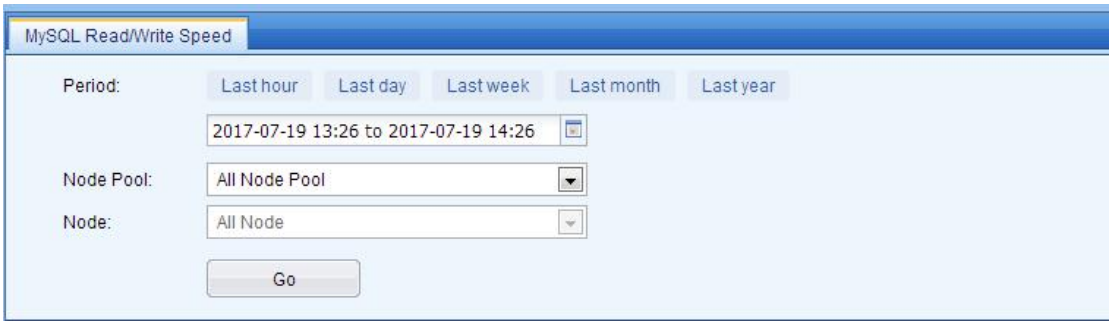
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Export: Click the button to export the concurrent connections chart based on the above criterial then save the statistics as PDF file.

MySQL Read/Write Speed

MySQL Read/Write Speed is used to statistic MySQL Read/Write Speed of specific node pool and node, as shown in the following figure:

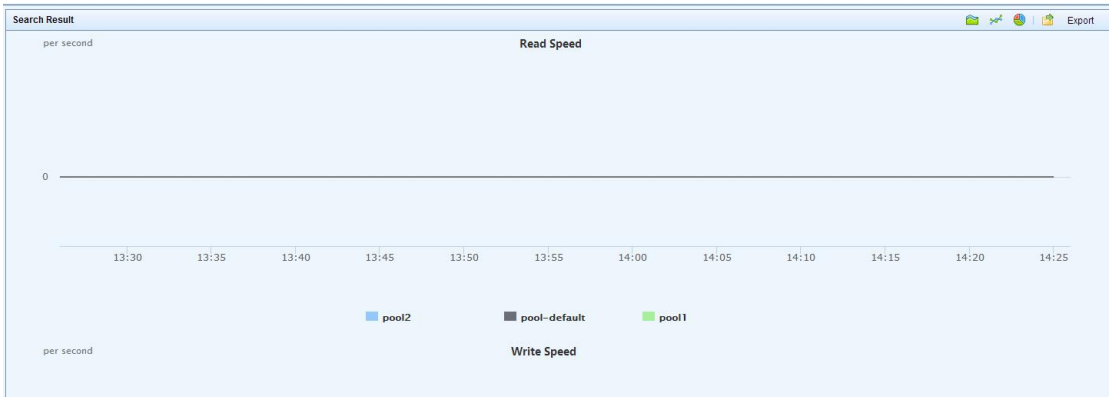


Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and.specify the start and end date/time of the time range.

Node Pool: Specify a specific node pool.

Node: Specify a specific node.

Go: Click the button to inquiry and generate results.

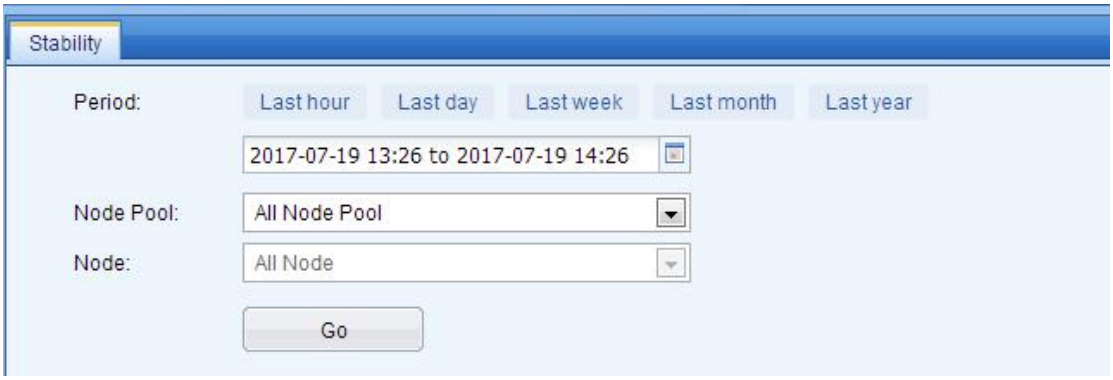


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Export: Click the button to export the MySQL Read/Write Speed chart based on the above criterial then save the statistics as PDF file.

Stability

Stability is used to statistic stability of specific node pool and node, as shown in the following figure:

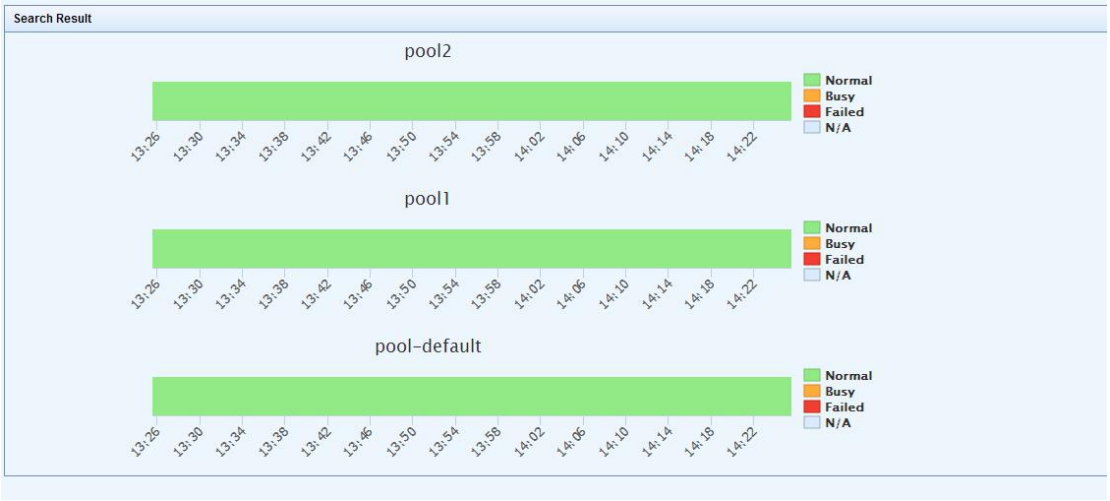


Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and.specify the start and end date/time of the time range.

Node Pool: Specify a specific node pool.

Node: Specify a specific node.

Go: Click the button to inquiry and generate results.



Export: Click the button to export node pool/node status chart based on the above criterial then save the statistics as PDF file.

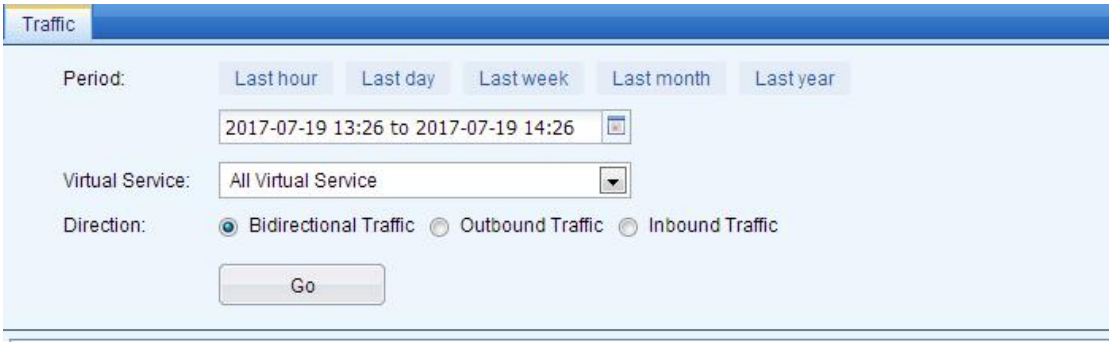
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

4.3.3 Virtual Service

Virtual Service is used to statistic virtual service, including **Traffic, Access Trend, URL Traffic** and **Stability**.

Traffic

Traffic is used to statistic traffic of virtual service, as shown in the following figure:

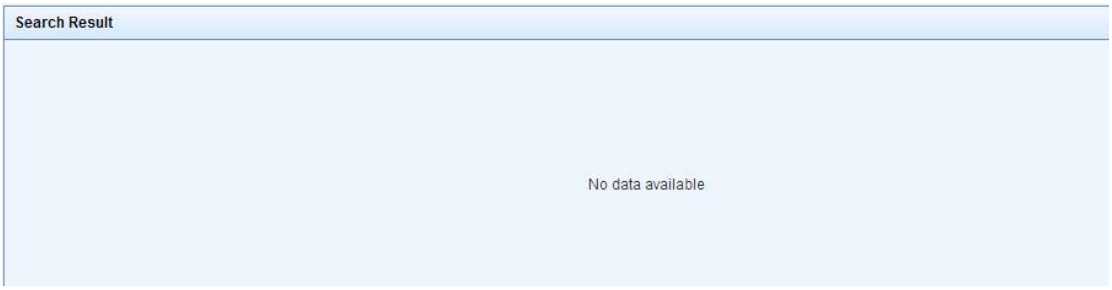


Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and.specify the start and end date/time of the time range.

Virtual Service: Select a virtual service to view the traffic statistics.

Direction: Specifies the traffic type, **Bidirectional Traffic**, **Outbound Traffic** and **Inbound Traffic**.

Go: Click the button to inquiry and generate results.

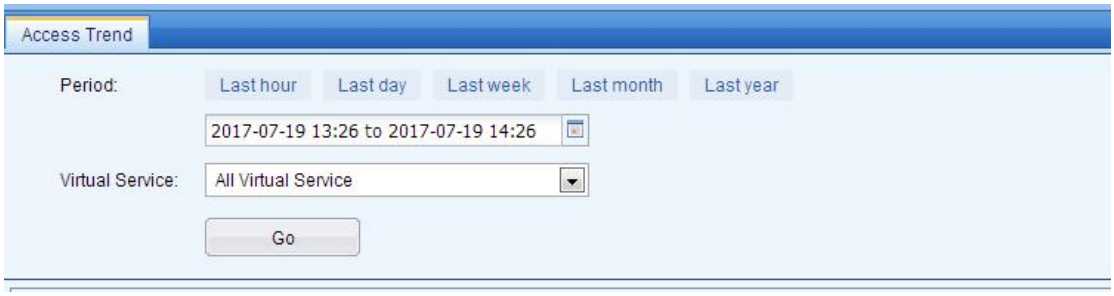


Export: Click the button to export flow chart based on the above criterial then save the statistics as PDF file.

Access Trend

Access Trend is used to statistic total access count of virtual service, as shown in the following figure:

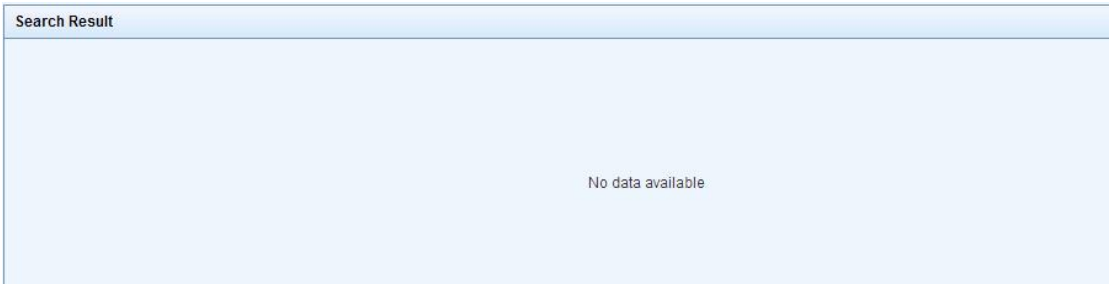
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and.specify the start and end date/time of the time range.

Virtual Service: Select a virtual service to view the access trend statistics.

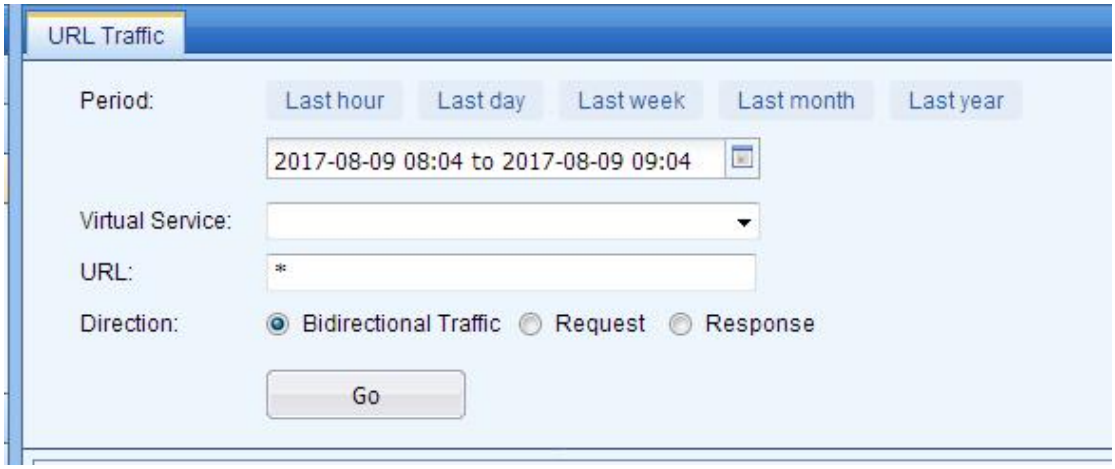
Go: Click the button to inquiry and generate results.



Export: Click the button to export access trend chart based on the above criterial then save the statistics as PDF file.

URL Traffic

URL Traffic is used to statistic URL traffic of virtual service, as shown in the following figure:



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and.specify the start and end date/time of the time range.

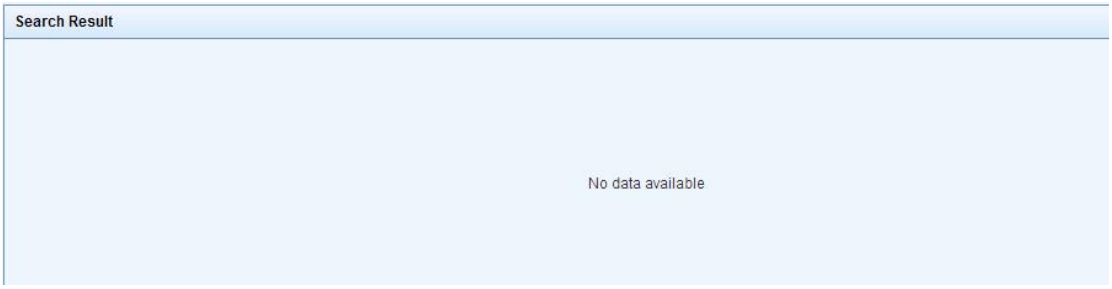
Virtual Service: Select a virtual service to view the URL traffic statistics.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

URL: Specifies the URL required to match, and statistics are filled in with "*".

Direction: Select the traffic type, **Bidirectional Traffic**, **Request** and **Response**.

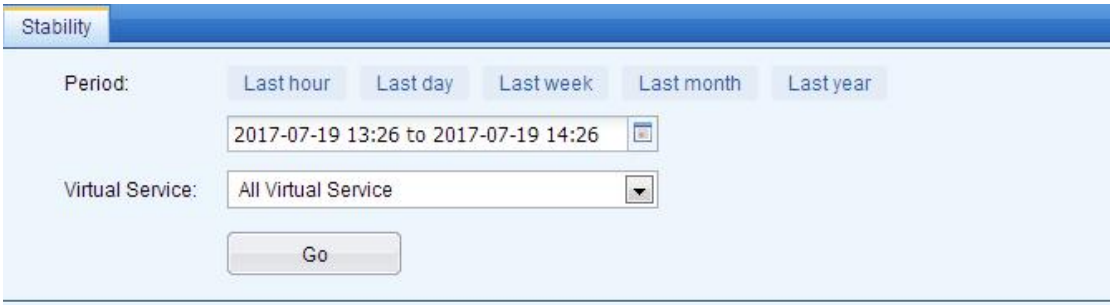
Go: Click the button to inquiry and generate results.



Export: Click the button to export URL traffic chart based on the above criterial then save the statistics as PDF file.

Stability

Stability is used to statistic stability of virtual service, as shown in the following figure:



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and.specify the start and end date/time of the time range.

Virtual Service: Select a virtual service to view the stability statistics.

Go: Click the button to inquiry and generate results.

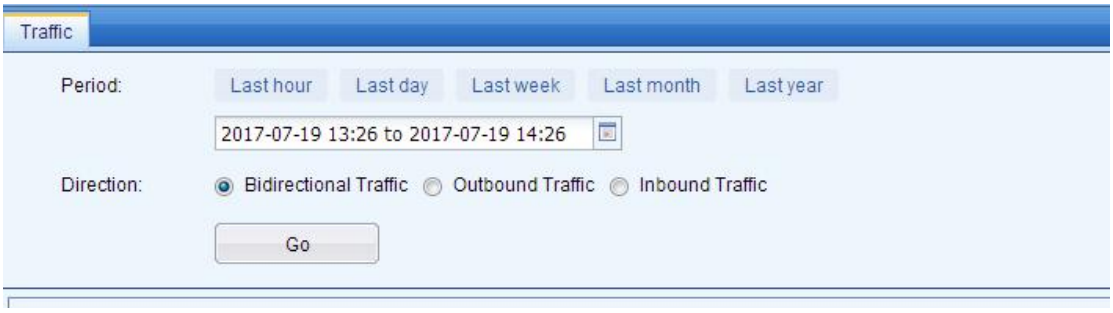
Export: Click the button to export stability chart based on the above criterial then save the statistics as PDF file.

4.3.4 Policy-Based Routing

Policy-Based Routing is mainly used to statistic policy-based routing, including Traffic and Access Trend.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

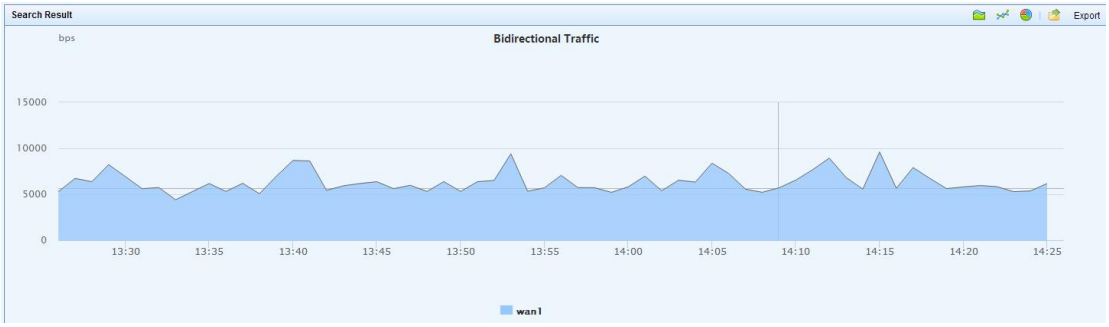
Traffic is used to statistic traffic information flow through ADC, as shown in the following figure:



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and.specify the start and end date/time of the time range.

Direction: Select the traffic type, **Bidirectional Traffic, Outbound Traffic** and **Inbound Traffic**.

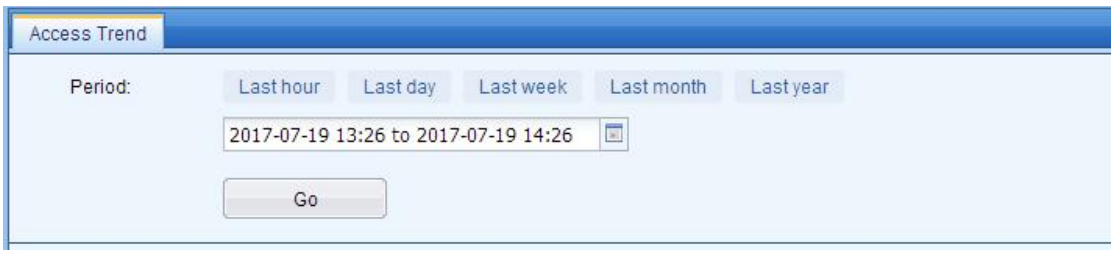
Go: Click the button to inquiry and generate results.



Export: Click the button to export flow chart based on the above criterial then save the statistics as PDF file.

Access Trend

Access Trend is used to statistic access trend, as shown in the following figure:



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last**

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

month or **Last year** and.specify the start and end date/time of the time range.

Go: Click the button to inquiry and generate results.



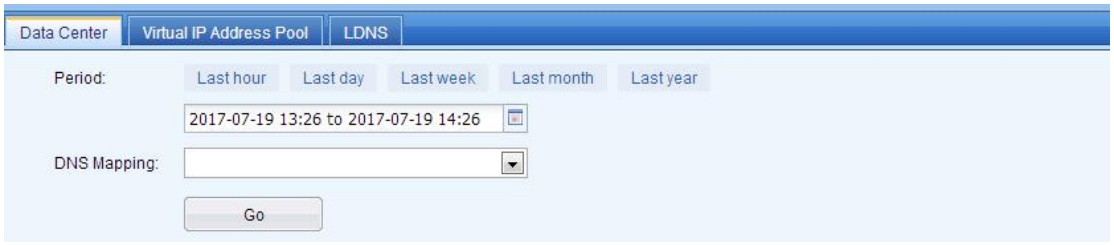
Export: Click the button to export access trend chart based on the above criterial then save the statistics as PDF file.

4.3.5 Intelligent DNS

Intelligent DNS includes **Access Trend, LDNS Source Distribution** and **Error Queries**.

Access Trend of Data Center

It provides number of accesses to DNS mappings based on data center, as shown in the following figure:



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

DNS Mapping: Click to set DNS mapping for statistic.

Go: Click the button to inquiry and generate results.

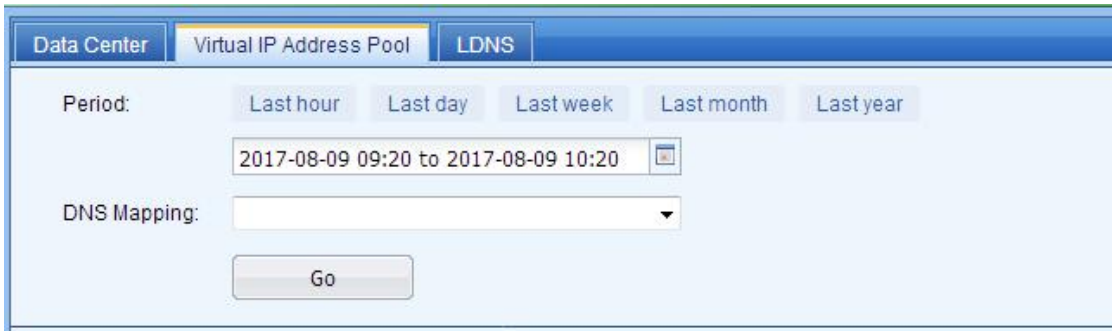
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Export: Click the button to export chart based on the above criterial then save the statistics as PDF file.

Access Trend of Virtual IP Address Pool

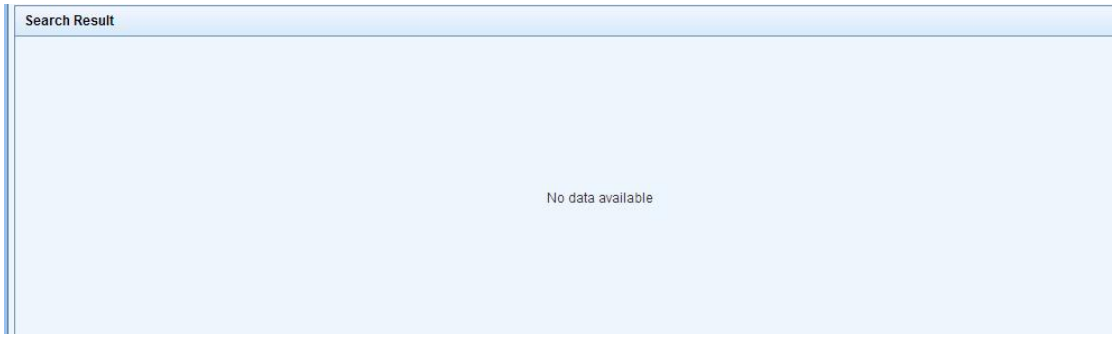
It provides number of accesses to DNS mappings based on global virtual IP pool, as shown in the following figure:



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

DNS mapping: Click to set DNS mapping for statistic.

Go: Click the button to inquiry and generate results.

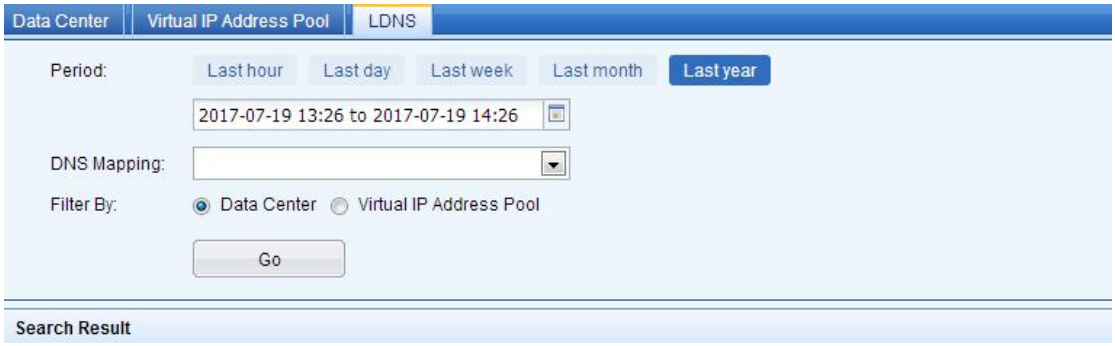


Export: Click the button to export chart based on the above criterial then save the statistics as PDF file.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

LDNS

LDNS is used to statistic number of accesses to LDNS based on data center or virtual IP address pool, as shown in the following figure:

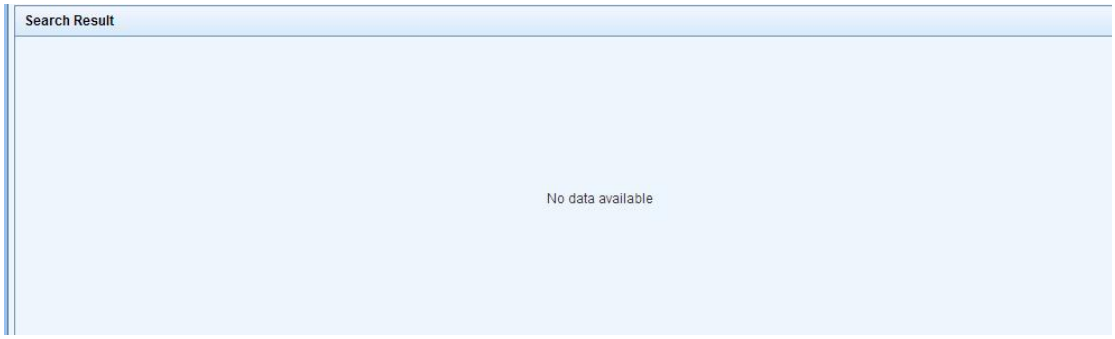


Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

DNS Mapping: Click to set DNS mapping for statistic.

Filter By: Select **Data Center** or **Virtual IP Address Pool**.

Go: Click the button to inquiry and generate results.

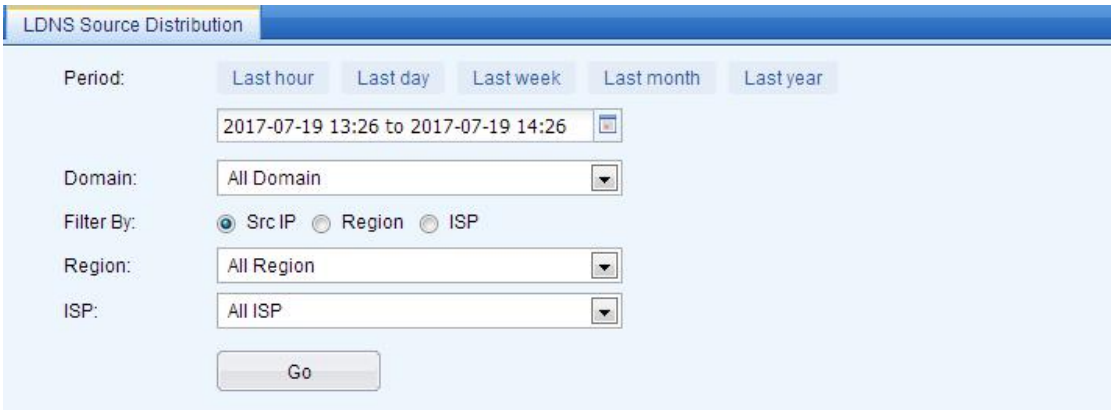


Export: Click the button to export chart based on the above criterial then save the statistics as PDF file.

LDNS Source Distribution

LDNS Source Distribution is used to statistic number of accesses to LDNS mapping based on domain, Region, ISP and address type, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

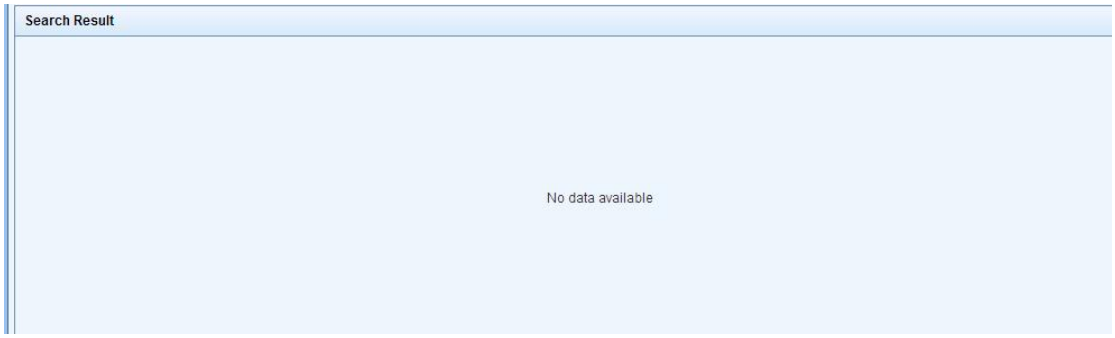
Domain: Click to select domain.

Filter By: Click to select **Src IP, Region** or **ISP**.

Region: Click to select region.

ISP: Click to select ISP.

Go: Click the button to inquiry and generate results.

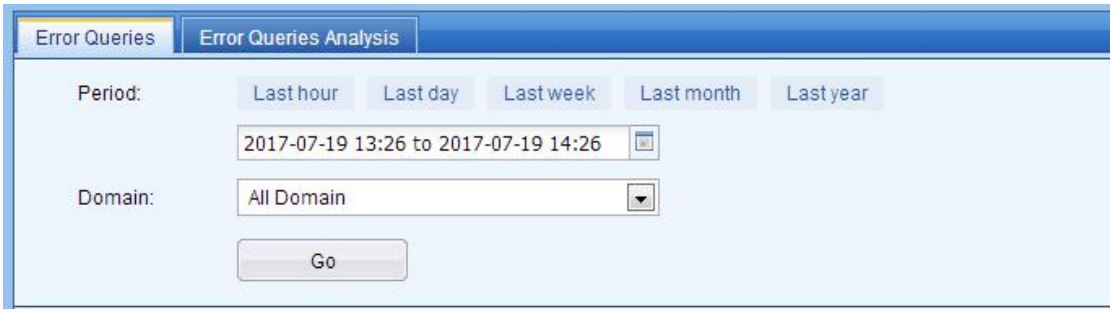


Export: Click the button to export chart based on the above criterial then save the statistics as PDF file.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Error Queries

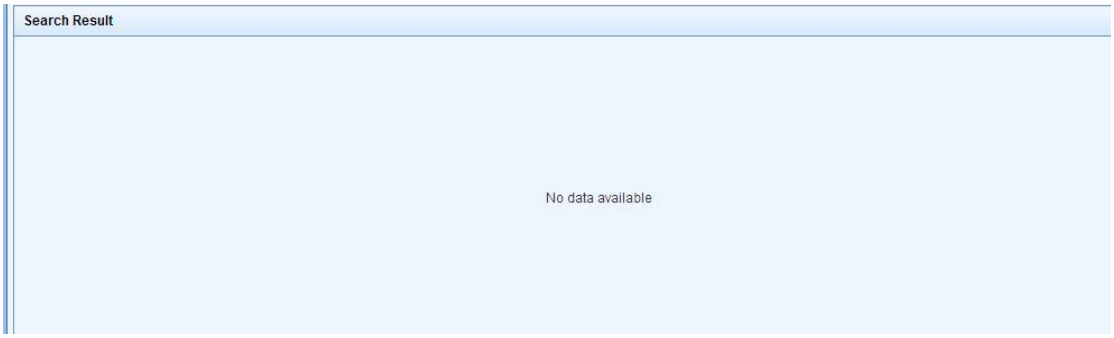
Error Queries: It is used to statistic DNS failure counts and failures, as shown in the following figure:



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

Domain Name: Click to select domain

Go: Click the button to inquiry and generate results

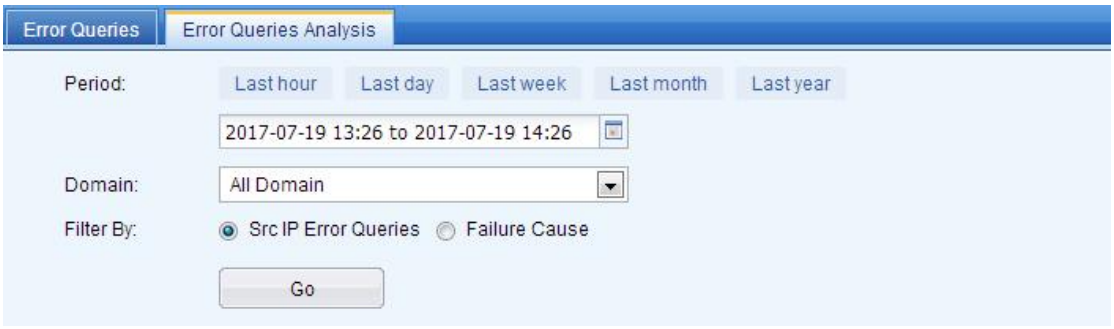


Export: Click the button to export chart based on the above criterial then save the statistics as PDF file.

Error Queries Analysis

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Error Queries Analysis: It is used to analyze DNS failures based on **Src IP Error Queries** and **Failure Cause**, as shown below:

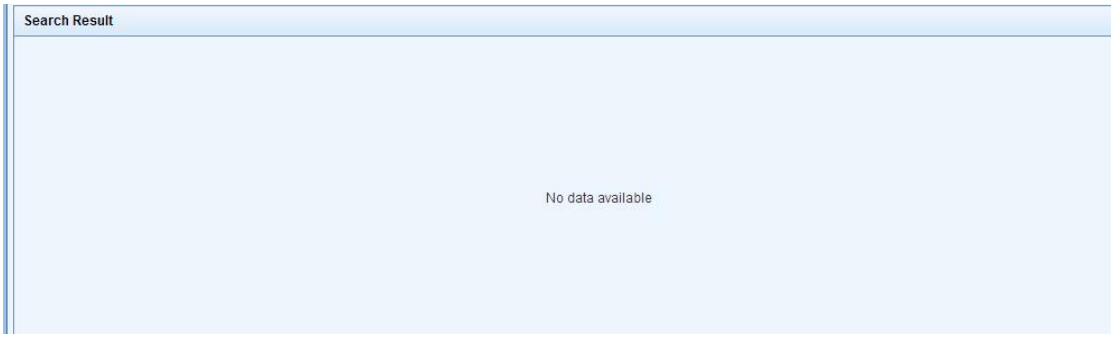


Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

Domain: Click to select domain

Filter By: Click to select **Src IP Error Queries** and **Failure Cause**

Go: Click the button to inquiry and generate results



Export: Click the button to export chart based on the above criterial then save the statistics as PDF file.

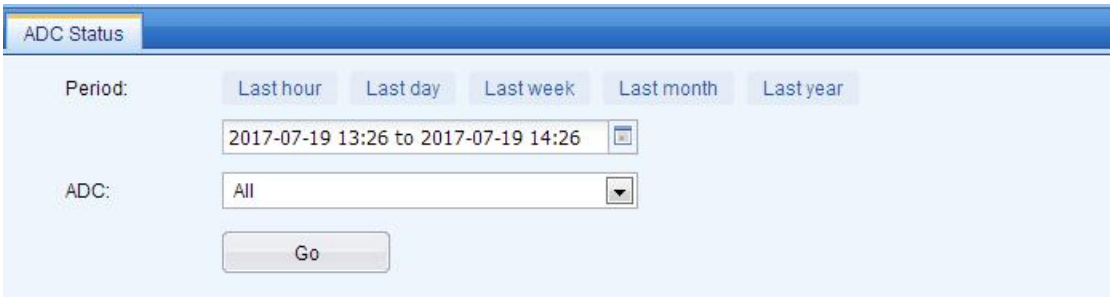
4.3.6 Cluster Status

Cluster Status includes **ADC Status, ADC Active Duration** and **Traffic Group Active Duration**.

ADC Status

ADC Status displays status of ADC during different periods of time, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

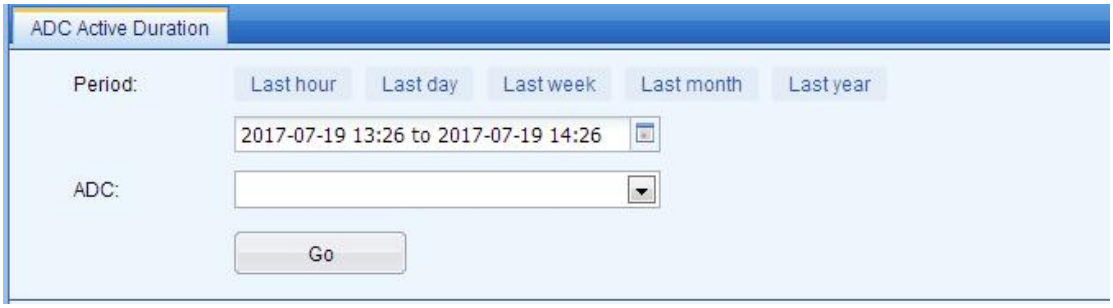
ADC: Click to select the device

Go: Click the button to inquiry and generate results

Export: Click the button to export chart based on the above criterial then save the statistics as PDF file.

ADC Active Duration

ADC Active Duration shows ADC status during different periods of time, as shown below:



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

ADC: Click to select device

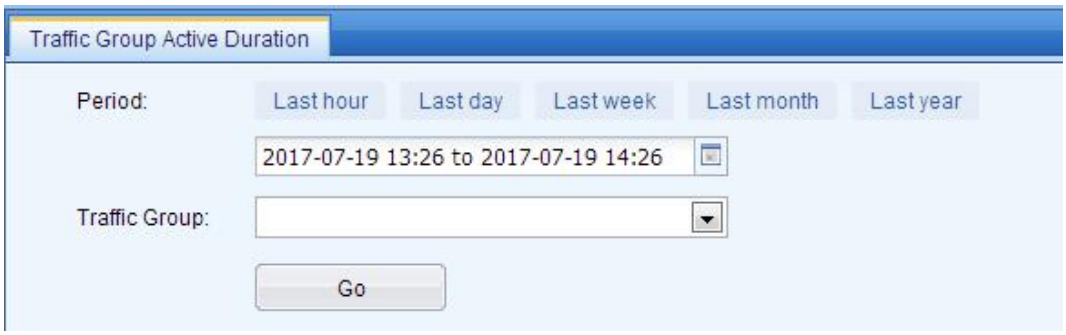
Go: Click the button to inquiry and generate results

Export: Click the button to export chart based on the above criterial then save the statistics as PDF file.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Traffic Group Active Duration

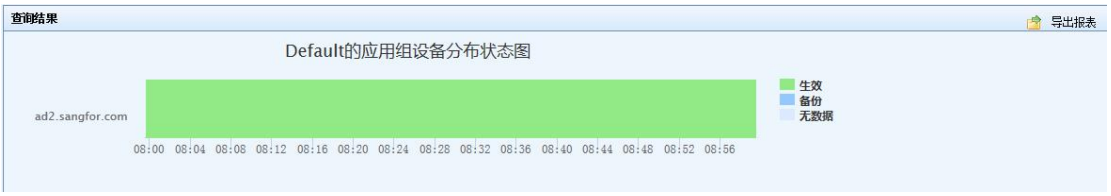
Traffic Group Active Duration shows status of traffic group during different periods of time:



Period: Click any of the buttons to view time type, **Last hour, Last day, Last week, Last month** or **Last year** and specify the start and end date/time of the time range.

Traffic Group: Click to select traffic group

Go: Click the button to inquiry and generate results



Export: Click the button to export chart based on the above criterial then save the statistics as PDF file.

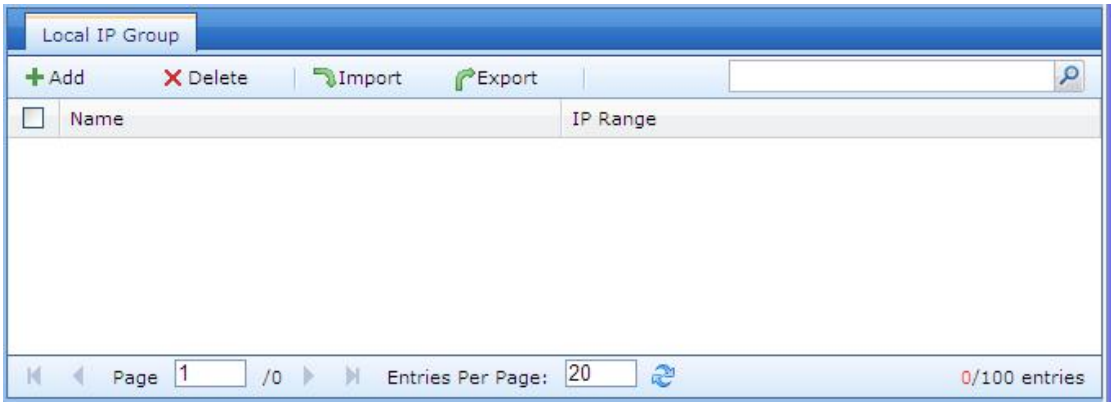
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 5 Objects

The objects are referenced by link and server load balance settings, including Local IP group, IP group, schedule and custom web page.

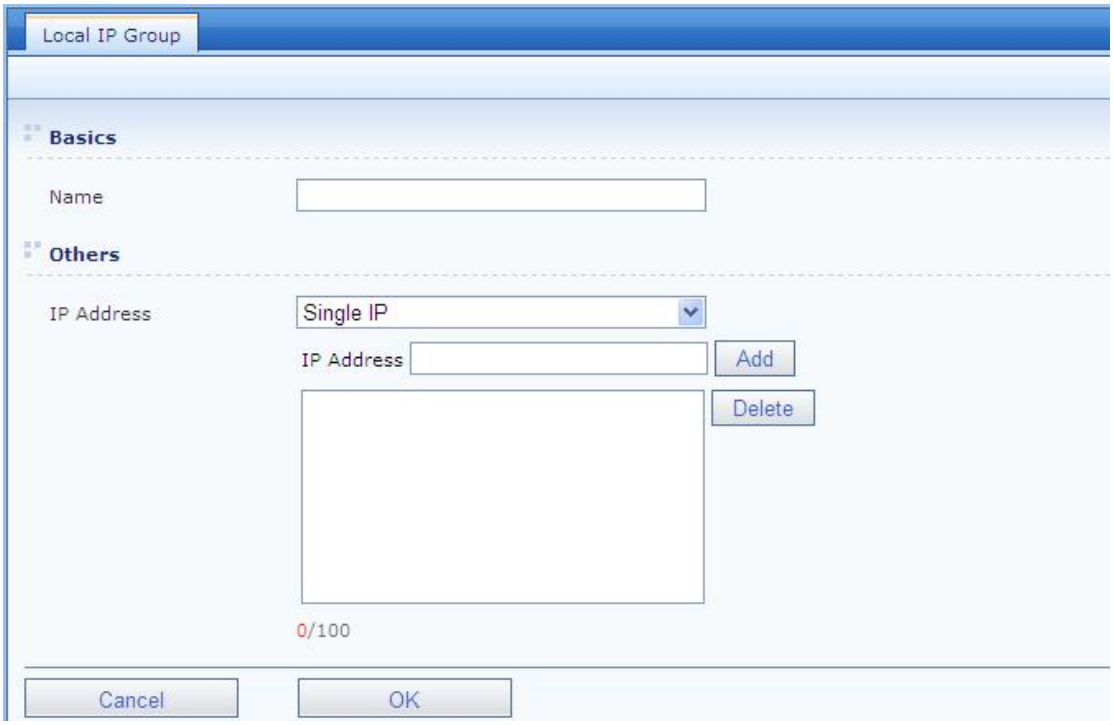
5.1 Local IP Group

A local IP group is a collection of IP addresses on internal network and referenced in policy-based routing settings. To view and configure local IP group, navigate to **Objects** > **Local IP Group**.



To remove a local IP group, select the IP group and click **Delete**.

To add a new local IP group, click **Add**.



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

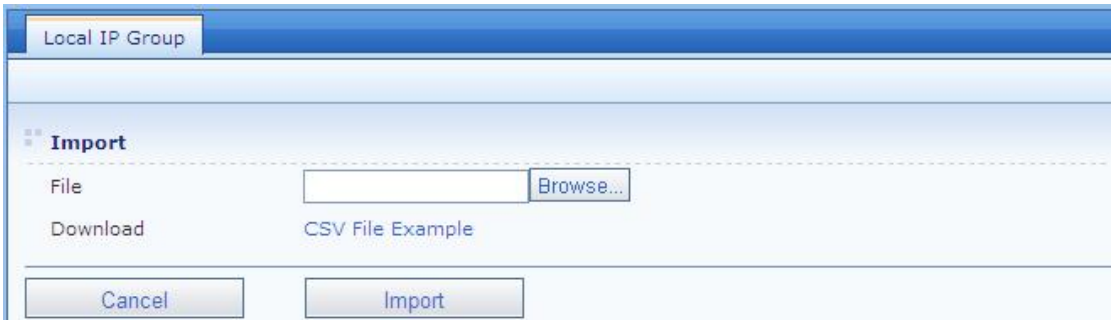
The following are the properties of a local IP group:

Name: Give the local IP group a distinguishable name.

IP Address: Specifies the IP address or range of the IP group. Either IPv4 or IPv6 address support. Mix of IPv4 and IPv6 addresses is not allowed). Type the IP address(range) and click **Add** to add it to the address list. To remove an entry, select the entry and click **Delete**.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

To import local IP groups in csv file, click **Import** to enter the following page:



Click **Browse**, select the csv file and click **Import**. In the CSV file example file, there are IP group examples, you can download the file and upload it again after changing the IP groups into required format.

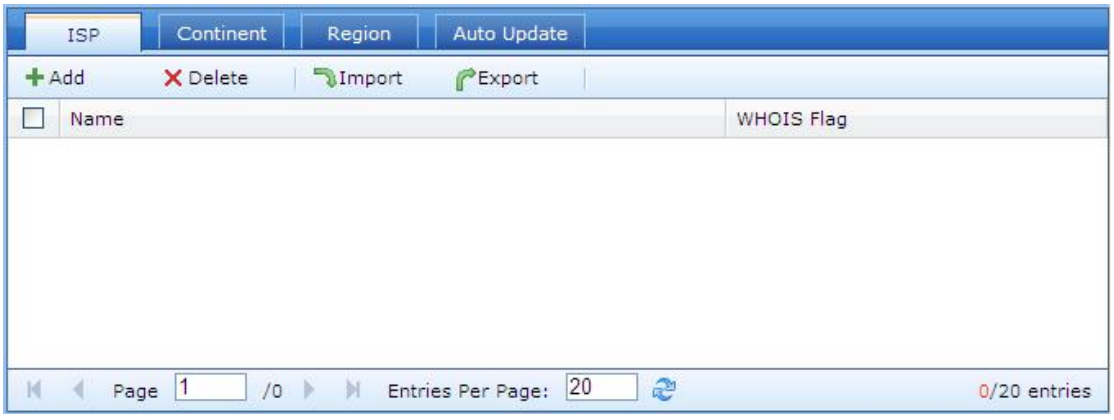
To export the IP groups as CSV file, click **Export**.

5.2 Configuring IP Group

IP group is a collection of IP addresses of the same category including ISP, Continent, Region and Auto Update.

5.2.1 ISP IP Group

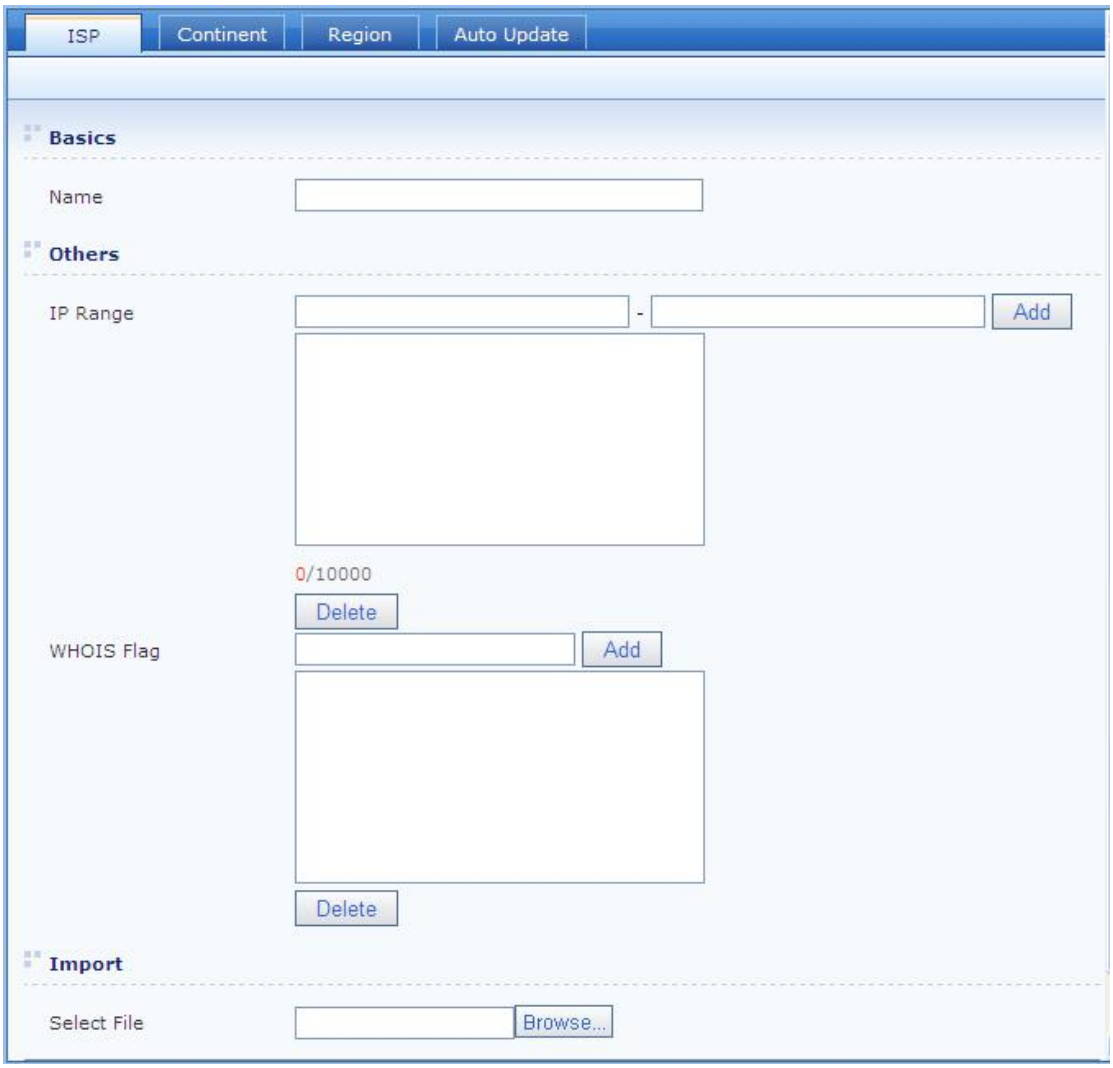
IP groups in **ISP** tab are IP addresses/ranges of Internet Service Provider(ISP), mainly used for policy-based routing configuration.



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

To remove IP group of an ISP, select the entry and click **Delete**.

To add IP group for a new ISP, click **Add** and configure the fields in the following picture:



Name: Specifies the ISP name.

IP Range: Specifies the IP addresses/ ranges of the ISP.

WHOIS Flag: Specifies the WHOIS flag corresponding to the ISP IP group, so that IP address of different ISPs can be distinguished. To add an entry, type the flag of address and click **Add**. To remove an entry, click the entry and click **Delete**.

To import IP groups from file, click browse a .txt file (ANSI encoding) and upload on to the ADC through the **Import** > **Select File** field.

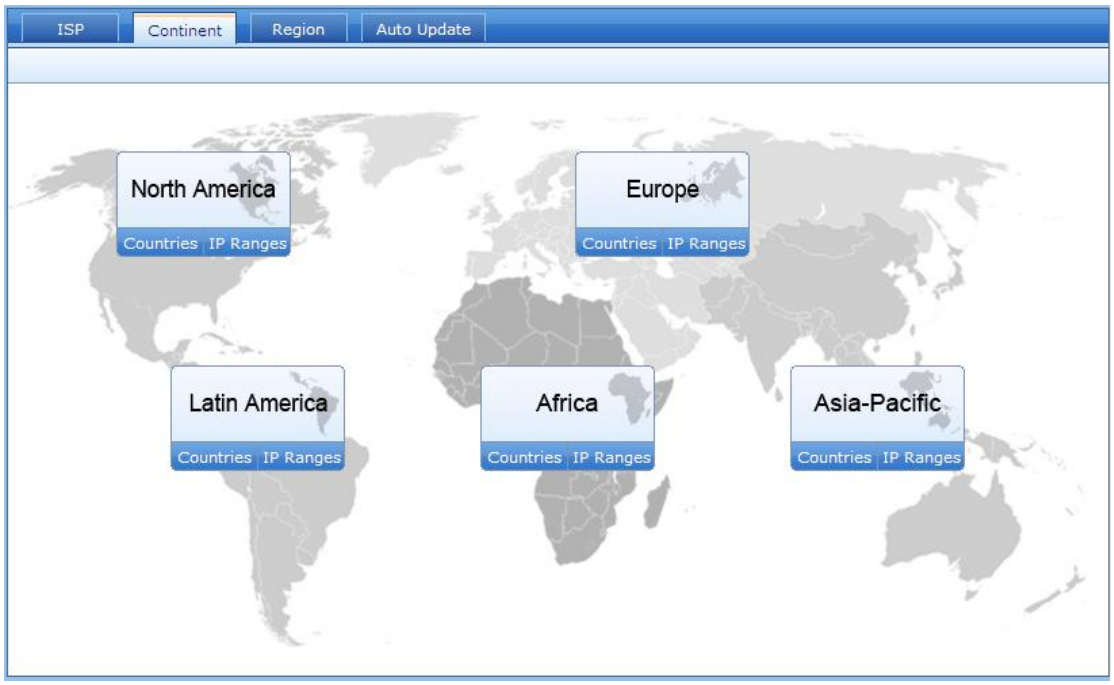
To save the settings, click **OK**; to give up the settings, click **Cancel**.

5.2.2 Continent IP Group

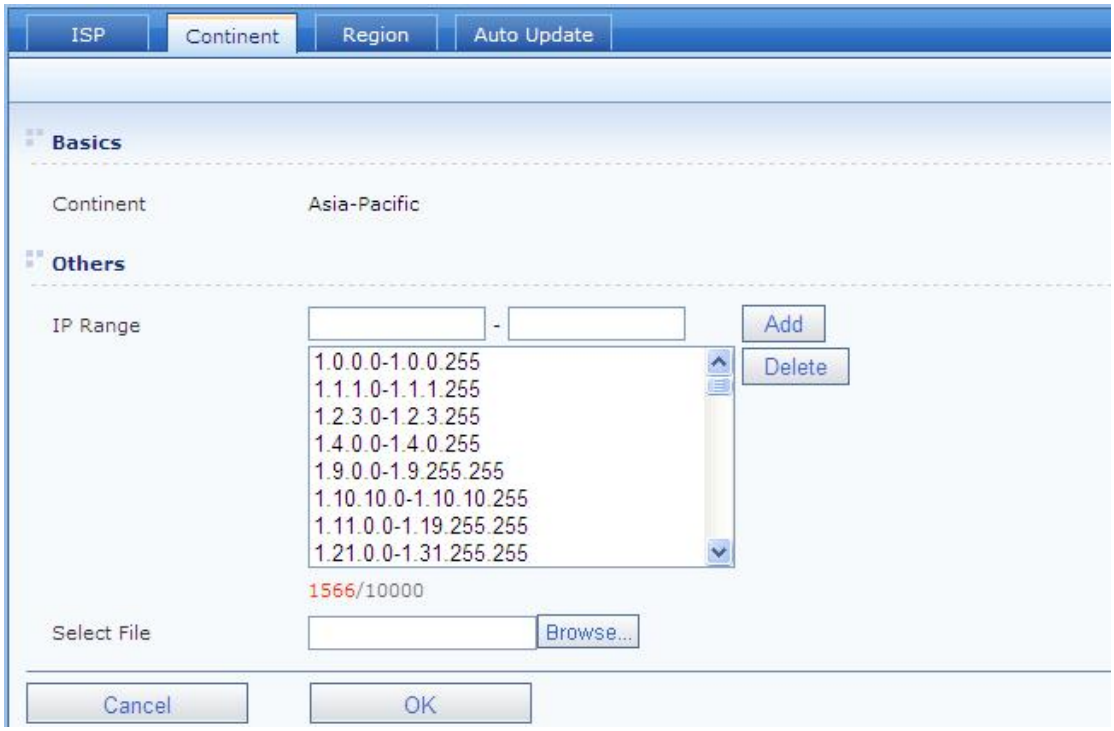
IP groups in **Continent** tab are IP addresses/ranges in the counties in each continent, which

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

are North America, Europe, Latin America, Africa and Asia-Pacific.



To view the countries on a continent, click **Countries**.



Continent: Indicates the continent on which the state is on.

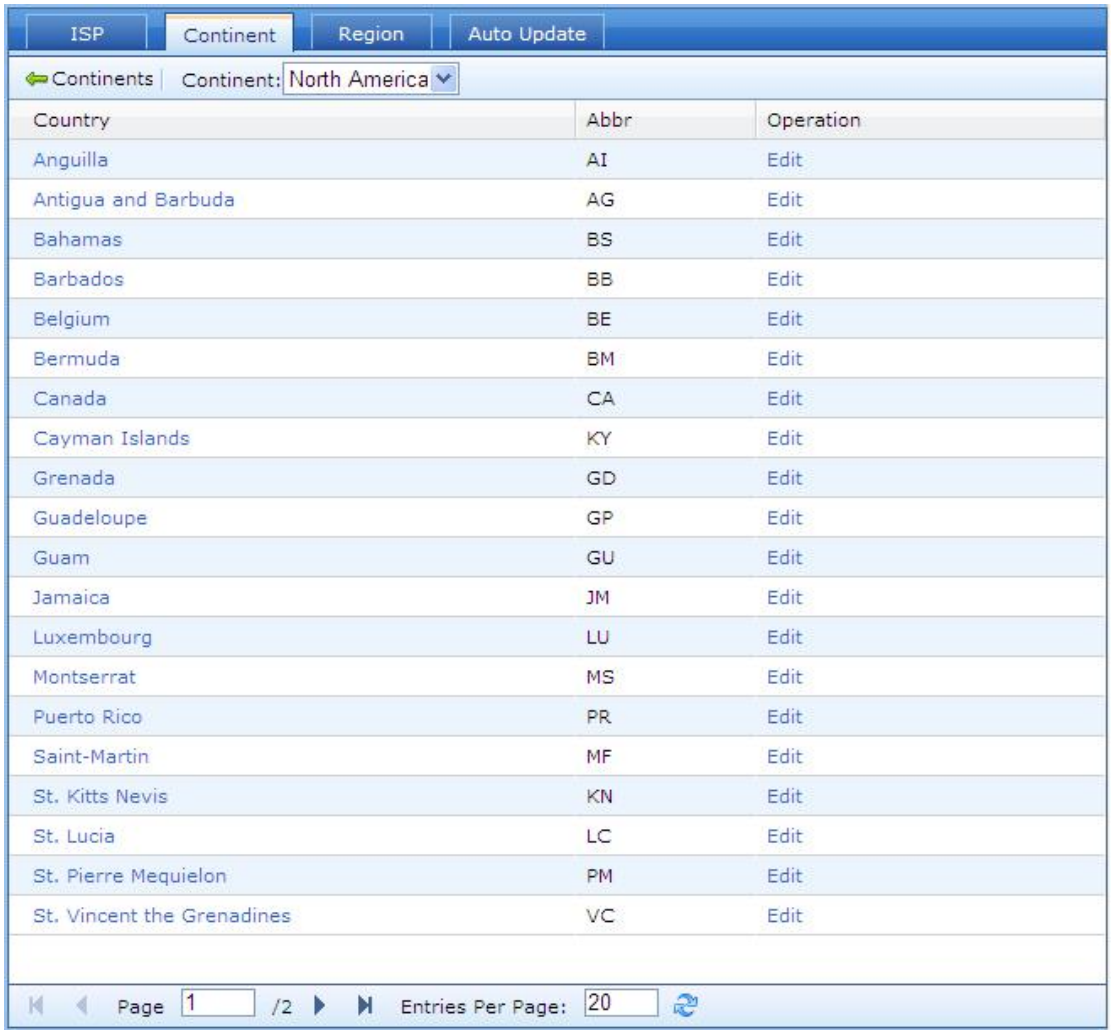
IP Ranges: Specifies the IP addresses/ranges in the state. To add an entry, enter the IP range and click **Add**. To remove an entry, select the entry and click **Delete**.

Select File: Browse a .txt file (ANSI encoding) to upload the IP ranges on to the ADC.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

To save the state settings, click **OK**; to give up the state settings, click **Cancel**.

To view the specific addresses on the continent, click **IP Ranges**. Take **North America** for example. Click **Countries**:



Above are the countries on the continent **North America**. To view countries on another continent, select the continent name form the pull-down list. **Export** option is added.

To view IP ranges on a specific country, click on the country name. Take **Anguilla** for example:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

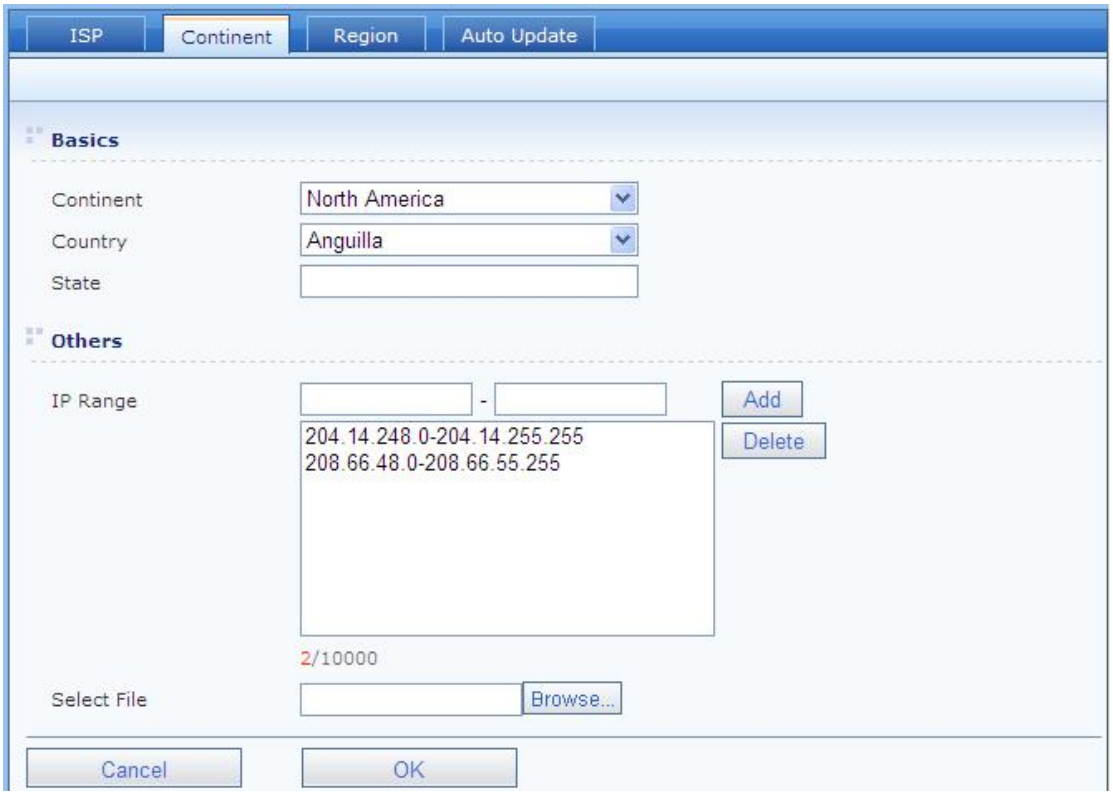


To go back to the continent list, click **Continents**.

To change to another continent, select the continent name from the **Continent** pull-down list.

To change to another country, select the country name from the **Country** pull-down list.

To add to state for a country, click the **New State** button to enter the following page:



Continent: Indicates the continent on which the state is on.

Country: Indicates the country on which the state is in.

State: Specifies name of the state in the country.

IP Ranges: Specifies the IP addresses/ranges in the state. To add an entry, enter the IP range and click **Add**. To remove an entry, select the entry and click **Delete**.

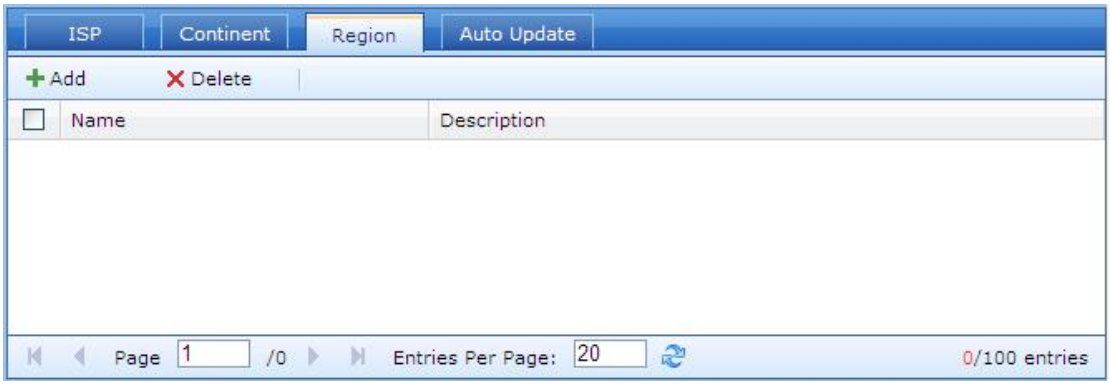
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Select File: Browse a .txt file (ANSI encoding) to upload IP ranges on to the ADC.

To save the state settings, click **OK**; to give up the state settings, click **Cancel**.

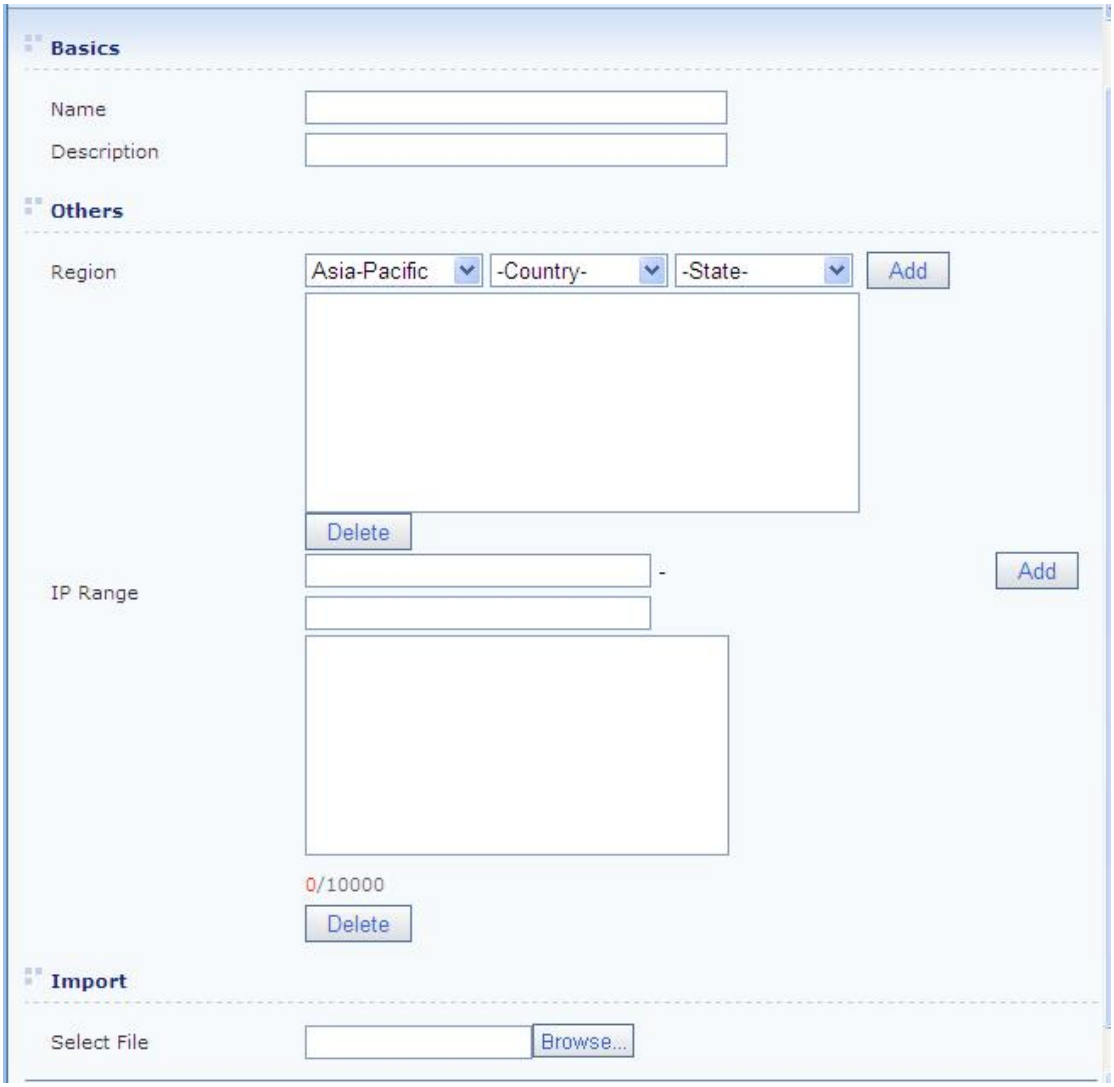
5.2.3 Region IP Group

IP groups in **Region** tab are IP addresses/ranges in regions. A region is distinguished from other regions by WHOIS flag and IP ranges.



To add a new region, click **Add** to enter the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Enter a name for the region.

Description: Give the region a brief description.

Region: Select the continent, country and state where the region is located.

IP Range: Specifies the IP range of the region. To add an entry, enter the IP range and click **Add**. To remove an entry, select the entry and click **Delete**.

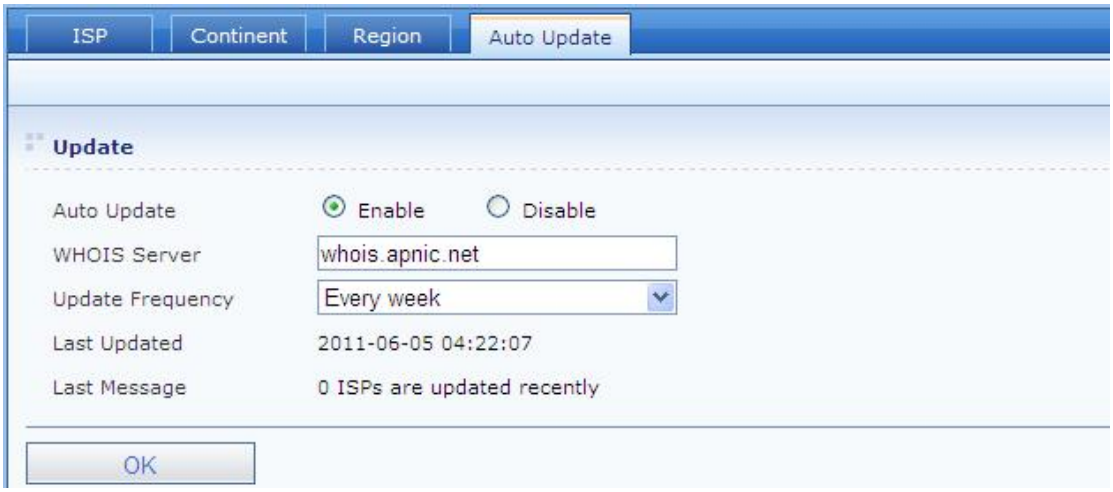
Select File: Browse a .txt file (ANSI encoding) to upload IP ranges on to the ADC.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

5.2.4 Auto Update of Region IP Ranges

If WHOIS server is configured, IP groups in regions can be updated periodically based on the WHOIS flag in that region.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



The following are the contents on the A**uto Update** tab:

Auto Update: Select Enable to enable automatic update

WHOIS Server: Specifies the WHOIS server to update IP range in each region.

Update Frequency: Specifies how often the regions are updated, every day, every week or every month.

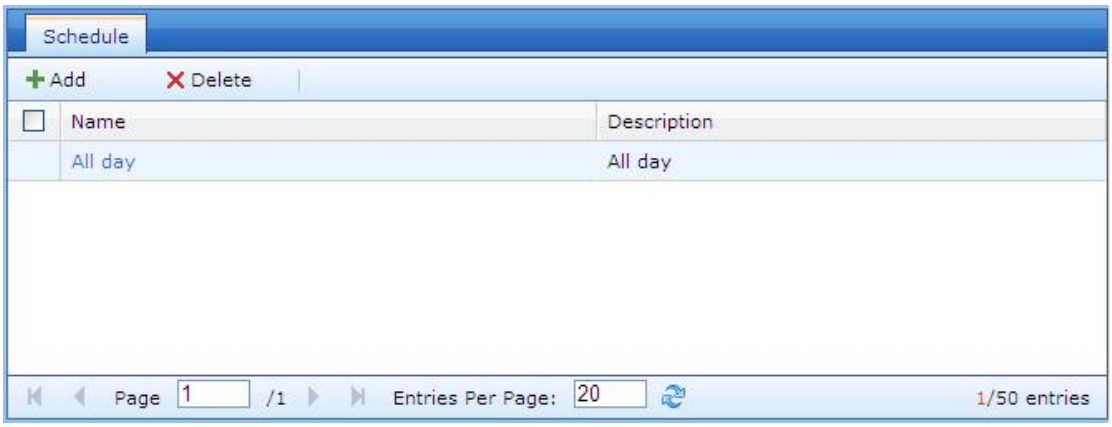
Last Updated: Indicates the last time regions are updated.

Last Message: Indicates the message for last auto update.

To save the settings, click **OK**.

5.3 Configuring Schedule

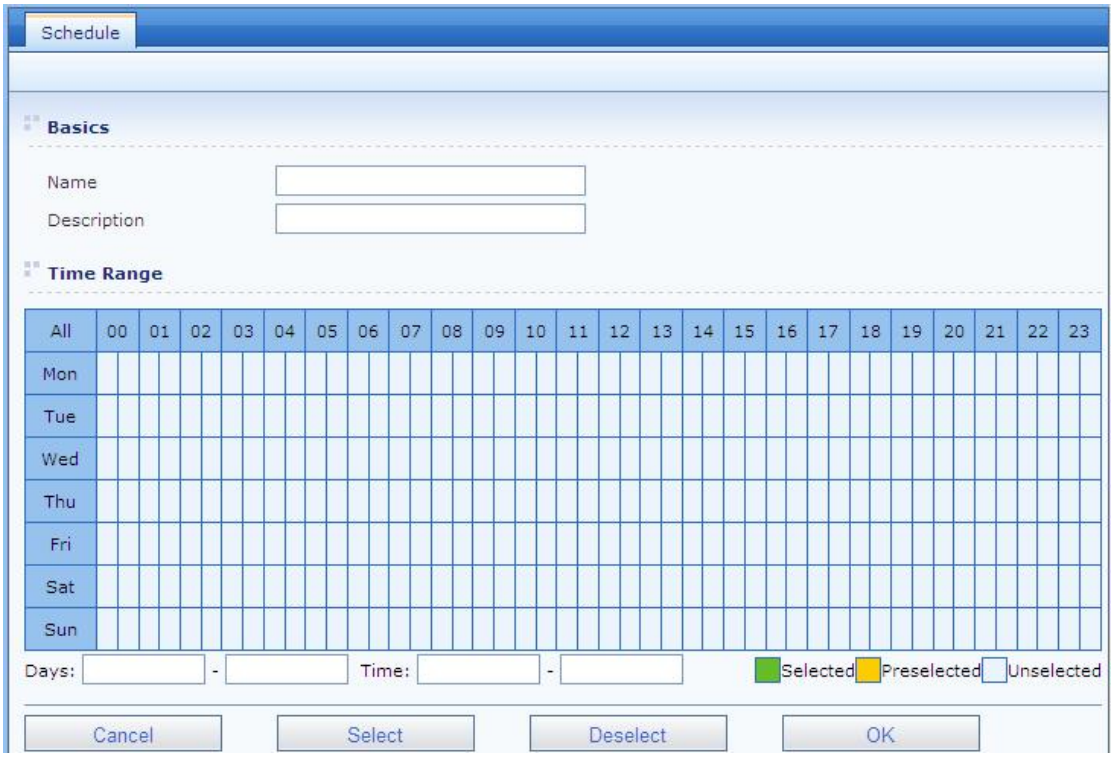
A schedule is a combination of time segments, which can be referenced by policy-based routing.



To remove a schedule, select the entry and click Delete. However, predefined schedule cannot be deleted.

To add a new schedule, click **Add** to enter following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Enter a name for the schedule.

Description: Give the schedule a brief description.

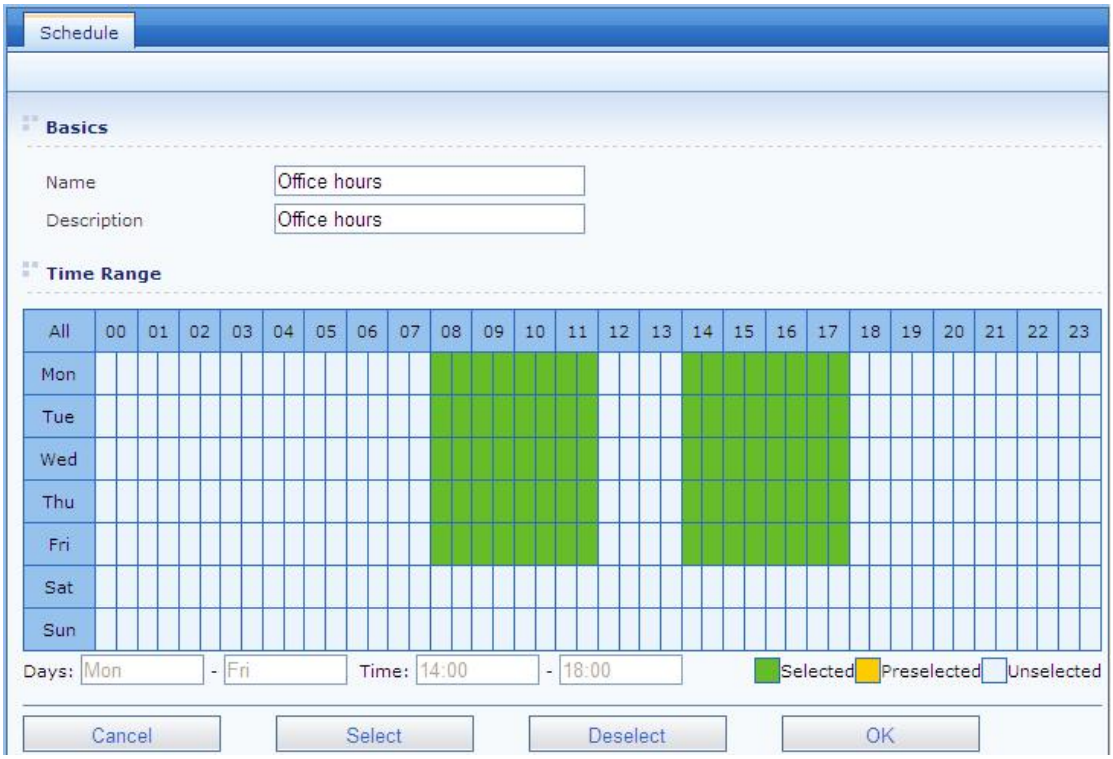
Select: Click this button to select the preselected time range.

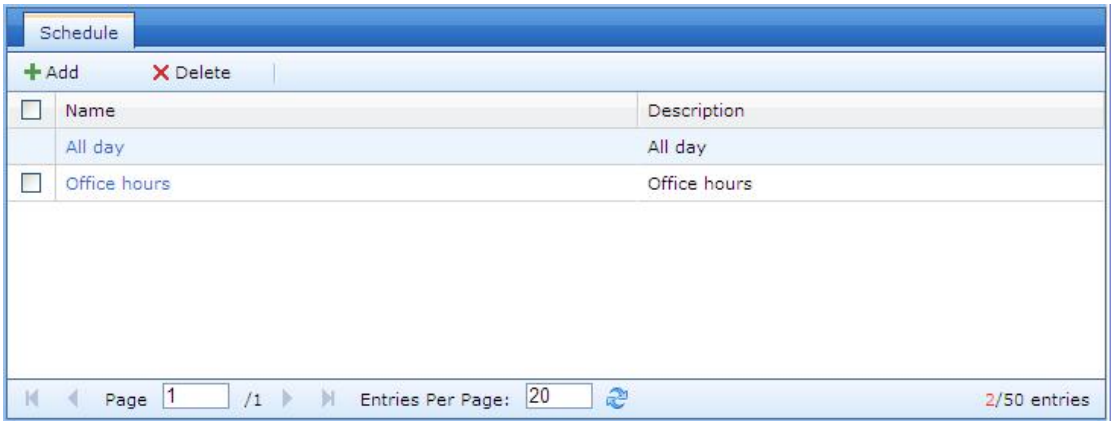
Deselect: Click this button to deselect the preselected time range.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

For example, to configure an schedule name **Office hours** (8:00-12:00am, 14:00-18:00 pm), select the time range and click **OK**, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

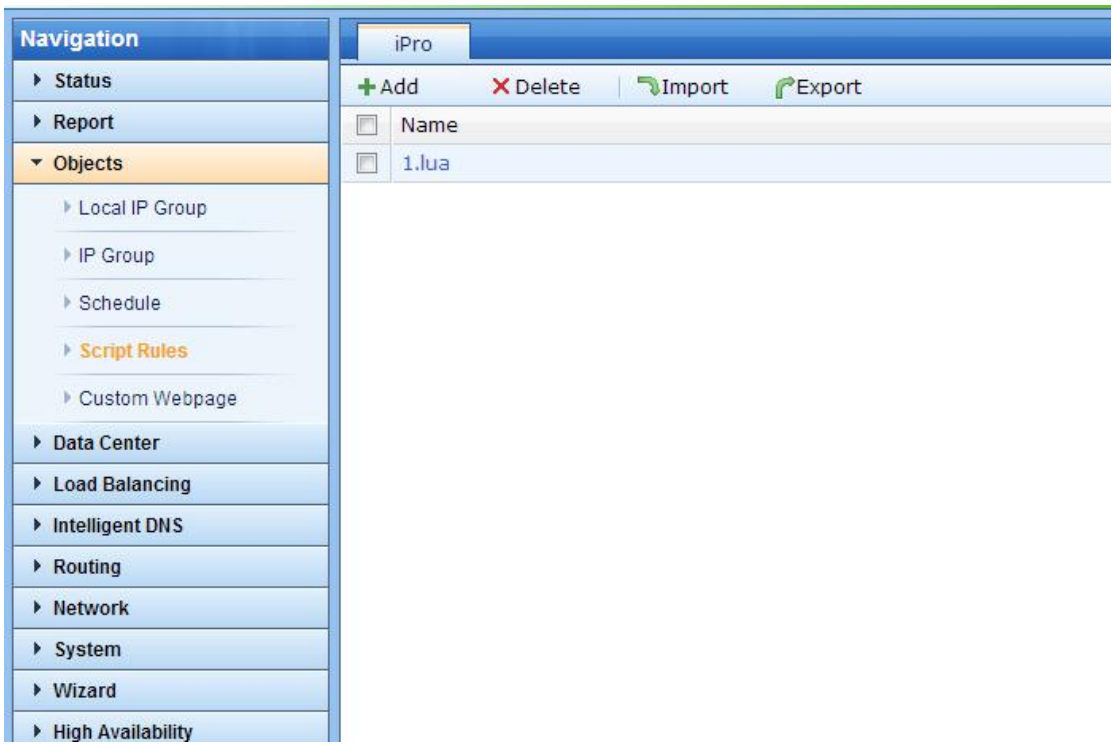




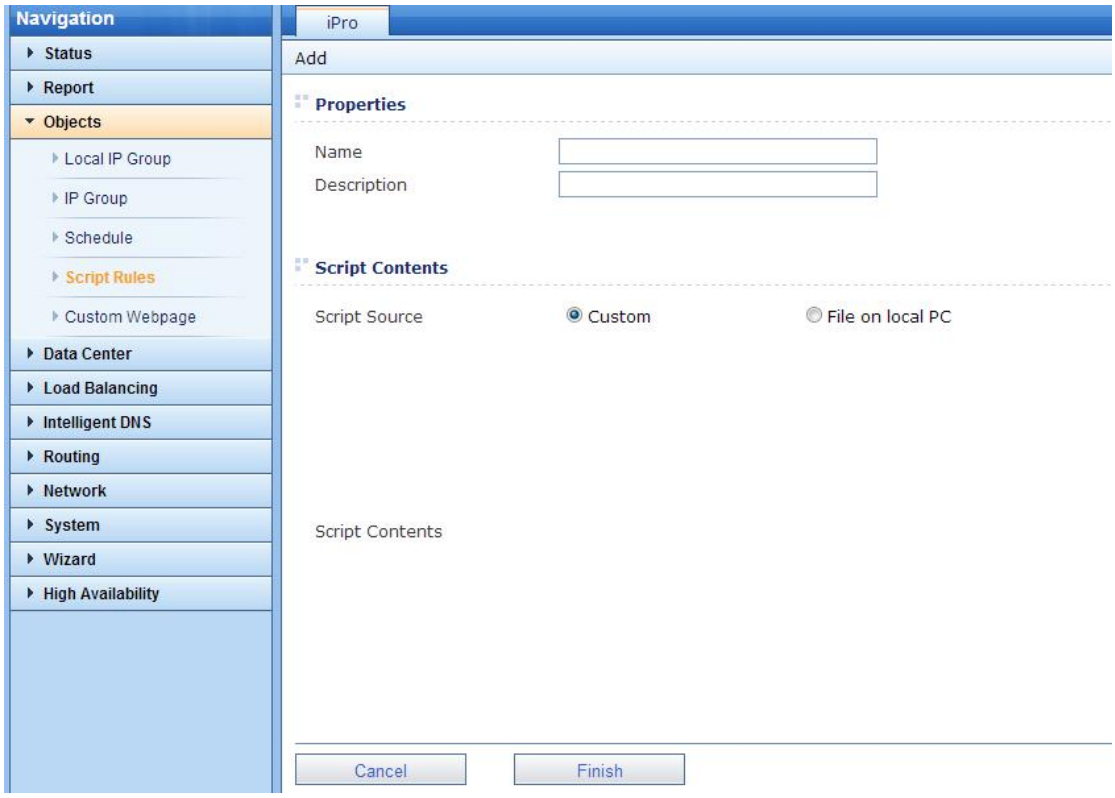
5.4 Script Rules

In **Objects** > **Script Rules**, you can custom script rules or upload script files from local PC.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Add: Click this button to add script rules, as shown below:



Name: Enter a name for the script rule.

Description: Give the script rule a brief description.

Script Source: Click **Custom** to customize script contents or click **File on local PC** to upload script file from the local PC.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

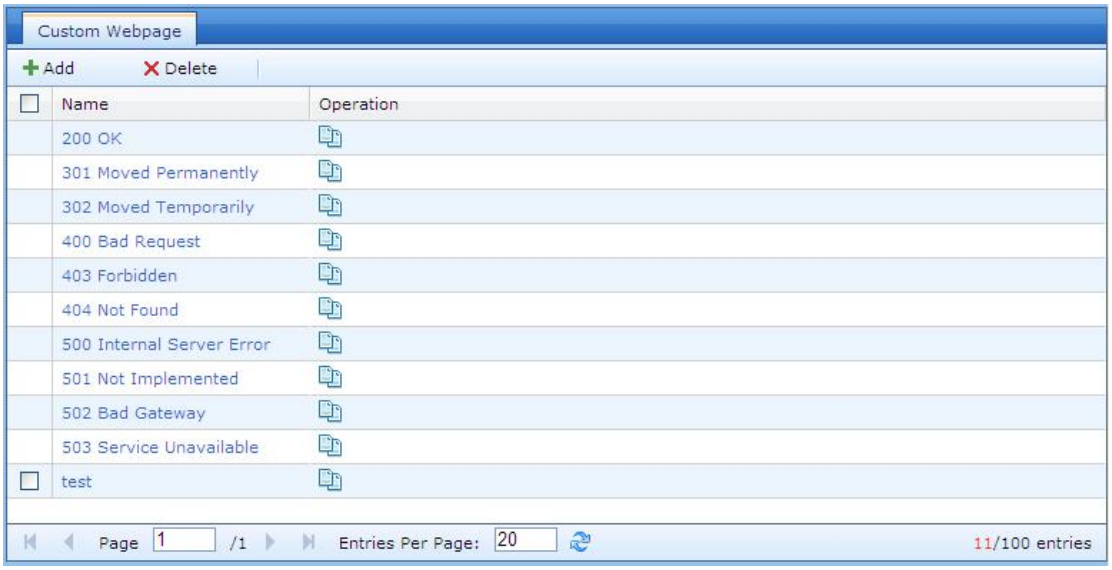
Script Contents: Enter script contents using Lua language.

To save the settings, click **Finish**.

To give up the settings, click **Cancel**.

5.5 Custom web page

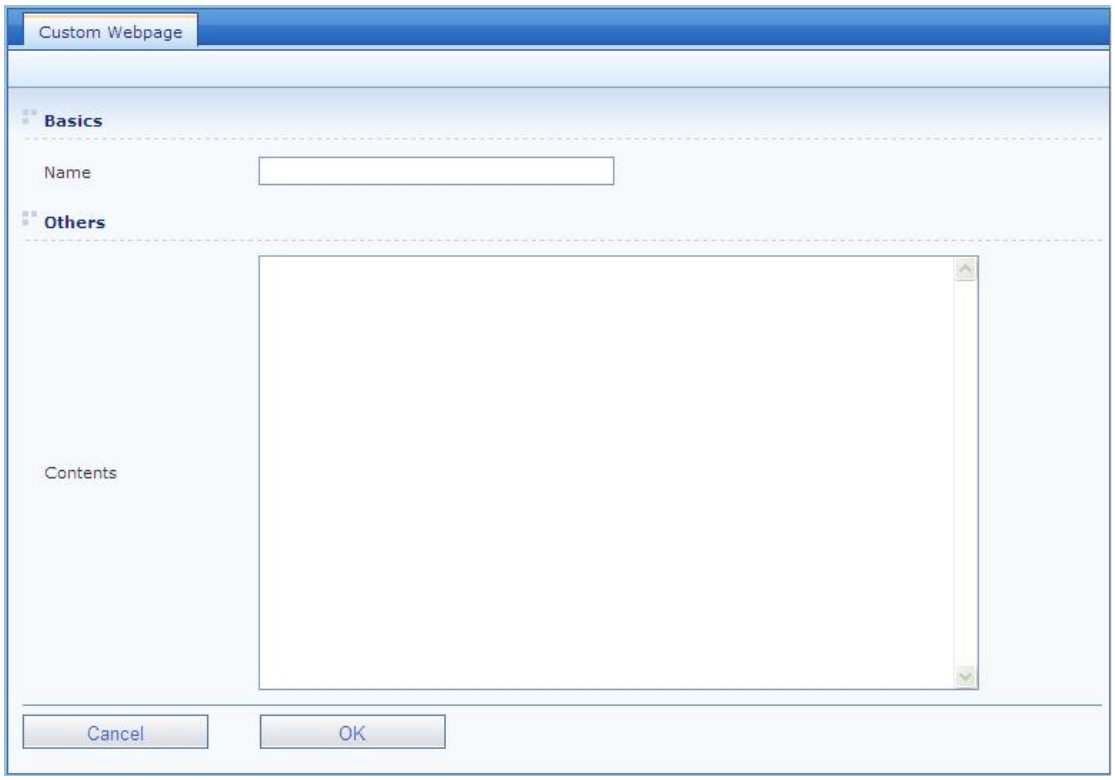
Custom web page is returned in specific situation and referenced by scheduling policy in **Load Balancing** > **Policy**.



To edit predefined web page, click on the name or on the icon in **Operation** column. Please note that predefined web page cannot be referenced by schedule policy. You can copy the contents of the page to create a new one.

To add a new web page, click **Add** and configure the following fields:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



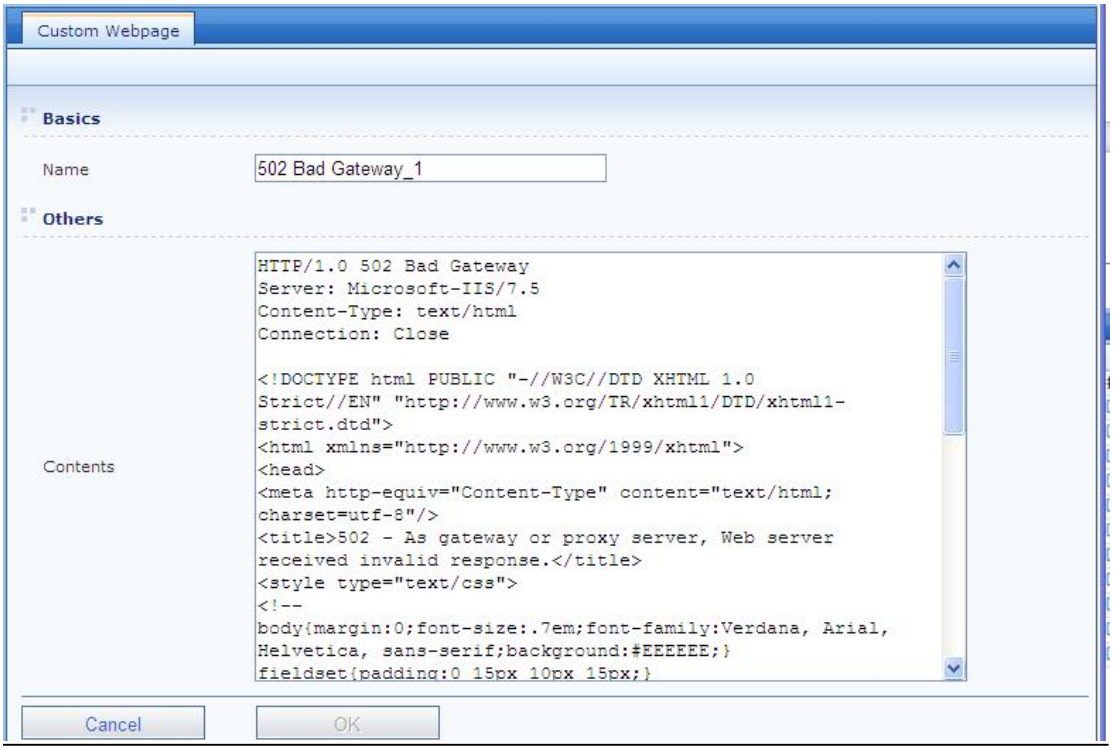
Name: Enter a name for the web page.

Description: Give the web page a brief description. Header and content can be configured separately in Header and Contents fields. Header will be automatically converted from Unix to DOS.

To save the settings, click OK;

For example, to create a web page returning 502 Bad gateway prompt, you can edit the predefined one and copy the contents, and then create a new one and paste the contents into the Contents field.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





Unlike custom web page, predefined web page cannot be deleted.

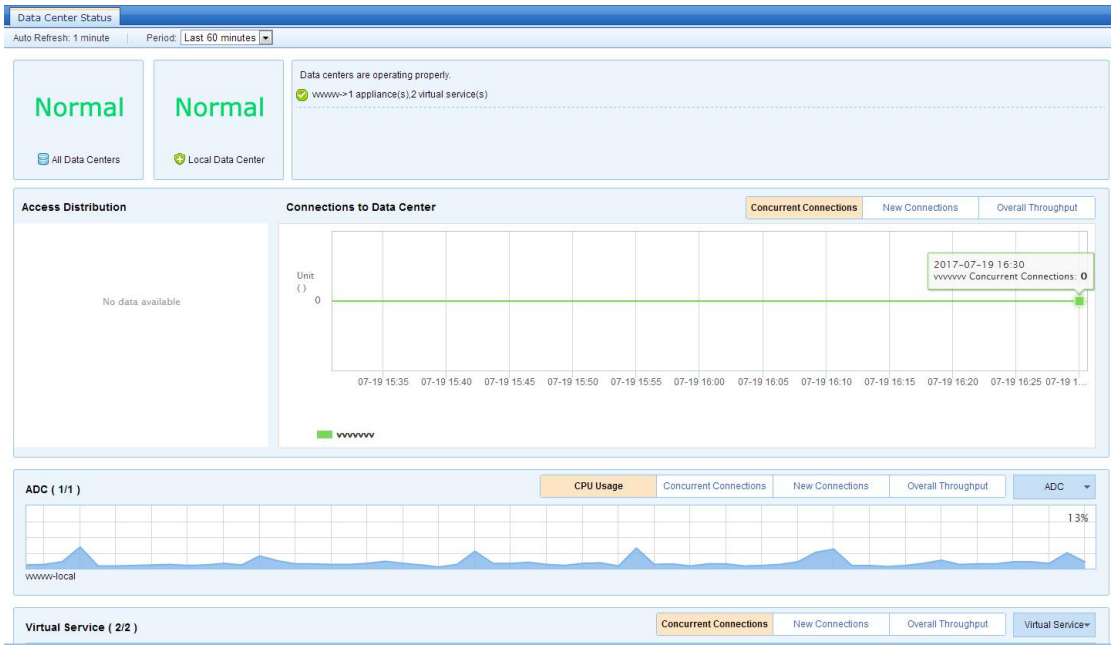
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 6 Data Center

In **Data Center**, you can make relevant configurations and view corresponding status of data center. **Data Center** contains **Overview, Data Center** and **Local Appliances**.

6.1 Overview

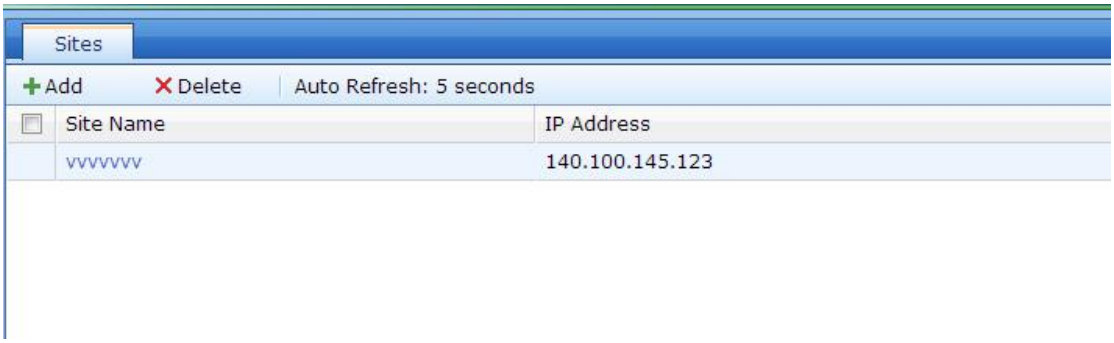
In **Overview**, you can check the status of data center and view corresponding data such as concurrent connections, new connections and overall throughput, as shown below:



6.2 DataCenter

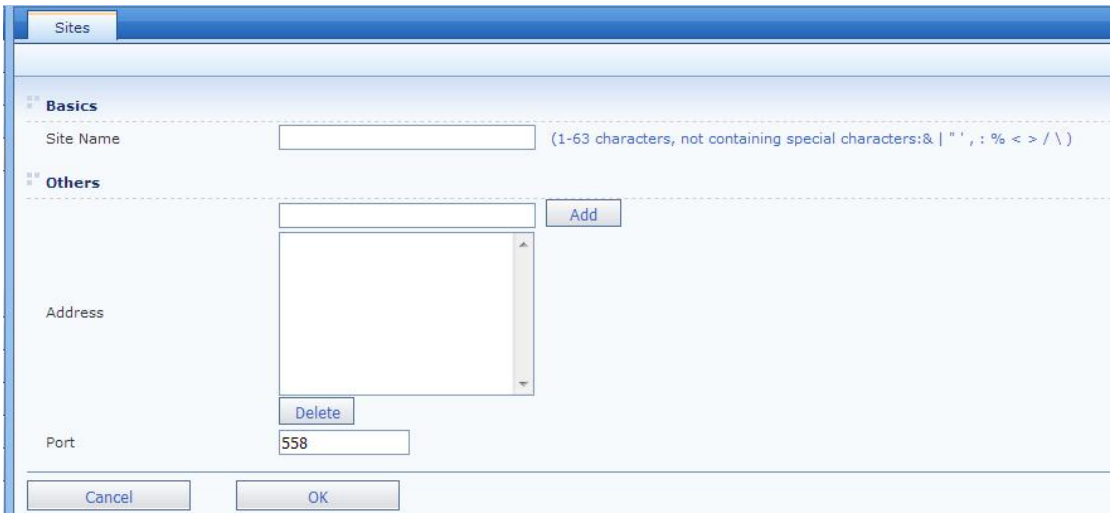
In **Data Center**, you can make relevant configurations, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Delete: Click to delete data center.

Add: Click to add data center, as shown in the following figure:



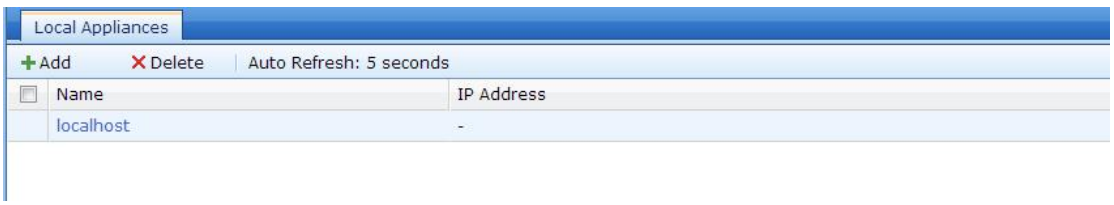
Site Name: Specifies name of the data center.

Address: Specifies address of the data center.

Port: Specifies port of the data center.

6.3 Local Appliances

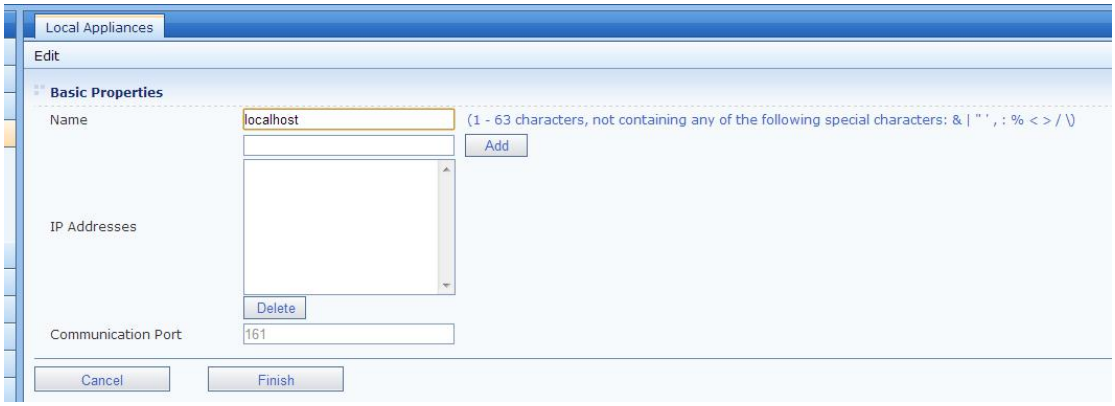
In **Local Appliances**, you can configure local appliances, as shown below:



Delete: Click to delete local device.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Add: Click to add local appliances, as shown in the following figure:



Name: Specifies name of the local appliance.

IP Address: Specifies IP address of the local appliance.

Communication Port: Specifies communication port of the local appliance.

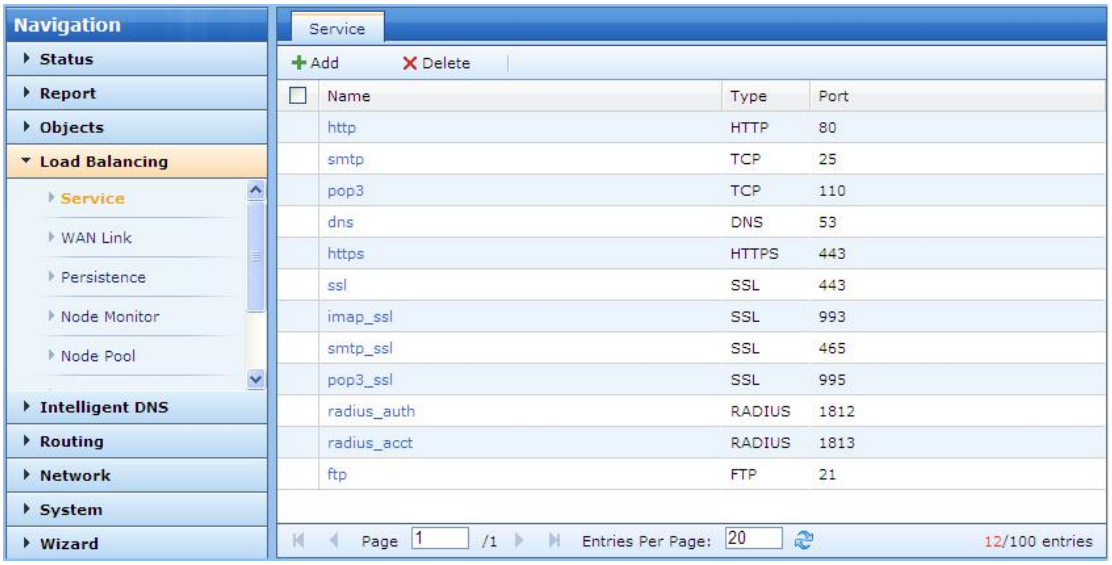
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 7 Load Balancing

Load balancing configuration makes application delivered to external network efficiently and flexibly.

7.1 Configuring Service

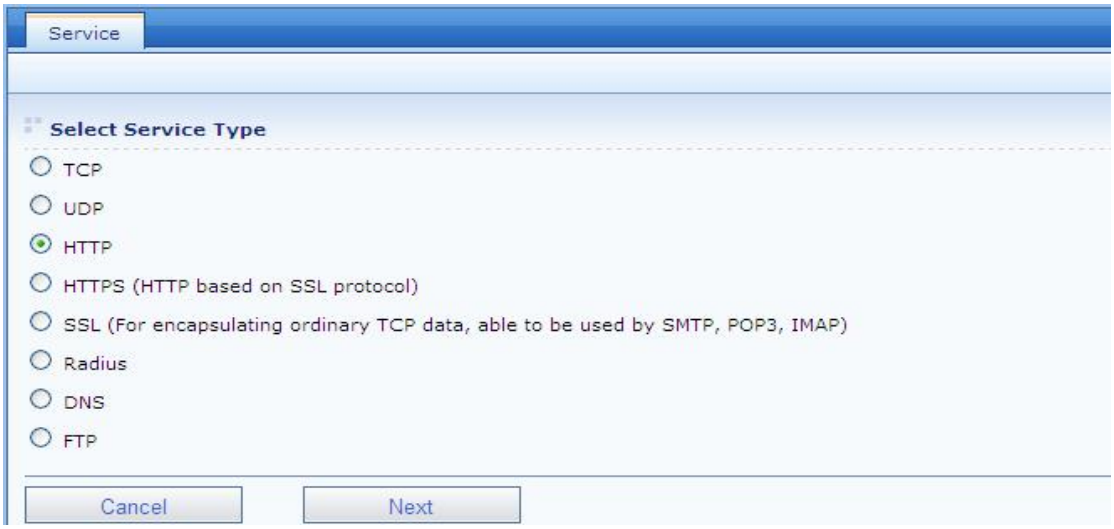
The services are service types that the delivered applications are in, and often referenced by policy and virtual service settings.



To remove a service, select the service and click **Delete**. note that predefined services cannot be deleted.

If you cannot find the desired service type in the predefined services, edit the predefined service or click Add to create a new one on required port. Suppose you need to provide HTTP service on TCP port 81. You can edit the existing HTTP service or create a new one on port 81.

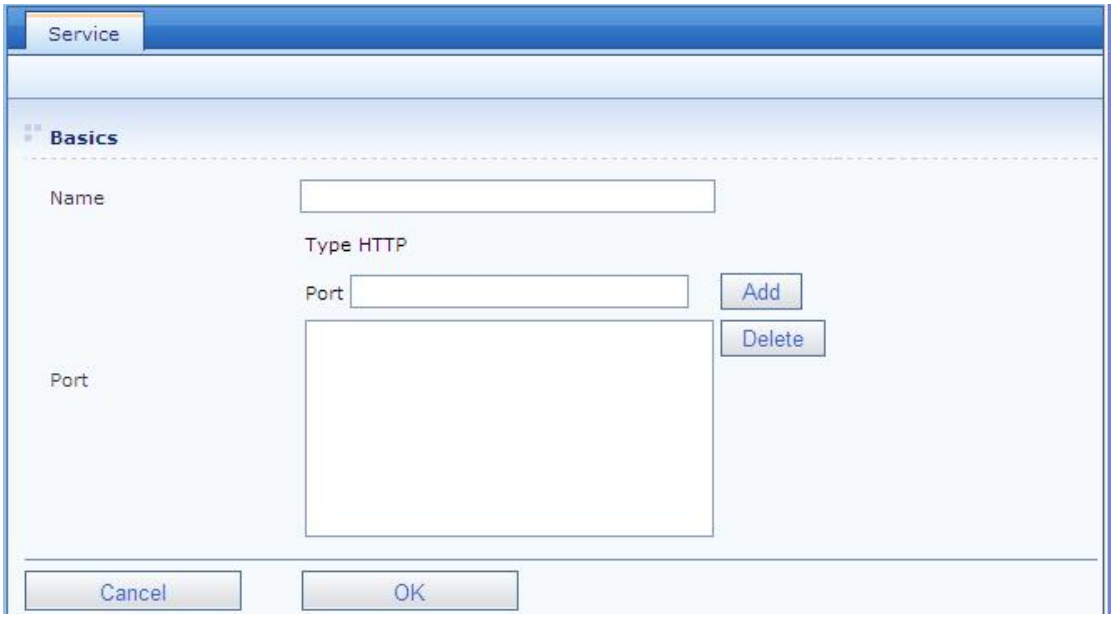
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To create a new one, perform the following steps:

Click **Add** and select service type HTTP.

Click **Next** and specify the following properties.



The following are the basic properties of a service:

Name: Give it a distinguishable name.

Type: Indicates the service type.

Port: Specifies the service port. To add a port entry, enter the port number and click **Add**. To remove a port entry, select the entry and click **Delete**. Port should be between 1 and 65535. A maximum of 16 entries allowed.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

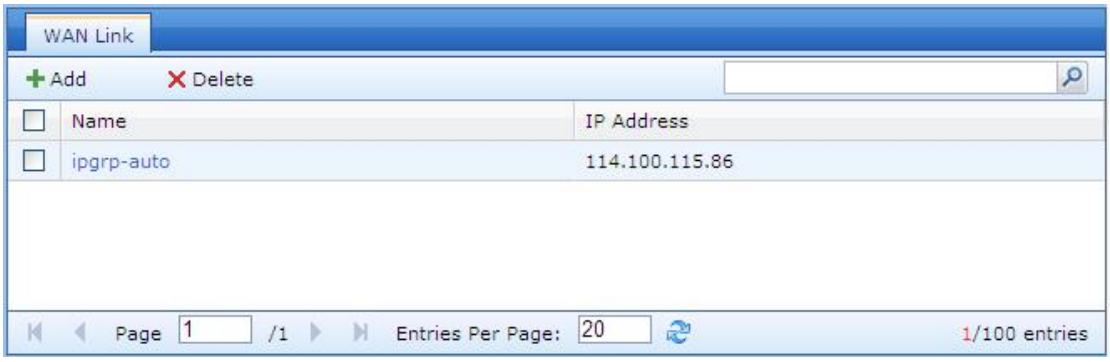


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Unlike custom service, predefined service cannot be deleted.

7.2 WAN Link

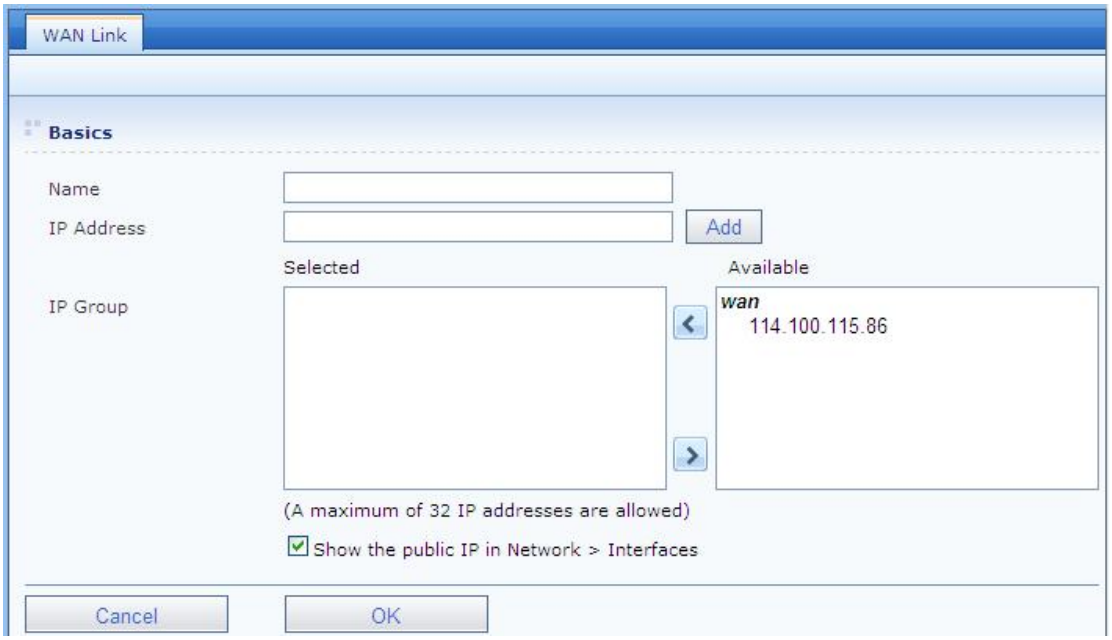
WAN link is used to deliver application, and referenced by virtual IP pool and virtual service settings.



To search for a specific WAN link, enter the link name into the text on the upper right corner and click search icon.

To remove a WAN link, select the link and click **Delete**.

To create a new WAN link, click **Add** and configure the following fields:



The following are the properties of a WAN link:

Name: Give it a distinguishable name.

IP Address: To add an IP address, enter the IP address and click Add to add it into the IP group field. To select a WAN link IP address, click the item and the **<** arrow button to move it

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

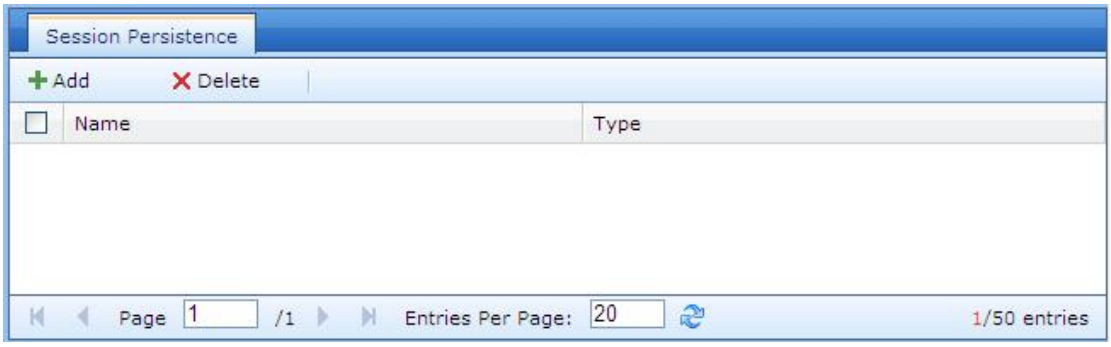
into the **Selected** box from the **Available** box. To remove a selected WAN link, select the item and click the **>** arrow button.

Show the public IP in Next > Interface: Select this option, and the public IP of interface will be seen in the specified page.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

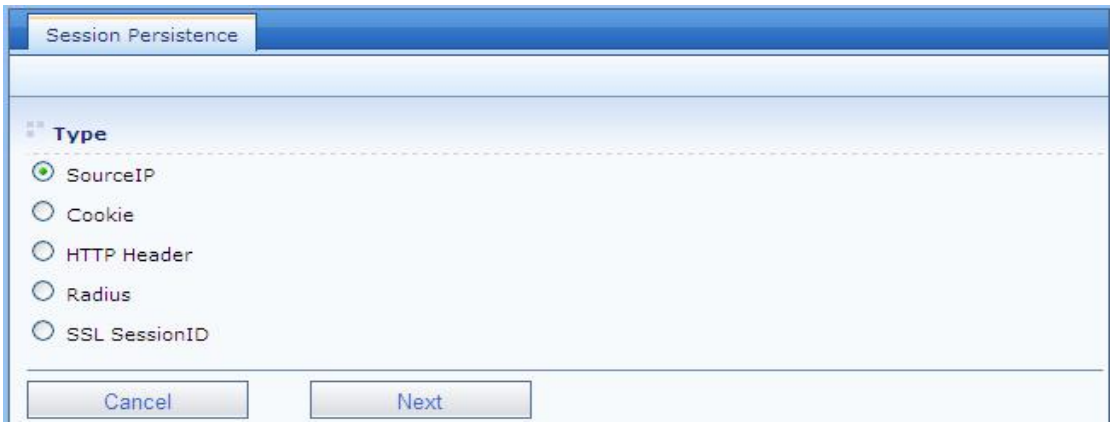
7.3 Session Persistence

Session persistence is the ways that application delivery employs. It is referenced by node pool settings.



To remove a session persistence, select the entry and click **Delete**.

To create a new session persistence, click **Add**.

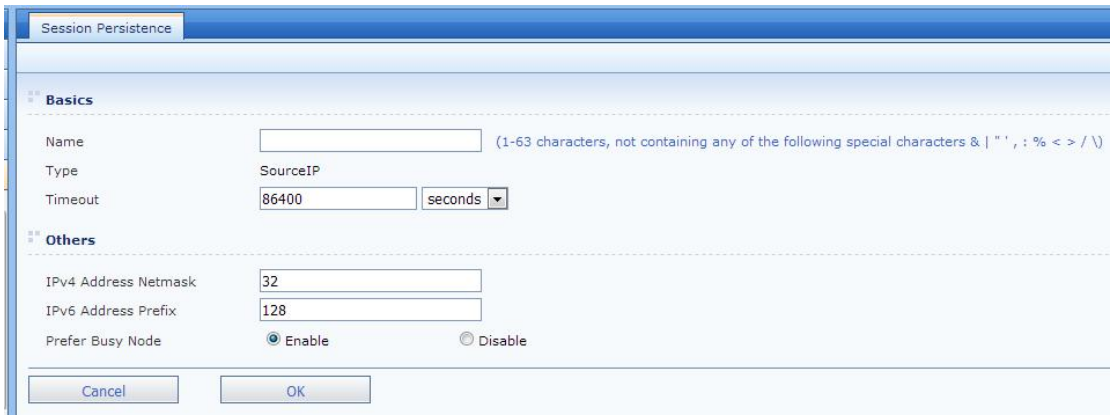


Specify type of session persistence, **Source IP** based, **Cookie** based, **HTTP Header** based, **Radius** based or **SSL SessionID** based.

7.3.1 Source IP Session Persistence

Properties of **Source IP** based session persistence are as follows:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Type: Indicates the SourceIP type of session persistence.

Timeout: Specifies the timeout of session persistence, in second, minute,hour,day.

IPv4 Address Netmask: Specifies the netmask of client IPv4 address that employs Source IP-based session persistence.

IPv6 Address Prefix: Specifies the prefix of client IPv6 address that employs Source IP-based session persistence.

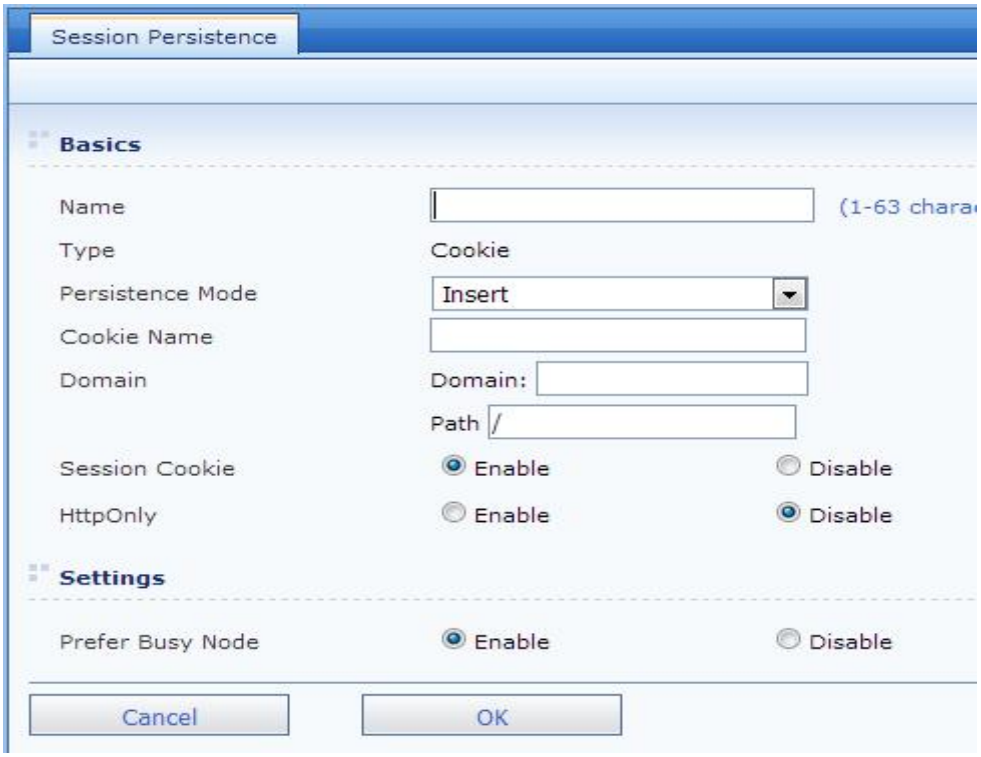
Prefer Busy Node: You can select **Enable** to enable session persistence on busy node or select **Disable** to support session persistence regardless of whether the node is busy or not.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

7.3.2 Cookie Session Persistence

Properties of **Cookie** based session persistence are as follows:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Type: Indicates the type of session persistence.

Persistence Mode: Indicates the persistence method of Cookie. Options are **Insert**, **Passive**(interface) and **Rewrite**. For **Insert** method, when the ADC receives response from server, it insert a **Set-cookie** field in the header of the HTTP response. The field includes the following contents: Cookie name, domain, path and timeout. For **Passive** mode, after analyzing the Set-cookie field in the header of HTTP response and finding the Cookie information, the ADC remembers the Cookie and server information and use on next scheduling. For **Rewrite** method, the ADC rewrites Cookie name in Set-cookie in the header of HTTP response and inserts the server information, to achieve persistence based on server information when sending request.

Cookie Name: Specifies the Cookie name returned to client based on this persistence. Please note that cookie name for different persistence must not be the same.

Domain: Specifies domain name so that the cookie persistence is also applicable to the sub-domains. This is necessary when virtual service is delivered, but sub-domains also need to be visited. For example, virtual server **www.test.com** is delivered to external network. When users visit the sub-domain **news.test.com**, this persistence is not applicable, and scheduling needs be performed again without ensuring positive result. By configuring the domain here, you will have persistence also applicable to access to the sub-domains.

Session Cookie: Select **Enable** to enable session-based cookie.

HTTP Only: Select **Enable** to enable HTTPOnly or select **Disable** to disable HTTPOnly.

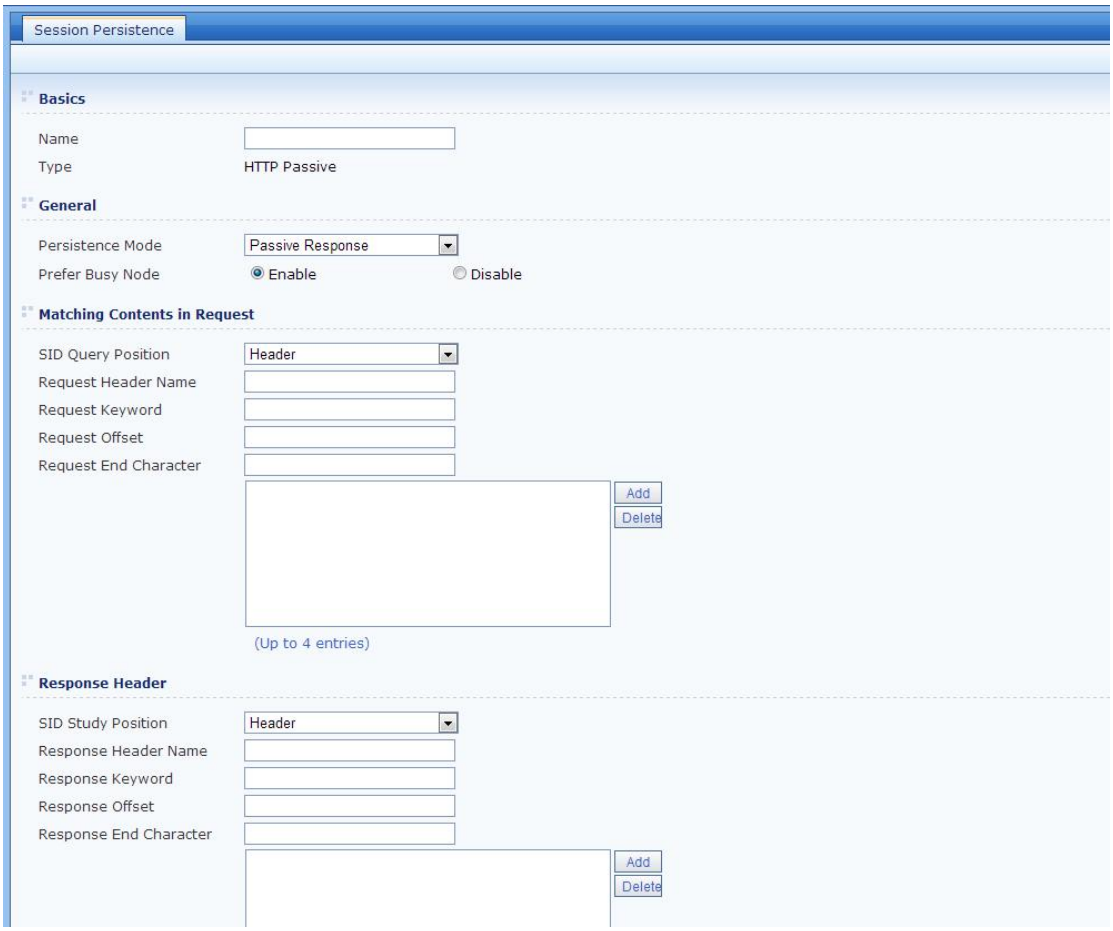
Prefer Busy Node: Select **Enable** to enable session persistence on busy node or select **Disable** to support session persistence regardless of whether the node is busy or not.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

To save the settings, click **OK**; to give up the settings, click **Cancel**.

7.3.3 HTTP Header Session Persistence

Properties of **HTTP Header** based session persistence are as follows:



Name: Give it a distinguishable name.

Type: Indicates the HTTP Passive type of session persistence.

Persistence Mode: Select **Passive Request** or **Passive Response** to achieve session persistence based on a field in request or response.

Prefer Busy Node: Select **Enable** to enable session persistence on busy node or select **Disable** to support session persistence regardless of whether the node is busy or not.

SID Query Position: Select **Header**, **URL** or **Body**.

Request Header Name: Specifies header name in HTTP request.

Request Keyword: Specifies the keyword in request.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Request Offset: Specifies the offset in the request starting from keyword.

Request End Character: Specifies the end characters of keyword in the request.

SID Study Position: Select **Header** or **Body**.

Response Header Name: Specifies the header name in the HTTP response.

Response Keyword: Specifies the keyword in response.

Response Offset: Specifies the offset in the response starting from keyword.

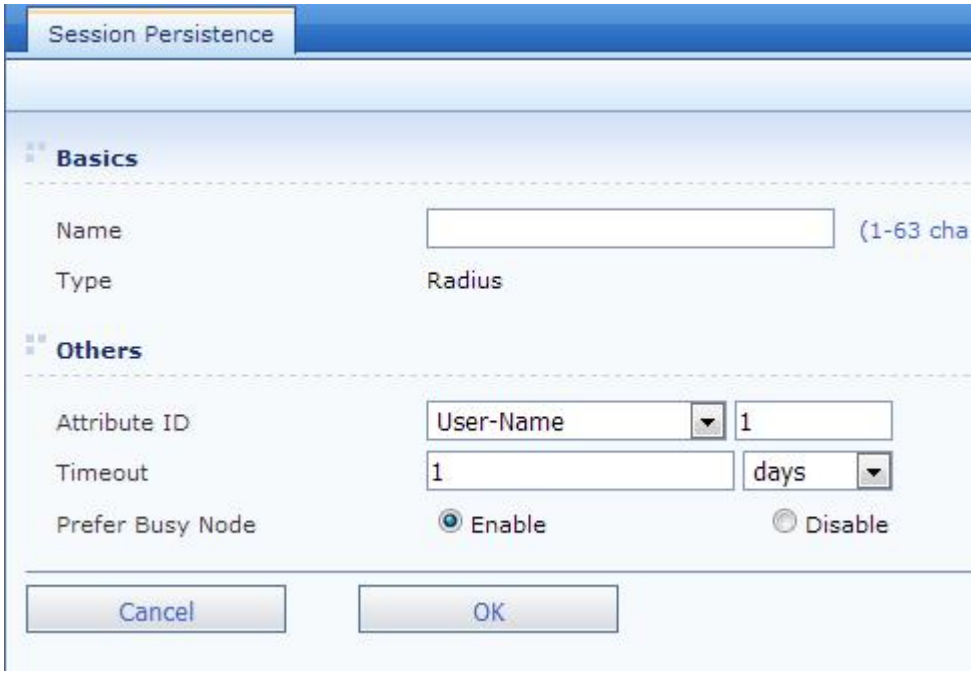
Response End Character: Specifies the end characters of keyword in the response.

Timeout: Specifies the timeout of session persistence, in second.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

7.3.4 RADIUS Session Persistence

Properties of **RADIUS** based session persistence are as follows:



Name: Give it a distinguishable name.

Type: Indicates the type of session persistence.

Attribute ID: Specifies which Attribute attribute value is persistence is based. You can select a built-in attribute and ID or specify a new ID.

Timeout: Specifies the timeout of session persistence, in second.

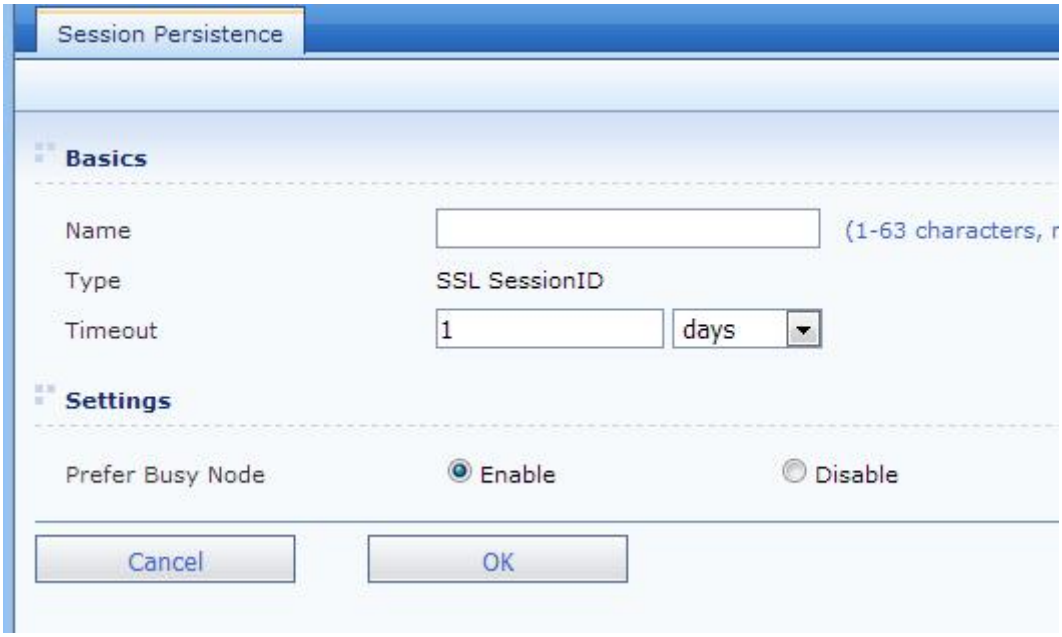
Prefer Busy Node: Select **Enable** to enable session persistence on busy node or select **Disable** to support session persistence regardless of whether the node is busy or not.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

To save the settings, click **OK**; to give up the settings, click **Cancel**.

7.3.5 SSL Session ID

Properties of **SSL Session ID** based session persistence are as follows:



Name: Give it a distinguishable name.

Type: Indicates the SSL SessionID type of session persistence. This type of persistence makes sure that SSL requests from a user can be scheduled to a same server.

Timeout: Specifies the timeout of session persistence, in day.

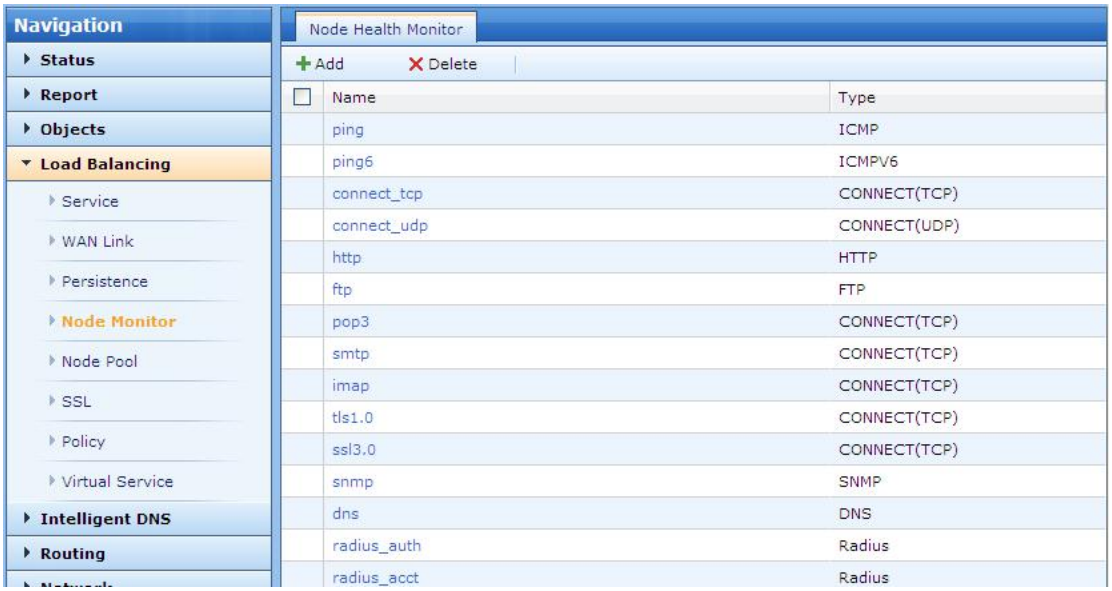
Prefer Busy Node: Select **Enable** to enable session persistence on busy node or select **Disable** to support session persistence regardless of whether the node is busy or not.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

7.4 Node Monitor

Node monitor probes status of node that launches applications. It is referenced by node pool settings.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To remove a node monitor, select the monitor and click **Delete**. Please note that predefined monitors cannot be deleted. To add a new monitor, click **Add** to enter the following page:



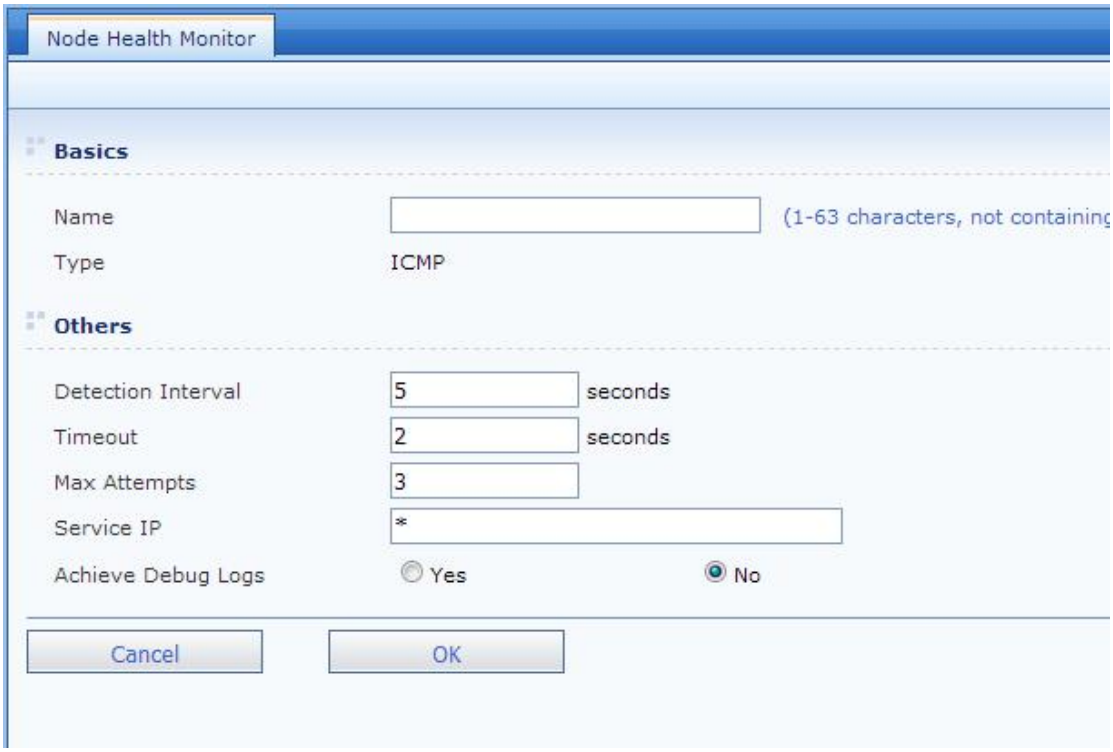
Select a type and click **Next**.

7.4.1 ICMP Monitor

For **ICMP**-based node monitor, the ADC will send an IPv4 ICMP packet to probe status of

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

node. The following are the properties about an ICMP-based node monitor:



Name: Give it a distinguishable name.

Type: Indicates the type of node monitor.

Detection Interval: Specifies the interval between two node status probes. Unit is second.

Timeout: Expiration of probe duration, in second.

Max Attempts: Maximum number of attempts for probing status of node.

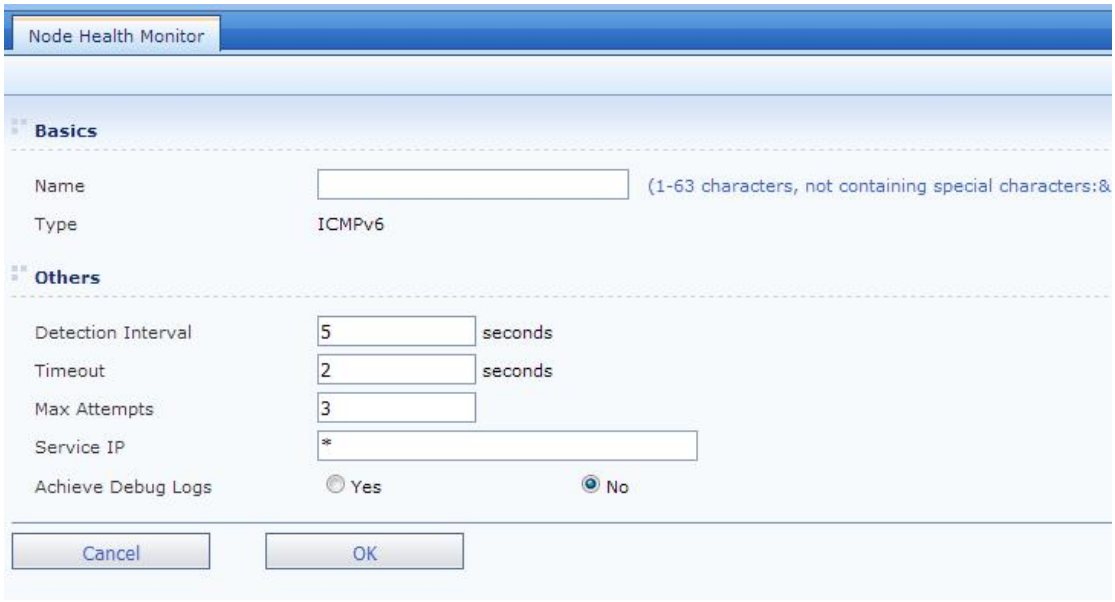
Service IP: Specifies the node IP address being watched. * indicates all addresses.

Archive Debug Logs: Choose whether to archive debug log of the node monitoring. If **Yes** is selected, the related debug logs will be store in logs database on the ADC.

7.4.2 ICMPv6 Monitor

For **ICMPv6**-based node monitor, the ADC will send an IPv6 ICMP packet to probe status of node. The following are the properties about an ICMPv6-based node monitor:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Type: Indicates the type of node monitor.

Detection Interval: Specifies the interval between two node status probes. Unit is second.

Timeout: Expiration of probe duration, in second.

Max Attempts: Maximum number of attempts for probing status of node.

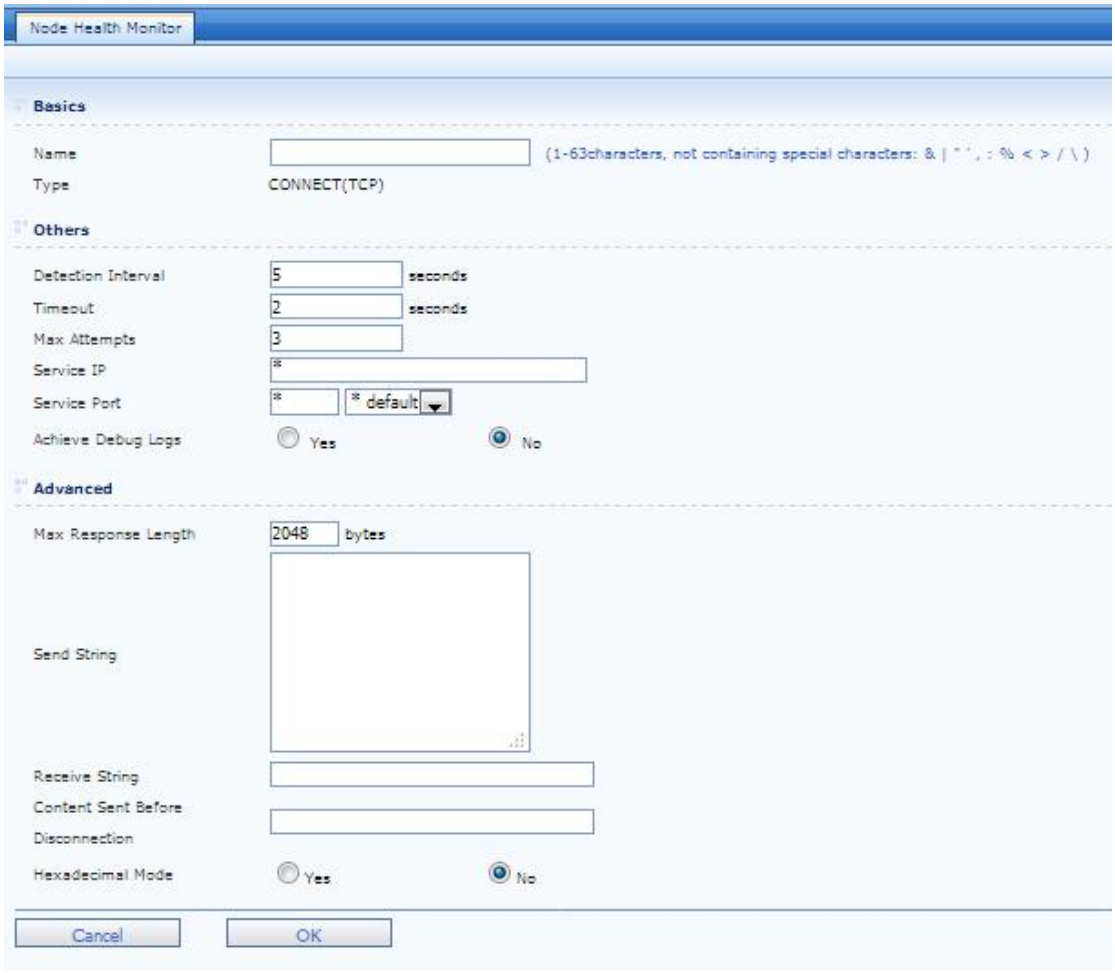
Service IP: Specifies the node IP address being watched. * indicates all addresses.(It is standard address fro IPV6)

Archive Debug Logs: Choose whether to archive debug log of **ICMPv6**-based node monitoring. If **Yes** is selected, the related debug logs will be stored in logs database on the ADC.

7.4.3 Connect(TCP) Monitor

For **CONNECT(TCP)**-based node monitor, the ADC will initiate a TCP connection to the node, to probe the status of the node. The following are the properties about a **CONNECT(TCP)**-based node monitor:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Service Port: Specifies the ports being watched. You can select **default**, **http**, **ftp, smtp, pop3, imap, https** or **other** to monitor the standard port. When **other** is selected, it is allowed to specify other ports.

Archive Debug Logs: Choose whether to archive debug log of CONNECT-based node monitoring. If **Yes** is selected, the related debug logs will be stored in logs database on the ADC.

Max Response Length: Specifies the maximum length of contents in response, in byte.

Send String: Specifies the contents sent after connection setup.

Receive String: Specifies the contents must be contained in received packet.

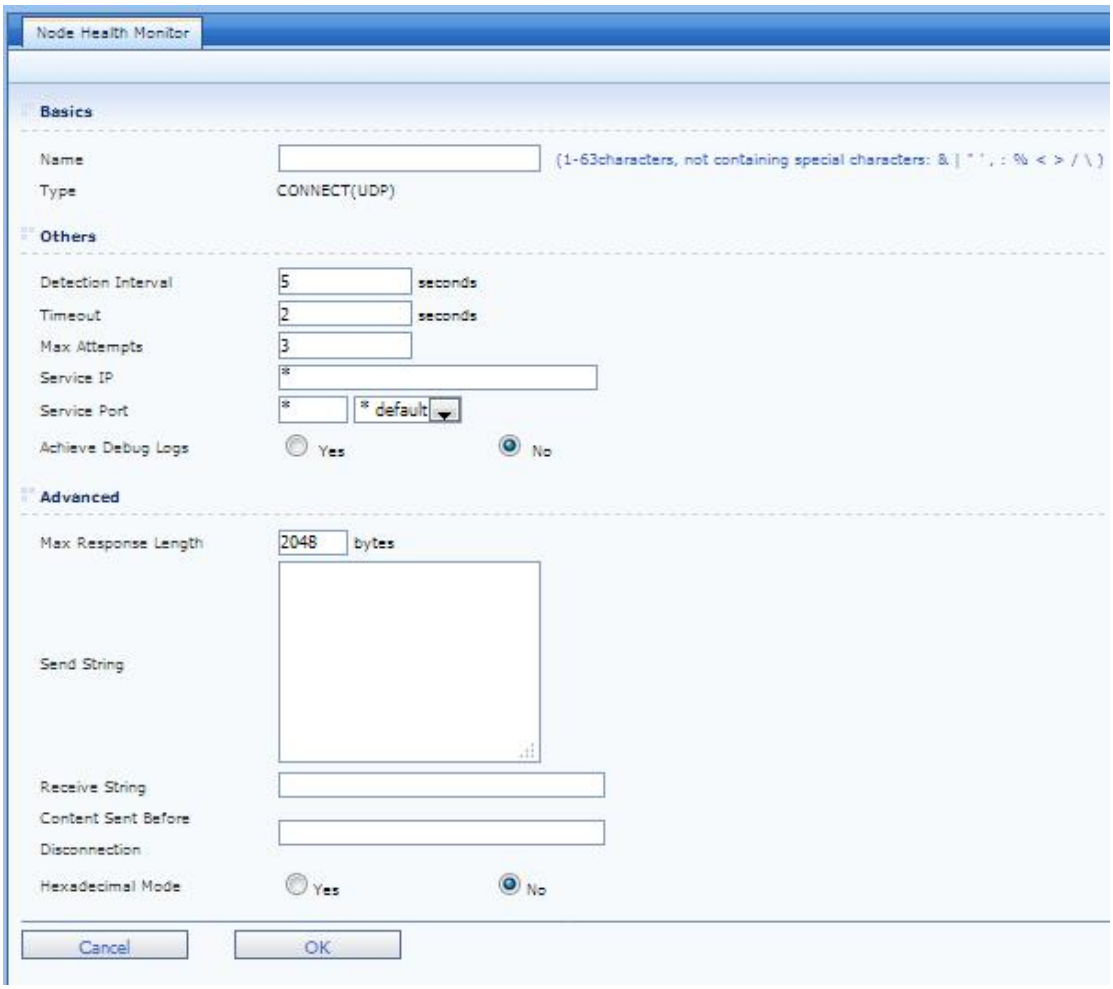
Content Sent Before Disconnect: Specifies the contents sent in the packet before connection is closed.

Hexadecimal Mode: Choose whether contents sent and received is in hexadecimal.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

7.4.4 Connect(UDP)

For **CONNECT(UDP)**-based node monitor, the ADC will initiate a UDP connection to the node, to probe the status of the node. The following are the properties about a **CONNECT(UDP)**-based node monitor:



Service Port: Specifies the ports being watched. You can select **default**, **http**, **ftp, smtp, pop3, imap, https** or **other** to monitor the standard port. When **other** is selected, it is allowed to specify other ports.

Archive Debug Logs: Choose whether to archive debug log of CONNECT(UDP)-based node monitoring. If **Yes** is selected, the related debug logs will be store in logs database on the ADC.

Max Response Length: Specifies the maximum length of contents in response, in byte.

Send String: Specifies the contents sent after connection setup.

Receive String: Specifies the contents must be contained in received packet.

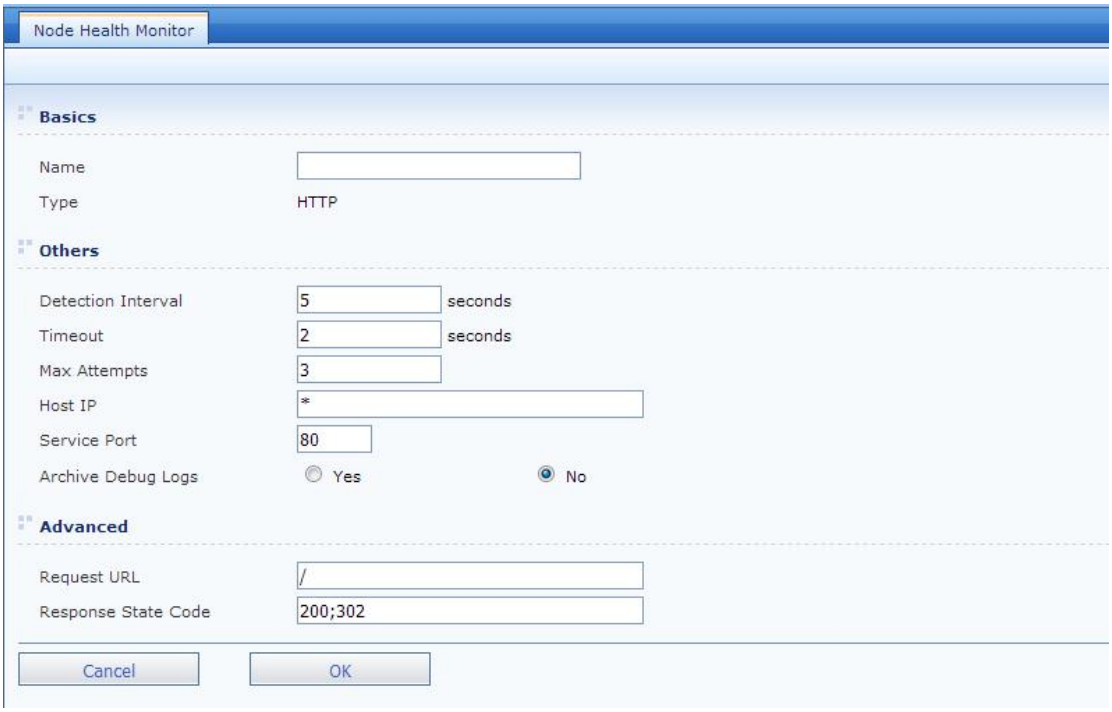
Content Sent Before Disconnect: Specifies the contents sent in the packet before connection is closed.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Hexadecimal Mode: Choose whether contents sent and received is in hexadecimal.

7.4.5 HTTP Monitor

The following are the properties about an **HTTP**-based node monitor:



Service Port: Port of HTTP service. Default is 80.

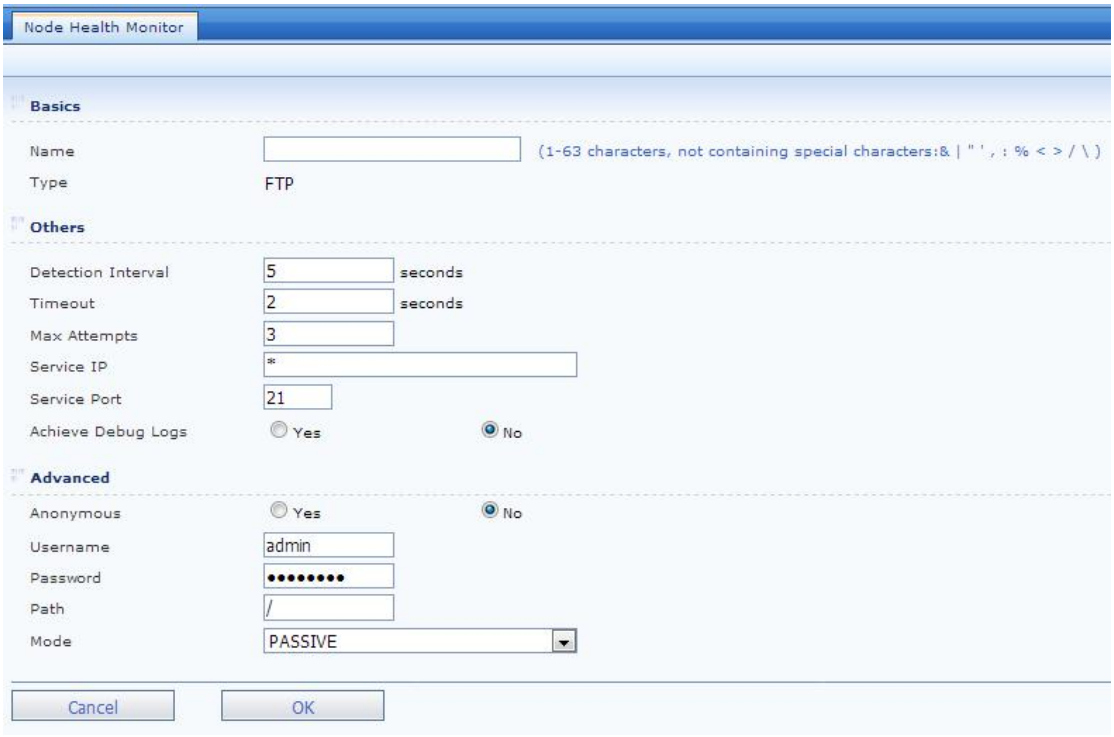
Request URL: Specifies the URL that can be identified automatically and watched. The following are URL examples: a). http://www.abc.com; b). www.abc.com; c). /a/b

Response State Code: Specifies the response state code of HTTP server. This can give hint that if the server is online or offline.

7.4.6 FTP Monitor

The following are the properties about an **FTP**-based node monitor:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Service Port: Port of FTP service. Default is 21.

Archive Debug Logs: Choose whether to archive debug log of **FTP**-based node monitoring. If **Yes** is selected, the related debug logs will be store in logs database on the ADC.

Anonymous: Choose whether to log in to the FTP server anonymously.

Username, Password: Specifies the account used for login to the FTP server.

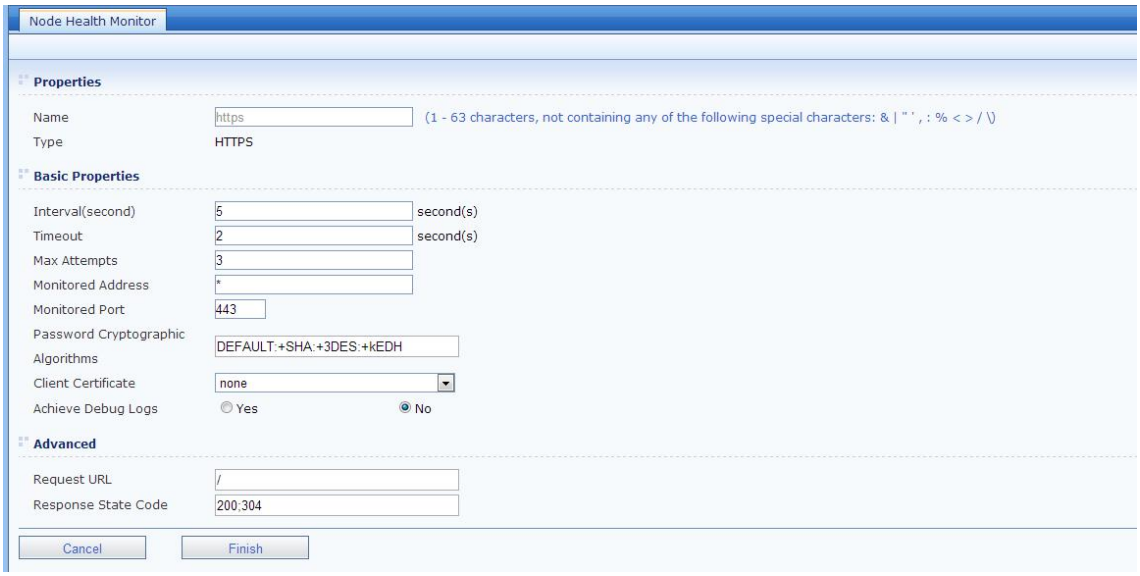
Path: Specifies path of the FTP server.

Mode: Specifies operating mode of the FTP server.

7.4.7 HTTPS Monitor

The following are the properties about an HTTPS-based node monitor:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



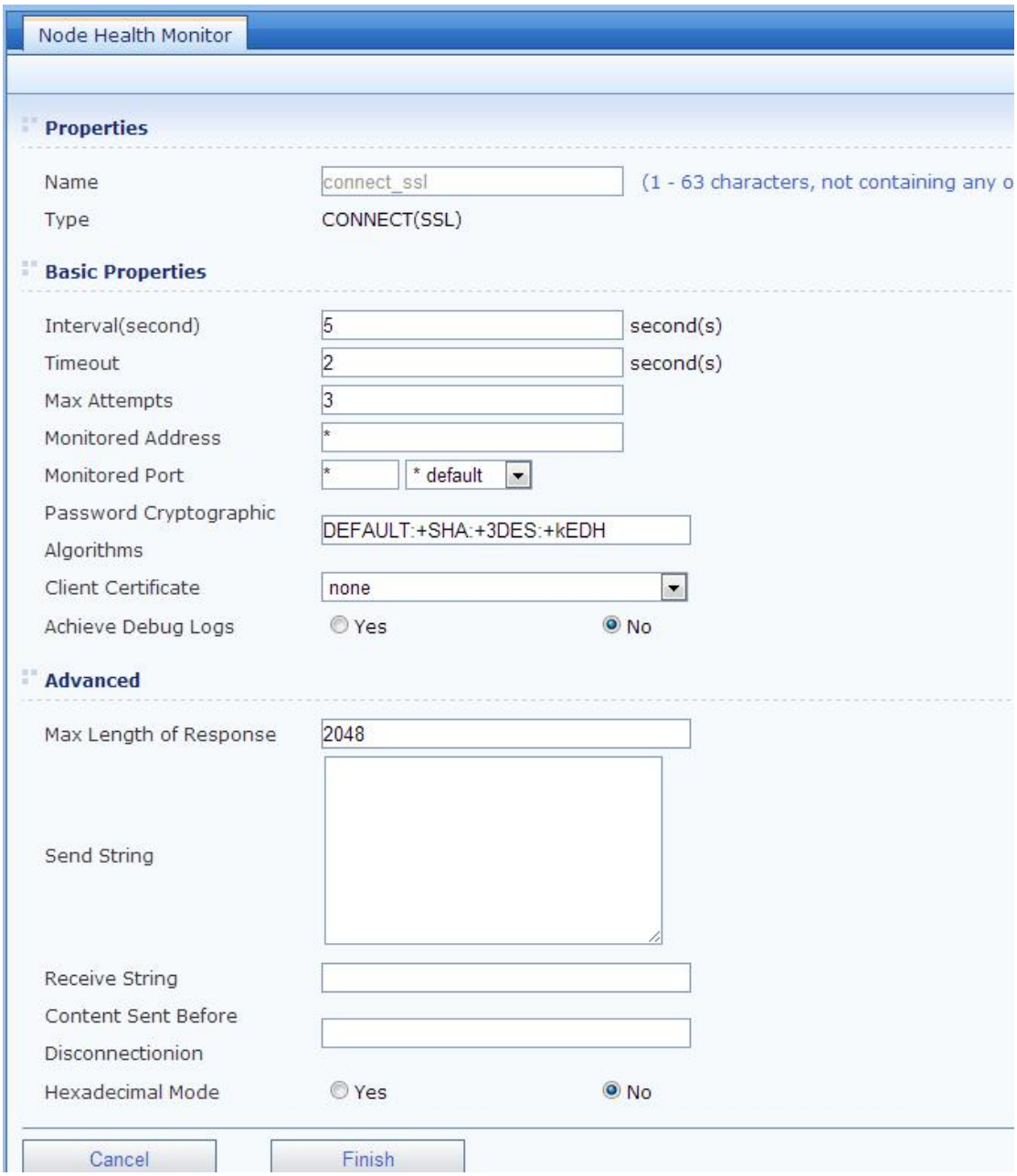
Monitored Port: Specifies monitored port. Default is 443.

Request URL: Specifies the URL that can be identified automatically and watched. The following are URL examples: a). http://www.abc.com; b). www.abc.com; c). /a/b
Response State Code: Specifies the response state code of HTTP server. This can give hint that if the server is online or offline.

7.4.8 Connect(SSL) Monitor

Connect(SSL) is used to monitor on service nodes that use SSL encryption,as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Monitored Port :Click it to select http,tp/smtp/pop3/imap/https or other type port,and when you select other you can custom port

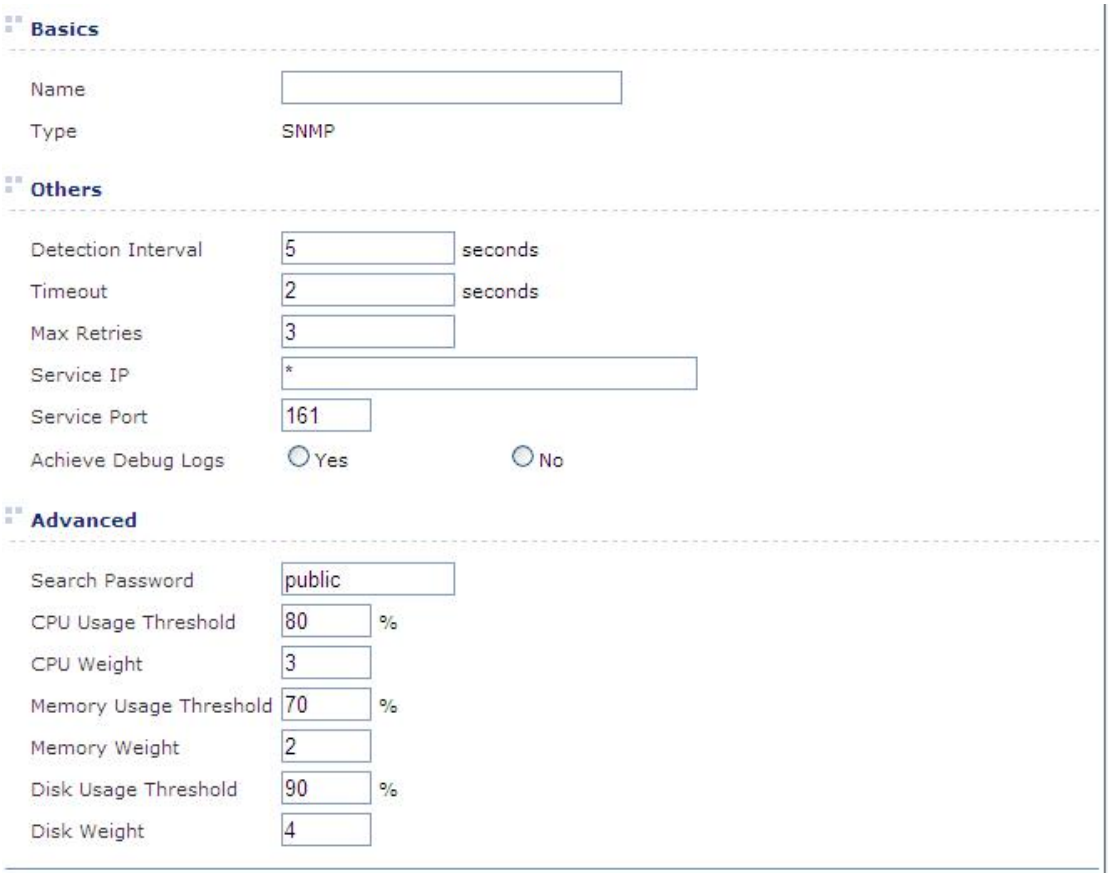
Client Certificate is used to whether submitting client certificates for authentication when configuring HTTPS monitoring.Certificate configuration refer to Chapter 6.6 for details.

Client Certificate is used to whether submitting client certificates for authentication when configuring HTTPS monitoring.Certificate configuration refer to Chapter 6.6 for details.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

7.4.9 SNMP Monitor

The following are the properties about an **SNMP-**based node monitor:



Service Port: Specifies the ports being watched. Default is 161.

Archieve Debug Logs: Choose whether to archive debug log of SNMP-based node monitoring. If Yes is selected, the related debug logs will be store in logs database on the ADC.

Search Password: Specifies the community string. Default is **public**. You can also set it to some other value according to your specific case.

CPU Usage Threshold: Specifies the upper limit of CPU usage. If CPU usage exceeds this threshold, the node is thought busy.

CPU Weight: Specifies the weight of the CPU, which is used in node load balancing mode **Dynamic feedback** (Refer to 6.5 Node Pool for details).

Memory Usage Threshold: Specifies the upper limit of memory usage. If memory usage exceeds this threshold, the node is thought busy.

Memory Weight: Specifies the weight of the memory, which is used in node load balancing mode **Dynamic feedback** (Refer to 6.5 Node Pool for details).

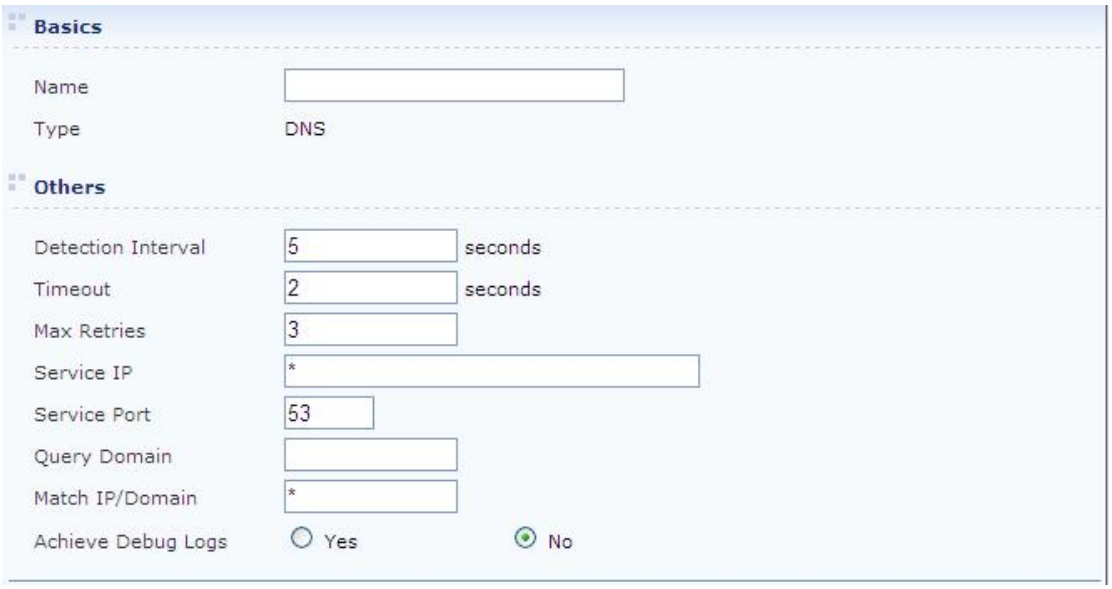
Disk Usage Threshold: Specifies the upper limit of disk usage. If disk usage exceeds this threshold, the node is thought busy.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Disk Weight: Specifies the weight of the disk, which is used in node load balancing mode **Dynamic feedback** (Refer to 6.5 Node Pool for details).

7.4.10 DNS Monitor

The following are the properties about a **DNS**-based node monitor:



Service Port: Specifies the ports being watched. Default is 53.

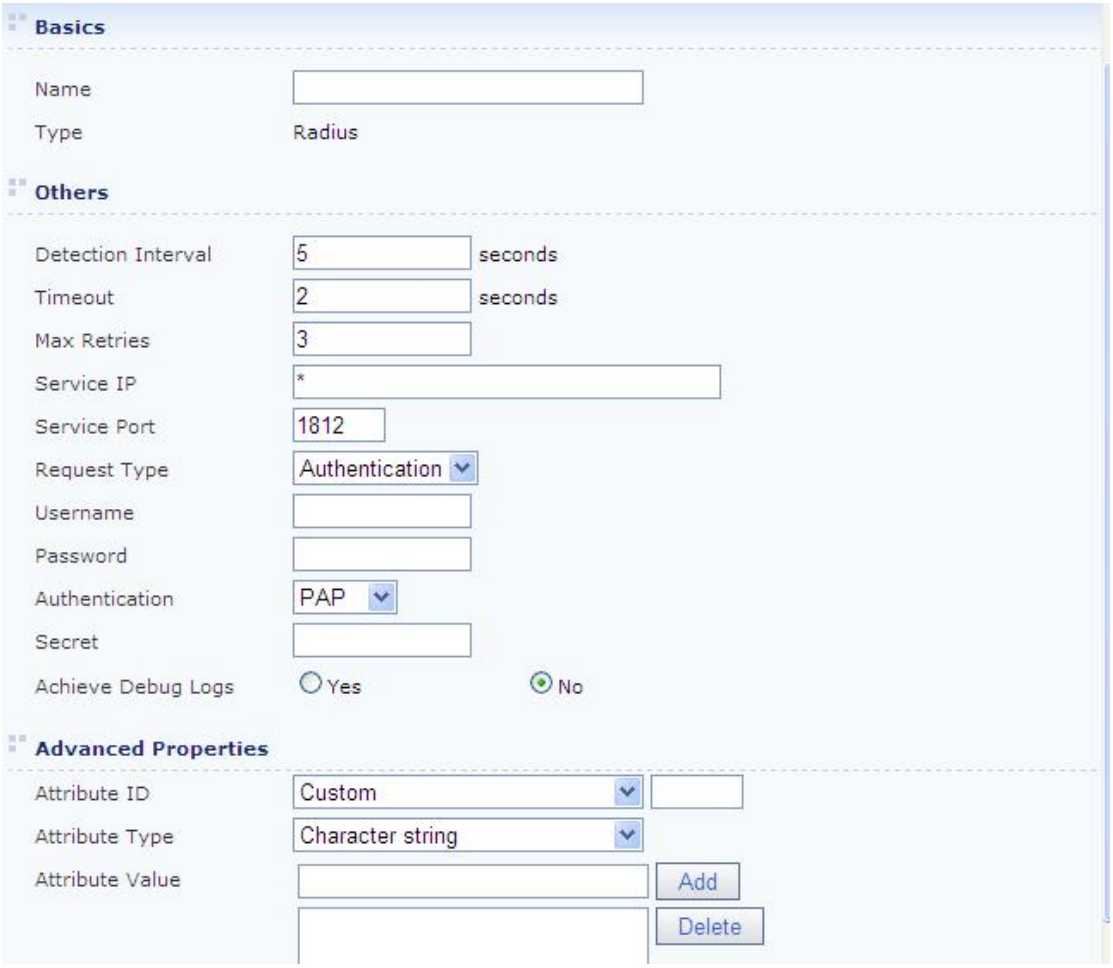
Query Domain: Specifies the domain name sent to DNS server for resolution.

Match IP/Domain: Specifies the address to check if returned information from DNS server is matching. If address is IPv4 address, monitor requests A record. If address is IPv6 address, monitor requests AAAA records. If address is domain name, monitor requests CNAME record. If address is *, monitor requests ANY record.

7.4.11 RADIUS Monitor

The following are the properties about a **RADIUS**-based node monitor:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Service Port: Specifies the ports being watched. Default is 1812.

Request Type: Options are **Authentication** and **Accounting**.

Username, Password: Specifies the account for configuring RADIUS authentication request.

Authentication: Specifies the encryption method used in RADIUS authentication request. Options are **PAP** and **CHAP**.

Secret: Specifies the password used during RADIUS authentication.

Archive Debug Logs: Choose whether to archive debug log of RADIUS-based node monitoring. If **Yes** is selected, the related debug logs will be store in logs database on the ADC.

Attribute ID: Specifies the ID of RADIUS attribute. Attribute can be specified.

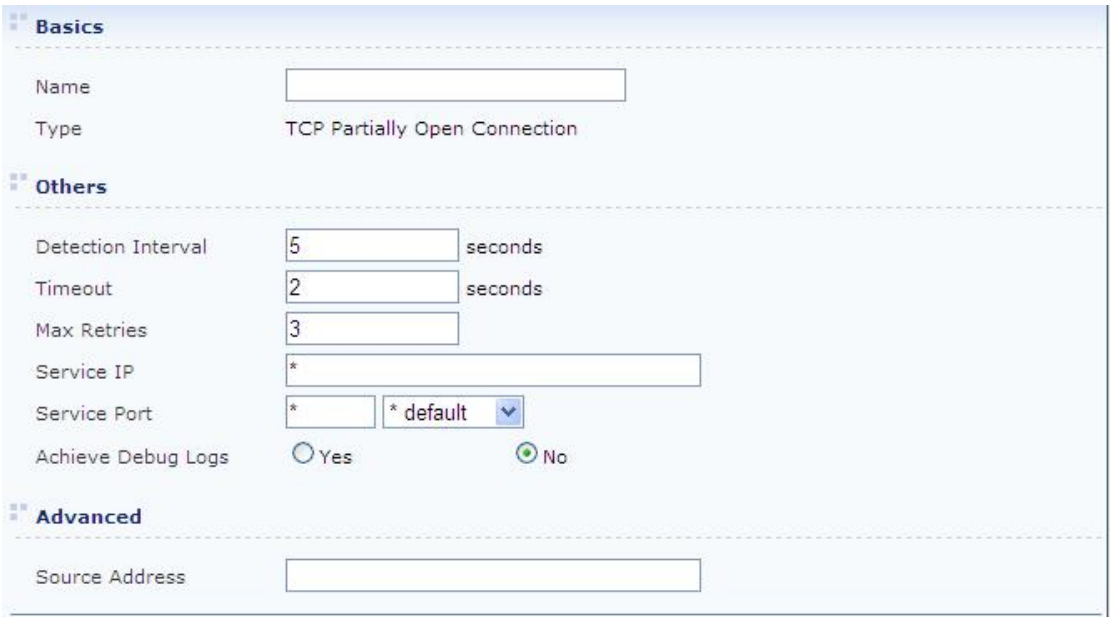
Attribute Type: Specifies the RADIUS attribute on the server. Options are **Character string**, **Decimal string**, **Hex string**, **IP address(v4)** and **IP address(v6)**.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

7.4.12 TCP Partially Open Connection Monitor

The following are the properties about a **TCP partially open connection** based node monitor:



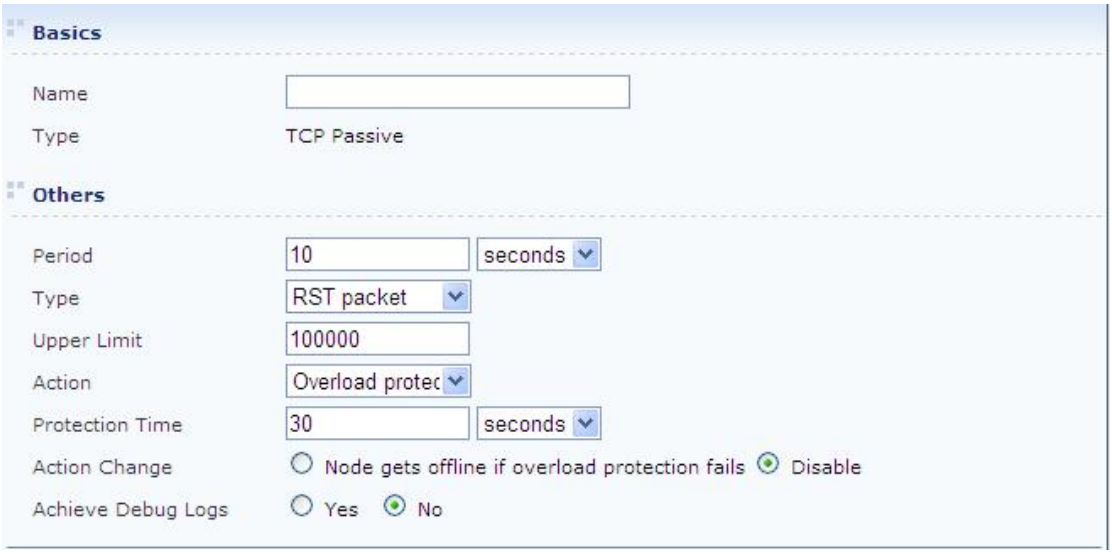
Service Port: Specifies the ports being watched. You can select **default**, **http**, **smtp**, **pop3**, **imap** or **ftp** to monitor the standard port, or specify other ports.

Source Address: Specifies the source IP address of the monitor. It must be IPv4 address of AD network port that watches the node.

7.4.13 TCP Passive Monitor

The following are the properties about a **TCP passive-**based node monitor:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Period: Specifies the period for statistic for monitor.

Type: Select TCP event type to monitor including RST packet and Zero window.

Upper Limit: Deploy the upper limit that the specified TCP events occurring during the statistical period, otherwise strike node action

Action: Specifies the action if the above upper limit is reached, Overload protection or Node gets offline.

Protection Time: Specifies the above action execution time.

Action Change: Select **Disable**, or **Node gets offline if overload protection fails** if number of attempts of closing connection by RST packet reaches the upper limit.

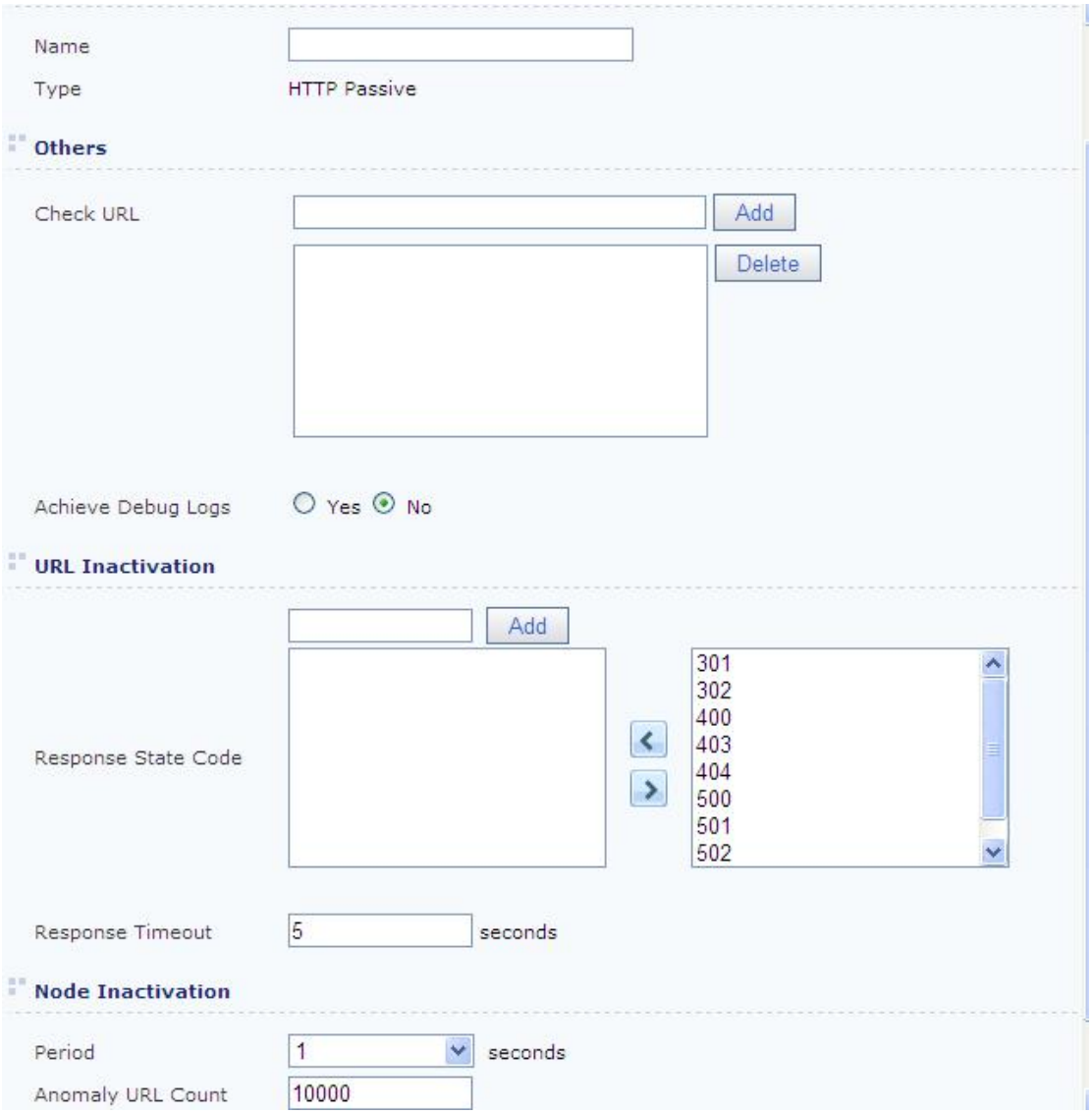
Action Change is used to set whether the monitor implements node offline action after setting in the implementation of overload protection protection over time but node status is still busy.

7.4.14 HTTP Passive Monitor

The following are the properties about an **HTTP passive**-based node monitor:

Click HTTP passive-based node monitor to monitor state monitoring node by monitoring the HTTP request response status code,as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Response State Code: Specifies the state code in response to check whether URL is invalid. That is to say, when this state code in response is matched, the URL is thought invalid.

Response Timeout: Specifies the timeout to receive response. If no response is received in due time, the URL is thought invalid.

Period: Specifies the period for checking URL validity.

Anomaly URL Count: During the specified period, if number of anomaly URL reaches this value, the node is though invalid.

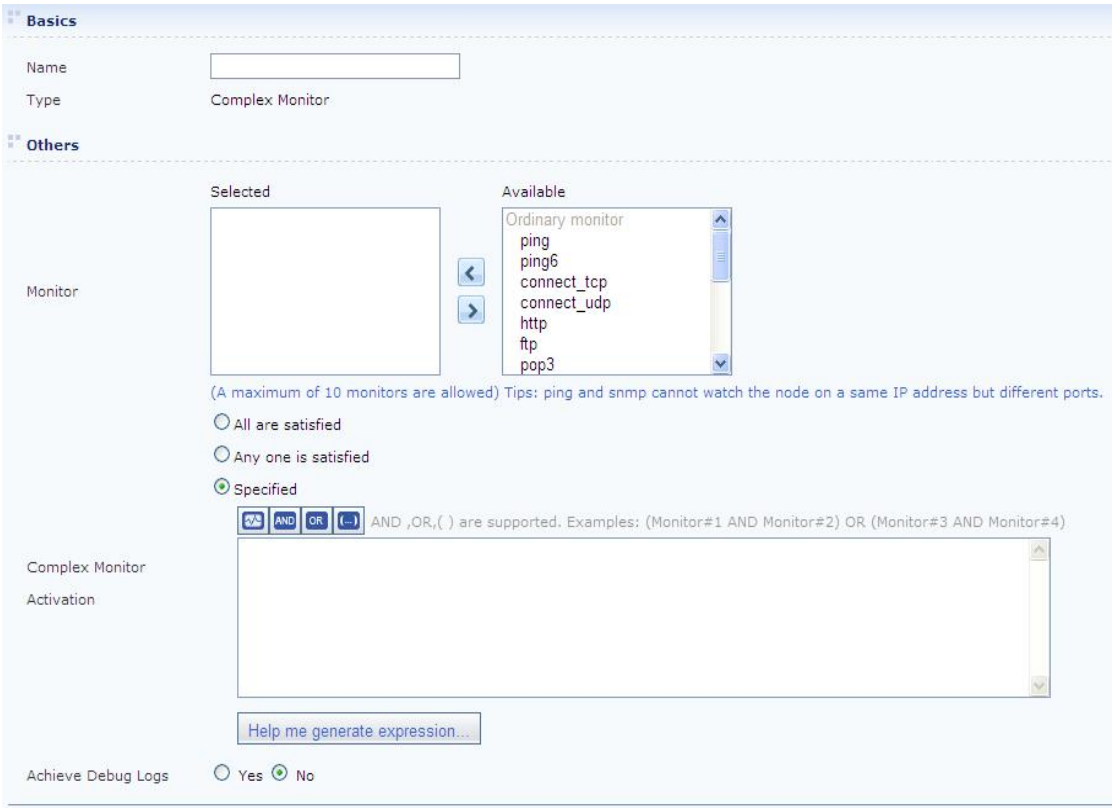
7.4.15 Complex Monitor

The following are the properties about a **Complex** monitor:

Click Complex monitor to select a series of monitors combination and monitor on nodes,as

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

shown in the following figure:



Monitor: Select more than one monitors from the available monitor list.

Complex Monitor Activation: If **All are satisfied** or **Any one is satisfied** is selected, all or any of the selected monitors must be satisfied. You can also select **Specified** to require specified monitor satisfied(which could be with **OR** or **AND** logic).

Click the icon to select and insert a selected monitor; click the AND icon to insert an **AND** into the statement; click the OR icon to insert an **OR** into the statement; click the () icon to insert a parenthesis.

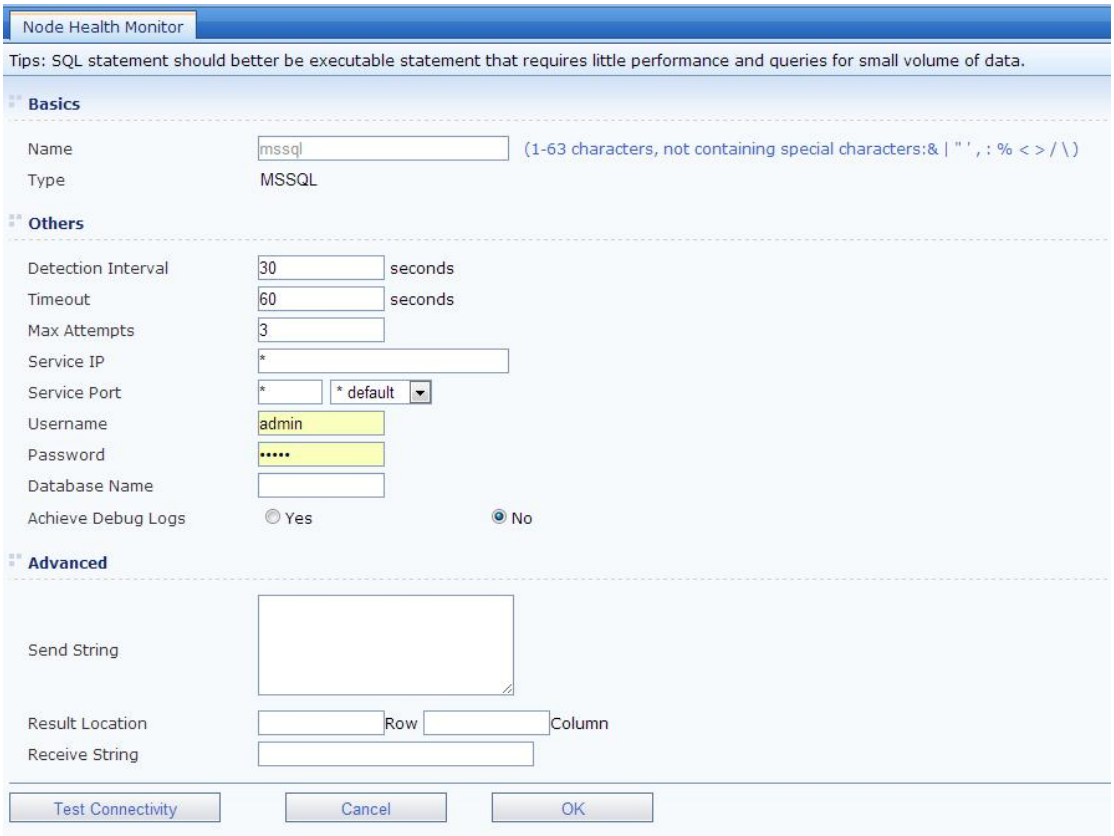
Once the statement is completed, click **Help me generate expression** button to generate the expression

Archive Debug Logs: Choose whether to archive debug log of complex node monitoring.

7.4.16 MYSQL Monitor

The following are the properties about a **MYSQL-based node monitor:**

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Detection Interval: Node Health monitor node to obtain the state of the node frequency, is just after how long to monitor relative to the previous monitoring

Timeout: Timeout of node health monitor node execution

Max Retries: Maximum number of execution attempts after exiting because of timeout or other abnormal situations.

Service IP: Specifies the IP address of MYSQL database or * (indicates all addresses).

Service Port: Specifies the ports or MYSQL database. Default includes ports of **ORACLE**, **MSSQL** and **MYSQL**. To set it to port of other database, select **other** and enter the port number.

Username, Password: The account used to log in to the database and execute the SQL statement. It must have the privilege to execute SQL statement.

Database Name: Specifies name of the database against which SQL statement is executed.

Archive Debug Logs: Choose whether to archive the related debug logs.

Send String: Specifies the SQL statement,please try to use executable SQL statement do not wear performance and with small data size.

Result Location: Specifies where should the result be located in the returned data.

Receive String: Specifies what contents should the returned result of SQL statement execution contain.

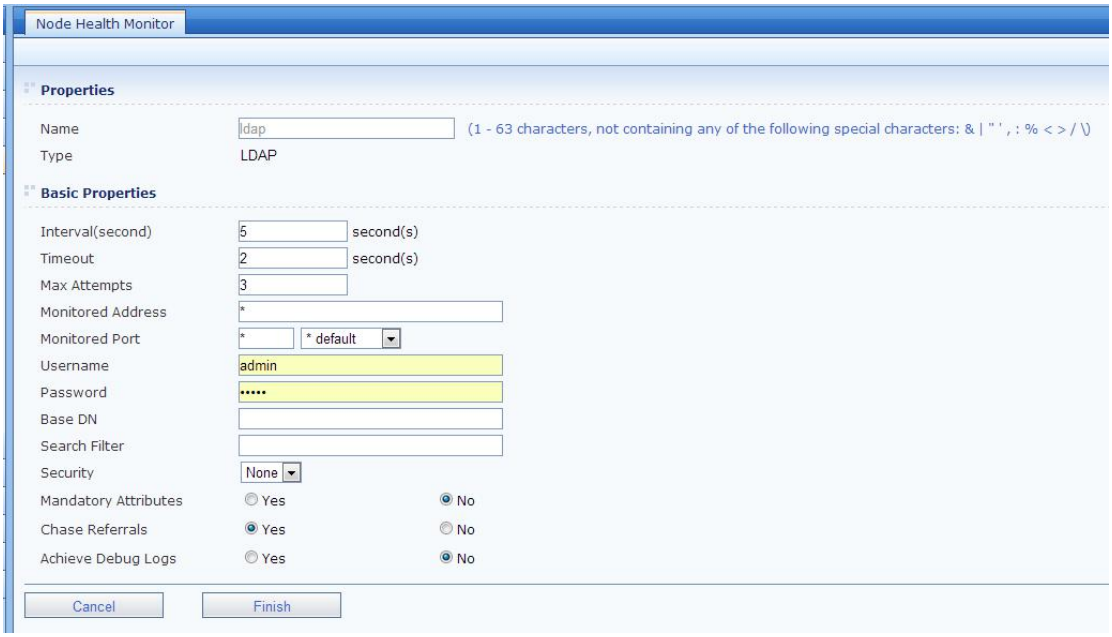
To save the settings, click **OK**; to give up the settings, click **Cancel**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Test Connectivity is used to test database connections,input server address and port,click Test to test and show results.

7.4.17 LDAP Monitor

The following are the properties about a **LDAP node monitor:**



Username indicates user name if monitored goal needs authentication.

Password indicates password if monitored goal needs authentication.

Base DN indicates the location in LDAP tree when health test is started from monitor,such as dc=bigip-test,dc=net.

Search Filter : Monitor search for specified LDAP secret key such as objectclass=*.

Security specifies the security protocol type to connect with goal.

Mandatory Attribuates indicates whether the goal must contains attributes in the response.

Chase Referrals indicates whether it will convert after receiving LDAP quotations ,default choice is positive.

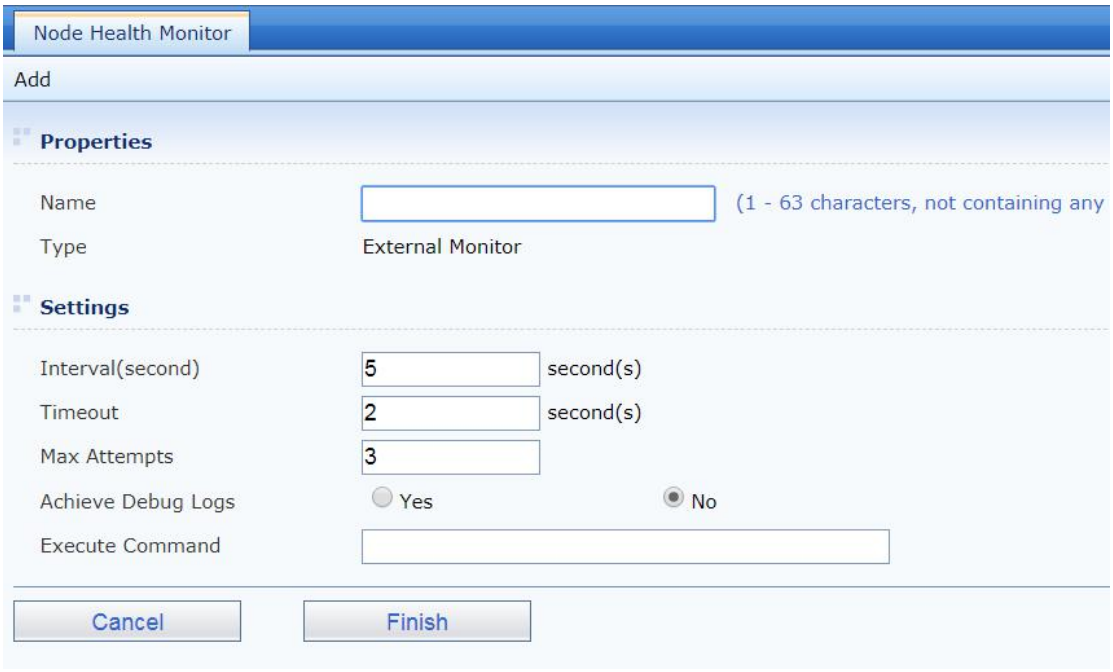
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Archive Debug Logs will print node health monitor's debug log in service logs.

Click **Cancel** to cancel this deployment.Click **Finish** to finish this deployment.

7.4.18 External Monitor

The following are the properties about a **Outer Application node monitor:**



Detection Interval: Node Health monitor node to obtain the state of the node frequency, is just after how long to monitor relative to the previous monitoring

Timeout: Timeout of node health monitor node execution

Max Retries: Maximum number of execution attempts after exiting because of timeout or other abnormal situations.

Archive Debug Logs will print node health monitor's debug log in service logs.

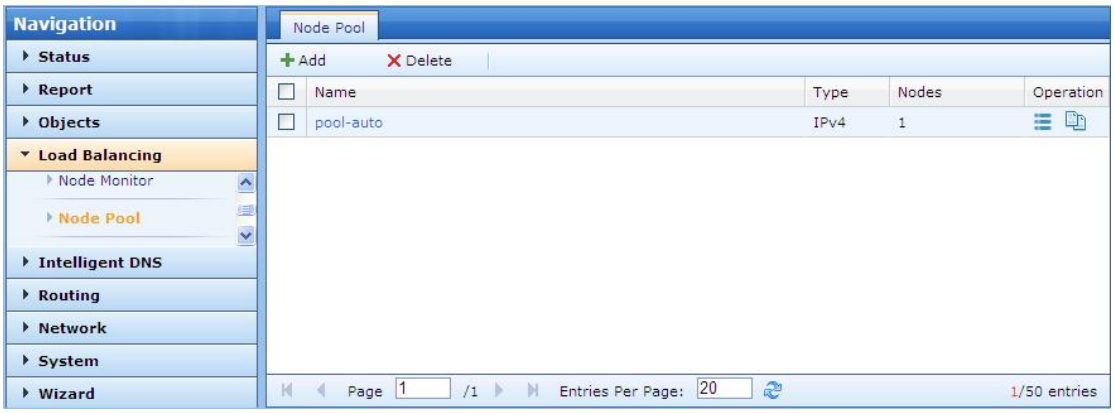
Executable code specifies the code monitor executes including inner variable,${rs_ip} represents ip and ${rs_ip} represents node port.If the nodes are healthy,it will print "monitor:success" to standard output, otherwise the node are unhealthy.we take java for example,java -cp /usr/monitor HttpMonitorDemo ${rs_ip} ${rs_port};for python,python /usr/monitor/HttpMonitorDemo.py ${rs_ip} ${rs_port}.(To ensure that the commands run properly, the Java specifies the search path, and the python uses absolute path)

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Click **Cancel** to cancel this deployment.Click **Finish** to finish this deployment.

7.5 Node Pool

A node pool includes a bunch of nodes that are used to deliver applications to external networks, and specifies the way how server load are kept balanced. Node pool is often referenced by policy and virtual service.



Click node pool name and there comes out a button **view node** ,then click it to jump to node list page.

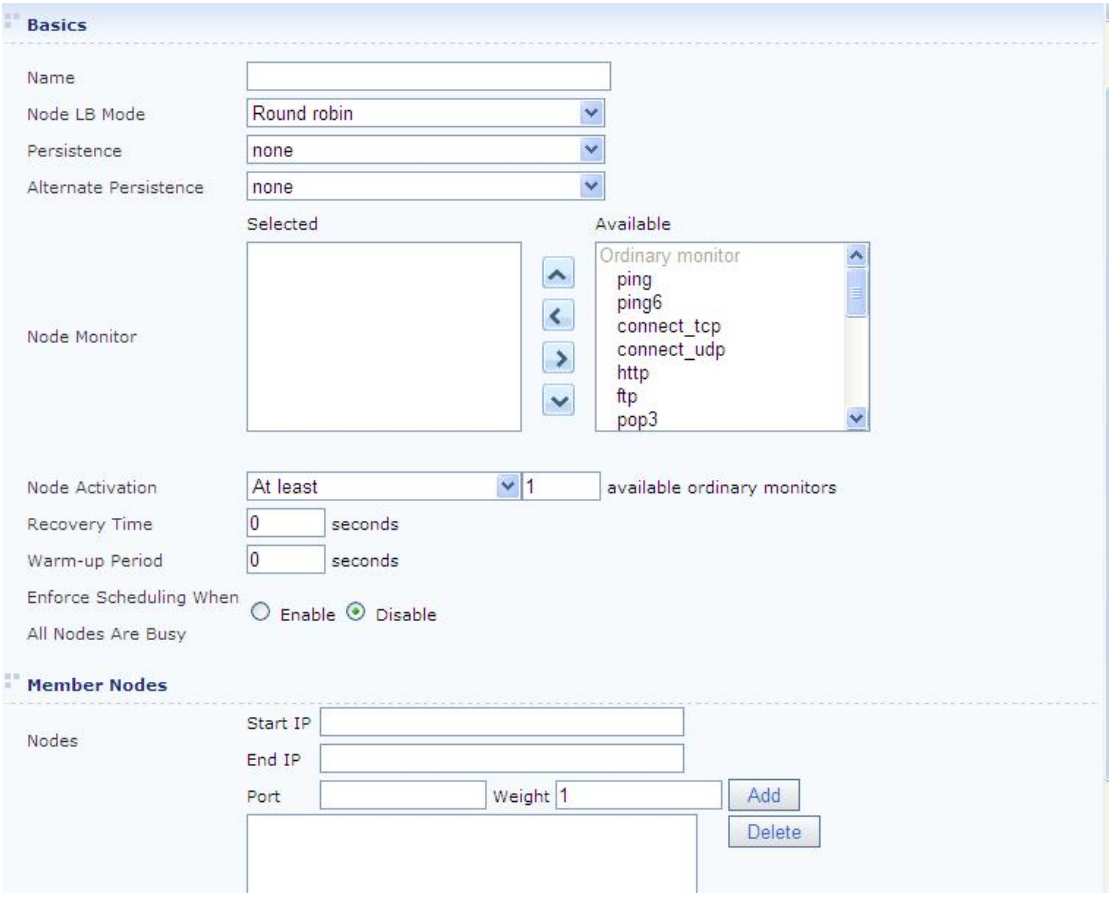
To remove a node pool, select the pool and click **Delete**.

To view the node members in this node pool, click the **Node List** icon in the **Operation** column.

To clone a node pool and create a new one, click the **Clone** icon in the **Operation** column.

To create a new node pool, click **Add** to enter the following page.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Node LB Mode: Select the load balancing mode for the nodes in this pool. The following are description of each option:

Round robin: Nodes take turns to undertake load.

Weighted round robin: Load is scheduled to node with higher weight.

Weighted least connections: Load is scheduled to node with higher weight and least connections.

Least response time: Load is scheduled to the node that takes the least time to respond.

Dynamic feedback: Load balancing is achieved by choosing the node after considering the SNMP monitoring result, CPU weight, memory weight and disk weight settings in the SNMP-based node monitor.

Priority: Load is scheduled to the node with higher priority. When node with higher priority is unavailable, load is scheduled to node with relatively lower priority.

Hash: Based on the specified hash field (such as URL, HOST, etc), hash values are obtained, and load are then scheduled to the nodes in the pool evenly.

Persistence: This is persistence method. To create or edit persistence, you can go to **Load Balancing** > **Persistence**.

Alternate Persistence: This is the alternative of session persistence. It comes into use when

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

the preferred persistence turns invalid.

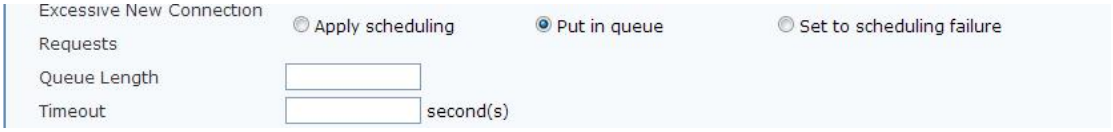
Node Monitor: Select the monitor and move it from the available monitor list. The selected monitors will be used to probe node status.

Node Activation: Specifies how many node monitors must give positive result to prove that the node is available. If **All** is selected, all the node monitors must give positive result.

Recovery Time: Specifies how long a node can recover to normal to provide service. Before the node recovers, the ADC does not forward requests to the node immediately after health check.

Warm-up Period: Specifies the period during which increasing requests are forwarded to the node and reach the maximum. Once a node recovers, it does not receive all requests immediately after recovery but takes the load gradually until load reaches the maximum.

Excessive New Connection: choices are **Apply scheduling,Put in queue** and **Set to scheduling failure** and **put in queue** policy has to deploy queue length and timeout.

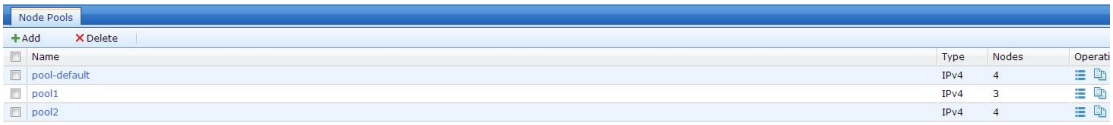


Connections selects **All in any status** by default which includes the connections of all status and All in established status which only statistic successful connections is also supported.Connections show in node status.

Enter the IPv4 or IPv6 address into the **Start IP** and **End IP** address fields. Note that IP address must be either IPv4 or IPv6 addresses. **Port** is the port for monitoring; if not specified, it is the same with virtual service port. **Weight** is useful for Weighted round robin and Weighted least connection LB mode. Finally, click the **Add** button to add the address/port entry. To delete an entry from the list, select that entry and click **Delete**.

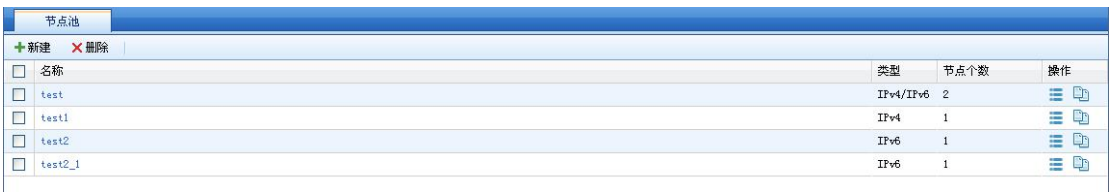
To save the settings, click **OK**; to give up the settings, click **Cancel**.

The page after deploying is as shown in the following figure:



Click **Clone** to select part deployments in the node which is in the selected pool and deploy a new node pool.

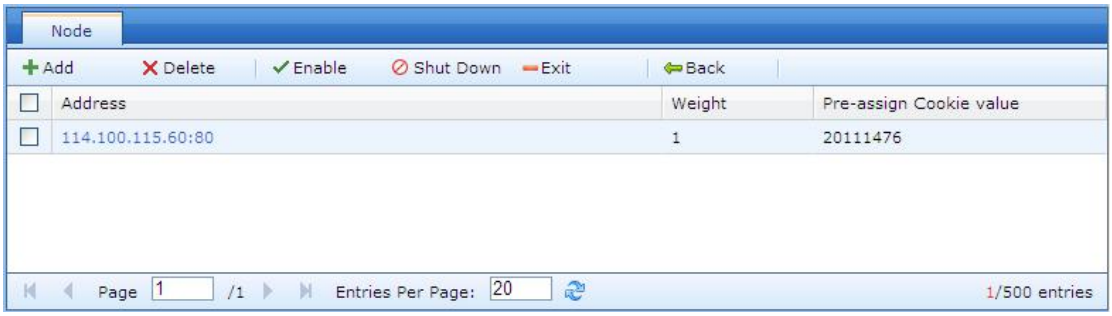
The page after deploying is as shown in the following figure:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

If you want to make an advanced deployment such as make a constriction on node's connections,etc,you can edit on defined node in the pool.Node list is used to deploy nodes in the pool.

If the **Node List** icon is clicked, the following node tab will appear, as shown in the figure below:



The attributes below **Node** include **Address**,**Weight** and **Pre-assign Cookies value**.

To enable a node, select the item and click **Enable**.

To disable or shut down a node, select the item and click **Shut Down**. Disabled node will still be active and keep the existing connections but not allow new connections.

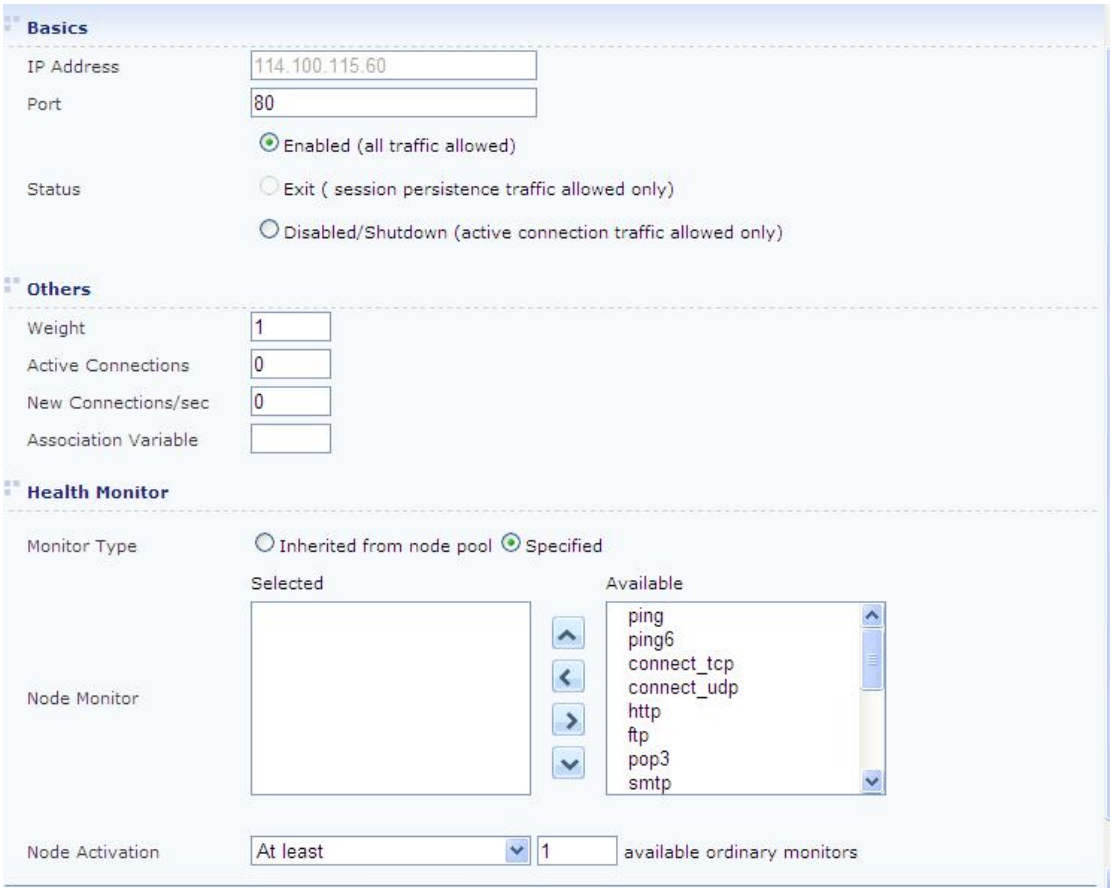
To have a node keep the existing connections and session persistences but not allow new connections before the complete exit, select the item and click **Exit**. This way of exist does not interrupt running businesses.

To remove a node from the node pool, select the item and click **Delete**.

To add a new node into the pool, click **Add**. Please refer to the following section.

To edit a node, click on the node name to enter the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



IP Address: Specifies the IP address of the node. Unlike creating a node, this is not editable.

Port: Specifies the port for delivering applications and it is enabled when monitor type is CONNECT and monitor port is default.

Status: Specifies the state of the node, **Enabled**, **Exit** or **Disabled/Shutdown**. Disabled node can keep the exiting active connections but will not allow new connection.

Weight: Specifies weight for load balancing.

Active Connections: Specifies the maximum number of connections could be persisted by the node. 0 means no limitation.

New Connections/Sec: Specifies the maximum of new connections could be establish with the node. 0 means no limitation.

Max HTTP Requests Per :Specifies the maximum of HTTP requests could be establish with the node. 0 means no limitation.

Association Variable: This is the variable rewritten during HTTP header rewriting.

Monitor Type: Specifies whether monitor is inherited from node pool settings or specified. If Specified is selected, select the monitor from the list.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

IP addresses of nodes in a pool must be the same type, IPv4 addresses or IPv6 addresses. IPv4 and IPv6 addresses can co-exist.

Attention:Null pool is ok.

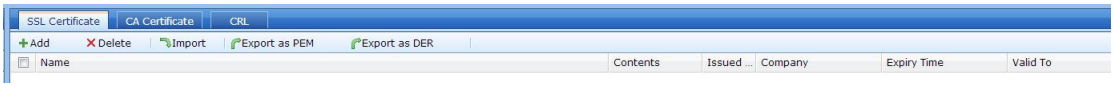
7.6 SSL

SSL(Secure Sockets Layer) is used to establish encrypted connection between the ADC(Application Delivery Controller) and the client.

If the application server has server certificate, you can import that certificate onto the ADC, to reduce load on the server. If the application server has not server certificate, you can generate a server certificate with the local CA on the ADC or apply for a third-party certificate. With a legitimate server certificate, connection between client and ADC can be encrypted, and therefore access to application is encrypted.

The certificate for encryption can be referenced by virtual service settings.

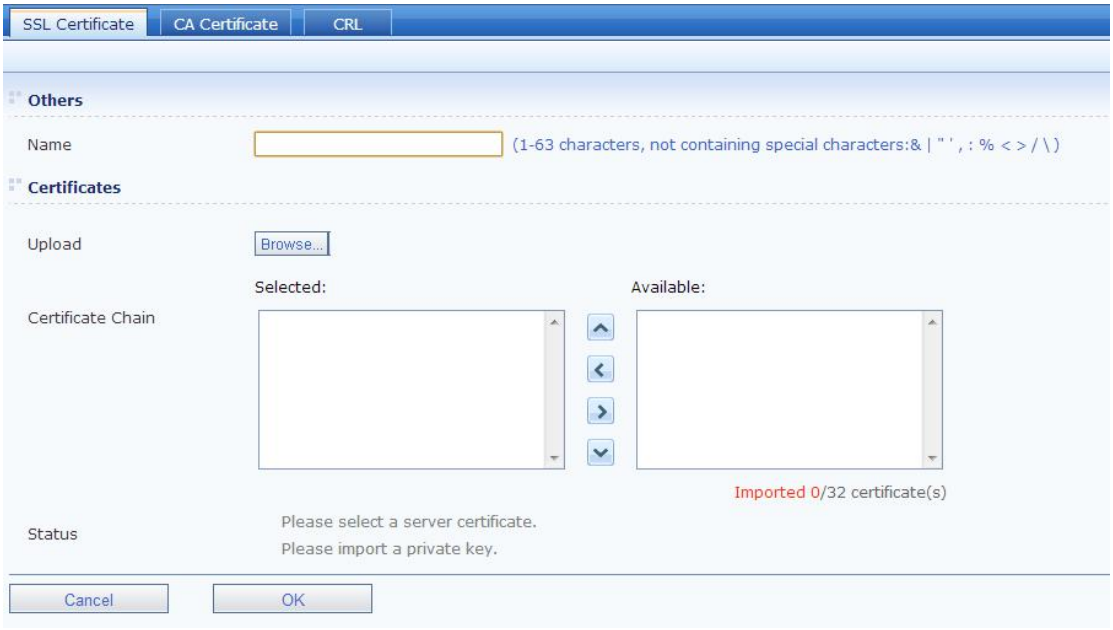
7.6.1 Generating SSL Certificate



To **remove** a SSL certificate, select the item and click **Delete**. Please note that the SSL certificate associated with virtual service cannot be deleted.

To **import** a certificate issued by third-party Certificate Authority(CA), click **Import** to enter the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

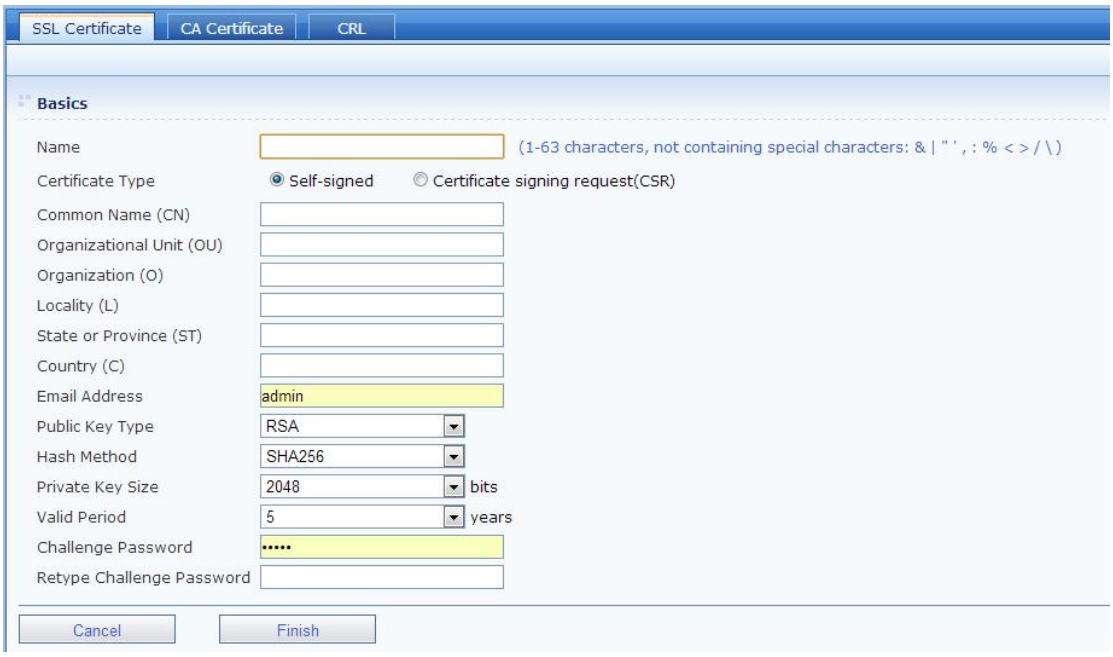


Name: Specifies name of the certificate.

Upload:Click the button and you can import certificate several times.It supports pem,der,pkcs12,pkcs7,etc(postfix are crt/cer/key/pem/der/pfx/p12/pvk/p7b/spc).If certificate includes password it will prompt you to input password and it won't stop unless you have input correct password.You can close it by click "x" in the upper right corner.

Certificate Chain is used to select pointed certificate which supports auto-sort.

To **create** a server certificate, click **Add** and configure the following:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

The following are the contents when the certificate type is **Self-signed** certificate:

Name: Specifies name of the certificate.

Certificate Type: Specifies what you want to create, self-signed certificate or create a certificate signing request(CSR) that needs to be sent to and signed by a third-party CA.

Issued To: Specifies whom this certificate is issued to.

Department: Specifies what department the certificate user is in.

Company: Specifies what company or organization the certificate user is in.

City: Specifies which city the certificate user is in.

State: Specifies which state the certificate user is in.

Country: Specifies which country the certificate user is in. It should be two-letter abbreviation.

Email Address: Specifies email address of the certificate user.

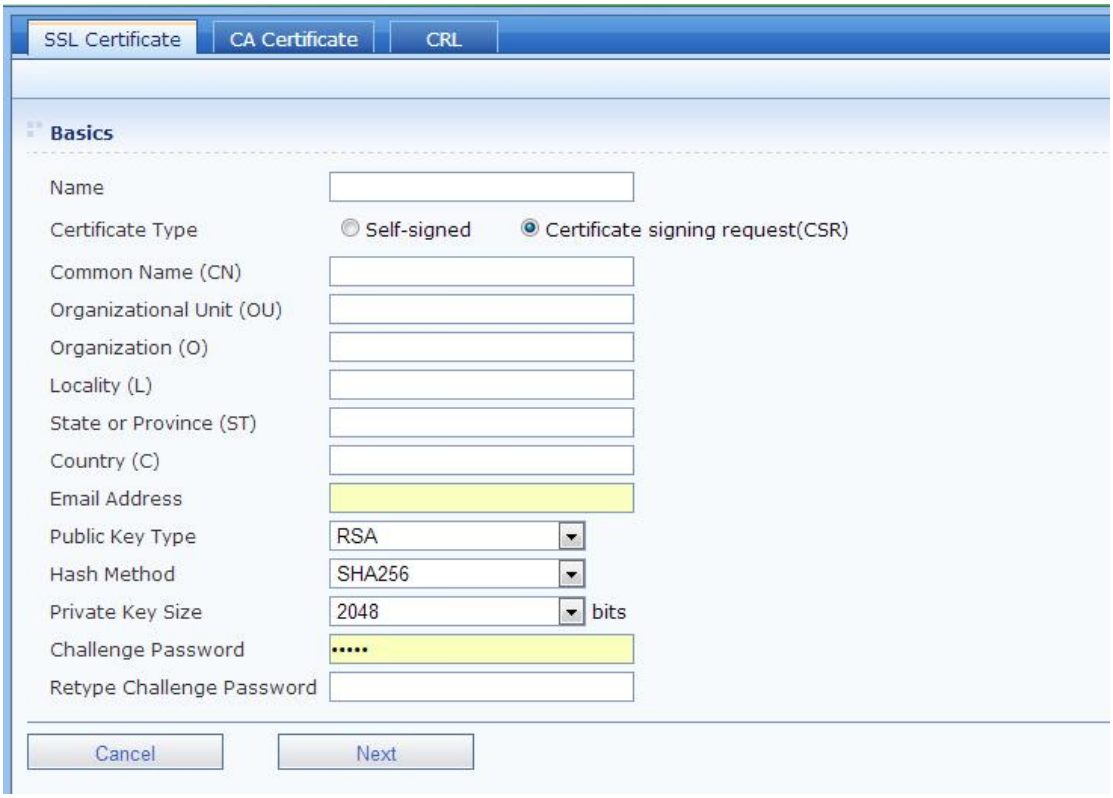
Public Key Type includes RSA,ECDSA and SM2(OSCCA).

Hash Method includes SHA256,SHA1 and SM3(OSCCA).

Valid Period: Specifies after how long a time will the certificate turns invalid.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

The following are the contents when the certificate type is **Certificate Signing Request**:



Name: Specifies name of the certificate.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Certificate Type: Specifies what you want to create, self-signed certificate or create a certificate signing request(CSR) that needs to be sent to and signed by a third-party CA.

Issued To: Specifies whom this certificate is issued to.

Department: Specifies what department the certificate user is in.

Company: Specifies what company or organization the certificate user is in.

City: Specifies which city the certificate user is in.

State: Specifies which state the certificate user is in.

Country: Specifies which country the certificate user is in. It should be two-letter abbreviation.

Email Address: Specifies email address of the certificate user.

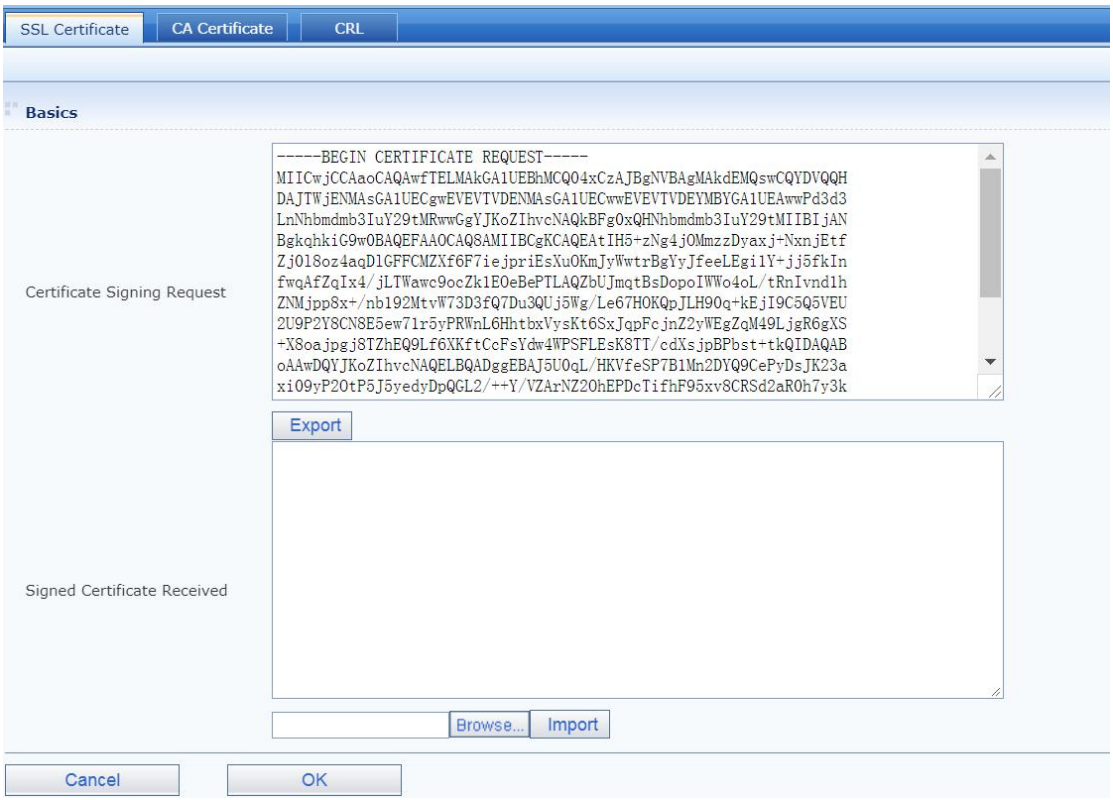
Public Key Type includes RSA,ECDSA and SM2(OSCCA).

Hash Method includes SHA256,SHA1 and SM3(OSCCA).

Private Key Size: Specifies size of the private key of server certificate.

Valid Period: Specifies after how long a time will the certificate turns invalid.

Next: Click this button to generate the certificate signing request, as shown in the following figure:



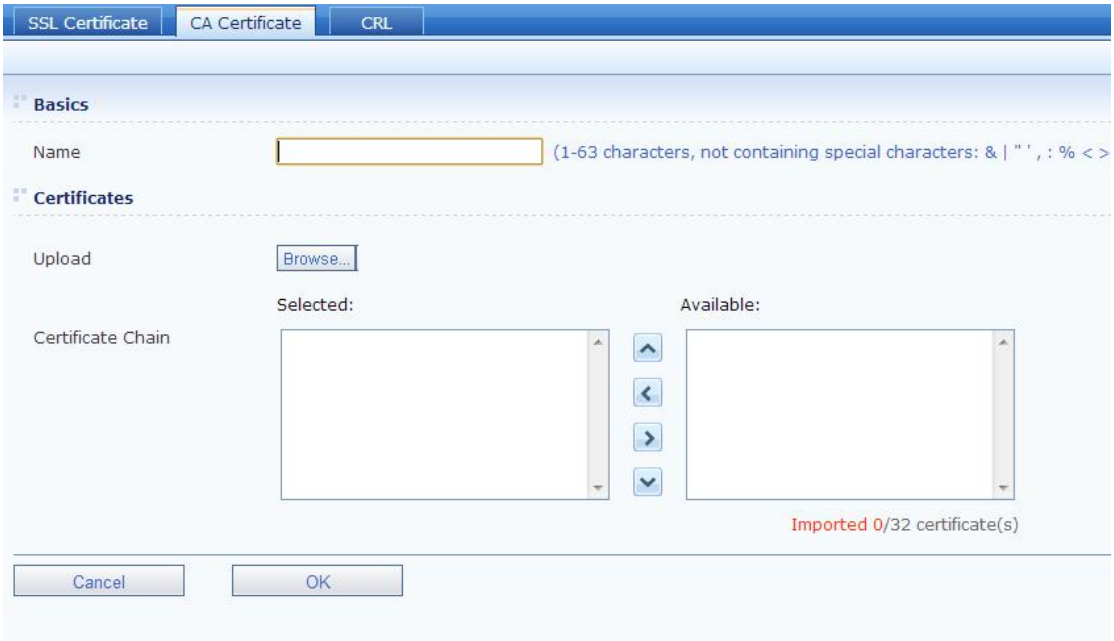
Export as CSR: Click this button to export the CSR contents into a file and send the request to a third-party CA. Once you get the certificate from the third-party CA, enter this page again

and import the third-party certificate onto the ADC simply by clicking the **Browse**, selecting the certificate file and clicking the **Import** key.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

7.6.2 CA Certificate

To add a new root CA certificate, click **Add** and enter the following page:



Name: Specifies the name of the root CA certificate.

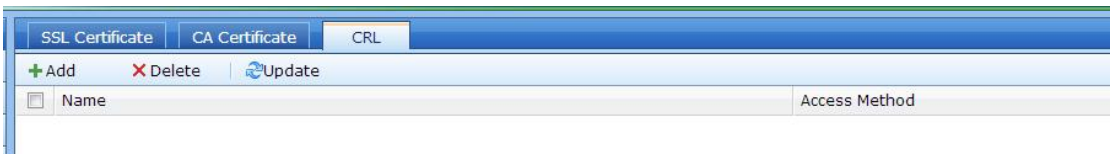
Upload:Click the button and you can import certificate several times.It supports pem,der,pkcs12,pkcs7,etc(postfix are crt/cer/key/pem/der/pfx/p12/pvk/p7b/spc).If certificate includes password it will prompt you to input password and it won't stop unless you have input correct password.You can close it by click "x" in the upper right corner.

Certificate Chain is used to select pointed certificate which supports auto-sort.

Select the certificate which support auto sorting and then click **OK** to add it onto the ADC.

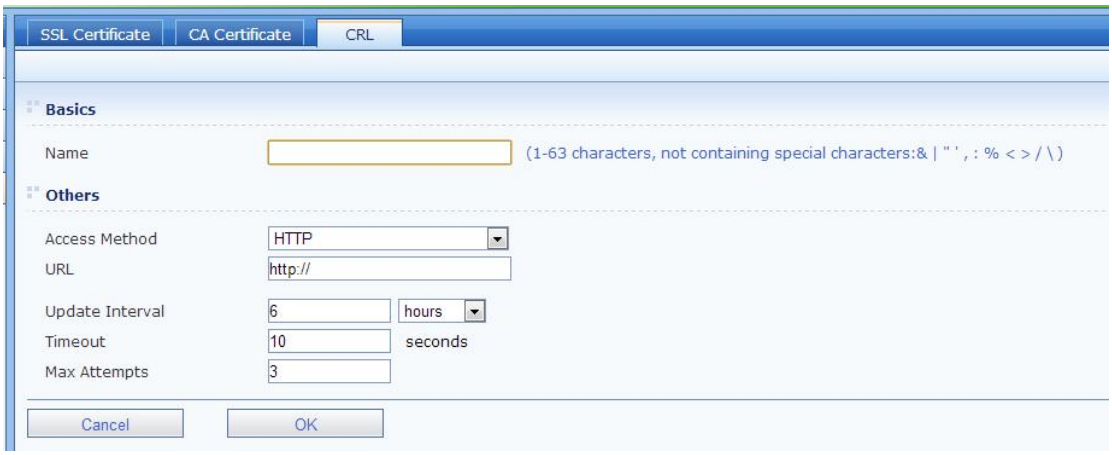
7.6.3 CRL

In this tab, you can specify how CRL(Certificate Revocation List) is obtained and updated.



To add a new CRL, click **Add** and enter the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



The following are the contents when access mode is **HTTP**:

Name: Specifies the name of the CRL entry.

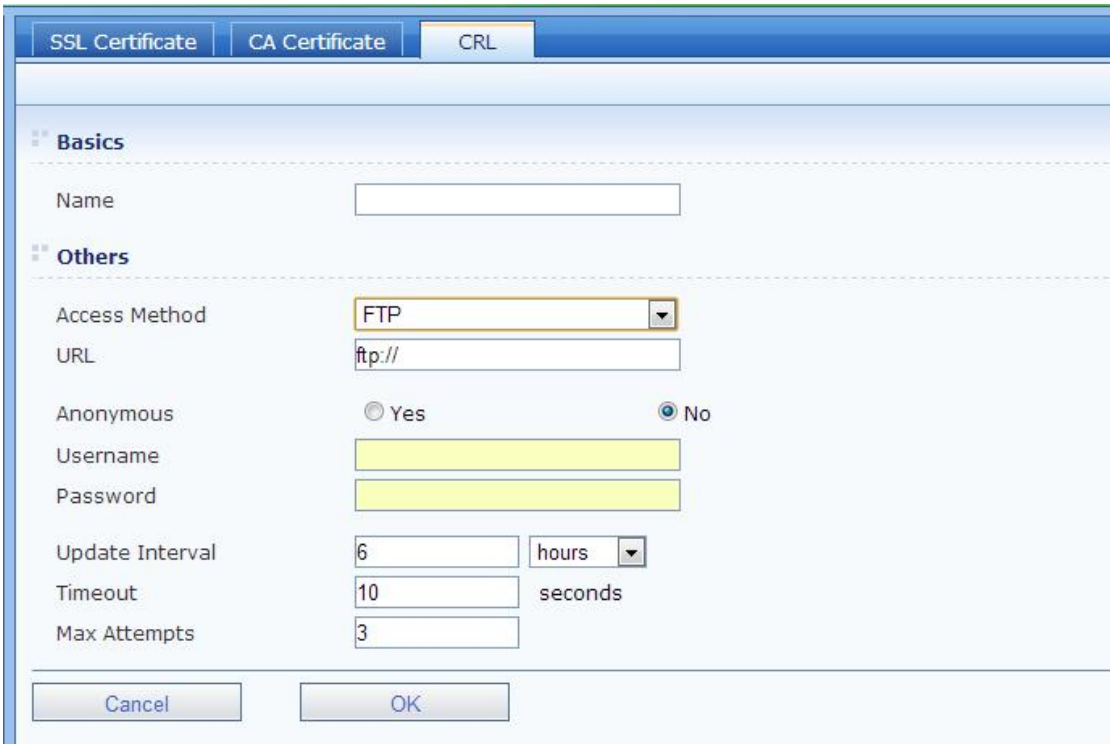
Access Mode: Specifies how the CRL is accessed, via HTTP, FTP or uploaded from local PC.

URL: Specifies the URL address of the CRL.

Update Interval: Specifies how often CRL is downloaded from the above address. Maximum interval is 30 days.

Timeout: Specifies the timeout for updating CRL. If CRL is not obtained in due time, it will try again.

Max Retries: Specifies the maximum number of update attempts.



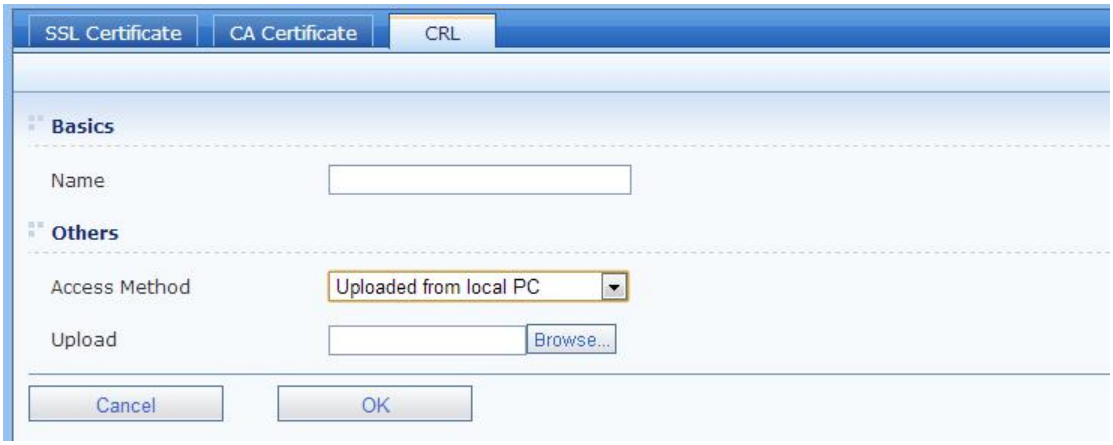
The following are the contents when access mode is **FTP**:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

URL: Specifies the URL address of the CRL.

Anonymous: Select **Yes** if you allow anonymous login to the FTP server. Or select the **No** and specify **Username** and **Password** for access to the FTP server.

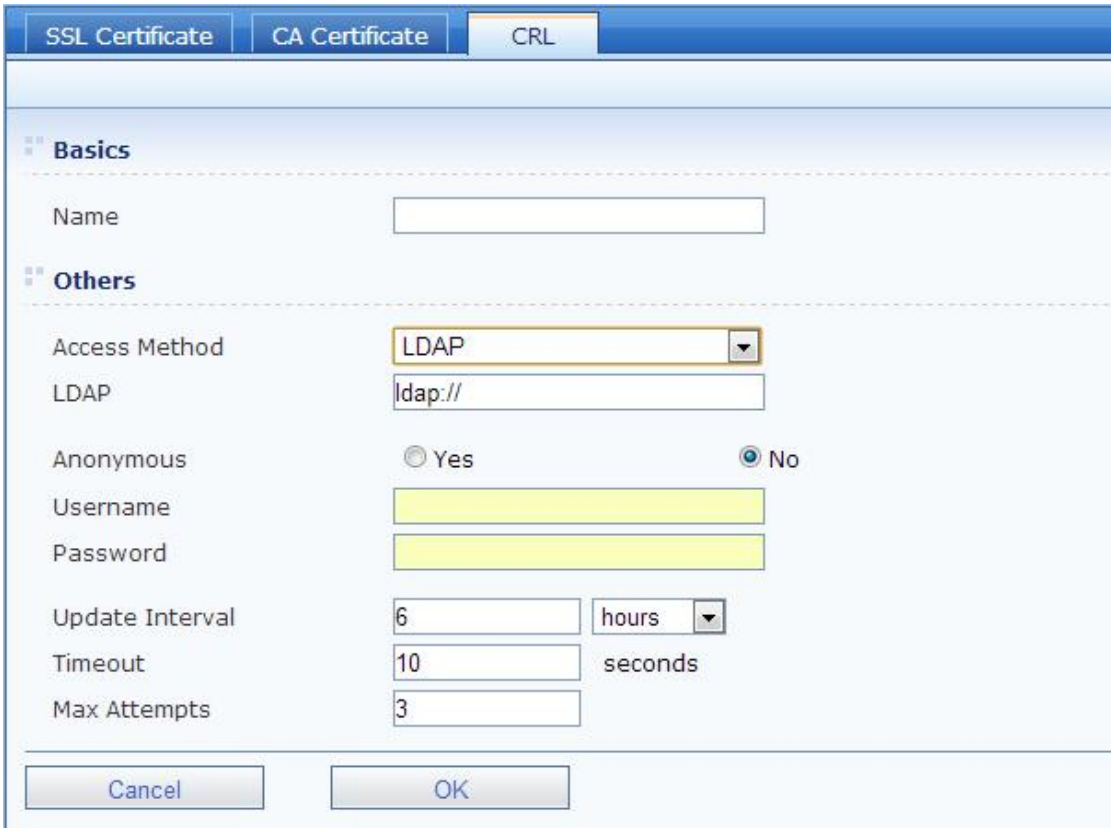
Update Interval: Specifies how often CRL is downloaded from the above address. Maximum interval is 30 days.



If access mode is **Uploaded from local PC**, you can select the file and upload it onto the ADC.

To save the settings, click **OK.**

If access mode is **LDAP**, as shown in the following figure:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Name: Specifies the name of the CRL entry easy to memorize.

Access Mode: Specifies how the CRL is accessed.

LDAP:Specifies how the CRL is accessed.

Anonymous: Specifies whether you are anonymous.

Username:Specifies username LDAP is accessing.

Password::Specifies password LDAP is accessing.

Update Interval: Specifies how often CRL is downloaded from the above address. Maximum interval is 30 days.

Timeout: Specifies the timeout for updating CRL. If CRL is not obtained in due time, it will try again.

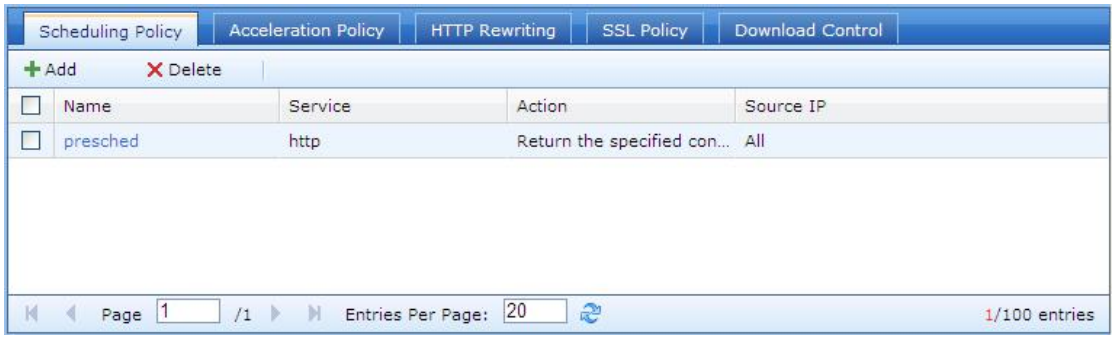
Max Retries: Specifies the maximum number of update attempts.

Click **OK** to save the deployment.

7.6 Policy

7.6.1 Scheduling Policy

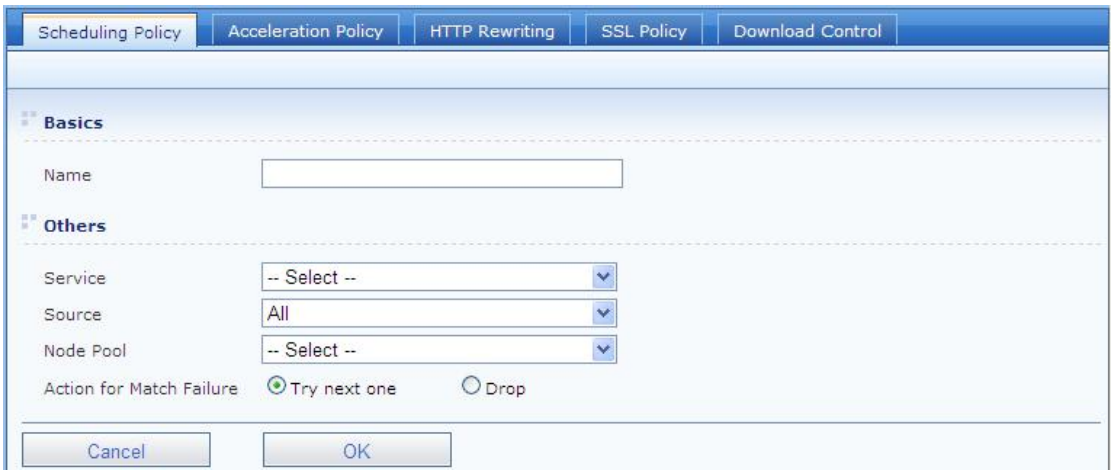
A scheduling policy defines to which node pool the requests from specific users are forwarded.



To delete a scheduling policy, select the policy and click **Delete**.

To add a new scheduling policy, click **Add** and configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

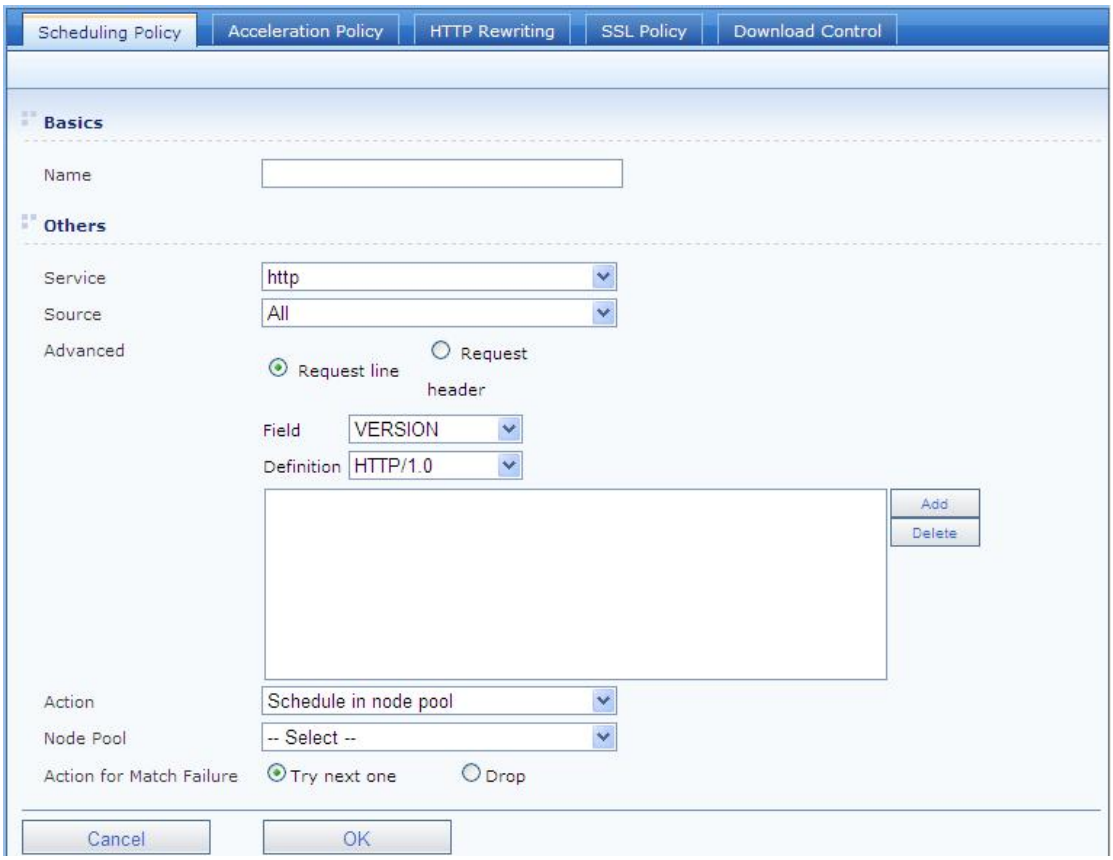


Name: Give it a distinguishable name.

Service: Specifies the service that may match this policy.

Configuring Scheduling Policy for HTTP Services

1. Navigate to **Load Balancing** > **Policy** > **Scheduling Policy**, and click **Add**.

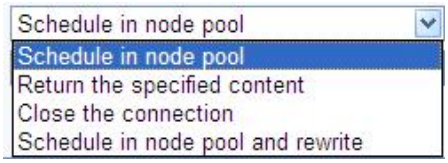


2. Configure the fields on the above page, as follows:

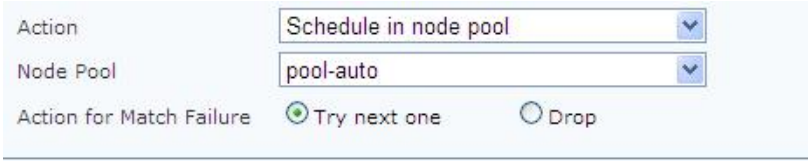
   - **Name:** Give it a distinguishable name.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

- **Service:** Select **HTTP** to have the scheduling policy apply to HTTP service.
- **Source:** Specifies the address type of applicable source address. Options are **All**, **Single IP**, **IP ranges**, **Subnet** and **Local IP Group**.
- **Advanced:** Select **Request line** or **Request header** and set credential. Request line could be **VERSION**, **METHOD** or **URI**, while Request header could be **HOST**, **COOKIE**, **USER-AGENT** or specified field.
- **Action:** Options are Schedule in node pool, Return the specified content, Close the connection and Schedule in node pool and rewrite.

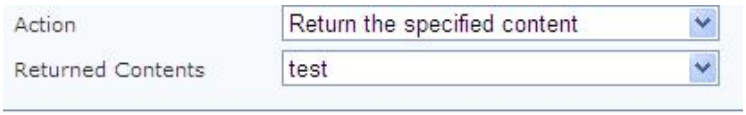


3. If action is **Schedule in node pool**, specify the node pool to have requests to specific virtual service from matching users forwarded to that node pool.



Then specify the **Action for Match Failure**, so that requests unable matching this policy could attempt to match the next scheduling policy, or simply be discarded.

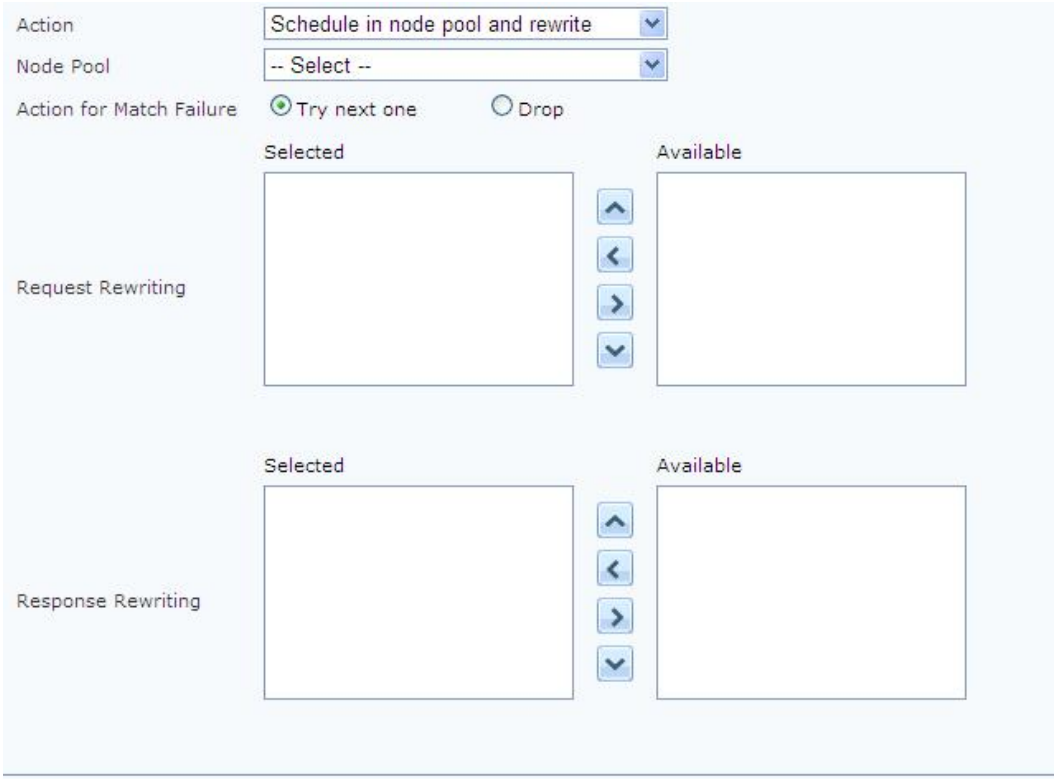
If action is **Return the specified content**, specify the contents you want it returns, which is predefined in **Objects** > **Custom web page**.



If action is **Close the connection**, the connection will be close if user is matching.

If action is **Schedule in node pool and rewrite**, you need to specify the contents in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Node Pool: Select a node pool to have requests to specific virtual service from matching users forwarded to that node pool

Action for Match Failure: Select an action so that requests unable matching this policy could attempt to match the next scheduling policy, or simply be discarded.

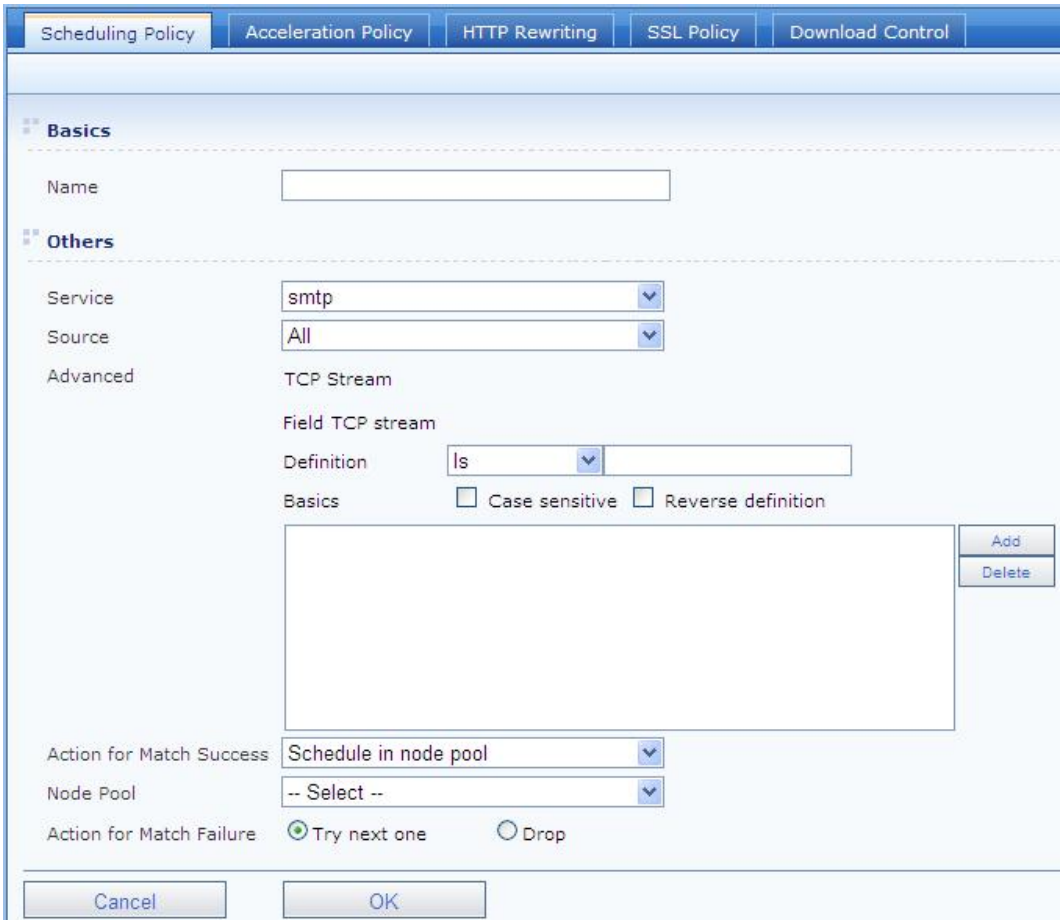
Request Rewriting: Select request rewriting policy from the available policies, which are predefined in **Load Balancing** > **Policy** > **HTTP Rewriting**(Refer to Chapter 6.7.3.1 for details)

Response Rewriting: Select response rewriting policy from the available policies, which are predefined in **Load Balancing** > **Policy**(Refer to Chapter 6.7.3.2 for details)

Configuring Scheduling Policy for TCP Services

1. Navigate to **Load Balancing** > **Policy** > **Scheduling Policy**, click **Add** and select a TCP service such as SMTP, POP3, etc., as shown in the figure below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



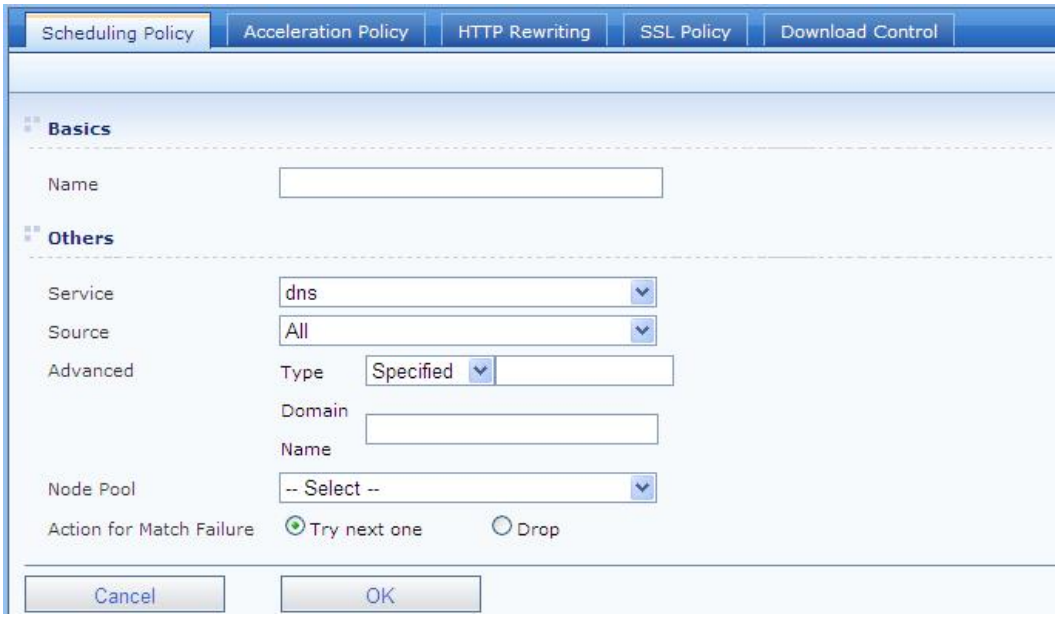
2. Configure the fields on the above figure, as introduced below:

   - **Name:** Give it a distinguishable name.
   - **Service:** Select **smtp** to have the scheduling policy apply to SMTP service.
   - **Source:** Specifies the address type of applicable source address. Options are **All**, **Single IP**, **IP ranges**, **Subnet** and **Local IP Group**.
   - **Advanced:** Set credential of TCP stream.
   - **Action for Match Success:** Indicates that the selected node pool will have requests to specific virtual service from matching users forwarded to that node pool.
   - **Action for Match Failure:** Select an action so that requests unable matching this policy could attempt to match the next scheduling policy, or simply be discarded.

Configuring Scheduling Policy for DNS Services

1. Navigate to **Load Balancing** > **Policy** > **Scheduling Policy**, click **Add** and select DNS service, as shown in the figure below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



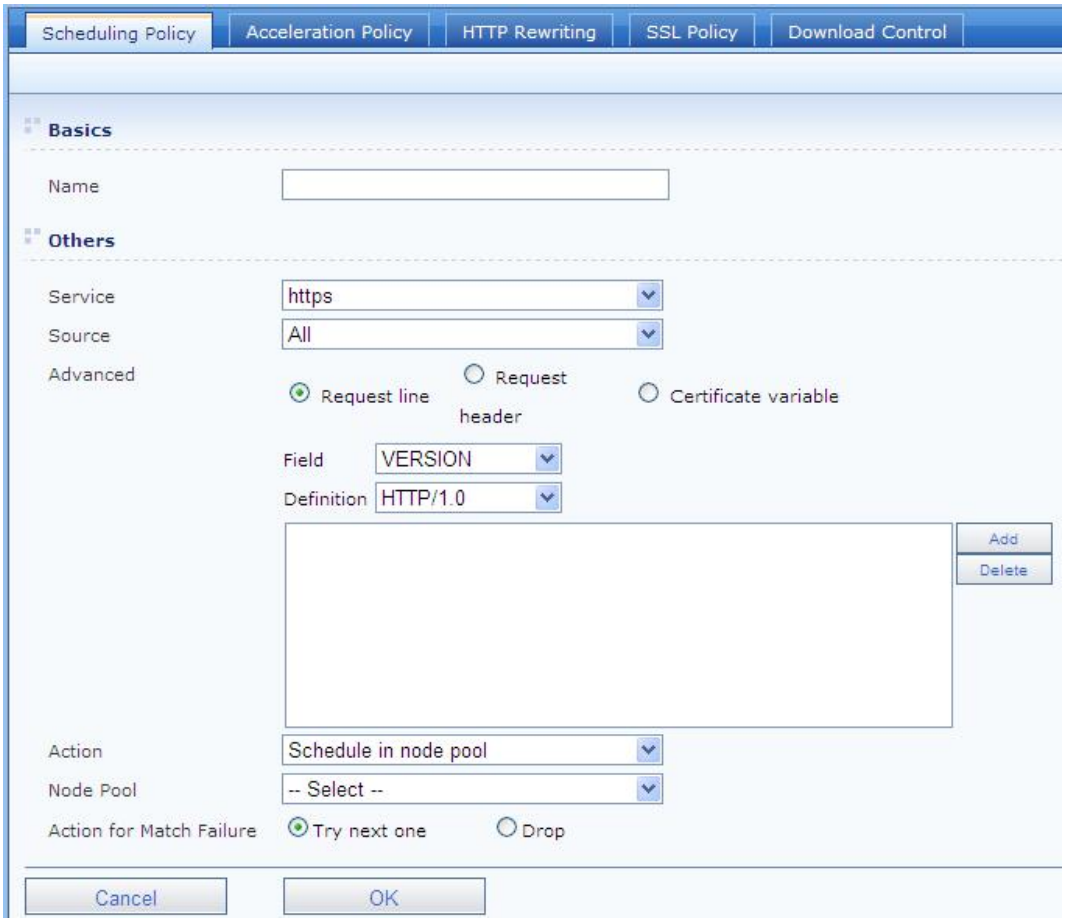
2. Configure the fields on the above figure, as introduced below:

   - **Name:** Give it a distinguishable name.
   - **Service:** Select **dns** to have the scheduling policy apply to DNS service.
   - **Source:** Specifies the address type of applicable source address. Options are **All**, **Single IP**, **IP ranges**, **Subnet** and **Local IP Group**.
   - **Advanced** is used to set inquiry type and inquiry domain name requirements.Inquiry type includes ALL,A,NS,CNAME.
   - **Node Pool:** Select a node pool to have requests to specific virtual service from matching users forwarded to that node pool.
   - **Action for Match Failure:** Select an action so that requests unable matching this policy could attempt to match the next scheduling policy, or simply be discarded.

Configuring Scheduling Policy for HTTPS Services

1. Navigate to **Load Balancing** > **Policy** > **Scheduling Policy**, click **Add** and select HTTPS service, as shown in the figure below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



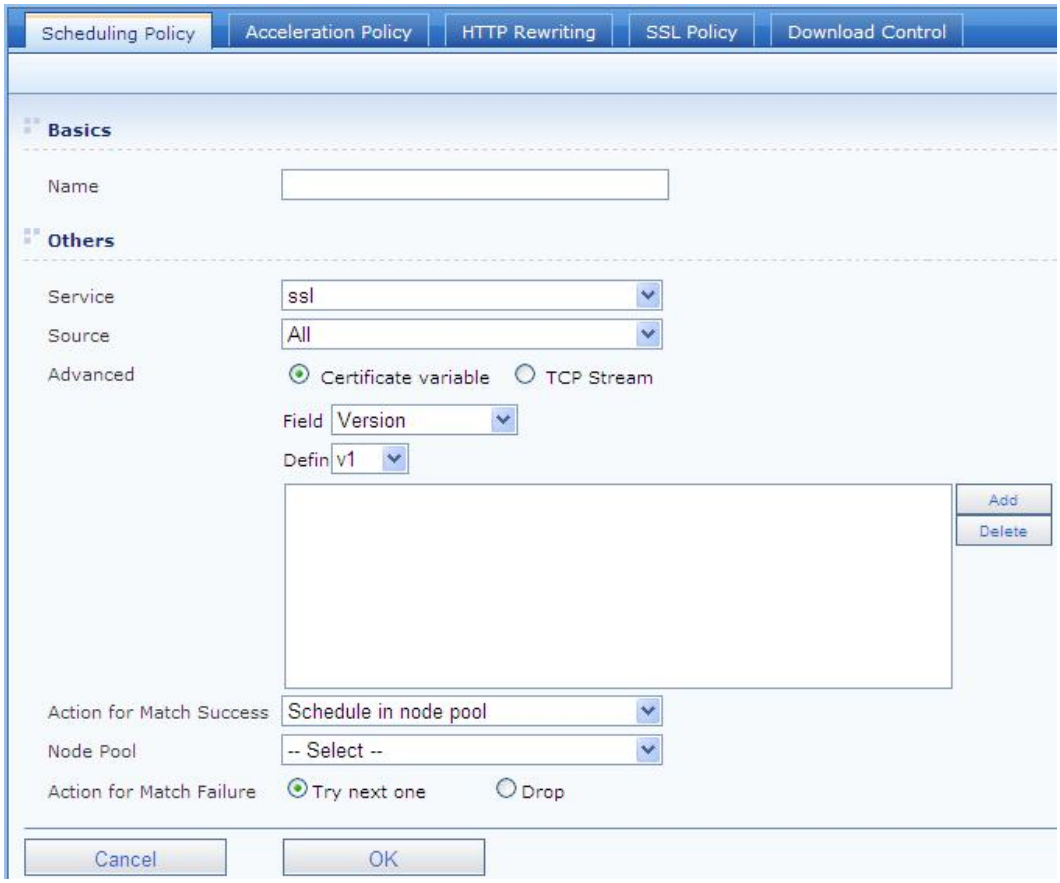
2. Configure the fields on the above figure, as introduced below:

- **Name:** Give it a distinguishable name.
- **Service:** Select **https** to have the scheduling policy apply to HTTPS service.
- **Source:** Specifies the address type of applicable source address. Options are **All**, **Single IP**, **IP ranges**, **Subnet** and **Local IP Group**.
- **Advanced:** You can select request line,request header and certificate variable.Request line can set matched requirement according to [VERSION], [METHOD],and [URI];Request header can set matched requirement according to [HOST], [COOKIE], [USER-AGENT] and custom section;Certificate variable certificate variable [Version], [Issuer], [Subject], [Common Name], [Email Address], [Organization], [Organizational Unit], [Locality], [State or Province] and [Country].
- **Action:** Options are Schedule in node pool, Return the specified content, Close the connection and Schedule in node pool and rewrite.
- **Node Pool:** Select a node pool to have requests to specific virtual service from matching users forwarded to that node pool.
- **Action for Match Failure:** Select an action so that requests unable matching this policy could attempt to match the next scheduling policy, or simply be discarded.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Configuring Scheduling Policy for SSL Services

1. Navigate to **Load Balancing** > **Policy** > **Scheduling Policy**, click **Add** and select SSL service, as shown in the figure below:



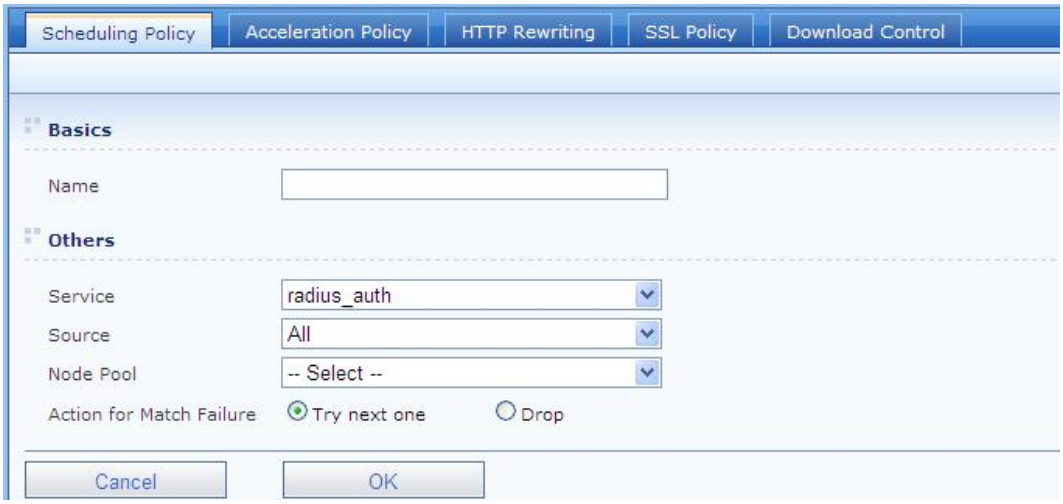
2. Configure the fields on the above figure, as introduced below:

   - **Name:** Give it a distinguishable name.
   - **Service:** Select **SSL** to have the scheduling policy apply to SSL service.
   - **Source:** Specifies the address type of applicable source address. Options are **All**, **Single IP**, **IP ranges**, **Subnet** and **Local IP Group**.
   - **Advanced:** You can select certificate variable and TCP stream.Certificate variable can set matched requirement according to [Version], [Issuer], [Subject], [Common Name], [Email Address], [Organization], [Organizational Unit], [Locality], [State or Province] and [Country];TCP stream can set matched requirement according to equals, contains, wildcards, regular matches.
   - **Action:** Option is **Schedule in node pool**. Select a node pool to have requests to specific virtual service from matching users forwarded to that node pool.
   - **Action for Match Failure:** Select an action so that requests unable matching this policy could attempt to match the next scheduling policy, or simply be discarded.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Configuring Scheduling Policy for RADIUS Services

1. Navigate to **Load Balancing** > **Policy** > **Scheduling Policy**, click **Add** and select RADIUS service, as shown in the figure below:



2. Configure the fields on the above figure, as introduced below:

   - **Name:** Give it a distinguishable name.
   - **Service:** Select **radius_auth** to have the scheduling policy apply to RADIUS service.
   - **Source:** Specifies the address type of applicable source address. Options are **All**, **Single IP**, **IP ranges**, **Subnet** and **Local IP Group**.
   - **Node Pool:** Select a node pool to have requests to specific virtual service from matching users forwarded to that node pool.
   - **Action for Match Failure:** Select an action so that requests unable matching this policy could attempt to match the next scheduling policy, or simply be discarded.

7.6.2 Acceleration Policy

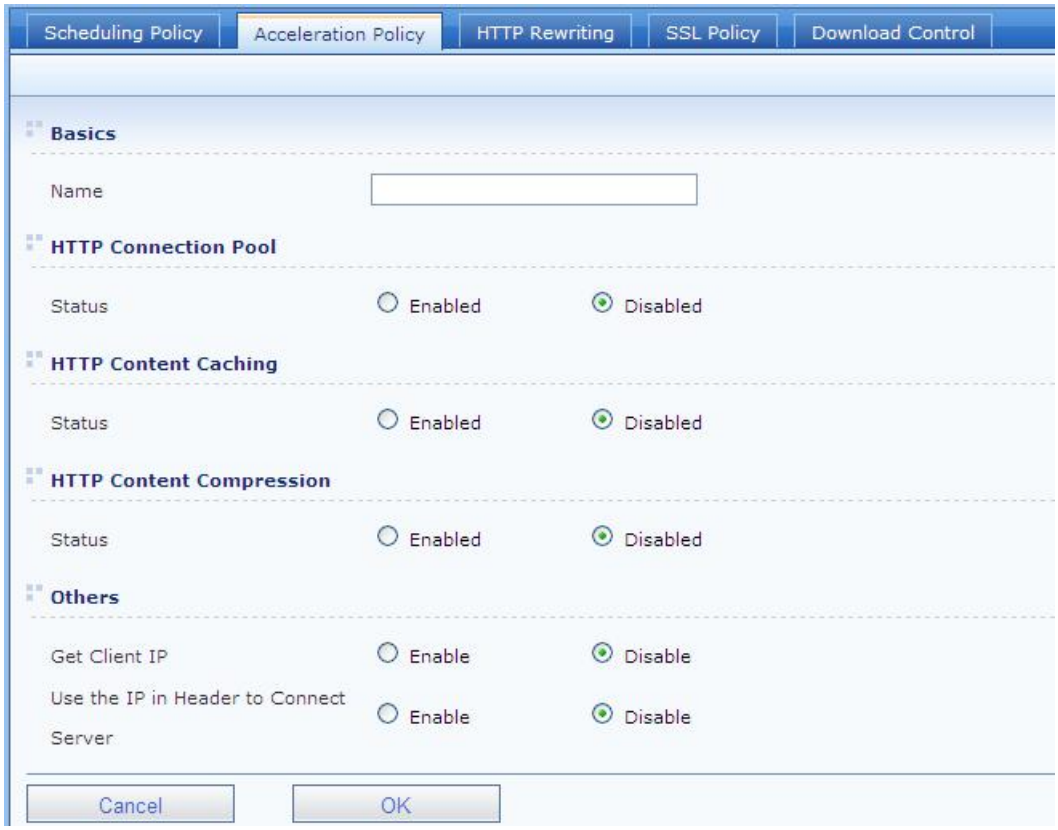
1. Navigate to **Load Balancing** > **Policy** > **Acceleration Policy**.



To remove an acceleration policy, select the entry and click **Delete**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

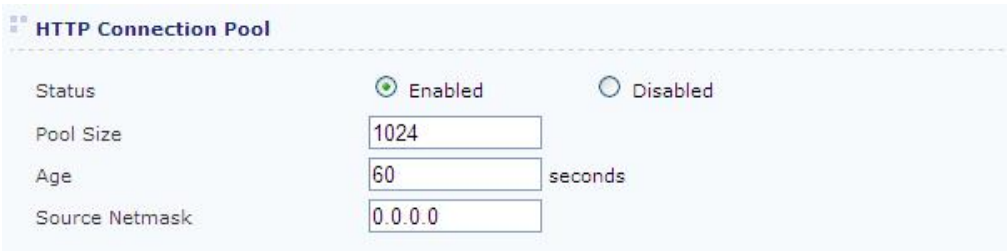
2. To create a new acceleration policy, click **Add** and configure the following contents:



The following are the contents included on the above figure:

- **Name:** Give it a distinguishable name.
- **HTTP Connection Pool :** It realizes that a HTTP connection can send several requests at the same time which reduces server new connections,lessens server burden and enhances server response efficiency.If virtual service enables HTTP connection pool then keep-alive is enabled by default in the server.If you disabled keep-alive in the server by default,keep-alive in the client is enabled no matter whether virtual service enables HTTP connection pool.

  Select **Enabled** and specify the following expanded fields:



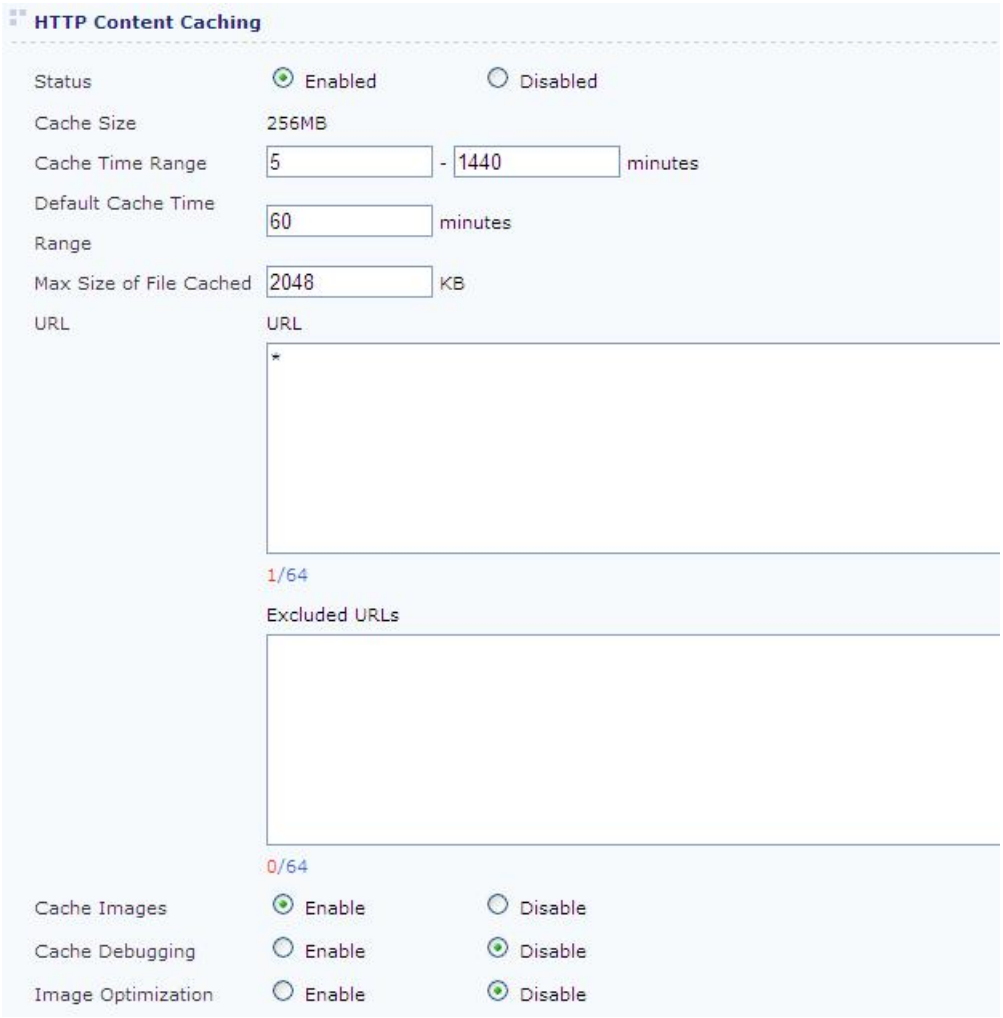
  Pool Size: Specifies the maximum number of connections can be persisted by the pool.

  Age: Specifies the time for persisting an HTTP connection.

  Source Netmask: Specifies the source IP range applicable to HTTP connection multiplexing.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

- **HTTP Content Caching:** HTTP caching can dramatically reduce redundant requests, and therefore the load of application server. Select **Enabled** and specify the following expanded fields:



Cache Size: Specifies the space of HTTP cache.

Cache Time Range: Specifies how long objects can be cached. If valid period of a web page is less than 5 minutes, the objects will be cached for 5 minutes. If valid period of a web page is more than 1440 minutes, the objects will be cached for 1440 minutes. If specified time range is 5-1440 minutes, objects will be cached until the web page gets expired.

Default Cache Time Range: This cached is taken when server response dos not contain cache time or cache time cannot be calculated.

Max Size of File Cached: Specifies the maximum size of file that will be cached. Files larger than that will not be cache.

URL: Response to requests for the specified URLs can be cached.

Excluded URLs: These URL will be excluded from HTTP caching, i.e., response to the requests for those URLs will not be cached.

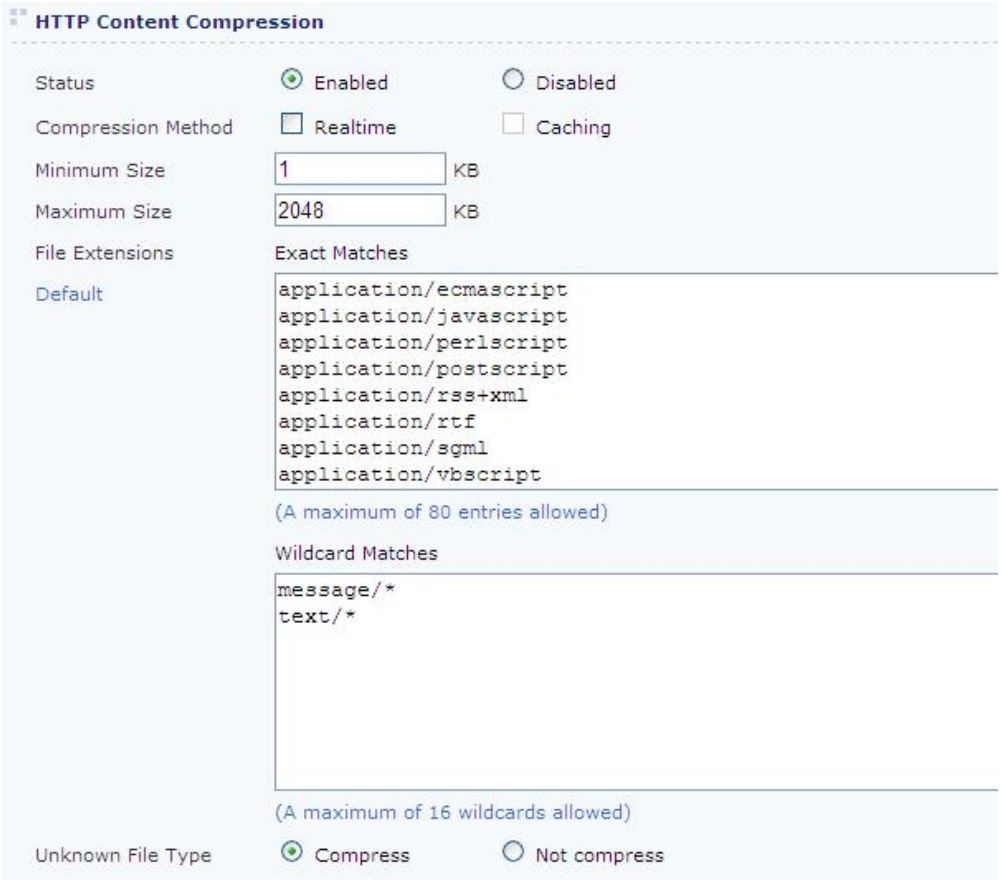
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Cache Images: Select **Enable** to cache images by force.

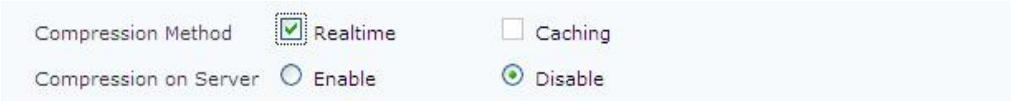
Cache Debugging: Select **Enable** to allow cache debugging.

Image Optimization: Select **Enable** to have images transferred to **webp** or **jpeg** file, so that image traffic could be reduced.

- **HTTP Content Compression:** Compression is applied to the data in HTTP cache and the packets returned from server at real time. This feature requires support of additional algorithm and client to improve caching efficiency and bandwidth utilization. Select **Enabled** and specify the following expanded fields



Compression Method: With HTTP content compression enabled, you can choose to perform compression at real time, and ask the server not compress the HTTP contents to reduce server load, as shown in the screen shot below:



Minimum Size: Specifies the min size of the object. Objects smaller than that will not be cached.

Maximum Size: Specifies the max size of the object. Objects larger than that will not b e cached.

File Extensions: Only specified or matching file types could be cached.

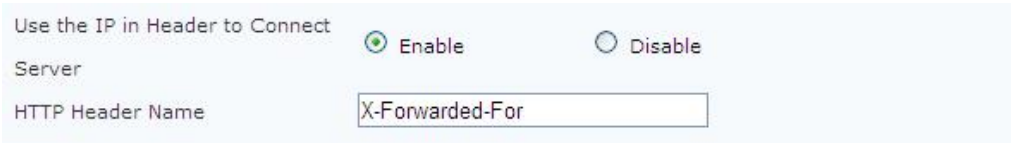
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Unknown File Type: Specifies how to deal with the packets that Web response header does not contain **content-type**, compress by force or not compress.

- **Others:** It includes two options, **Get Client IP** and **Use the IP in Header to Connect Server**. Select the **Enable** option next to **Get Client IP**, and you will see the expanded field, **HTTP Header Name**. This feature is a specific design for bypass deployment of the ADC with SNAT rule taking effect. It allows the server to get the true source address of the client, but service must be HTTP service. Please note that the header name name must be a non-standard header name.



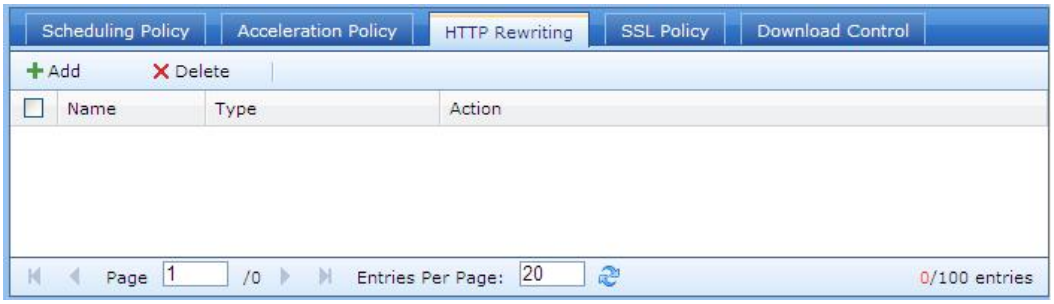
Select the **Enable** option next to **Use the IP in Header to Connect Server**, and you will see the expanded field, **HTTP Header Name**. This feature is applicable for layer-7 load of HTTP and HTTPS virtual services, and allows connecting to server with the IP address contained in the request header from client.



3. Click **OK** to save the settings, or click **Cancel** to give up the settings.

7.6.3 HTTP Rewriting Policy

1. Navigate to **Load Balancing** > **Policy** > **HTTP Rewriting**.



To remove an acceleration policy, select the entry and click **Delete**.

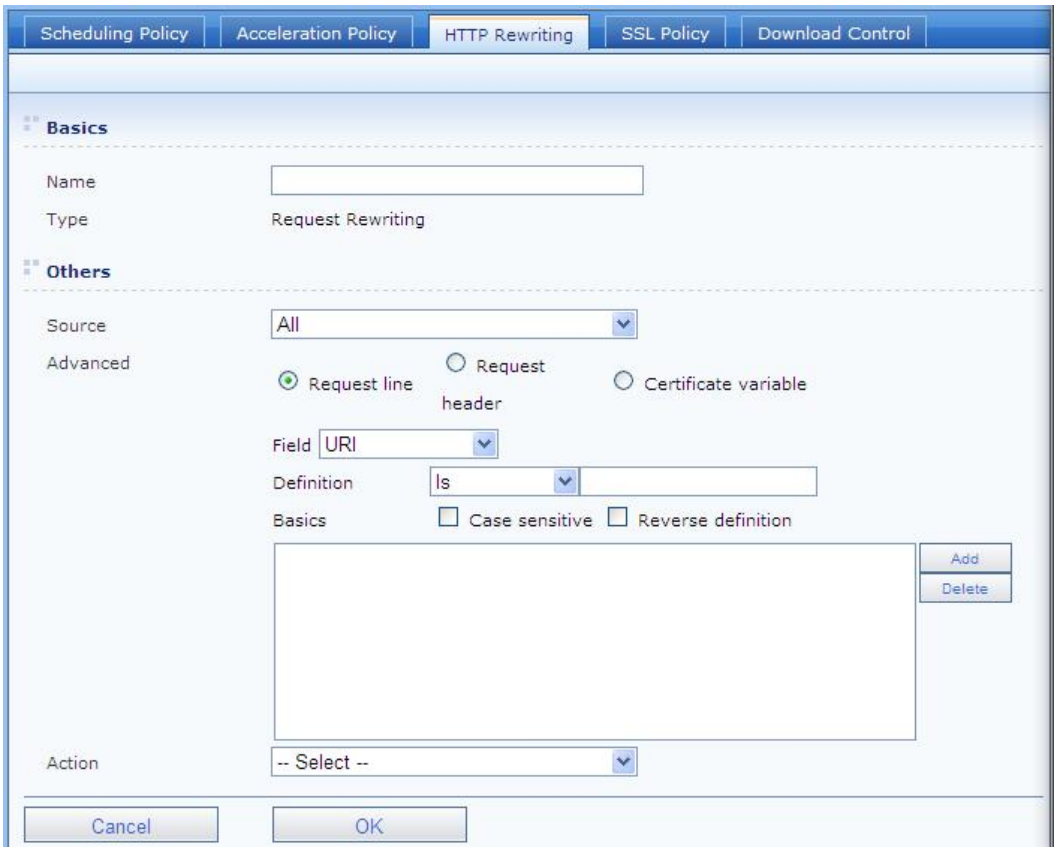
2. To create a new acceleration policy, click **Add.**

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



3. Select what you want to rewrite, **Request** or **Response.**

4. To insert to, remove, delete from **HTTP request** header something or edit URI, select **Request Rewriting**, Click **Next** and configure the following contents,as shown below:

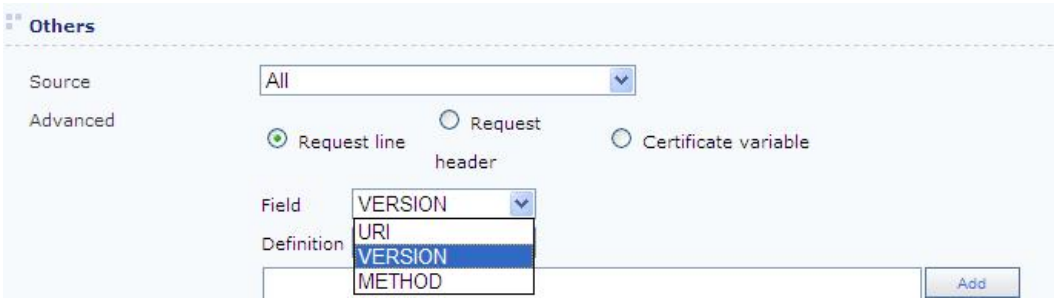


Name: Give the policy a distinguishable name.

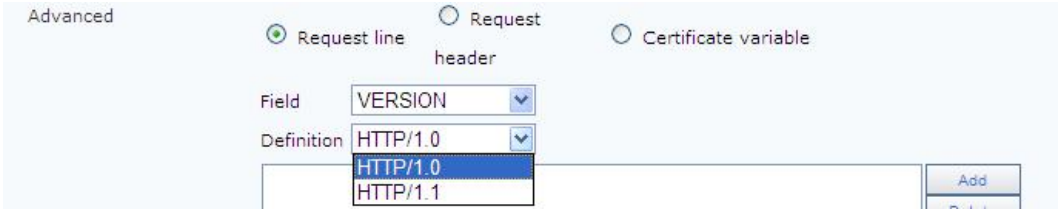
Source: Specifies the address type of applicable source address. Options are **All**, **Single IP**, **IP ranges**, **Subnet** and **Local IP Group**.

Advanced: Select **Request line**, **Request header** or **Certificate variable** and set credential. Request line field could be **VERSION**, **METHOD** or **URI.**

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



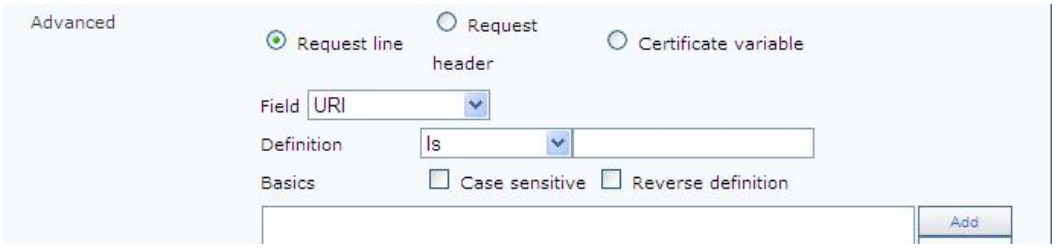
For request line **VERSION** field, you can specify **HTTP/1.0** or **HTTP/1.1**, as shown below:



For request line **METHOD** field, you can specify **GET** or **POST** as shown below:



For request line **URI** field, you can specify what it is, or what string it includes or what wildcard or regular expression should it mach, as shown below:

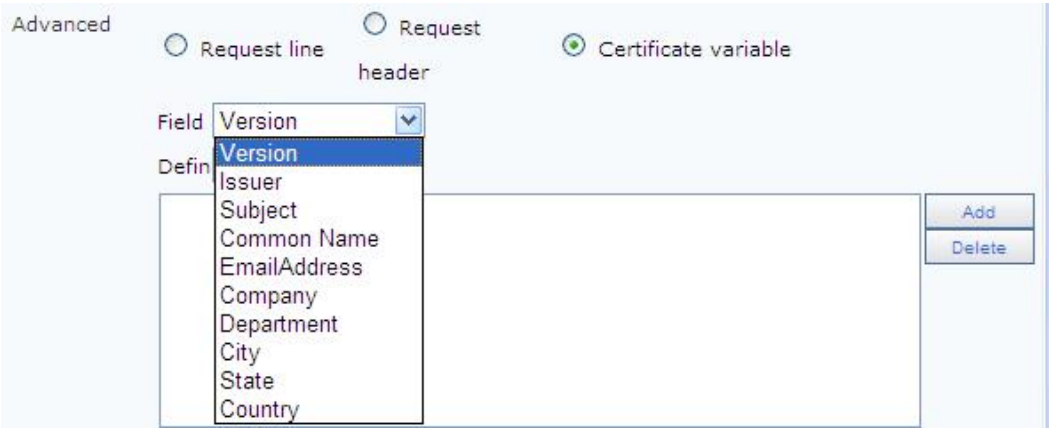


For **Request header** field options, there are HOST, COOKIE, USER-AGENT and specified. You can specify what it is, or what string it includes or what wildcard or regular expression should it mach, as shown below:

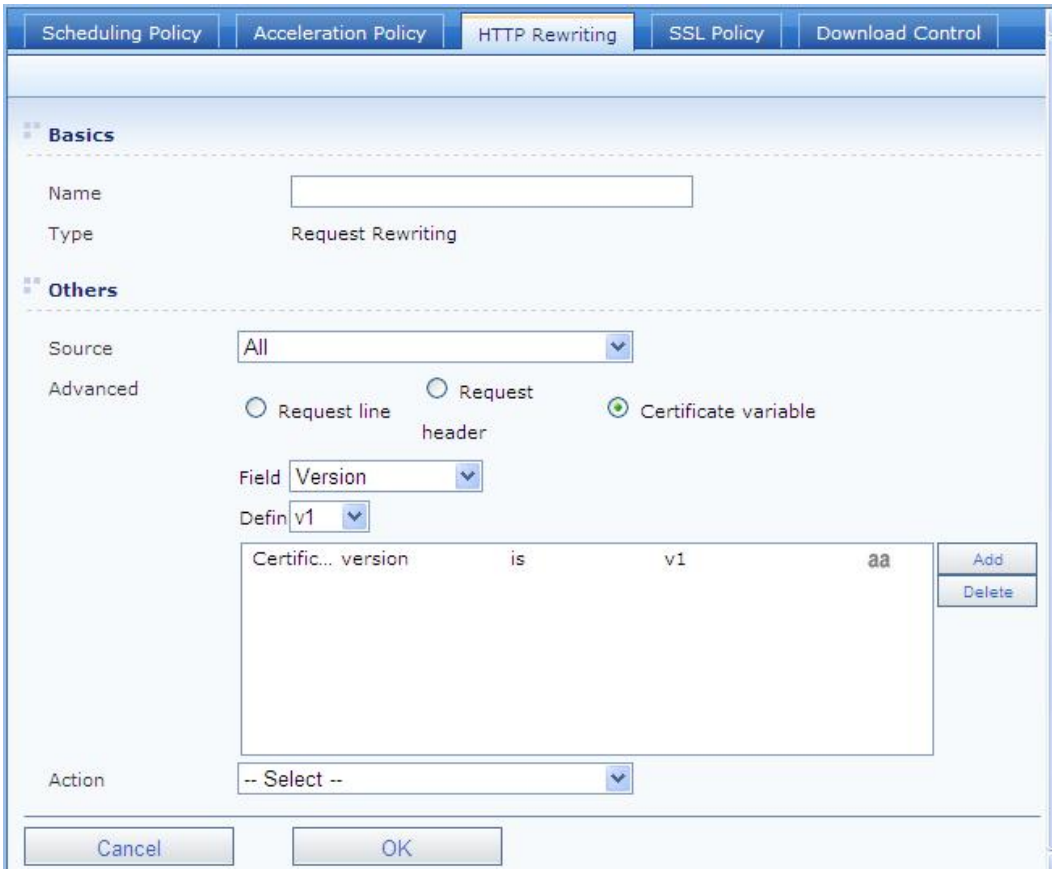


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

For **Certificate variable** field options, there are **Version**, **Issuer**, **Subject**, **Common Name**, **EmailAddress**, **Company**, **Department**, **City**, **State** and **Country**, as shown below:



Take version for example, select **v1** and click **Add**.



Action: Options are **Insert header**, **Delete header**, **Rewrite header**, **Rewrite URI** and **Rewrite content**.

If action **Insert header** is selected, you will see the two expanded fields, **Header Name** and **Inserted Content**, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



If action **Delete header** is selected, you will see the expanded field, **Header Name**, as shown below:



If action **Rewrite heade**r is selected, you will see the three expanded fields, **Header Name**, **Target String** and **Rewritten Content**, as shown below:



If action **Rewrite URI** is selected, you will see the two expanded fields, **Rewrite String** and **Rewritten Content**, as shown below:



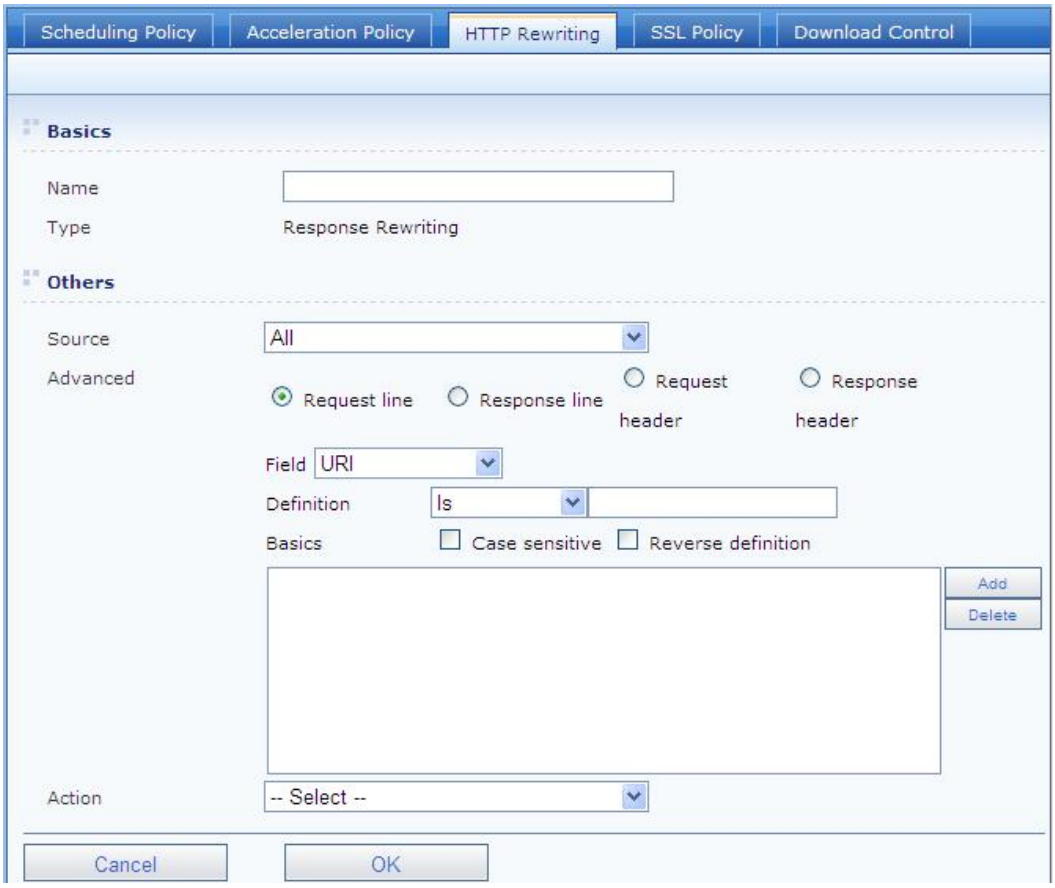
If action **Rewrite content** is selected, you will see the two expanded fields, **Target String** and **Rewritten Content**.



5. Click **OK** to save the settings, or click **Cancel** to give up the settings.

6. To insert to, remove, delete from **HTTP** response header something or edit URI, select **Response Rewriting**,Click **Next** and configure the following contents, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

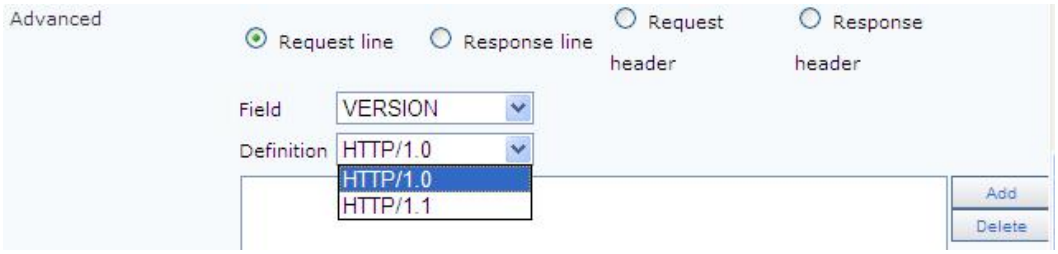


Name: Give the policy a distinguishable name.

Source: Specifies the address type of applicable source address. Options are **All**, **Single IP**, **IP ranges**, **Subnet** and **Local IP Group**.

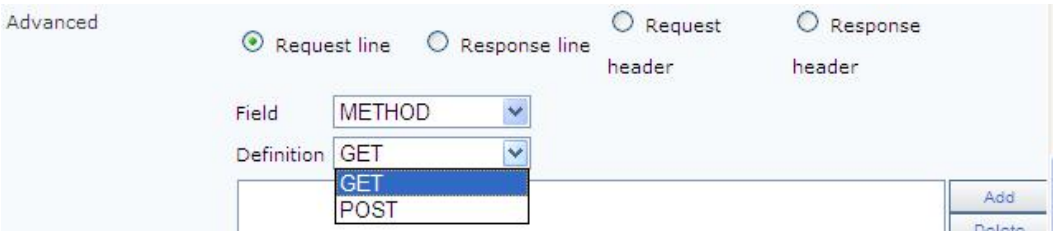
Advanced: Select **Request line**, **Response line, Request header** or **Response header** and set credential. Request line field could be **VERSION**, **METHOD** or **URI**, Response field could be **VERSION** or **STATUS-CODE**, Request header field could be **HOST**, **COOKIE**, **USER-AGENT** or specified, while Response header field could be **CONTENT-TYPE**, **LOCATION**, **SET-COOKIE** and specified.

For request line **VERSION** field, you can specify **HTTP/1.0** or **HTTP/1.1**, as shown below:

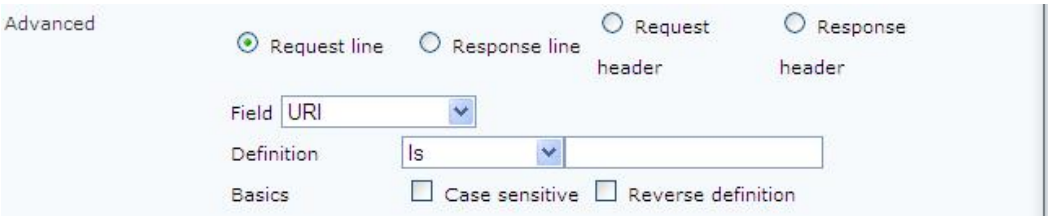


For request line **METHOD** field, you can specify **GET** or **POST** as shown below:

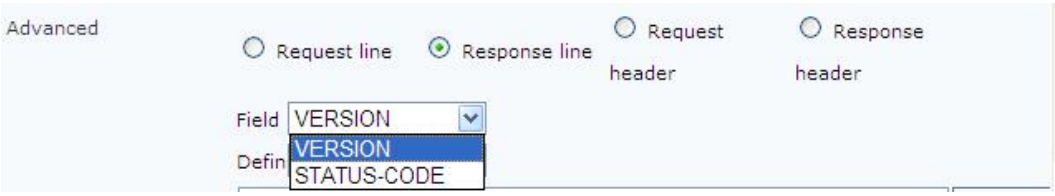
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



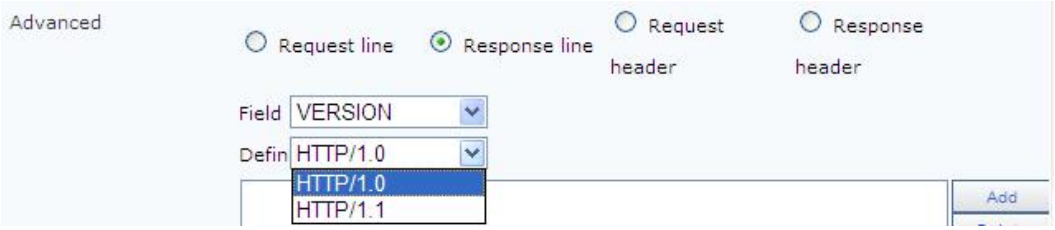
For request line **URI** field, you can specify what it is, or what string it includes or what wildcard or regular expression should it mach, as shown below:



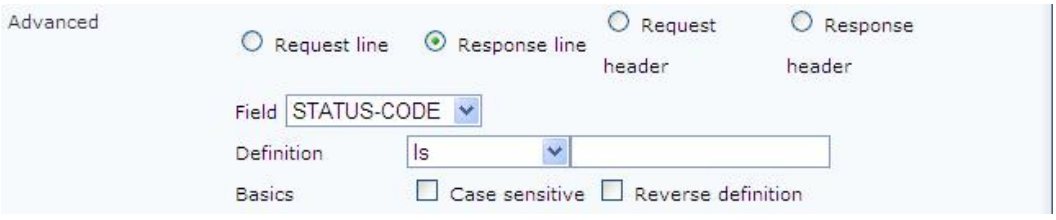
For response line fields, you can specify VERSION or STATUS-CODE, as shown below:



For response line **VERSION** field, you can specify **HTTP/1.0** or **HTTP/1.1**, as shown below:

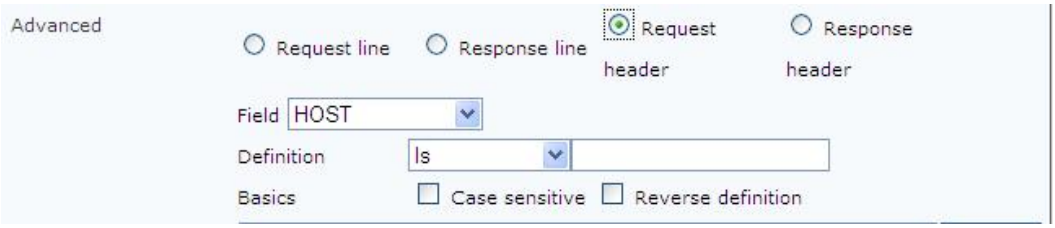


For response line **STATUS-CODE** field, you can specify what it is, or what string it includes or what wildcard or regular expression should it mach, as shown below:

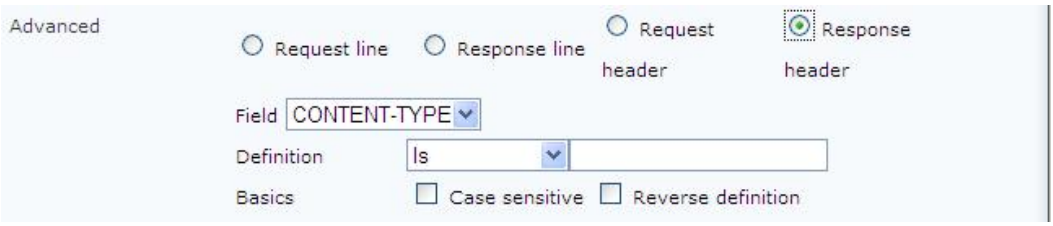


For **Request header** field options, there are HOST, COOKIE, USER-AGENT and specified. You can specify what it is, or what sting it includes or what wildcard or regular expression should it mach, as shown below:

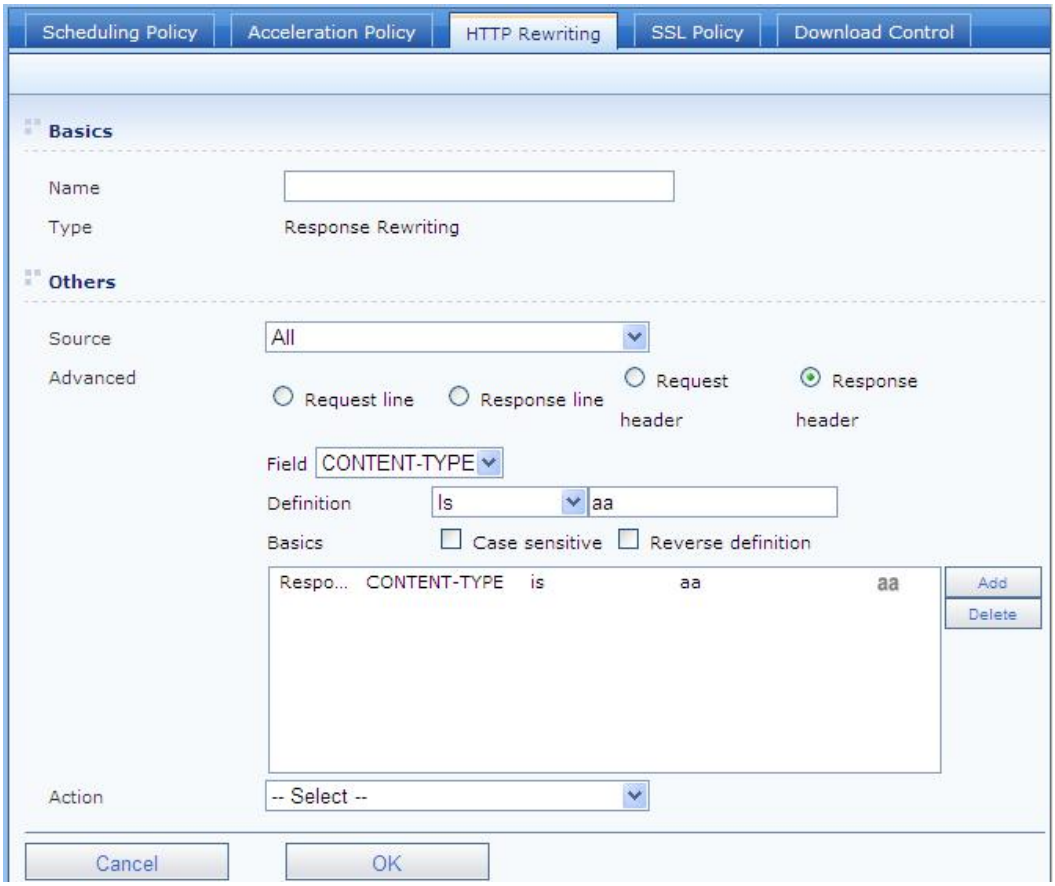
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



For **Response header** field options, there are CONTENT-TYPE, LOCATION, SET-COOKIE and specified fields. You can specify what it is, or what sting it includes or what wildcard or regular expression should it mach, as shown below:



Take CONTENT-TYPE for example, set it as **aa** and then click **Add**, as shown below:



Action: Options are **Insert header**, **Delete header**, **Rewrite header** and **Rewrite content**.

If action **Insert header** is selected, you will see the two expanded fields, **Header Name** and **Inserted Content**, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



If action **Delete header** is selected, you will see the expanded field, **Header Name**, as shown below:



If action **Rewrite header** is selected, you will see the there expanded fields, **Header Name**, **Target String** and **Rewritten Content**, as shown below:

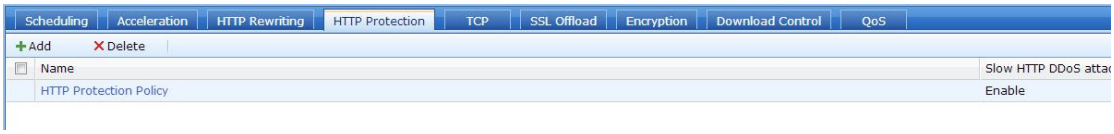


If action **Rewrite content** is selected, you will see the two expanded fields, **Target String** and **Rewritten Content**.



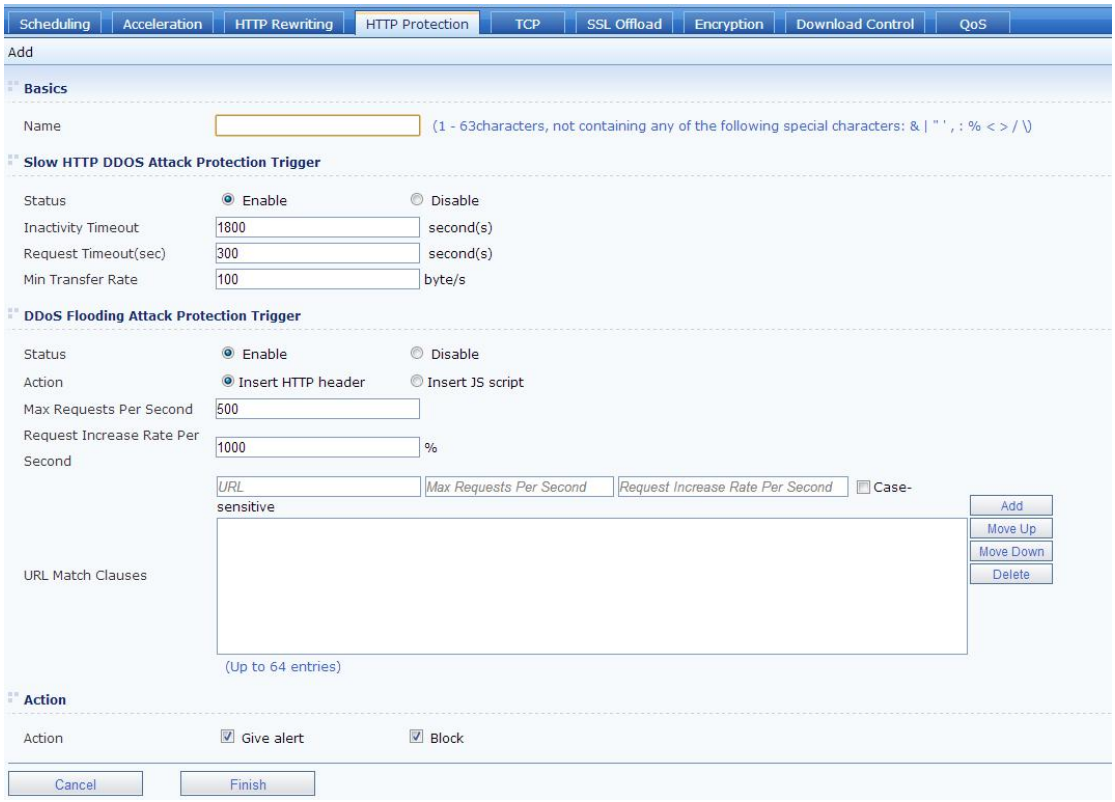
7. Click **OK** to save the settings, or click **Cancel** to give up the settings.

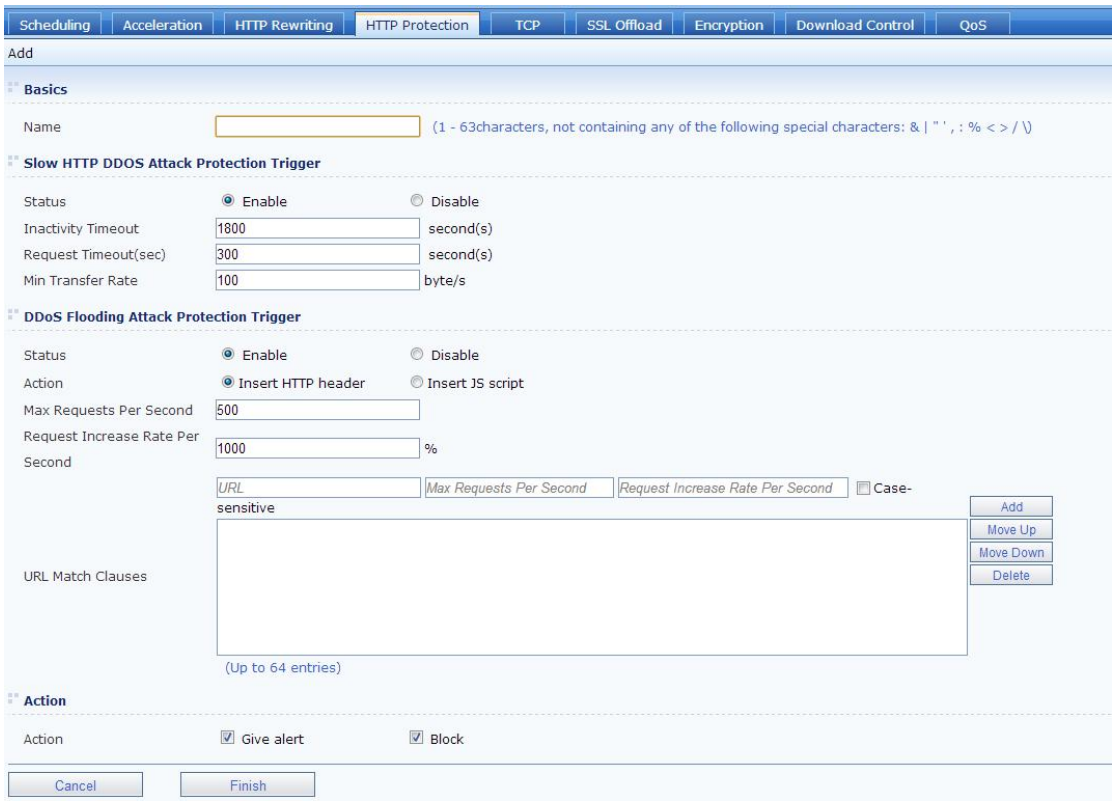
In **Load Balancing** > **Policy** > **HTTP Protection**,click it ,as shown in the following figure:



HTTP Protection shows **Name,Slow HTTP DDoS attack** and **Flooding attack**.
Click **Delete** to delete HTTP Protection.
Click **Add** to add HTTP Protection, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





Name: Specifies the name of the HTTP protection policy.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Slow HTTP DDOS Attack Protection Trigger:



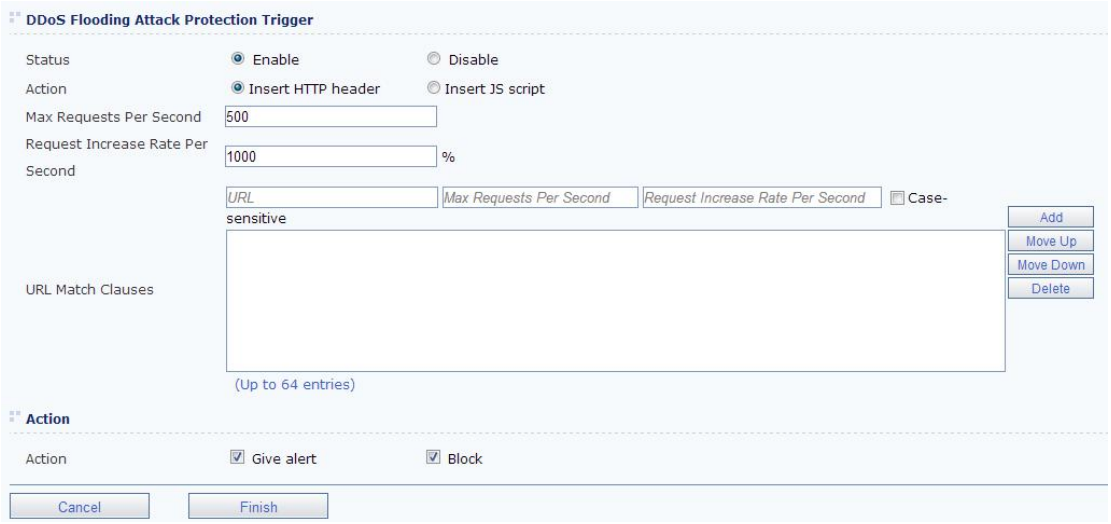
Status: Select **Enable** to enable HTTP protection policy.

Inactivity Timeout: Specifies the time period before TCP connection gets invalid.

Request Timeout(sec): Specifies the time period for receiving a complete HTTP request on TCP connection, beyond which, the TCP connection will be closed.

Min Transfer Rate: Specifies the minimum transfer rate for sending HTTP requests, below which, TCP connection will be closed.

DDOS Flooding Attack Protection Trigger:



Status: Select **Enable** to enable DDOS Flooding Attack Protection.

Action: Options are **Insert HTTP header** and **Insert JS script**. Select **Insert HTTP header**, 302 redirect will be returned. Select **Insert JS script**, JS script will be returned and will be

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

executed by browser.

Max Request Per Second: Specifies max requests per second. Once the threshold is reached, DDoS flooding attack protection will be triggered.

Request Increase Rate Per Second: Specifies request increase rate per second. When max request per second reaches half of the threshold and request increase rate per second reaches the threshold, DDoS flooding attack protection will be triggered.

URL Match Clauses: Specifies URL match clauses. Wildcard * and ? are supported. Example: www.xxx.com/index.html.

Action: Choices are **Give alert** and **Block.**

7.6.4 TCP Policy

Navigate to **Load Balancing** > **Policy** > **TCP**, as shown in the following figure:



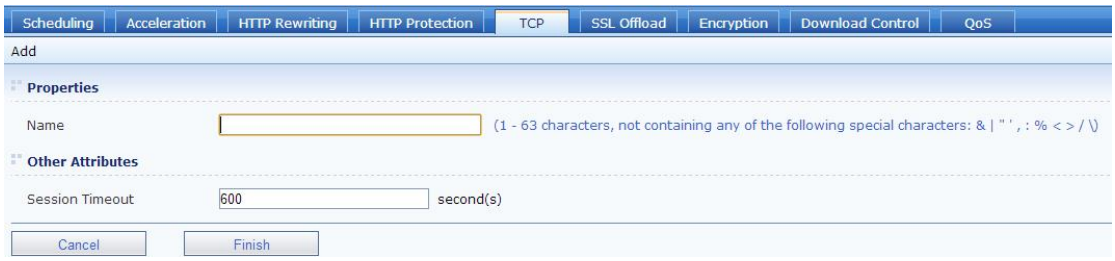
The default TCP policy cannot be edited.

Click **Add** and select mode. Choices are **Layer 4 Service** and **Layer 7 Service**.



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

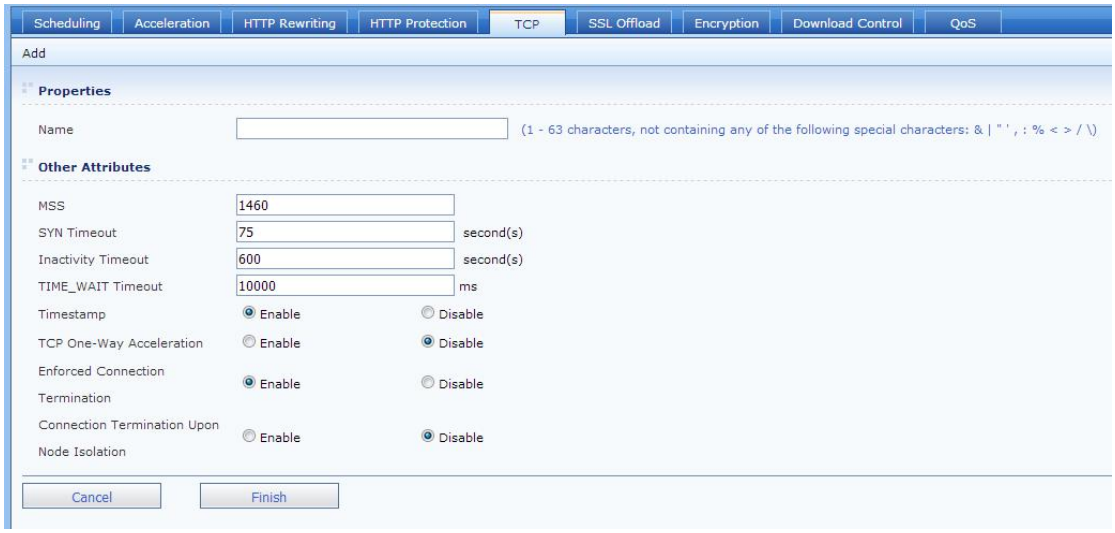
Select **Layer 4 Service** to enter the following page, as shown below:



Name: Specifies name of the TCP policy.

Session Timeout: Specifies time period before layer 4 TCP connection gets invalid.

Select **Layer 7 Service** to enter the following page, as shown below:



Name: Specifies name of the TCP policy.

MSS: Specifies maximum segment size. Configure according to network connection status.

SYN Timeout: Specifies the time period before the TCP connection gets invalid. Default is 75 seconds. Configure according to the network connection status.

Inactivity Timeout: Specifies the time period before layer 7 TCP connection gets invalid.

TIME_WAIT Timeout: Specifies the time period before layer 7 TIME_WAIT gets invalid.

Timestamp: Select **Enable** to prevent server from terminating connection.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

TCP One-Way Acceleration: This option is supported only when the corresponding license key is activated. Under circumstances of network latency or packet loss, this feature functions to accelerate network speed.

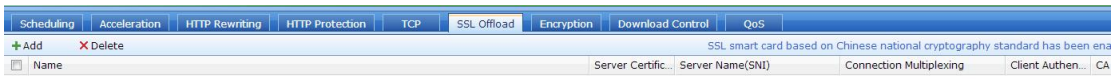
Enforced Connection Termination: Select **Enable** to send RST to terminate connection.

Connection Termination Upon Node Isolation: Select **Enable** to terminate connection when node gets isolated.

7.6.5 SSL Offload

Navigate to **Load Balancing** > **Policy** > **SSL Offload**, as shown below:

SSL Offload supports SM2, ECDSA, RSA Certificates, which will be selected based on algorithms supported by clients and algorithms supported by SSL offload policy.

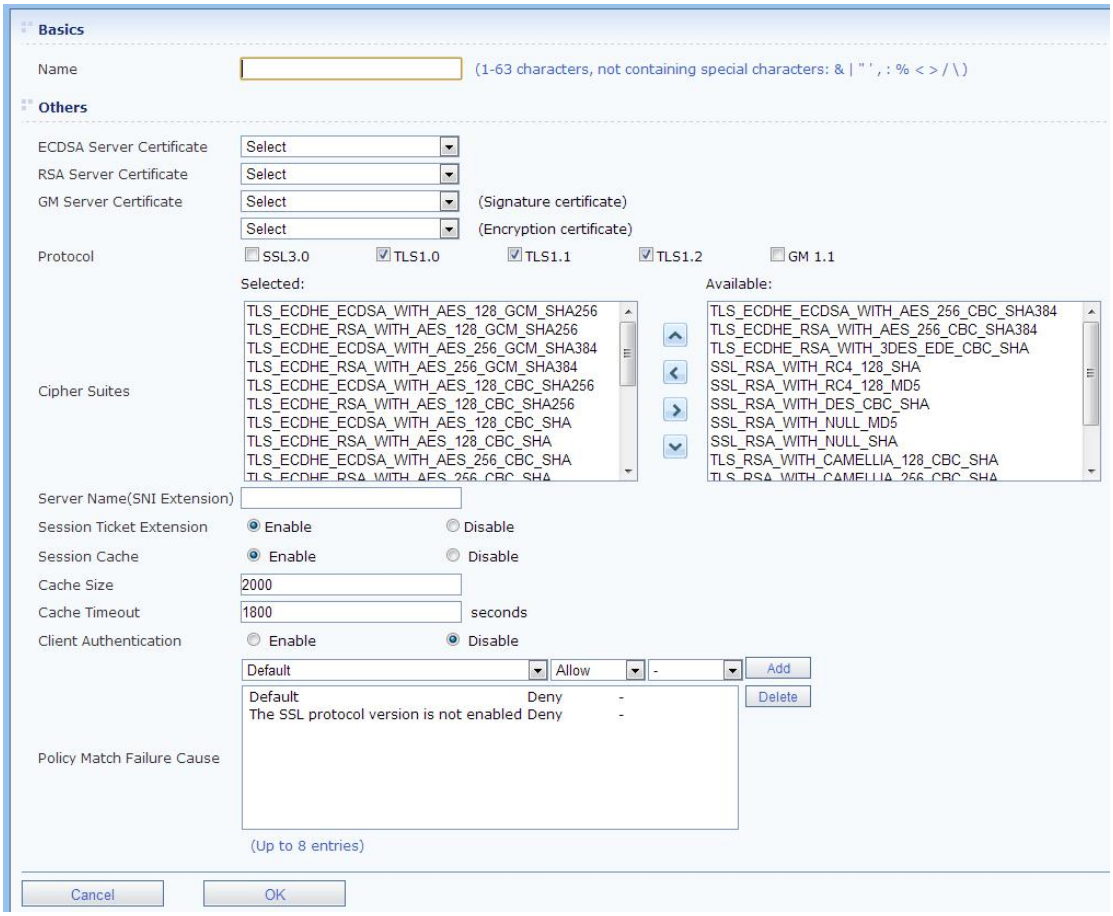


Under **SSL Offload** tab, there are **Name**, **Server Certificate**, **Server Name(SNI)**, **Connection Multiplexing**, **Client Authentication**, and **CA Certificate**.

Click **Delete** to delete offload policy.

Click **Add** to add offload policy, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Specifies a distinguishable name for the SSL offload policy.

ECDSA Server Certificate: Select an ECDSA certificate.

RSA Server Certificate: Select an RSA certificate.

GM Server Certificate: Select a GM certificate. Both signature certificate and encryption certificate are required.

Protocol: Options are SSL3.0, TLS1.0, TLS1.1, TLS1.2 and GM 1.1.

Cipher Suites: Select different algorithms based on SSL server certificates.

Server Name(**SNI Extension**): Specifies server domain name.

Session Ticket Extension: Session multiplexing for TLS, excluding SSL.

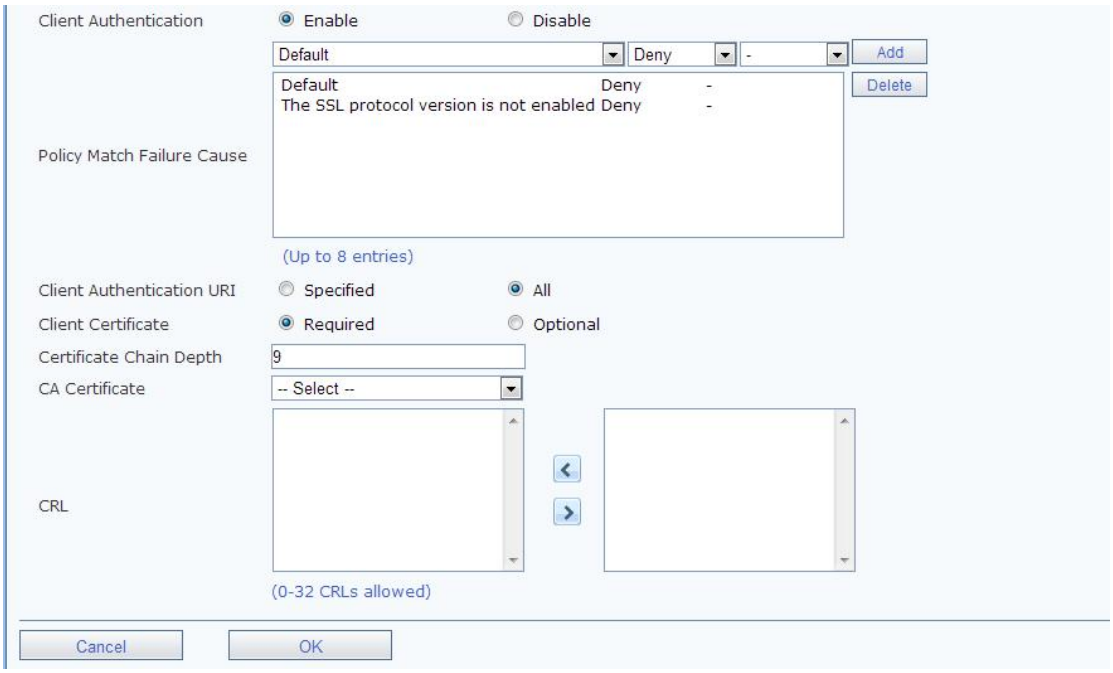
Session Cache: Select **Cache** to enable caching sessions.

Cache Size: Specifies cache size.

Cache Timeout: Specifies the time period before cached sessions get invalid.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Client Authentication: Specifies whether to enable client authentication. It will show as follows if client authentication is enabled:



Client Authentication URI: Specifies whether specified URIs or all the URIs should be authenticated. It will show as follows if **Specified** is selected.



Input specified URI in the input box. For example: /index.html. Wildcards such as ? and * are supported. * indicates that none of the URI need to be authenticated.

Client Certificate: Choices are **Required** and **Optional**. You may select either option when client authentication is enabled.

Required: It indicates that certificate is required.

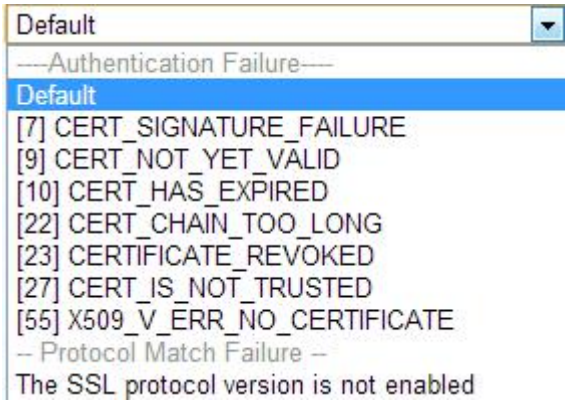
Policy Match Failure Cause: Configure **Policy Match Failure Cause** based on different errors

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

when authentication fails, as shown below:



Common error codes as listed as follows:



Actions can be **Deny**, **Redirect to specified web page** or **Allow**. The specified web pages are customed in **Custom web page**.



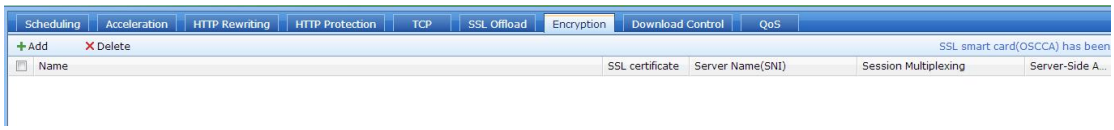
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Certificate Chain Depth: Specifies depth of certificate chain.
CA Certificate: Select a CA certificate.
CRL: Select CRL corresponding to the CA certificate.

To save the settings, click **OK**. To give up the settings, click **Cancel**.

7.6.6 Encryption Policy

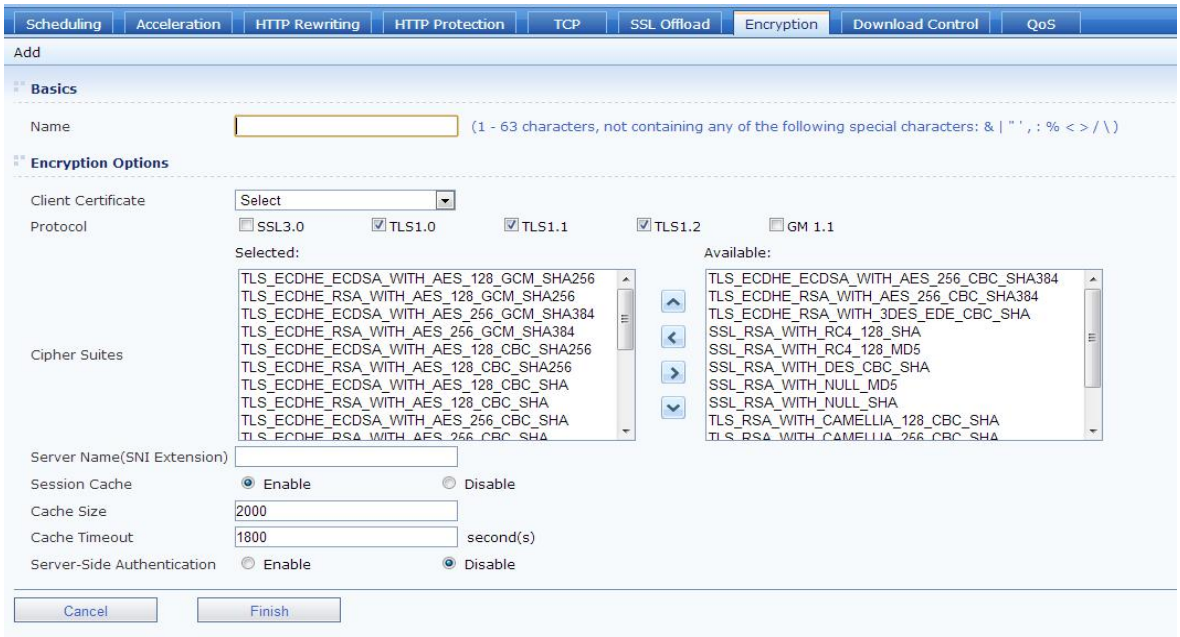
Navigate to **Load Balancing** > **Policy** > **Encryption**, as shown in the following figure:



On the **Encryption** page, there are **Name, SSL Certificate**, **Server Name(SNI)**, **Session Multiplexing**, **Server-Side Authentication** and **Root Certificate.**

To remove an encryption policy, select the entry and click **Delete**.

To create a new encryption policy, click **Add.**



Name: Give it a distinguishable name.

Client Certificate: Select a client certificate.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Protocol: Choices are SSL3.0, TLS1.0, TLS1.1, TLS1.2 and GM1.1.

Cipher Suites: Select corresponding cipher suites according to different types of SSL server certificates.

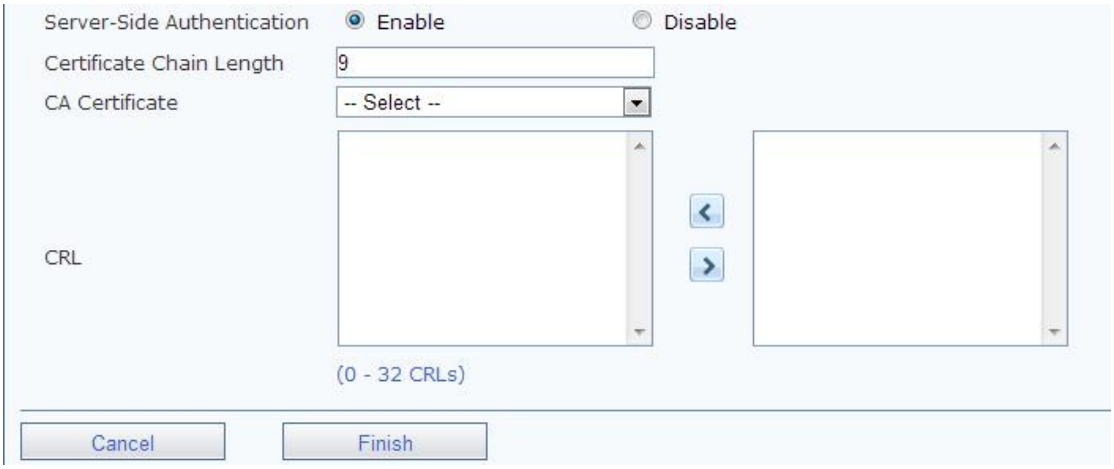
Server Name(SNI Extension): Specifies domain name of server.

Session Cache: Select **Enable** to avoid repeated authentication.

Cache size: Specifies the number of cached SSL connections.

Cache Timeout: Specifies timeout of cached SSL connections.

Server-Side Authentication: Specifies whether to enable authentication on the server side. It will show as follows if client authentication is enabled:



Certificate Chain Length: Specifies length of certificate chain.

CA Certificate: Select a CA certificate.

CRL: Select CRL corresponding to CA certificate.

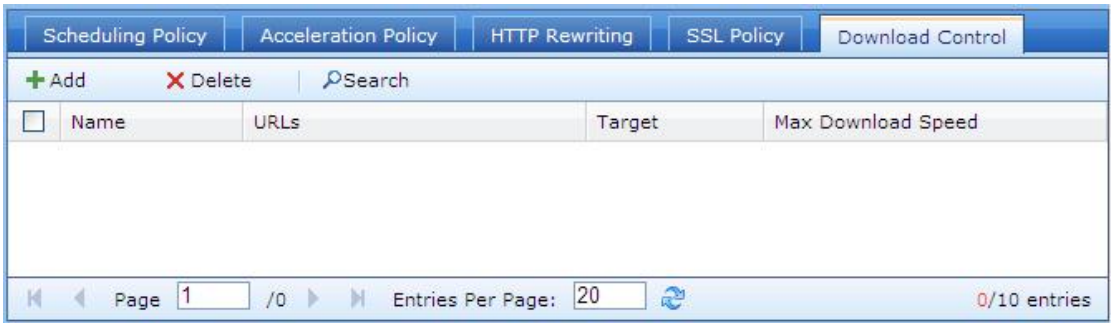
To save the settings, click **OK**. To give up the settings, click **Cancel**.

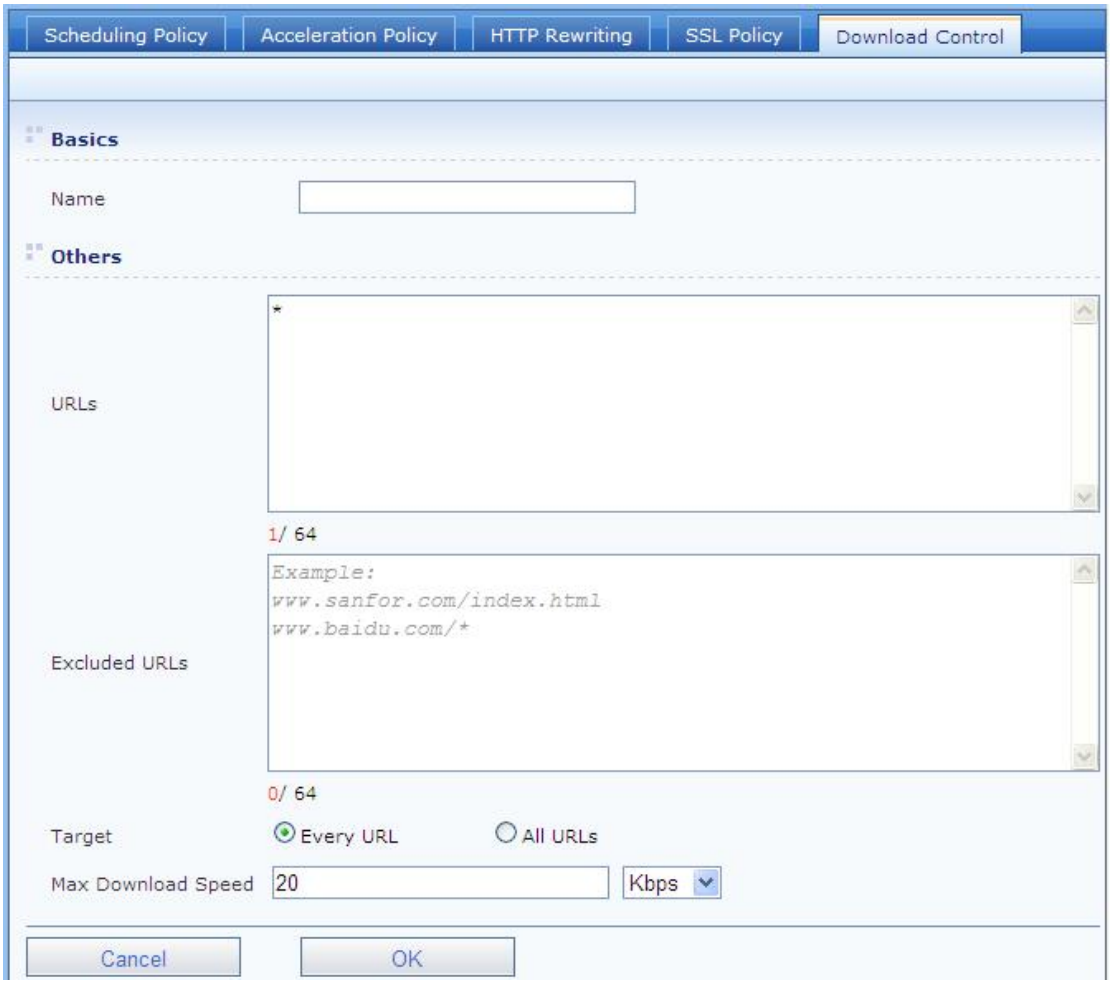
7.6.7 Download Control

A download control policy is used to restrain download speed from a specific URL address, since too large bandwidth taken by one URL access may preempt bandwidth for other URL access.

To create a download control policy, navigate to **Load Balancing** > **Policy** > **Download Control**, click **Add** and configure the following contents.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





Name: Give it a distinguishable name.

URLs: Specifies the URL addresses to control the speed of downloading data from those URL addresses. Wildcards are supported, such as 192.200.200.55/dedecms/a/ad/*

Excluded URLs: Specifies the URL addresses you want to exclude from download control.

Target: Specifies what URL addresses is applicable to download speed control, every URL or all URLs.

Max Download Speed: Specifies the maximum speed allowed for download from specified URLs.

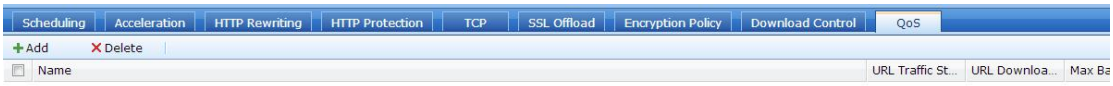
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Before creating download control policy for a URL address, better go to **Status** > **Virtual Service** > **URL Access Traffic** to check the traffic information first. If traffic volume is large, configure download control policy for that URL then.

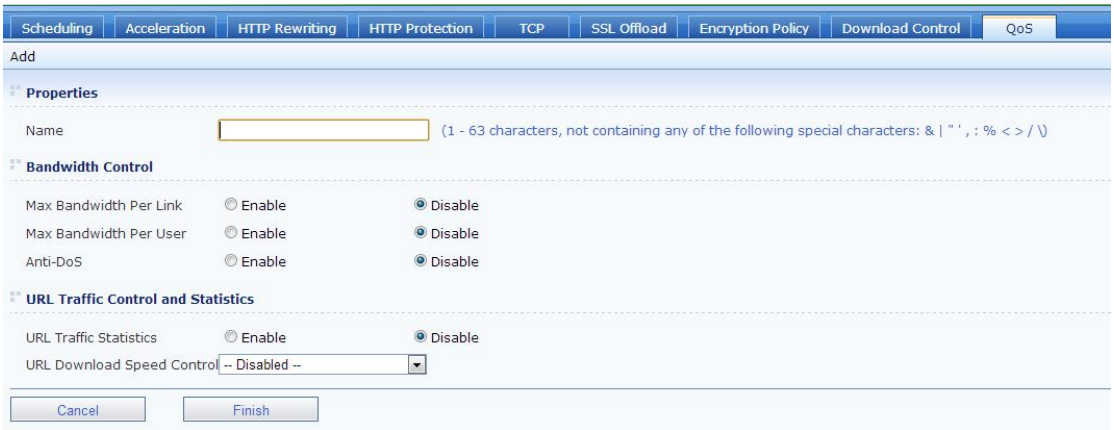
7.6.8 QoS Policy

Navigate to **Load Balancing** > **Policy** > **QoS**, as shown in the following figure:

QoS policy is used to manage bandwidth of links and users.

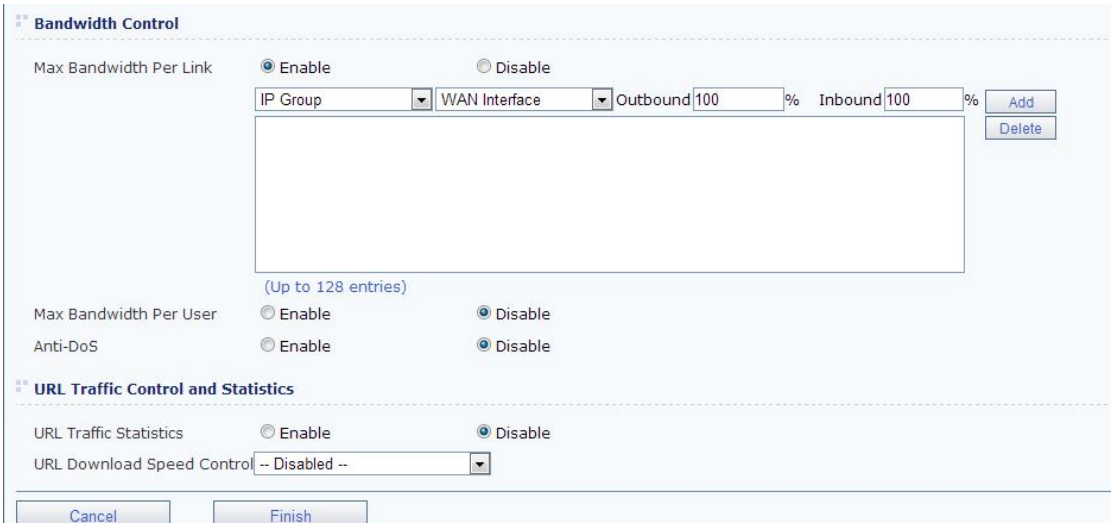


To create a new QoS policy, click **Add**, as shown in the following figure:



Name: Give it a distinguishable name.
Bandwidth Control: Specifies bandwidth based on IP group. Select **Enable** to enter the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Max Bandwidth Per User: Specifies max bandwidth for user. Select **Enable** to enter the following page:



Anti-DoS: Specifies whether to enable anti-DoS so as to prevent clients from launching denial-of-service attacks on the application layer. Choices for **Protocol** field are **HTTP(HTTPS)** and **DNS**.

Select **Enable** and select **HTTP** for **Protocol** field, as shown in the following figure:



When the total number of requests within a specified period reach the upper limit, a specific action will be performed and accesses will be denied.

The default action is to close link of all pages. You can configure to close link or redirect to specified web pages against specific web pages.

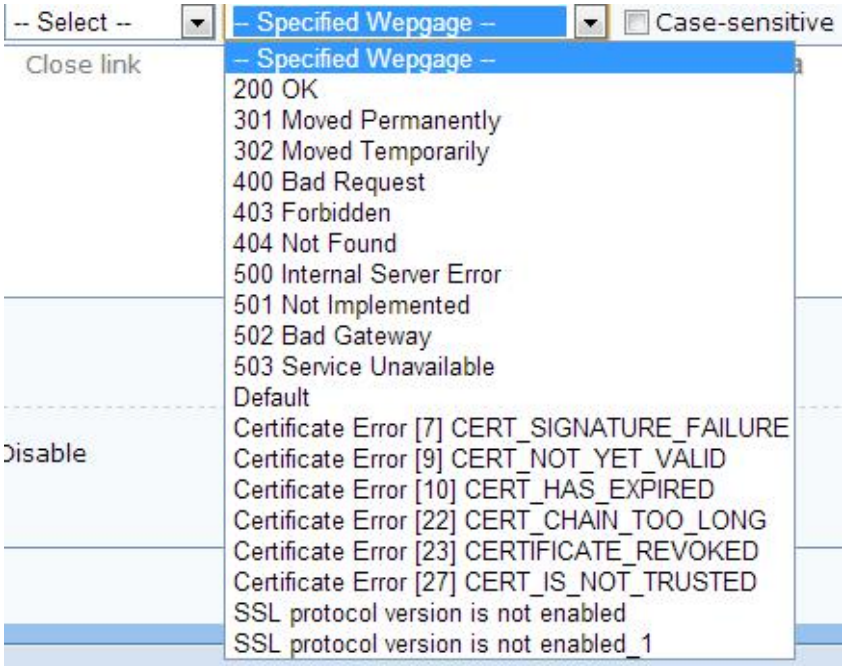
Specify web pages by inputing URL of the web pages in the input box. Wildcard is supported. You may also select **Case-sensitive** to differentiate URLs in upper case or lower case.

Close link: Choices are **Send FIN** and **Send RST**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Specified web page: Select the pre-defined web page which has been customed in **Custom web page**.



Anti-DoS: Select **Enable** and select **HTTP** for **Protocol** field, as shown in the following figure:



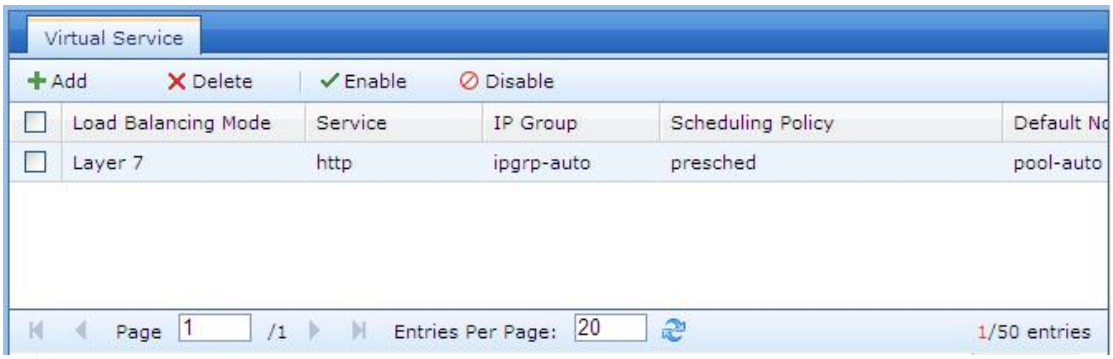
When the total number of requests within a specified period reach the upper limit, DNS requests from the client will be denied.

7.7 Virtual Service

7.7.1 Virtual Service

Navigate to **Load Balancing** > **Virtual Service**, you will see a list of virtual services. A virtual service specifies the applications that need to be delivered, through what WAN links and in what ways.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

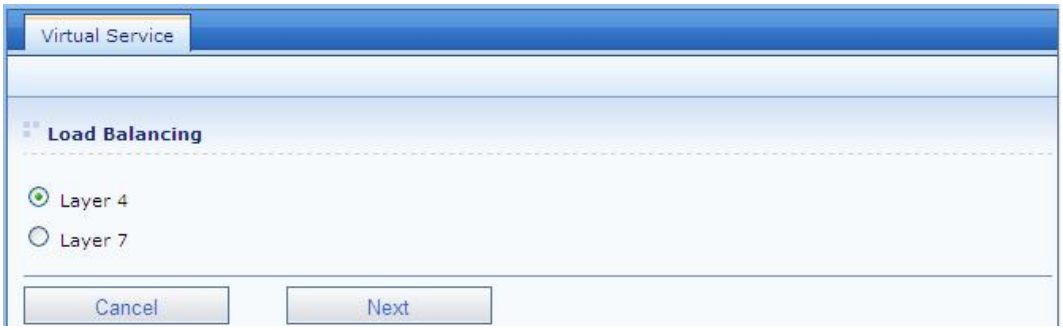


Click **Enable**, you can enable selected virtual service(s).

Click **Disable**, you can disable selected virtual service(s).

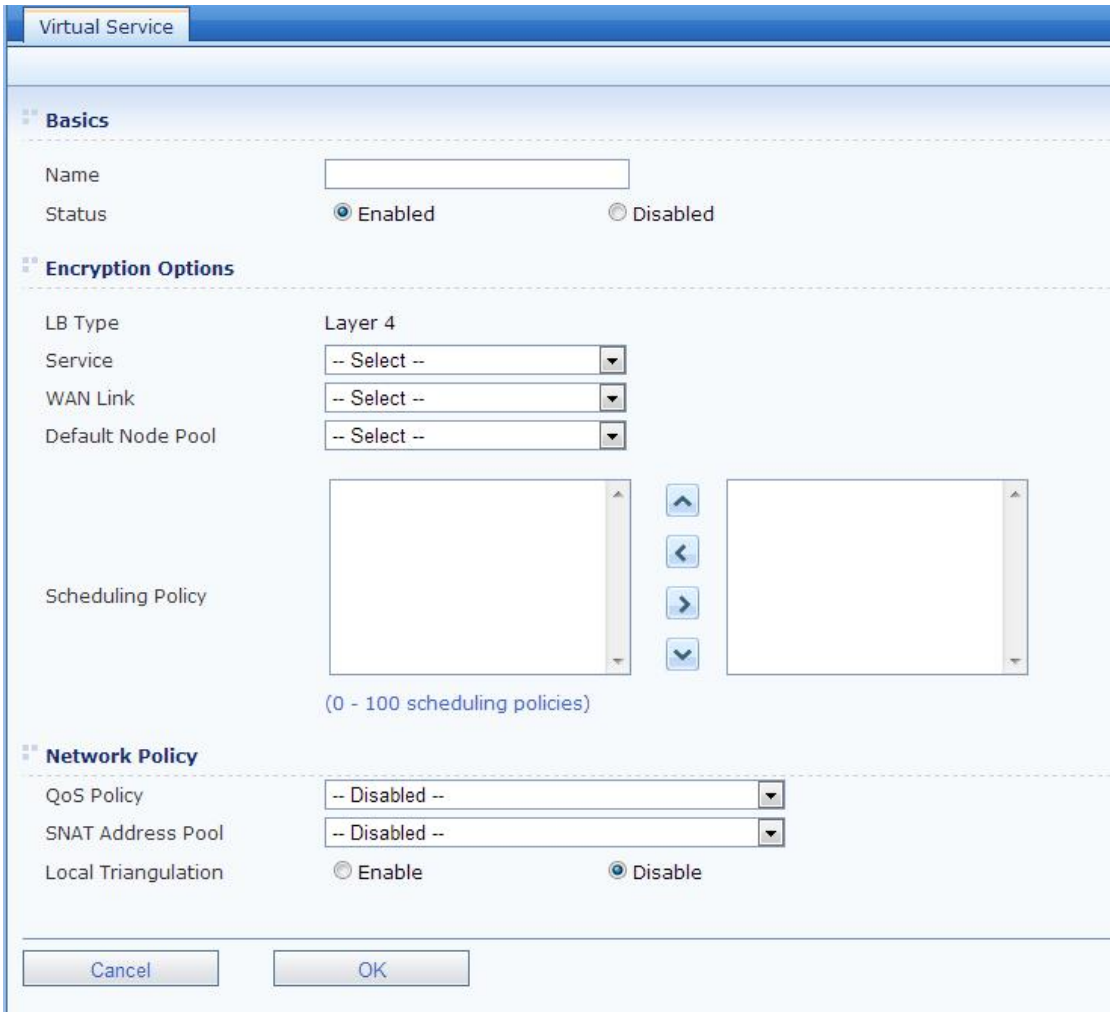
Click **Delete**, you can delete selected virtual service(s).

1. To create a new virtual service, click **Add** and select a load balancing mode, **Layer 4** or **Layer 7**, as shown below:



2. Select **Layer 4** or **Layer 7**. The following are the contents about **Layer 4 LB**:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Status: Select **Enabled** to enable the virtual service.

Load Balancing Mode: Indicates the LB mode selected in the above step.

Service: Select the service you want to deliver as virtual service. The services are predefined in **Load Balancing** > **Service**. Since it is layer 4 LB mode, service must be the predefined SMTP, POP3 or FTP service or custom TCP or UDP service.

WAN Link: Select the WAN link with which you want to deliver the virtual service. The WAN link is predefined in **Load Balancing** > **WAN Link**.

Default Node Pool: If no schedule policy is matching or scheduling failed, the request will be scheduled to the node in the default node pool.

Scheduling Policy: Select scheduling policy from the available policy list. If there are multiple scheduling policies, you can click **Select More** to select multiple policies.

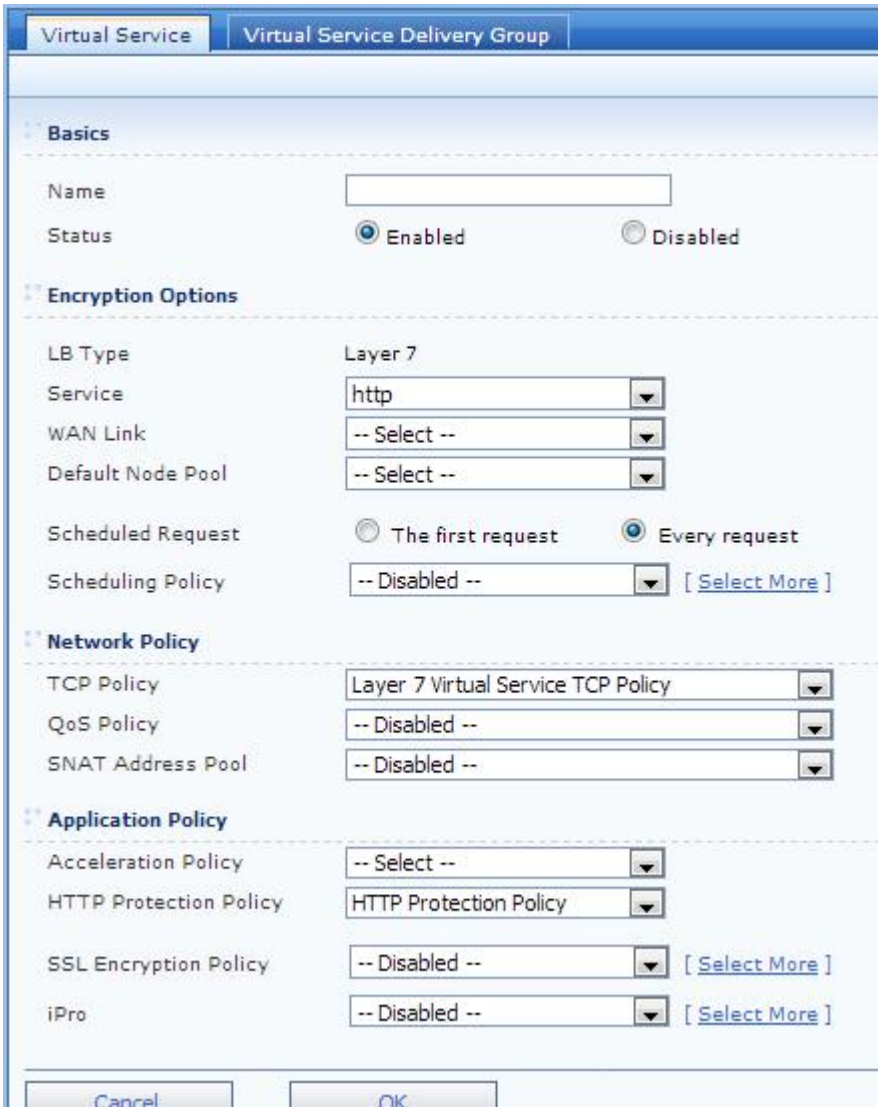
QoS policy: Select a bandwidth control policy against links and users.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

SNAT Address Pool: Once enabled, some IPs will be automatically selected to form an address pool and certain algorithm will be employed to select IP addresses from the pool.

Local Triangulation: This feature is needed when response packets from server does not flow through the ADC. If enabled. The request for virtual service from user will be scheduled to the real server by the ADC but response does not flow through the ADC.

The following are the contents about **Layer 7 LB**.



Name: Give it a distinguishable name.

Status: Select **Enabled** to enable the virtual service.

LB Type: Indicates the LB type selected in the above step.

Service: Select the service you want to deliver as virtual service. The services are predefined in **Load Balancing** > **Service**. Since it is layer 7 LB type, service must be the predefined service or custom HTTP, HTTPS, SSL, DNS, Radius, TCP or MYSQL service.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

WAN Link: Select the WAN link with which you want to deliver the virtual service. The WAN link is predefined in **Load Balancing** > **WAN Link**.

Default Node Pool: Select the default node pool from the available node pool list.

Scheduled Request: Select a scheduling method, options are **The first request** and **Every request**.

Scheduling Policy: Select scheduling policy from the available policy list. One scheduling policy can be associated with multiple virtual services. If there are multiple scheduling policies, click **Select More** to select more scheduling policies.

TCP Policy: Select a TCP policy for layer 7 virtual service.

QoS Policy: Select a QoS policy based on user bandwidth and link bandwidth.

SNAT Address Pool: Once Auto is selected, IP addresses will be selected automatically to form an address pool, and certain algorithms will be employed to select or allocate IP addresses from the address pool.

Acceleration Policy: Select an acceleration policy from the acceleration policy list.

HTTP Protection Policy: For HTTP and HTTPS virtual services, HTTP Protection Policy is enabled by default, but you can disable this option according to your own needs, and you may also go to **Load Balancing > Policy > HTTP Protection** to add a new HTTP protection policy or edit the default HTTP protection policy, but this operation may affect all the layer 7 virtual services associated with the default HTTP protection policy.

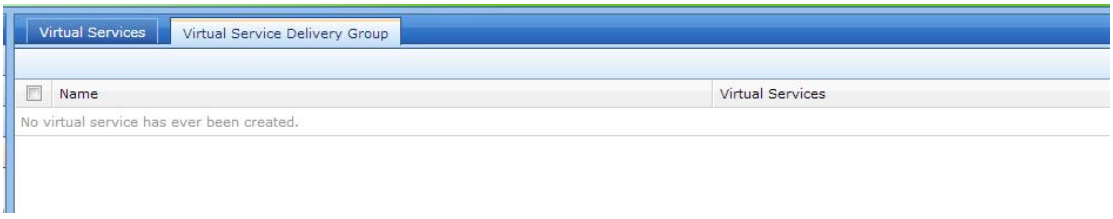
SSL Encryption Policy: Select an SSL encryption policy from the SSL encryption policy list. If there is more than SSL encryption policy, you can click **Select More** to select multiple SSL encryption policies.

iPro: A maximum of 5 iPro entries are supported, which can be configure in **Objects > Script Rules > iPro**. You can click **Select More** to select multiple iPro entries.

Click **OK** to save the settings, or click **Cancel** to give up the settings.

7.7.2 Virtual Service Delivery Group

Go to **Load Balancing > Virtual Service > Virtual Service Delivery Group**, as shown below:



This module is only available when cluster is enabled.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

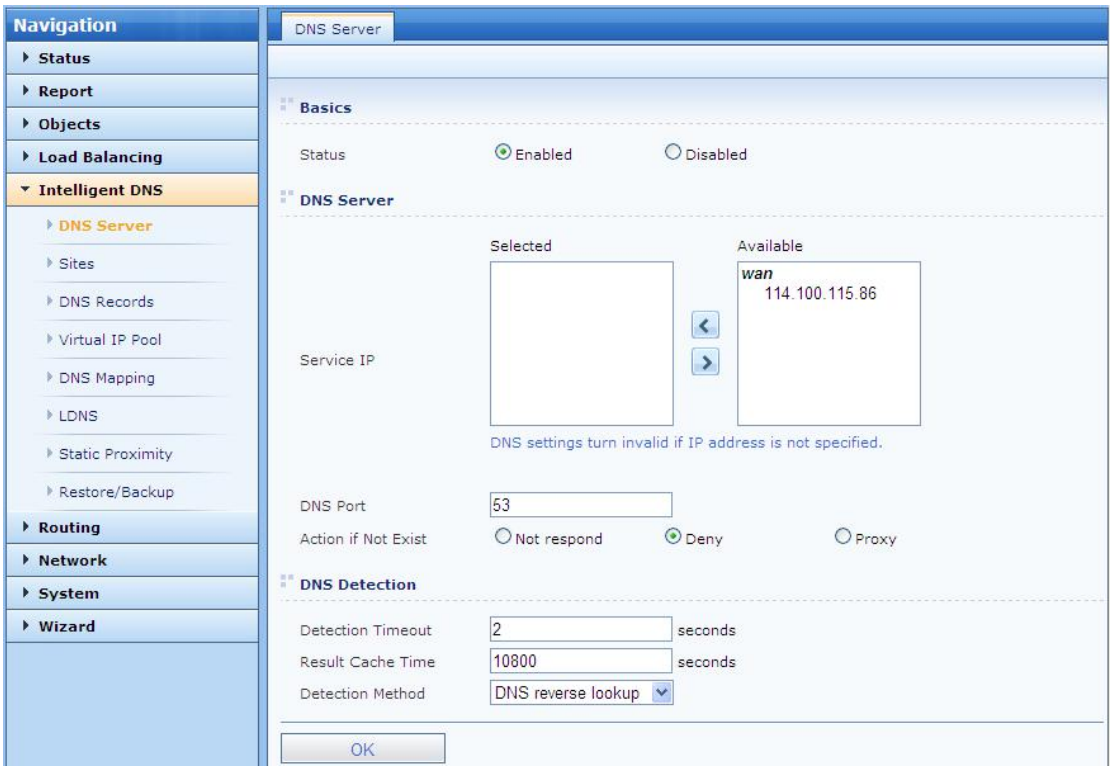
Virtual Service Delivery Group: Multiple virtual services that use the same IP address or node pool are in the same virtual service delivery group. The following shows the relationship between different virtual services.

Associated Traffic Group: Select a traffic group for the virtual service delivery group. The virtual services in the associated traffic group take effect on the devices where the associated traffic groups take effect.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 8 Intelligent DNS

In intelligent DNS, you can configure intelligent DNS service, on local site or global sites. Settings for global sites can be synchronized among each other, while for local site cannot be synchronized.

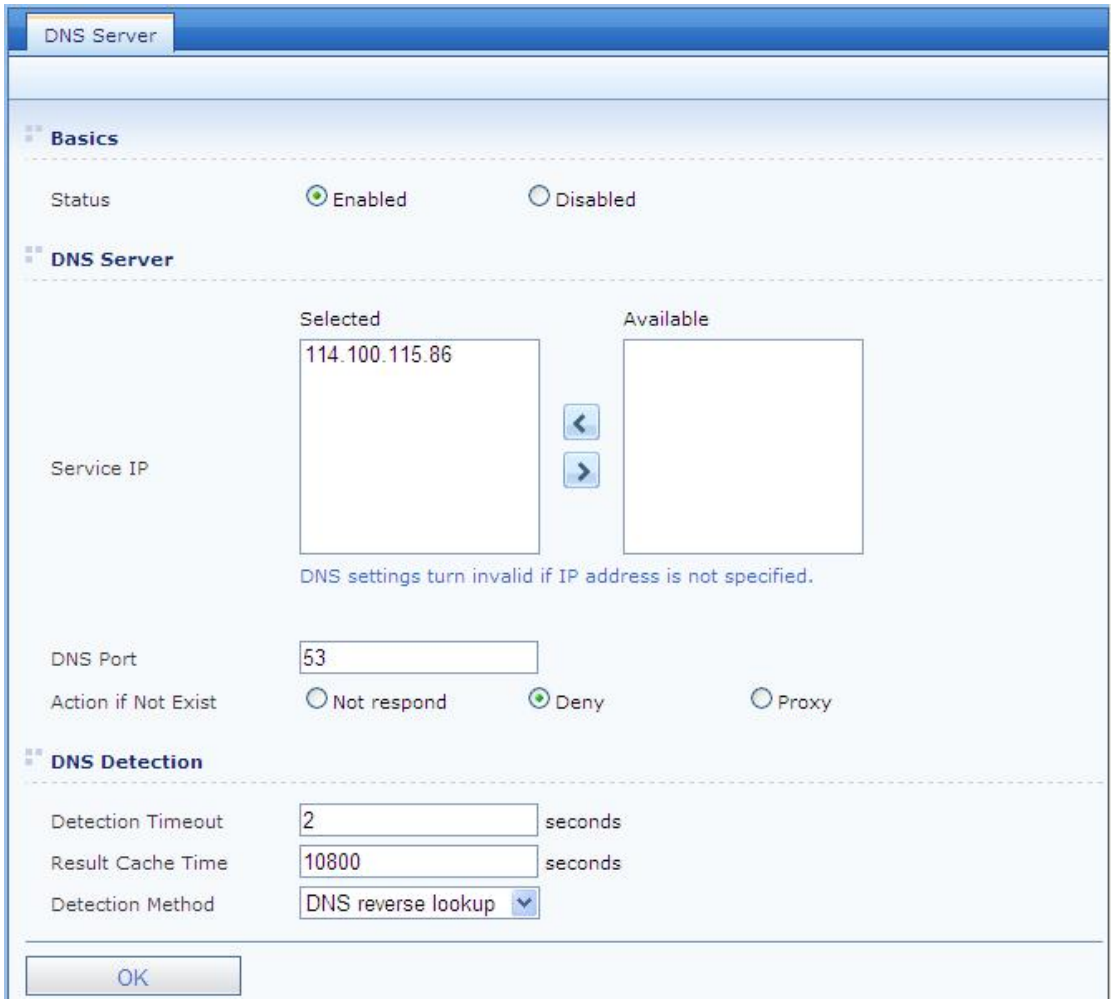


Availability of some configuration under **Intelligent DNS** requires the additional license, **Intelligent DNS global license**. They are Sites, Global DNS Record, Global Virtual IP Pool, Global DNS Mapping and Remote Site LDNS.

8.1 DNS Server

If you want the ADC also works as a DNS server, go to **Intelligent DNS** > **DNS Server** to configure the parameters.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Status: Select **Enable** to enable the DNS server. If disabled, DNS requests will not be resolved.

Service IP: Specifies an IPv6 or IPv4 address for DNS server to provide DNS service. If none is selected, the DNS sever settings will turn invalid.

DNS Port: Specifies the TCP and UDP port for DNS server to provide DNS service. Default is 53.

Action if Not Exist: Specifies how the ADC deals with the request if the domain name queries about does not exist, **Not respond**, **Deny** or perform **Proxy**. **Proxy** means the ADC will forward the request to the DNS module.

Detection Timeout: Specifies the time limit for DNS server to test the DNS response time.

Detection Method: Select a method to test DNS response time from the pull down list. Options are **DNS root**, **DNS reverse look up** and **Ping**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

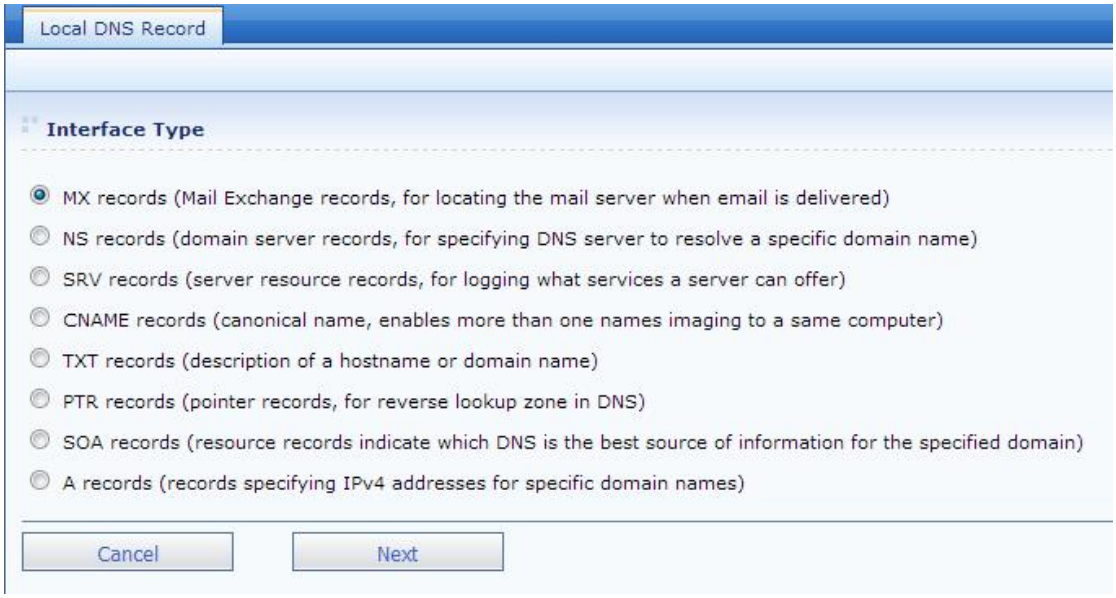
8.2 DNS Records

The DNS records are the records that need to be resolved by the Application Delivery Controller(ADC) when it works as DNS server. Record can be MX records, NS records, SRV records, CNAME records, TXT records, PTR records, SOA records and A records. .

8.2.1 Local DNS Record

Local DNS record is used in situation that there is only one site and the ADC also works as DNS server at the local site.

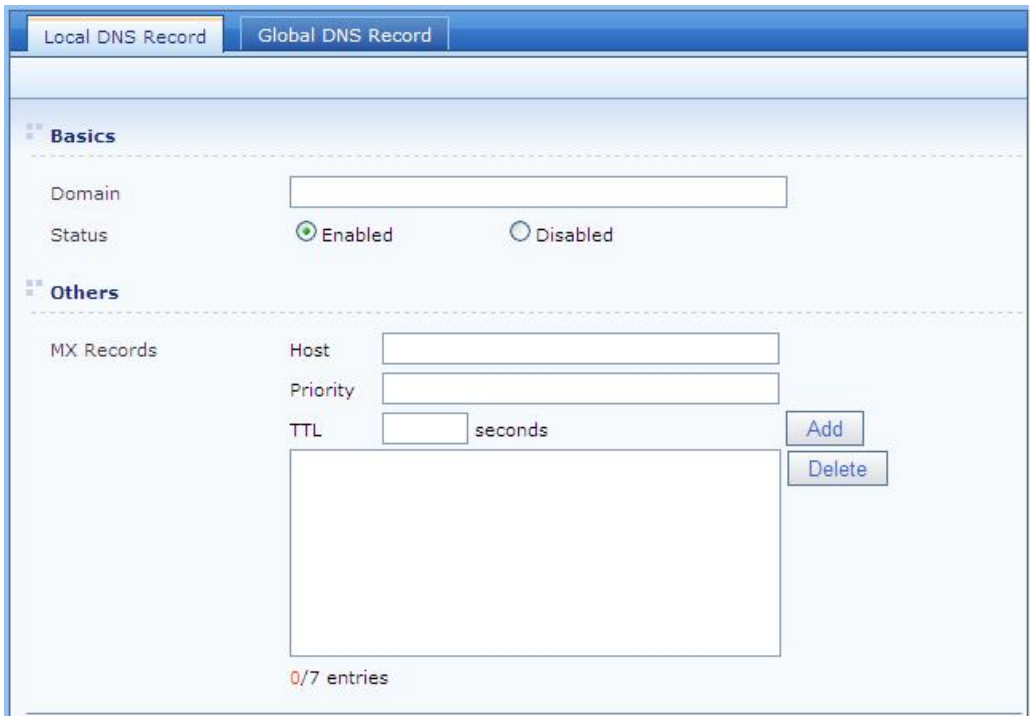
To add a local DNS record, navigate to **Intelligent DNS** > **DNS Records** > **Local DNS Record**.



Select the record type, and click **Next**.

For **MX record**, the attributes are as follows:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



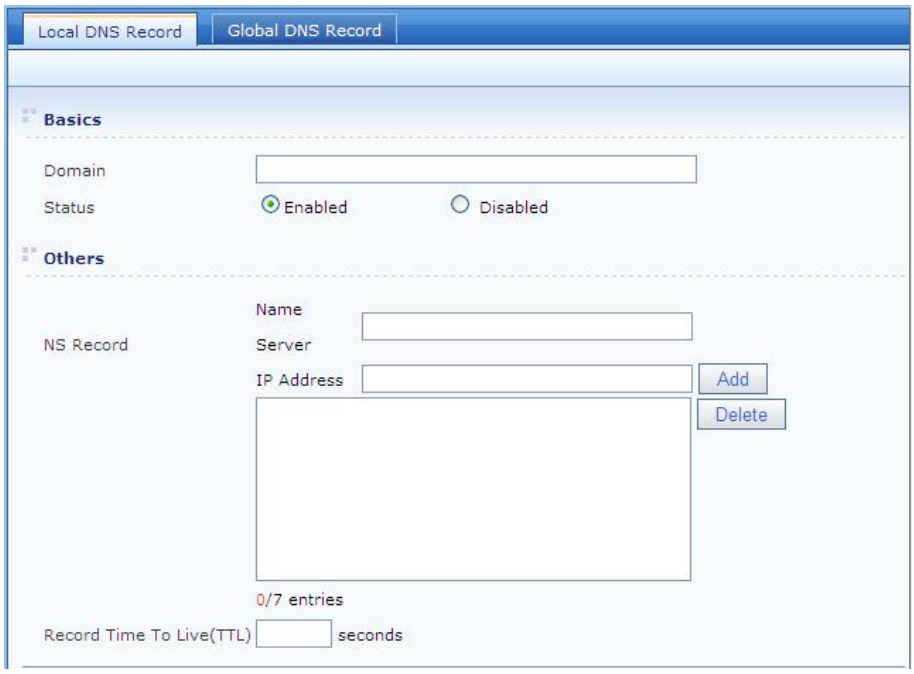
Domain: Specifies the domain name.

Status: Select **Enabled** to enable the MX record.

MX Records: Specifies the MX record corresponding to a domain. MX record is for locating the mail server based on the recipient address suffix when email is delivered. **Host** indicates the host name of the mail server. **Priority** indicates the priority of the MX record. The higher the value, the lower the priority. **TTL** indicates the time the record cached on the local DNS, in second.

For **NS record**, the attributes are as follows:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Domain: Specifies the domain name.

Status: Select **Enabled** to enable the NS record.

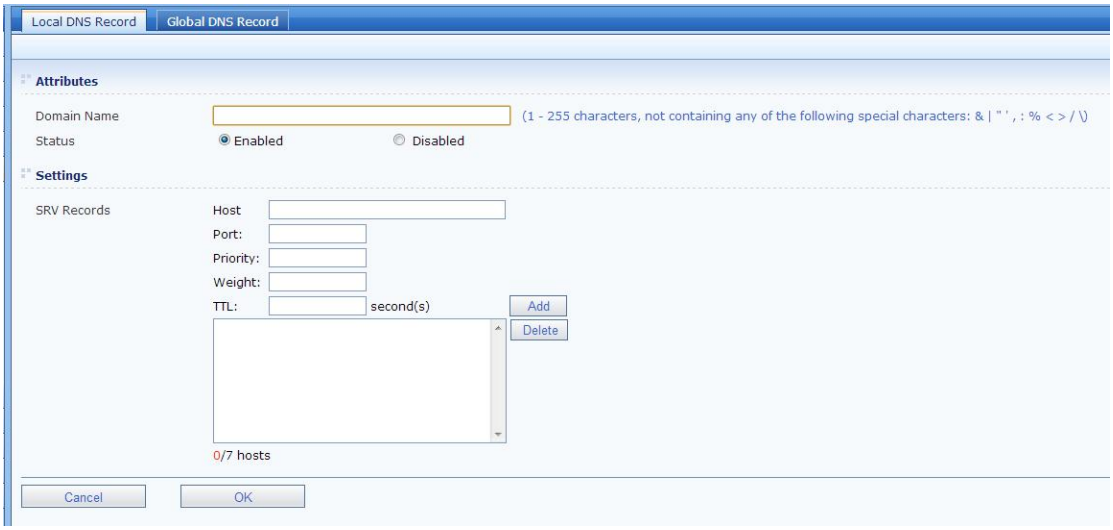
NS Record: Specifies the NS record corresponding to a domain. NS record is for specifying DNS server to resolve a specific domain name.

Name Server: Indicates the domain name of the name server.

IP Address: Indicates the IP address of the name server.

Record Time To Live(TTL): Specifies the time the record cached on the local DNS, in second.

For **SRV record**, the attributes are as follows:



Domain Name: Specifies the domain name.

Status: Select **Enabled** to enable the SRV record.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

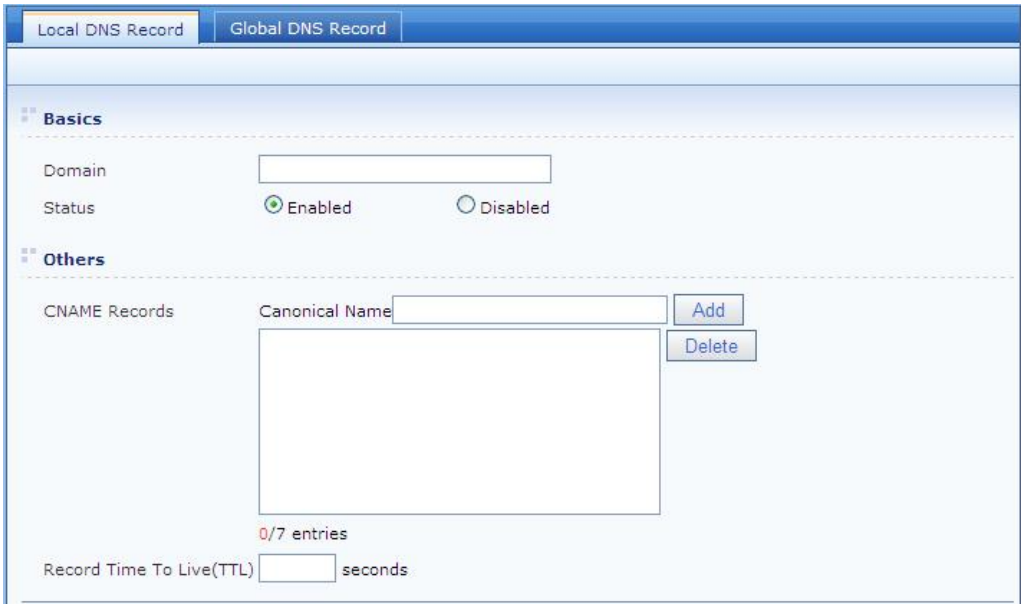
SRV Records: Specifies the SRV record corresponding to a domain. **Host** indicates the host name. **Port** indicates port of the host. **Priority** indicates the priority of the servers providing the same service. **Weight** indicates weight of the SRV record, the higher the value, the lower the priority. **TTL** indicates the time the record cached on the local DNS, in second.

Add: To add SRV record to the SRV records pool, click **Add**.

Delete: To delete the selected SRV record(s), click **Delete**.

To save the changes, click **OK**. To cancel the changes, click **Cancel**.

For **CNAME record**, the attributes are as follows:



Domain: Specifies the domain name.

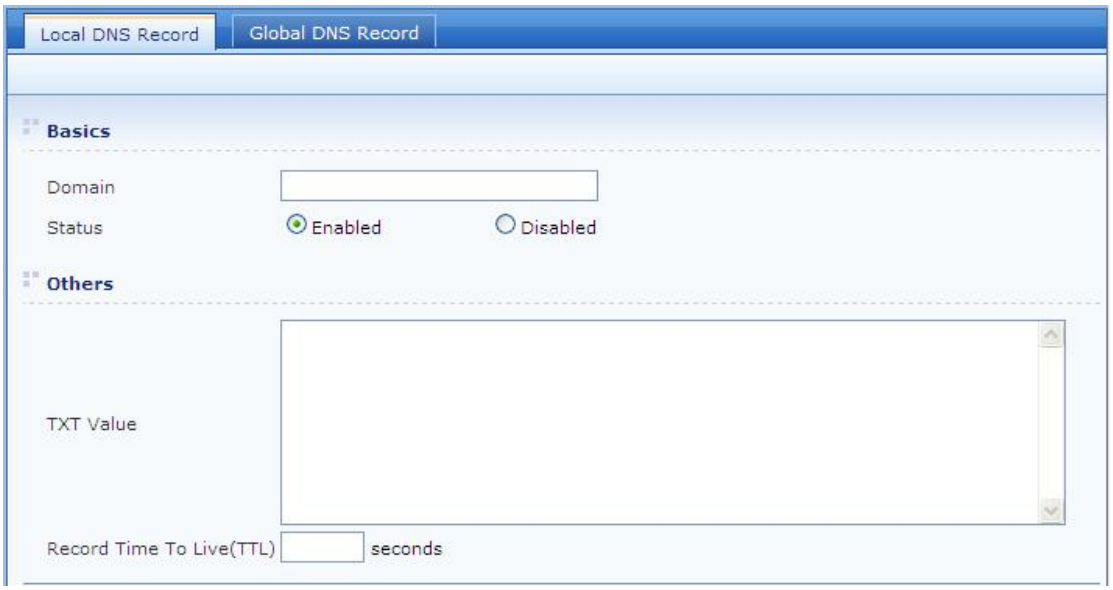
Status: Select **Enabled** to enable the CNAME record.

CNAME Records: Specifies the CNAME record corresponding to a domain. Canonical name indicates the name of the DNS record.

Record Time To Live(TTL): Specifies the time the record cached on the local DNS, in second.

For **TXT record**, the attributes are as follows:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



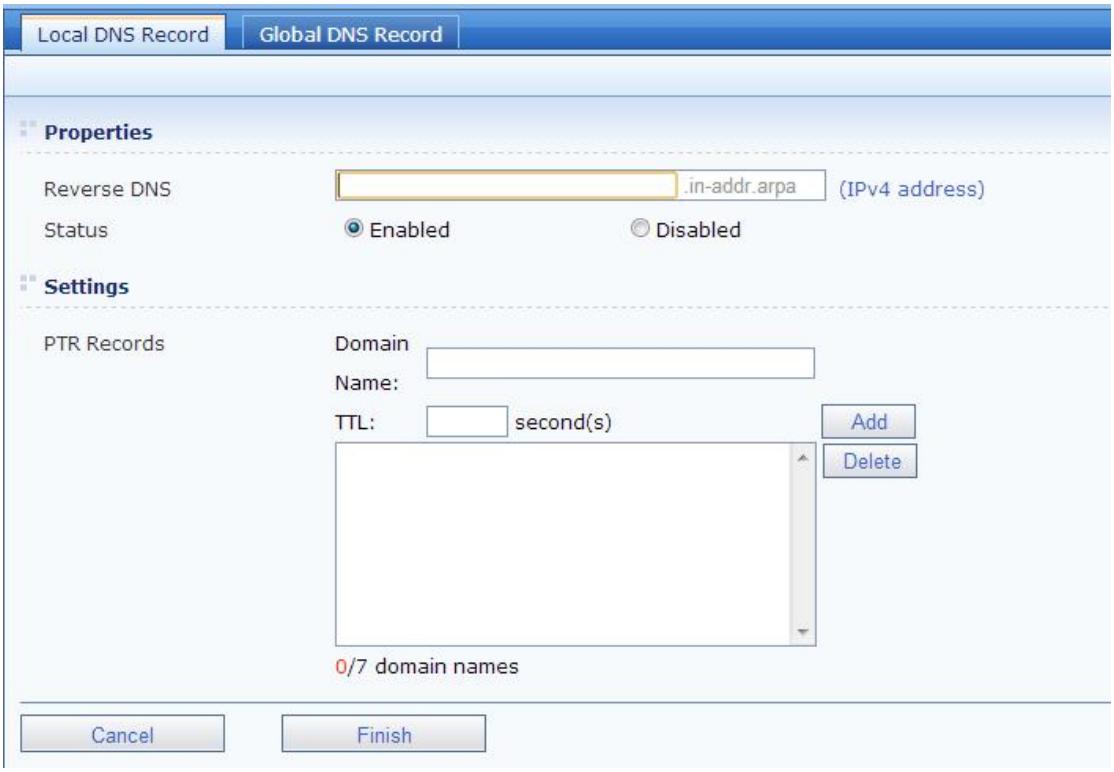
Domain: Specifies the domain name.

Status: Select **Enabled** to enable the TXT record.

TXT Value: Specifies the text.

Record Time To Live(TTL): Specifies the time the record cached on the local DNS, in second.

For **PTR records**, the attributes are as follows:



Reverse DNS: Specifies domain name of the PTR record. Enter an IPV4 address in an reversed

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

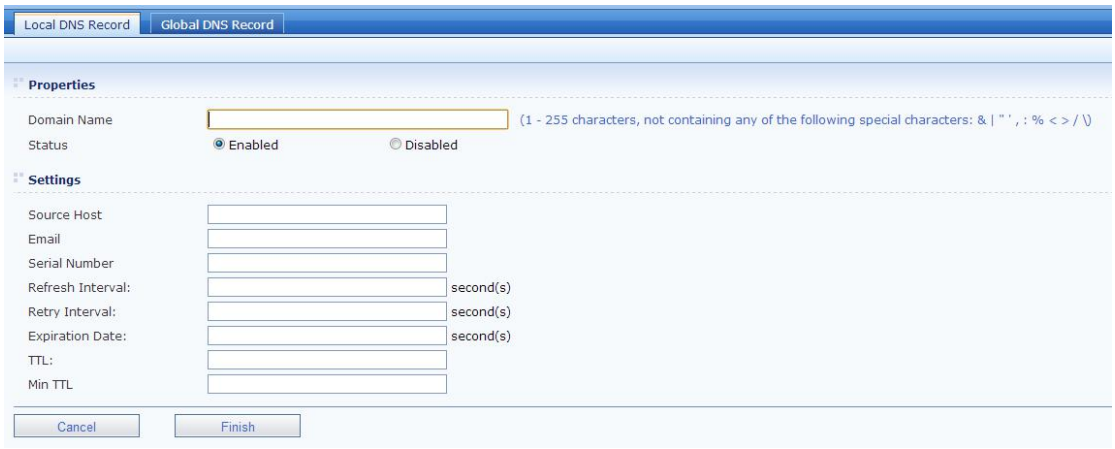
order.

Status: Select **Enabled** to enable the PTR record.

PTR Records: Specifies the PTR record corresponding to a domain**. Domain Name** indicates the domain name. **TTL** indicates the time the record cached on the local DNS, in second.

To save the changes, click Finish. To cancel the changes, click Cancel.

For **SOA records**, the attributes are as follows:



Domain Name: Specifies the domain name.

Status: Select **Enabled** to enable the SOA record.

Source Host: Specifies source host of SOA.

Email: Specifies email address

Serial Number: Indicates a hint when the zone was updated last time and is increased at every change.

Refresh Interval: Specifies how often a secondary will poll the primary server to see if the serial number for the zone has increased(so it knows to request a new copy of the data for the zone), in second. Default is 900 seconds(15 minutes).

Retry interval: If a secondary was unable to contact the primary at the last refresh, wait the retry value before trying again. It is typically some fraction of the refresh interval. Default is 600 seconds(10 minutes).

Expiration Date: How long a secondary will still treat its copy of the zone data as valid if it can't cantact the primary. This value should be greater than how long a major outage would typically last, and must be greater than the minimum and retry intervals, to avoid having a secondary expire the data before it gets a change to get a new copy. After a zone is expired a secondary will still continue to try to contact the primary, but it will no longer provide

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

nameservice for the zone. Default is 86,400 seconds(24 hours).

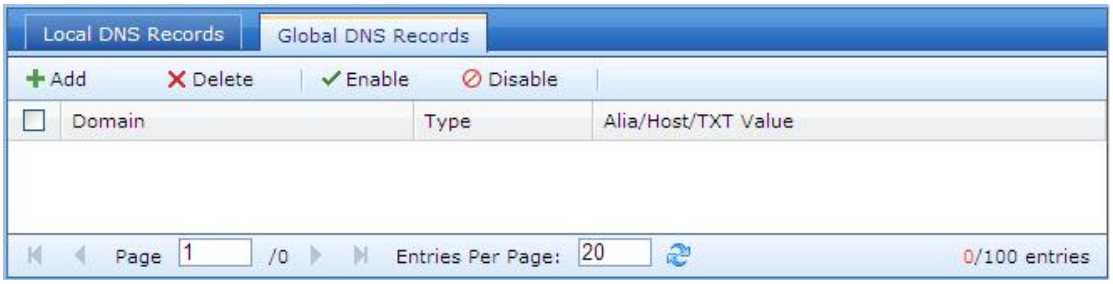
TTL: Indicates the time the record cached on the local DNS, in second.

Min TTL: Indicates the default time the record cached on the local DNS, in second.

To save the changes, click **OK**. To cancel the changes, click **Cancel**.

8.2.2 Configuring Global DNS Record

Global DNS record is used in situation that there are more than one sites. The records are the ones that need to be resolve by this ADC when it works as a global DNS server. Global DNS record configuration at each site can be synchronized among each other. To add a record, refer to the above section.



In cluster environment, global DNS records is not supported, only local DNS records is supported.

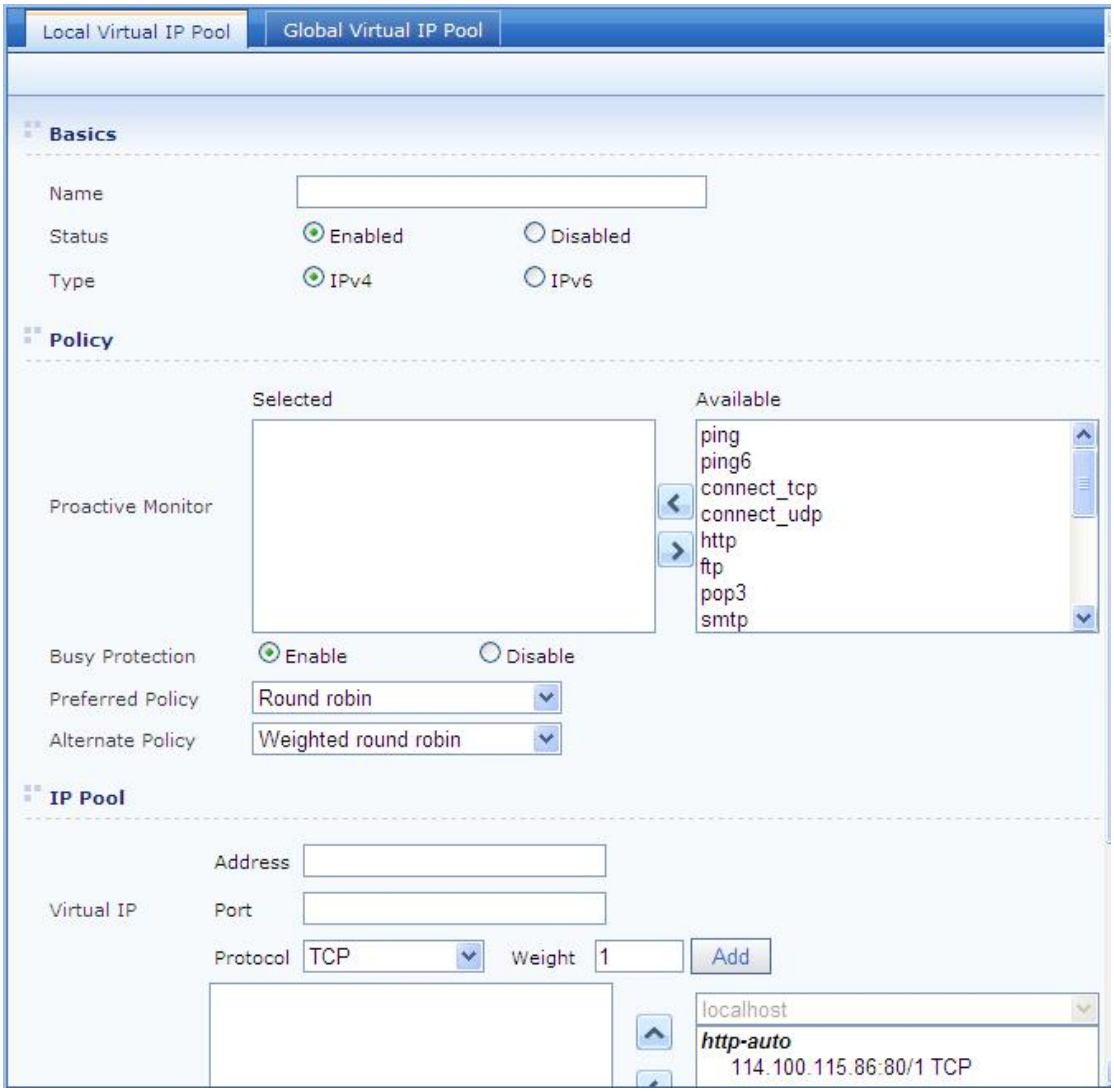
8.3 Virtual IP Pool

Virtual IP pool is used to schedule requests from client to a specific IP address or port. On the ADC, DNS mapping works as the first round of scheduling, while virtual IP pool works as the second round of scheduling. There are local virtual IP pool and global virtual IP pool, the former is applicable when there is only one site; the latter is applicable when there are a cluster of sites scattered across the network and virtual IP pool settings can be synchronized among the clustered sites.

8.3.1 Local IP Pool

To create a new local virtual IP pool, navigate to **Intelligent DNS** > **Virtual IP Pool** > **Local Virtual IP Pool**, click **Add** and configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Status: Select **Enabled** to enable the virtual IP pool.

Type: Choose what IP addresses are included in the virtual IP pool, IPv4 or IPv6 address.

Proactive Monitor: Select monitor from the available monitor list to monitor if the IP address and port in the pool are normal.

Busy Protection: Select **Enable** to enable so that busy IP address and port will not be forwarded with any request.

Preferred Policy: Specifies the policy preferred to perform scheduling among the virtual IP addresses in the pool. Options are **Round robin**, **Weighted round robin**, **The first is available**, **Hash**, **Weighted least connect**, **Weighted least traffic**, **Round trip time**, **Static proximity** and **Return all IP**.

Alternate Policy: Specify the alternative policy for scheduling among the virtual IP addresses in the pool. Options are **Round robin**, **Weighted round robin**, **The first is available**, **Hash**, **Weighted least connect**, **Weighted least traffic**, **Round trip time**, **Static proximity, Return all IP**, **Return standby IP**, **Deny** and **Drop**. The following are brief introductions to each option:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Round robin: IP addresses in the pool take turns to deal with new requests.

Weighted round robin: IP address in the pool is chosen to deal with new requests based on weight.

The first is available: IP addresses in the pool are matched from top to button, and the first matching IP address deal with the new request.

Hash: An IP address is recommended after hash calculation of source IP address in the DNS request.

Weighted least connect: The IP address with the least connections (calculated based on weight) will take the load.

Round trip time: The IP address taking the least DNS response time on specific link (tested based on DNS server setting) will take the load.

Weighted least traffic: The IP address loads the least traffic on specific link (tested based on weight) will take the load.

Static proximity: The IP address is chosen based on the LDNS setting in Intelligent DNS > Static Proximity > Virtual IP Pool Based static proximity (Refer to Chapter 7.7 Static proximity).

Return all IP: No IP address will be filtered. All the IP addresses in the pool are available to the client.

Deny: When scheduling based on the preferred policy fails, access denied information is returned to client.

Drop: When scheduling based on the preferred policy fails, DNS request packets are discarded, and no response is given.

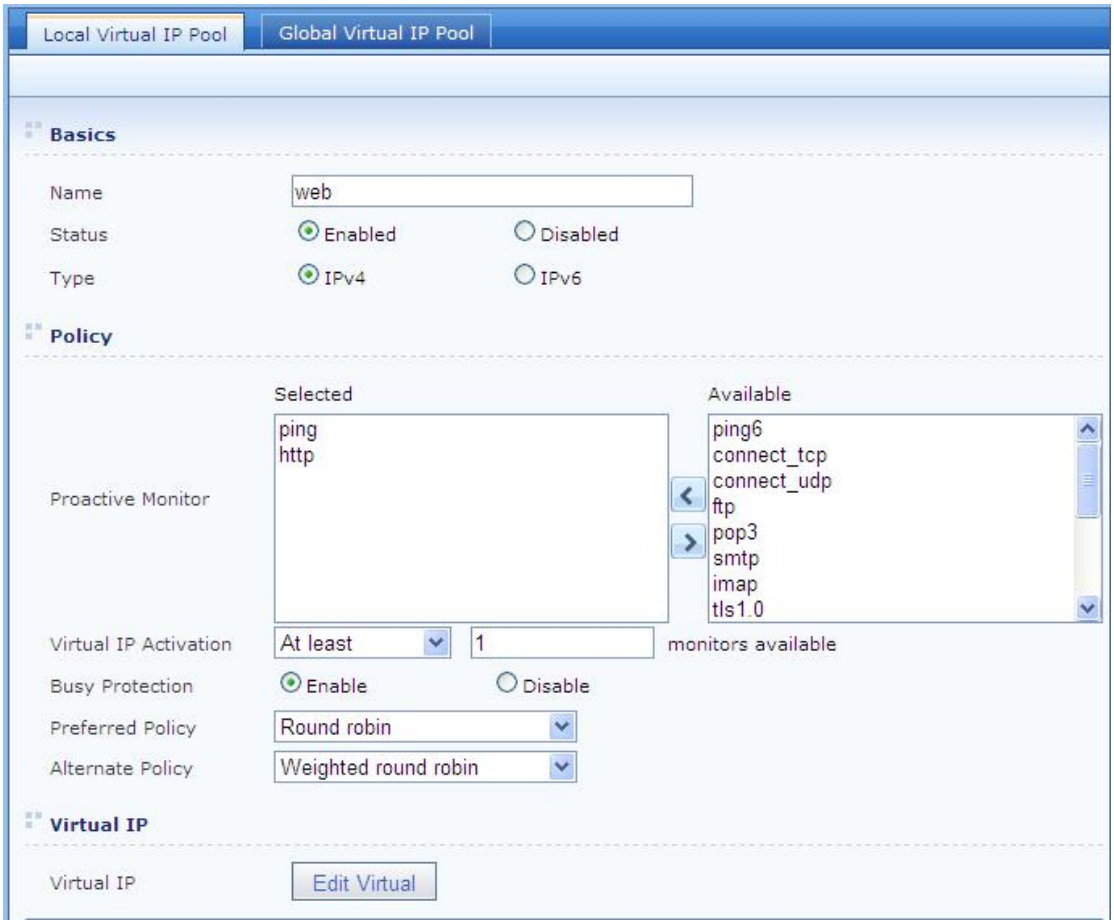
Return the standby IP: The specified IP address takes the load when scheduling based on the alternate policy fails. Setting is as follows:



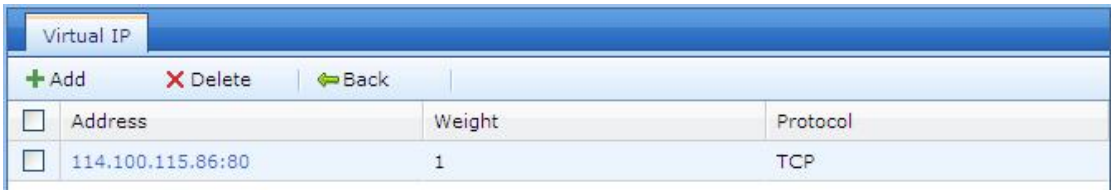
IP Address: Specifies the IP addresses and ports included in the virtual IP pool. They are launched to external network.

To edit an existing virtual IP pool, click on the pool name. Attributes of a pool are as follows:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To edit settings of a virtual IP address in the pool, click on the **Edit Virtual**button to enter the following page:



Click on the address. You can change the weight and monitor type only, as shown in the following page:

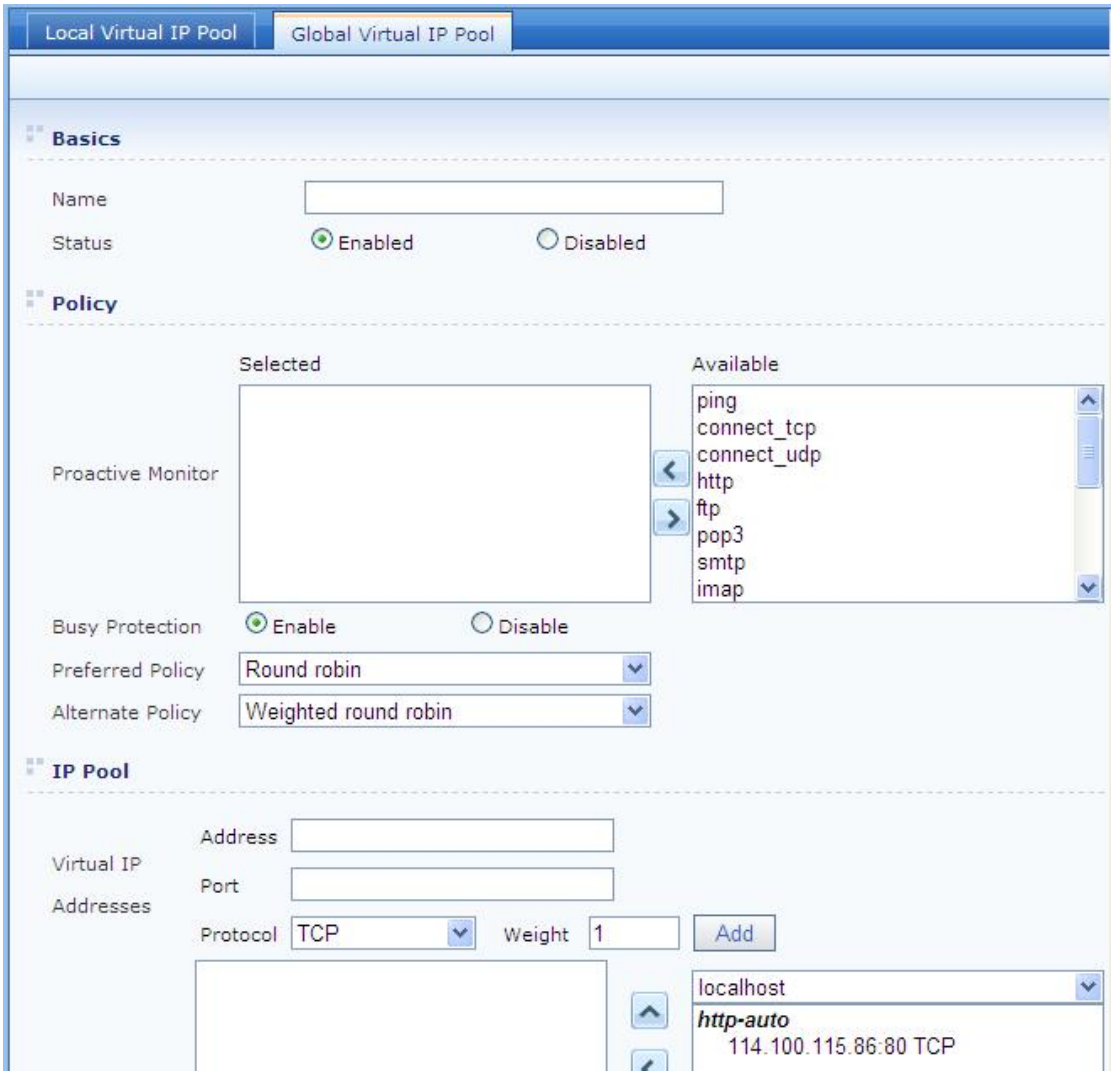


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

8.3.2 Global Virtual IP Pool

Global virtual IP pool is applicable when there are a cluster of sites scattered across the network and virtual IP pool settings can be synchronized among the clustered sites.

To add a global virtual IP pool, navigate to **Intelligent DNS** > **Virtual IP Pool** > **Global Virtual IP Pool**, click **Add** and configure the following contents:



Busy protection: Select **Enable** to enable so that busy IP address and port will not be forwarded with any request.

For other contents, see the above section.

In cluster environment, global DNS records is not supported, only local DNS records is supported.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

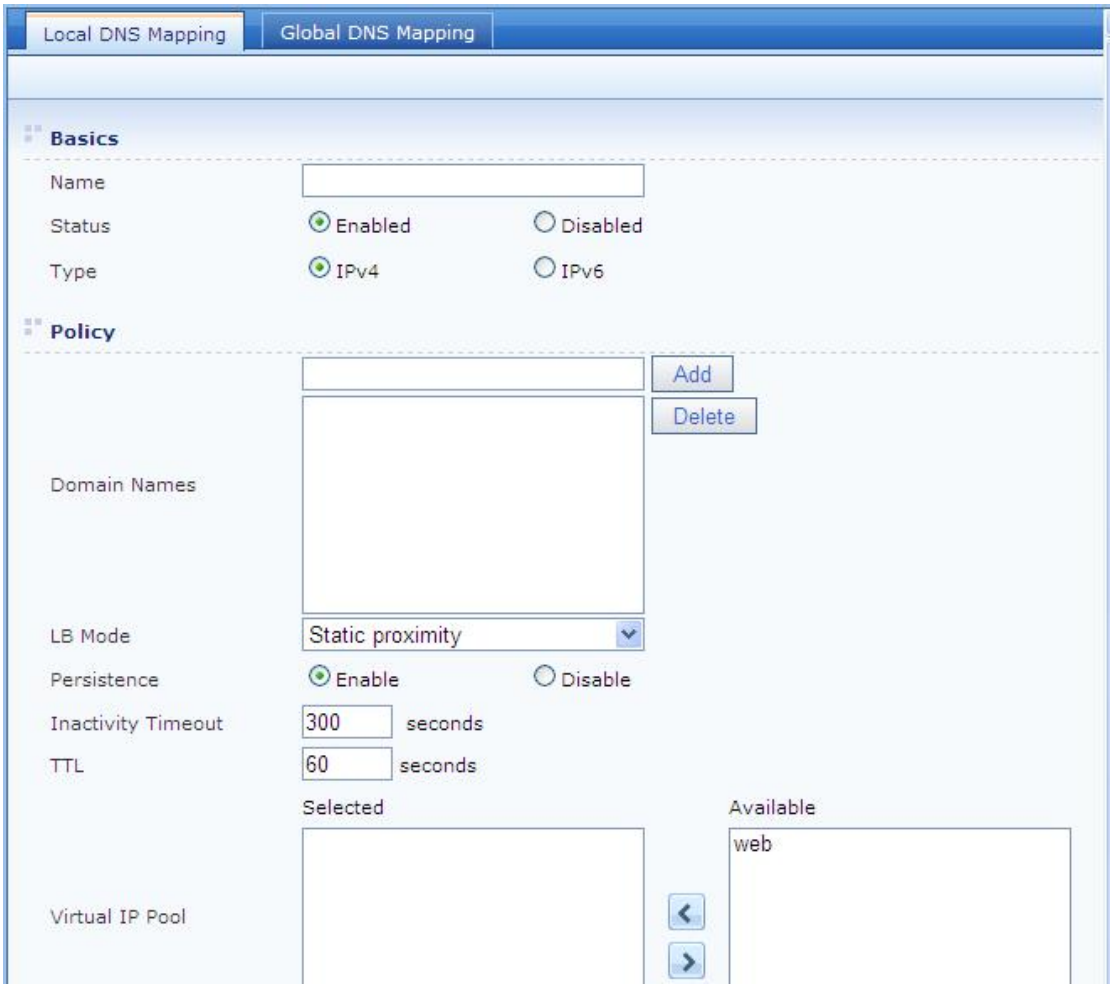
8.4 DNS Mapping

DNS mapping is the first round of scheduling for domain queries from client; request is scheduled to a virtual IP pool. Then comes the second round of scheduling; request is scheduled to a specific IP address and port in the virtual IP pool.

There are two types of DNS mappings, **Local** and **Global**. Like local and virtual IP pools, global DNS mappings are applicable when there are a cluster of sites scattered across the network and settings can be synchronized among the clustered sites, while local DNS mappings are applicable when there is only one site.

8.4.1 Local DNS Mapping

To create a new local virtual IP pool, navigate to **Intelligent DNS** > **Virtual IP Pool** > **Local DNS Mapping**, click **Add** and configure the following contents:



Name: Give it a distinguishable name.

Status: Select **Enabled** to enable the DNS mapping.

Type: Choose what type of IP address is applicable, IPv4 or IPv6 address.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Domain Names: Specifies the domains you want to map.

LB Mode: Specifies the scheduling policy of DNS mapping. Options are **Static proximity**, **Round robin** and **Weighted round robin**. The following are brief introductions to each option:

Static proximity: The virtual IP pool is chosen based on the LDNS setting in **Intelligent DNS** > **Static Proximity** > **Virtual IP Pool Based** static proximity.

Round robin: Virtual IP pool take turns to deal with new requests.

Weighted round robin: A virtual IP pool is chosen to deal with new requests based on weight.

Persistence: Select **Enable** to enable the persistence for the virtual IP pool chosen at the phase of DNS mapping, so that requests from same source before timeout are scheduled to a same virtual IP pool.

Inactivity Timeout: Specifies the time period before persistence gets invalid, in second.

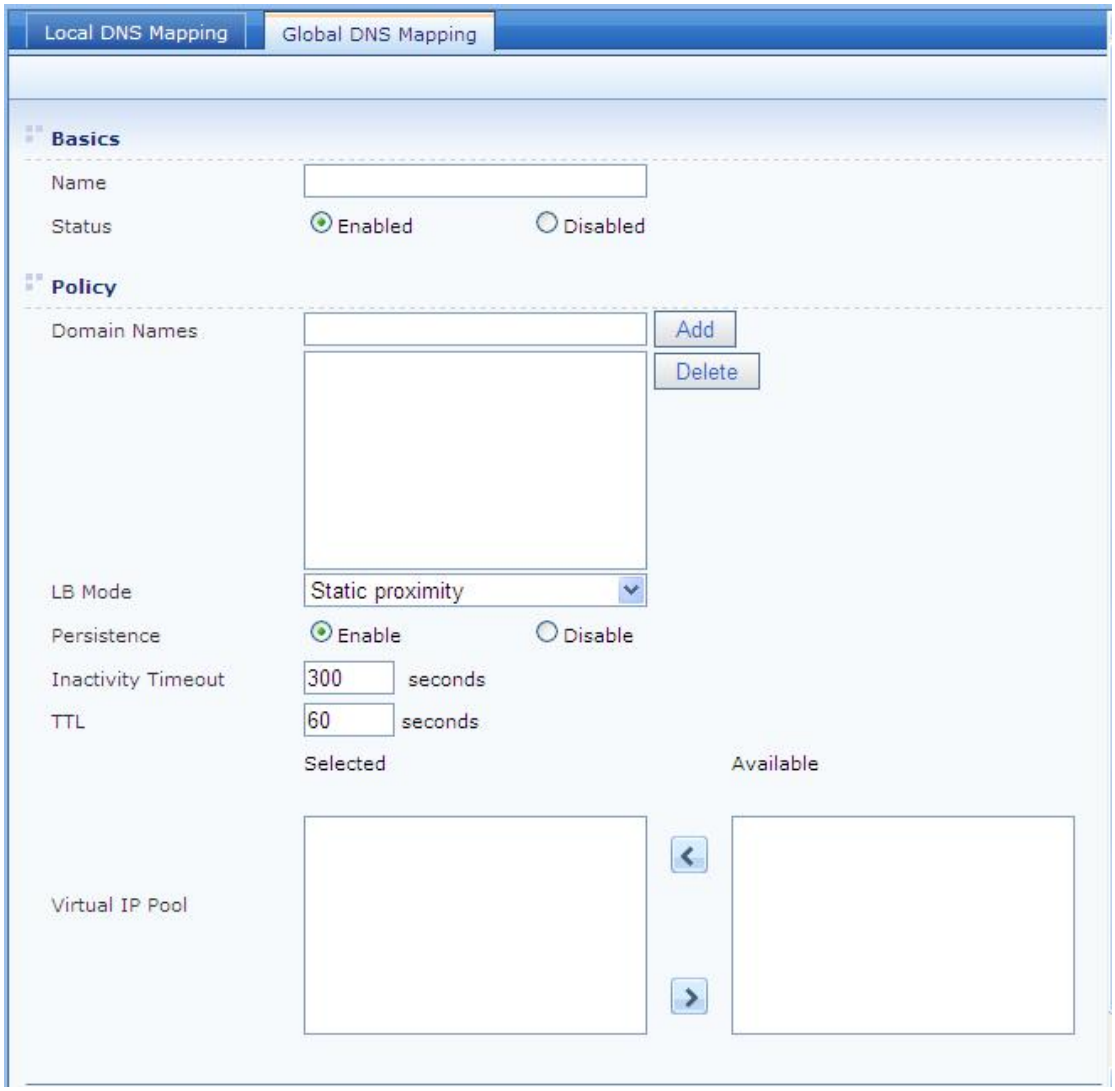
TTL: Specifies the time that mapped domain will be cached, in second.

Virtual IP Pool: Specifies the virtual IP pool to which the requests are scheduled during local DNS mapping phase.

8.4.2 Global DNS Mapping

Global DNS mappings are applicable when there are a cluster of sites scattered across the network. Scheduling is performed among many virtual IP pools configured on more than one sites and settings can be synchronized among the clustered sites.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



The contents are nearly the same with local DNS mapping. The only difference is the available virtual IP pools are configured in **Intelligent DNS** > **Virtual IP Pool** > **Global Virtual IP Pool**.

In cluster environment, global DNS records is not supported, only local DNS records is supported.

8.5 LDNS

In LDNS, you can define the network segments which the local DNS of each site is located in. They are also used in scheduling based on static proximity.

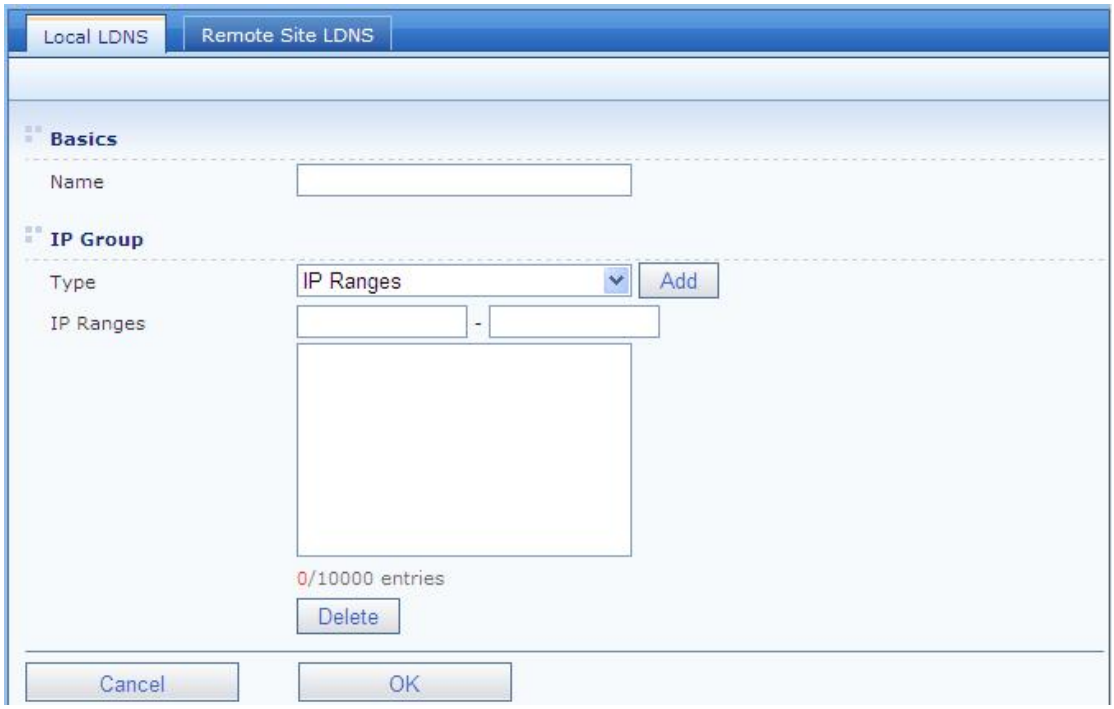
There are local LDNS and remote site LDNS. Like local and global virtual IP pools and DNS mappings, the remote site LDNS is applicable when there are a cluster of sites scattered across the network and settings can be synchronized among the clustered sites, while local

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

LDNS is applicable when there is only one site.

8.5.1 Local LDNS

To add a new local LDNS, navigate to **Intelligent DNS** > **LDNS** > **Local LDNS**, click **Add** and configure the following contents:



Name: Give it a distinguishable name.

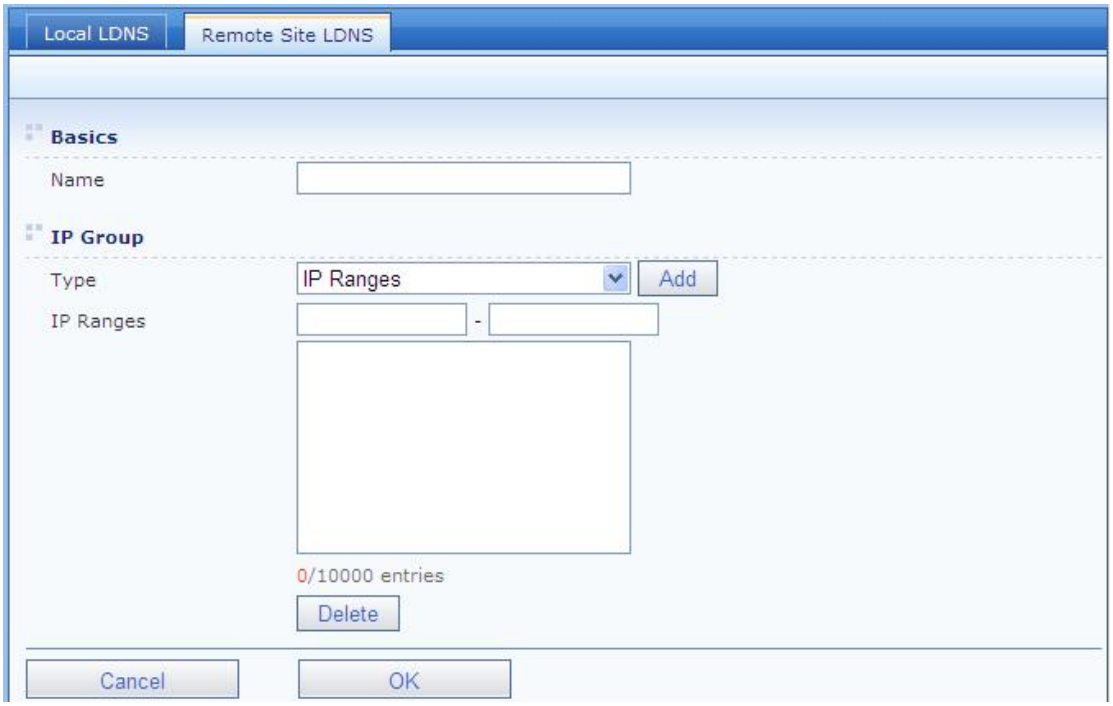
Type: Choose what type of IP address you want to add into the IP group, IP range, ISP, continent or .region IP address. For IP range, specify the start and end IP and then click **Add**. For **ISP**, select an ISP option from the pull-down list and then click **Add**; for **Continent**, select country, region or state to add IP addresses in the corresponding area and then click **Add**; for **Region**, select a region from the pull-down list and click **Add**.

It does not support the global DNS LOAD feature and only supports the local intelligent DNS in the cluster deployment environment.

8.5.2 Remote Site LDNS

They are also used in scheduling based on static proximity.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



For introduction to the above contents, see the above section.

8.6 Static Proximity

Static proximity specifies the scheduling algorithm and used in two phases of scheduling, DNS mapping and virtual IP pool.

8.6.1 DNS Mapping Based Static Proximity

Navigate to **Intelligent DNS** > **Static Proximity** > **DNS Mapping Based**, click **Add** and configure the following contents:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Status: Select **Enabled** to enable DNS mapping based static proximity.

Site: Select which sites you want the specified static proximity applied to, Local site or Remote sites.

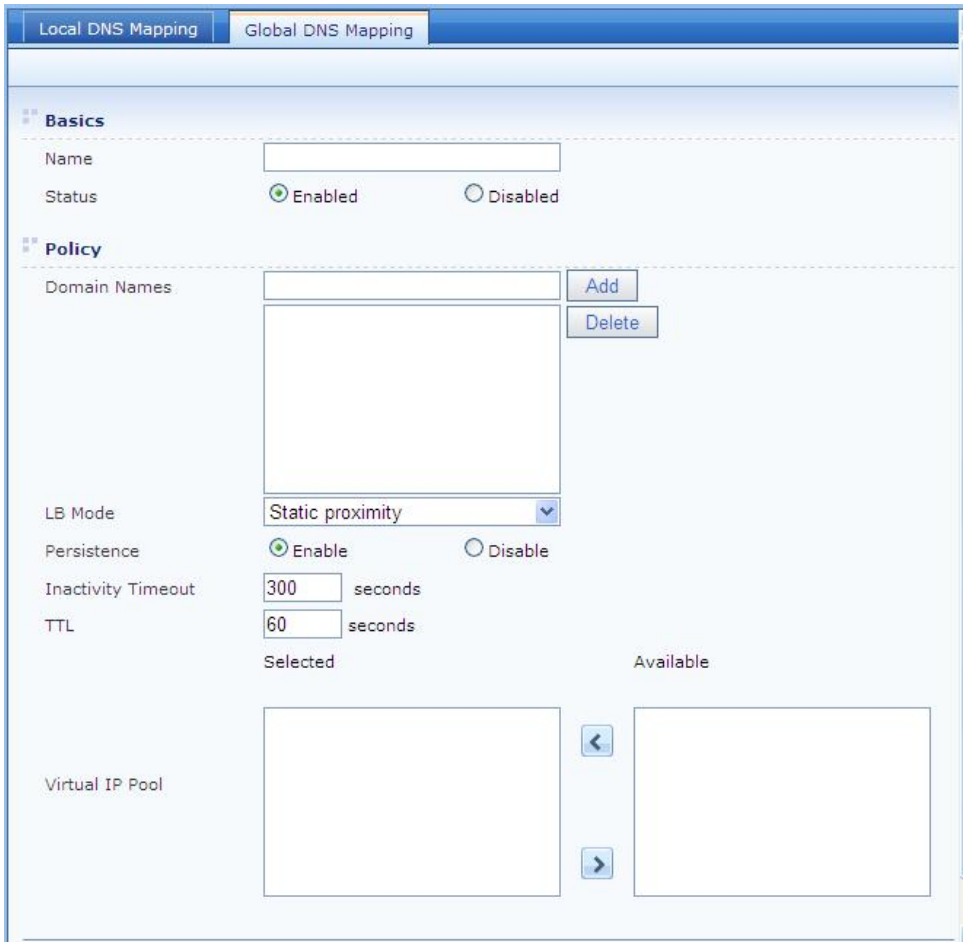
DNS Mapping: Specifies DNS mapping for the target domain. Options for local and remote site vary, since they come from the respective DNS mapping configurations.

LDNS: Specifies the LDNS for the region where the client is located. Options for local and remote site vary, since they come from the respective LDNS configurations.

Virtual IP Pool: Specifies the virtual IP pool that will be chosen to take the load if the above DNS mapping and LDNS credential are satisfied.

8.6.2 Configuring Global DNS Mapping

Global DNS mappings are applicable when there are a cluster of sites scattered across the network. Scheduling is performed among many virtual IP pools configured on more than one sites and settings can be synchronized among the clustered sites.



The contents are nearly the same with local DNS mapping. The only difference is the

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

available virtual IP pools are configured in **Intelligent DNS** > **Virtual IP Pool** > **Global Virtual IP Pool**.

It does not support the global DNS LOAD feature and only supports the local intelligent DNS in the cluster deployment environment.

8.7 Backup/Restore

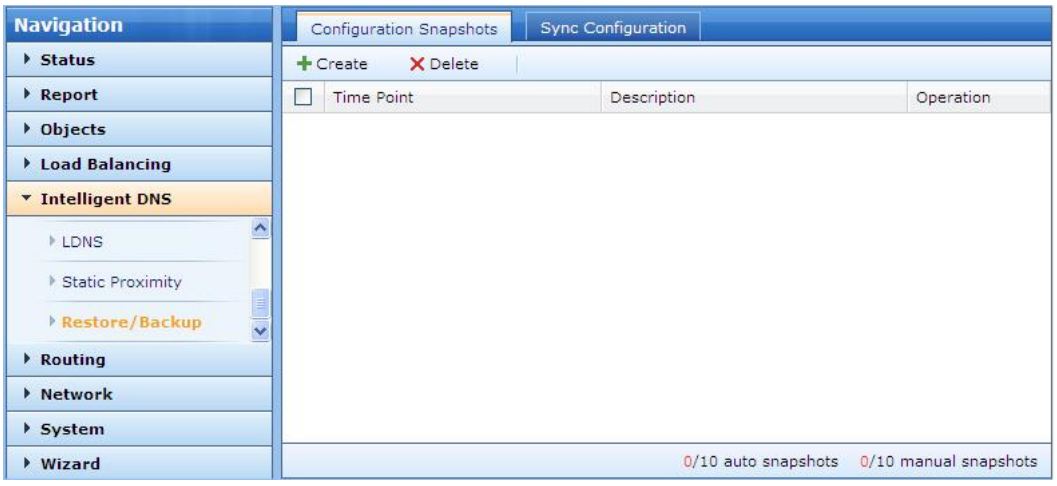
8.7.1 Taking Configuration Snapshot

Snapshot taken here is configuration of intelligent DNS and Web UI administrator accounts. If this ADC acts as server in cluster, you can also choose what configuration can be synchronized to other sites.

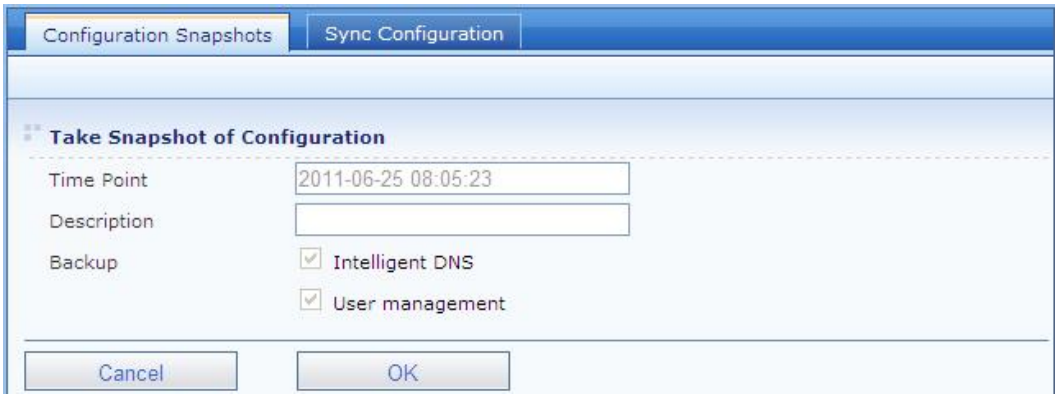
To back up the intelligent DNS configuration and Web UI administrator accounts, perform the following steps:

Configuration Snapshots.

1. Navigate to **Intelligent DNS** > **Restore/Backup** > **Configuration Snapshots**.



2. Click **Create** and configure the following contents:



Time Point: Indicates the time when the configuration snapshot is taken.

Description: Give it brief description.

Backup: Indicates what contents are backed up.

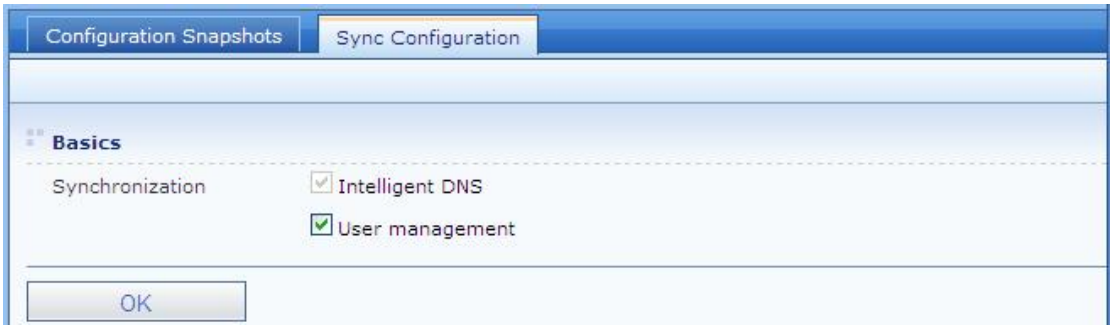
3. Click **OK** to save the settings, or click **Cancel** to give up the settings. A snapshot taken successfully is shown below:



4. To restore configuration to the time point, click **Restore**.

8.7.2 Synchronizing Configuration to Other Sites

If this ADC operates as server in cluster, you can also choose what configuration can be synchronized to other sites, simply by navigating to **Intelligent DNS** > **Restore/Backup** > **Sync Configuration** and selecting the options.



Intelligent DNS is selected and will be synchronized to other sites by default. It includes global settings, such as global DNS records, global virtual IP pool, global DNS mapping, remote site DLNS and the global setting part of statistics proximity. User management indicates the Web UI administrator accounts. It includes administrator and role settings.

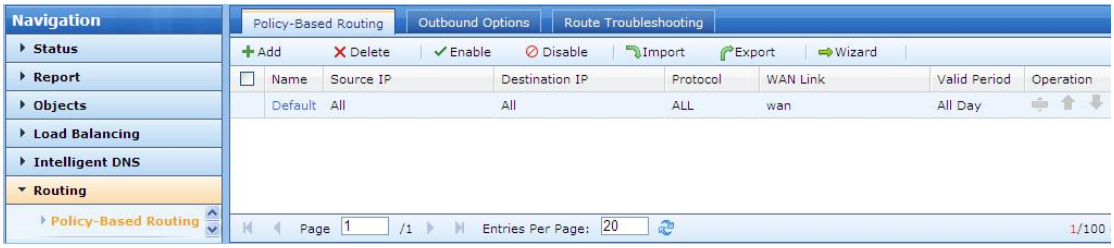
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 9 Routing

More than one routing options are available on the Application Delivery Controller(ADC) to meet various deployment requirements, namely, policy-based routing, static route, virtual route, IP anycast, RIP, OSPF and OSPFv3.

9.1 Policy-Based Routing

When there are more than one WAN interfaces, policy-based routing can be configured, so that data packets are routed on specific link and forwarded on specified WAN interface, based on the source and/or destination. Traffic separated in this way can improve bandwidth utilization.



Click **Enable** to enable a policy-based routing, or click **Disable** to disable it. Please note that the predefined policy-based routing can not be disabled.

To remove the selected policy-based routing, click **Delete**. But the predefined policy-based routing can not be deleted.

To import policy-based routing, click **Import** to enter the following page**.**



Click **Browse** to select a local backup file for policy-based routing. Click **Import** to add the file, or click **Cancel** to give up the operation.

Click **Wizard**, you will enter the following page:

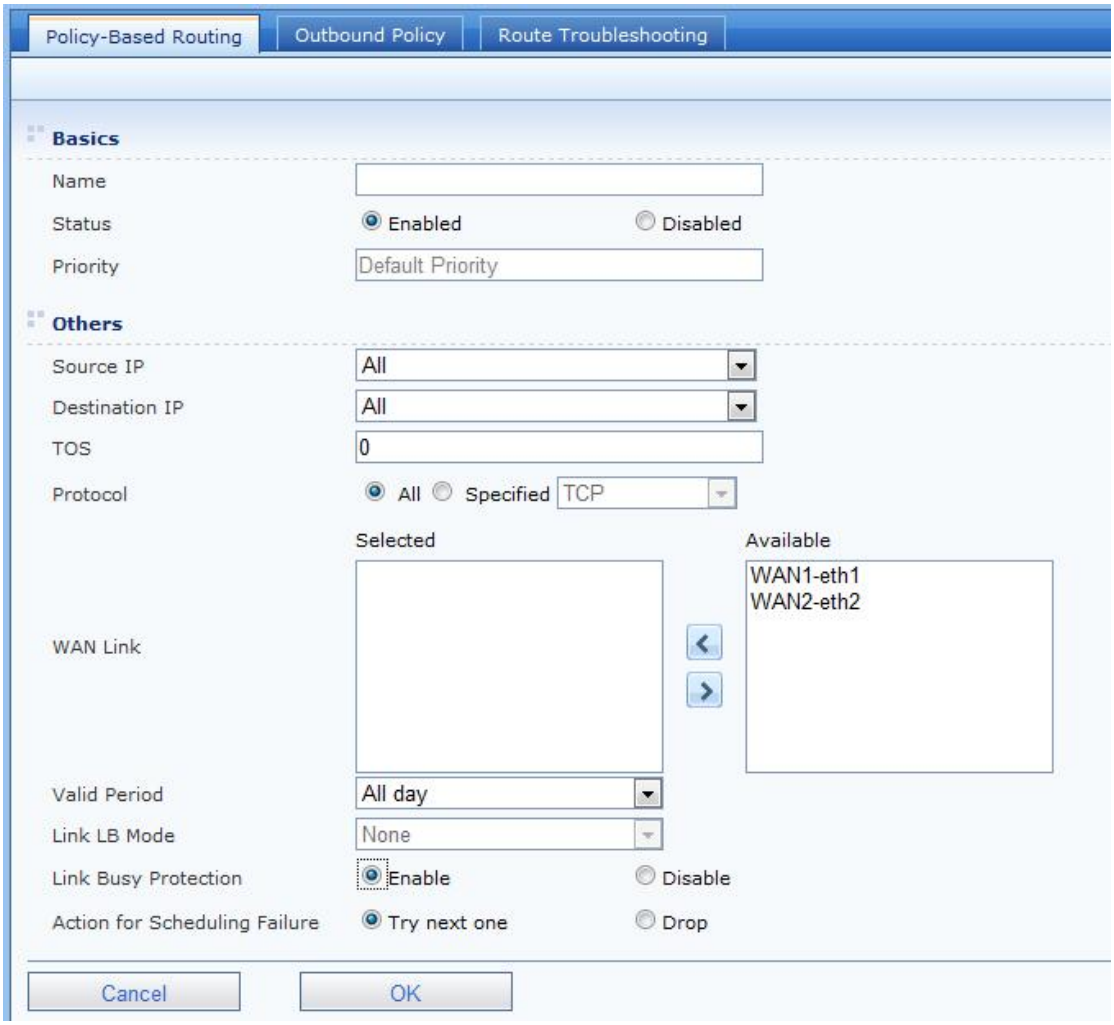
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To create a policy-based routing entry, perform the following steps.

9.1.1 Policy-Based Routing

Navigate to **Routing** > **Policy-Based Routing**, click **Add** and configure the following contents:



Name: Give it a distinguishable name.

Status: Select **Enabled** to enable the routing.

Source IP: Specifies the source IP address that matches the routing. It can be an IP address, IP range, subnet or local IP group.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Destination IP: Specifies the destination IP address that matches the routing. It can be an IP address, IP range, subnet, ISP IP group or domain.

TOS distinguishes application layer traffic and provides different links to policy-based routing. It supports application drainage, application identification and policy-based routing.

Protocol: Specifies a protocol for the policy-based routing. Options are **All** and **Specified**. If **Specified** selected, you can select TCP, UDP, ICMP or others, and define source and destination port number.

WAN Link: Select one WAN link from **Available** box and add it to **Selected** box.

Valid Period: Specifies a valid period for the policy-based routing. The policy-based routing is invalid beyond the specified valid period.

Link LB Mode: When the number of WAN links are not less than two, specify a link LB mode, including **Round robin**, **bandwidth usage**, **Weighted least traffic**, **Round Trip Time**.

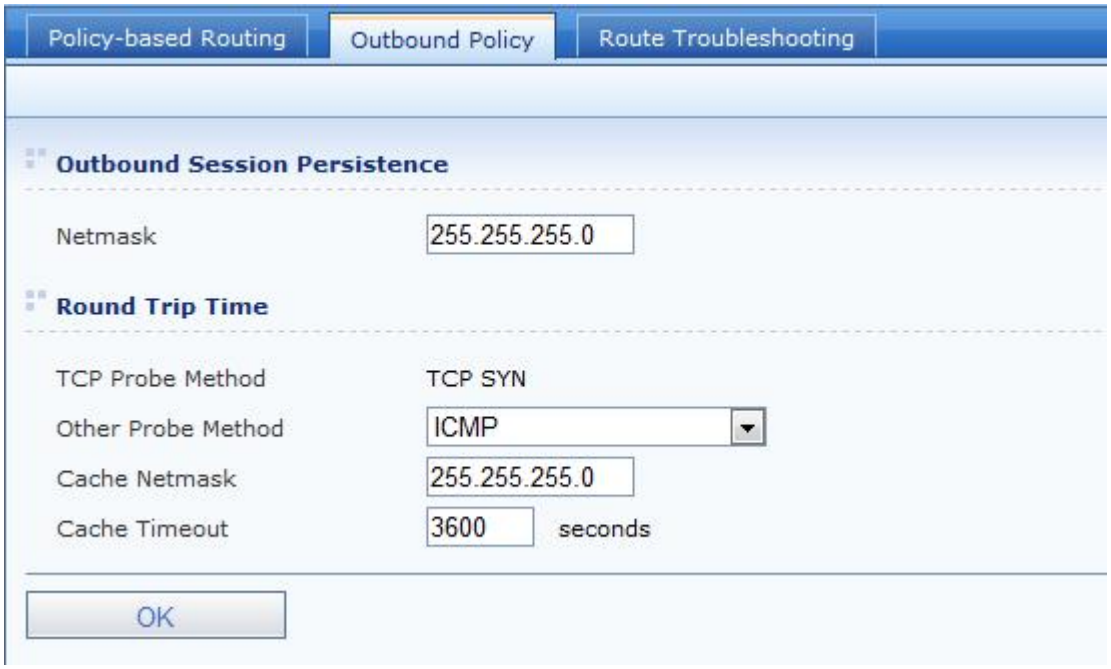
Link Busy Protection: If **Enable** selected, when the link is busy, it will no be scheduled; if all links are busy, then link scheduling will fail.

Action for Scheduling Failure: Select **Try next one** to match next rule when scheduling failure occurs.

Click **Finish** to save the settings, or **Cancel** to give up the changes.

9.1.2 Outbound Options

Navigate to **Routing** > **Policy-Based Routing** > **Outbound Policy**, set properties of outbound data, as shown in the following figure.



Netmask: Specifies a netmask. Make a same session persistence for the accesses from different external IP which belong to a same network number through that netmask.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

TCP Probe Method: Indicates the device will send TCP SYN to destination address for detecting, when the outbound based on TCP protocol requests a destination address.

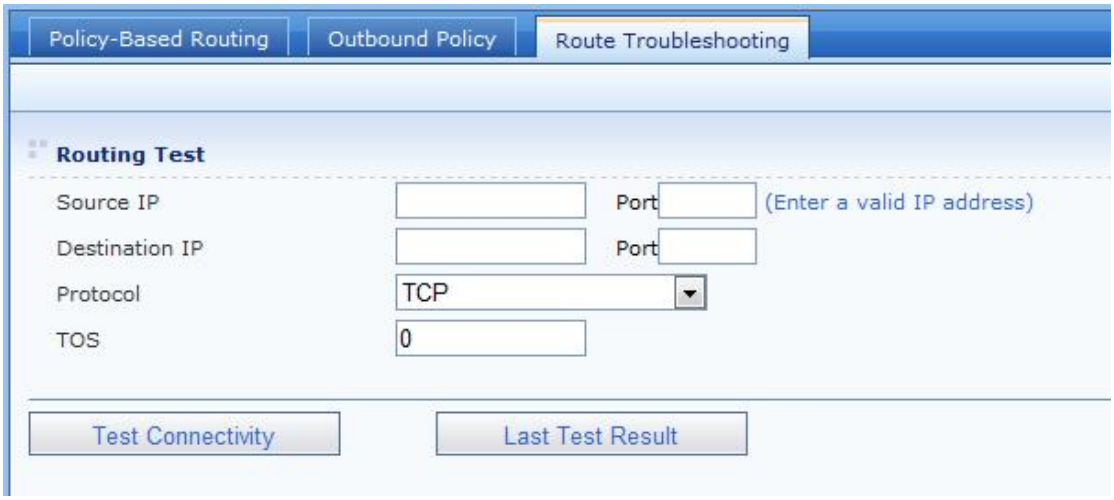
Other Probe Method: Specifies the probe method for the requests based on other protocols except for TCP protocol.

Cache Netmask: Specifies a netmask to make different external IP belonging the same network number use the same link selected by the Round Trip Time.

Cache Timeout: Specifies the timeout of caching round trip delay time.

9.1.3 Route Troubleshooting

Navigate to **Routing** > **Policy-Based Routing** > **Route Troubleshooting**, configure the following contents:



Source IP: Specifies source IPv4 address for routing rest. If the protocol is TCP/UDP, port number is needed.

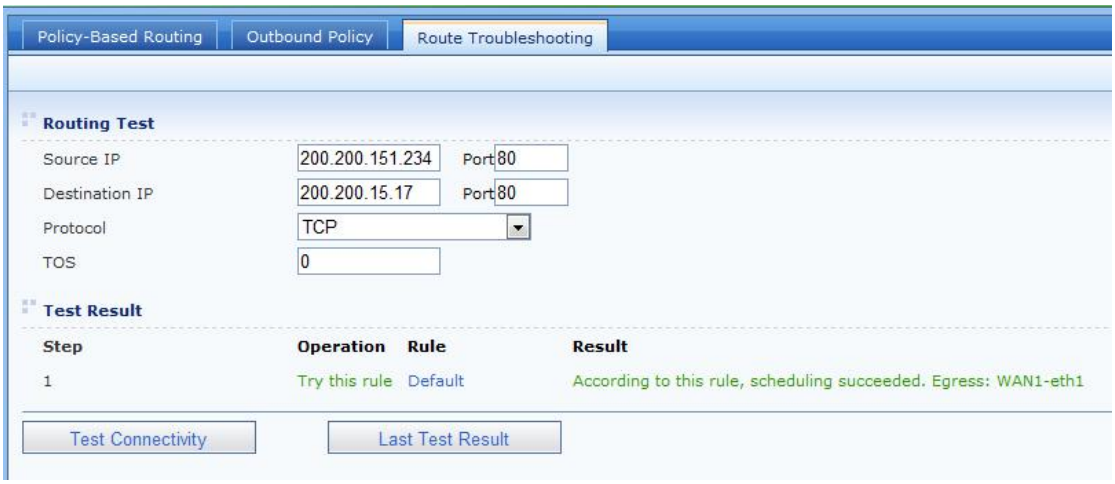
Destination IP: Specifies destination IPv4 address for routing rest. If the protocol is TCP/UDP, port number is needed.

Protocol: Specifies a protocol for test. If the protocol is not in the list, select **Others** and specify the protocol number.

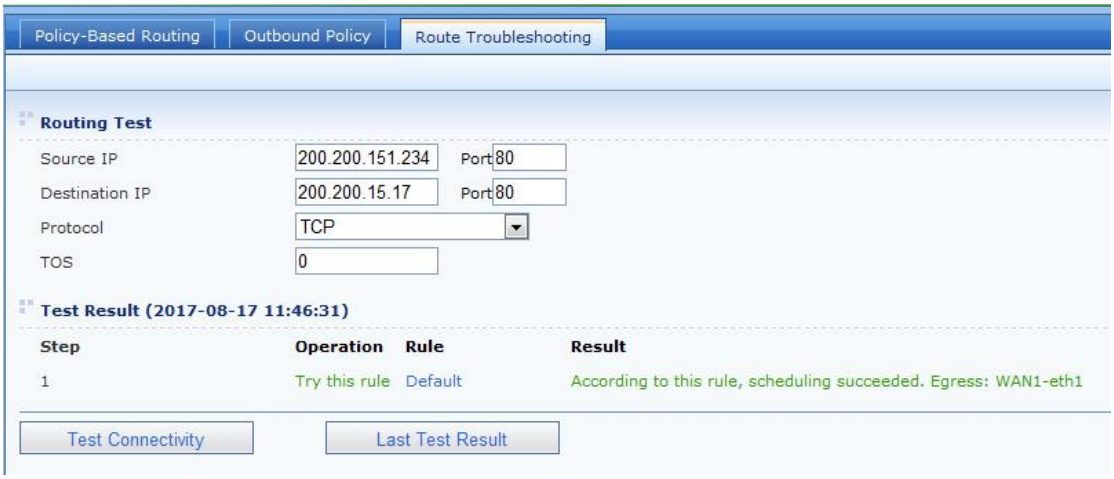
TOS: Specifies application layer traffic and provides different links to policy-based routing. It supports application drainage, application identification and policy-based routing.

Click **Test Connectivity**, route testing will be performed, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

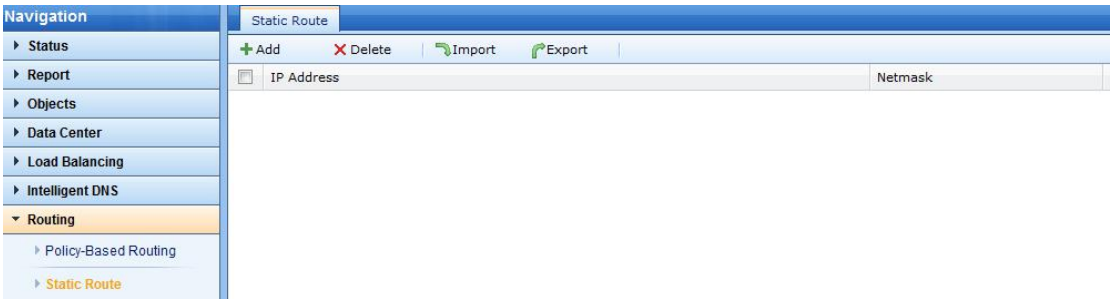


To view last routing test result and test time, click **Last Test Result,** as shown in the following figure:



9.2 Static Route

It' used to set routing entry for reaching non-ADC. And you can view the routing information here, as shown below:

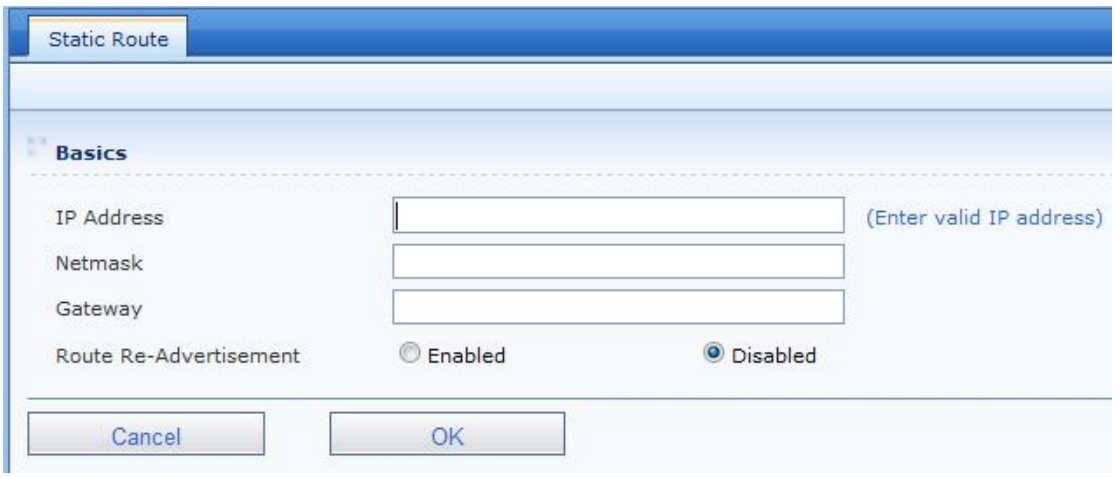


In **Routing** > **Static Route**, you can view the routing information of routing entries completed configuration.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

To remove the selected static routing, click **Delete**.

To create a new static routing, click **Add** and configure the following fields:



IP Address: Specifies a target network segment.

Netmask: Specifies the netmask of target network segment.

Gateway: Specifies next-hop IP address of target segment.

Route Re-Advertisement: Select **Enabled** to allow the static routing advertised through dynamic route protocol. when the target segment belongs to IPv6, this option is invalid.

Click **OK to** save the settings, or click **Cancel** to give up the settings.

To import a static routing, click **Import**, as shown in the following figure:



Click **Browse** to select a local backup file of static routing. Click **Import** to add the file to device, or click **Cancel** to give up the operation.

Click **CSV File Example**, download default example to edit static routing file manually.

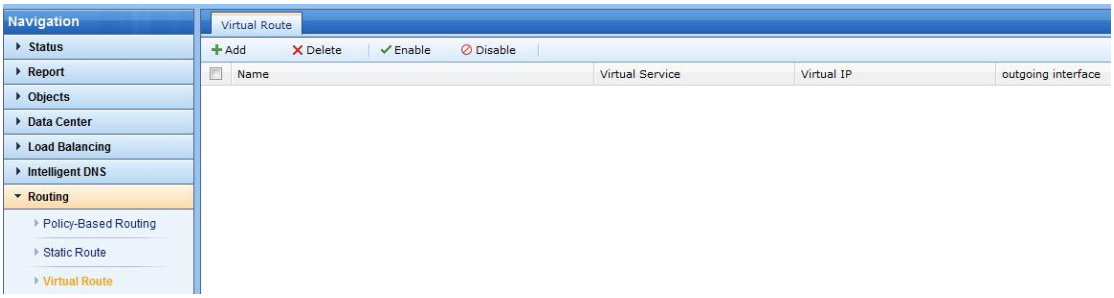
To back up custom static routing file, click **Export** and click **Save** to store it on local computer.

9.3 Virtual Route

It's used to specify an egress interface by force when access an IP for distributing virtual service. When external user accesses a distributed IP, you can make the access request flow

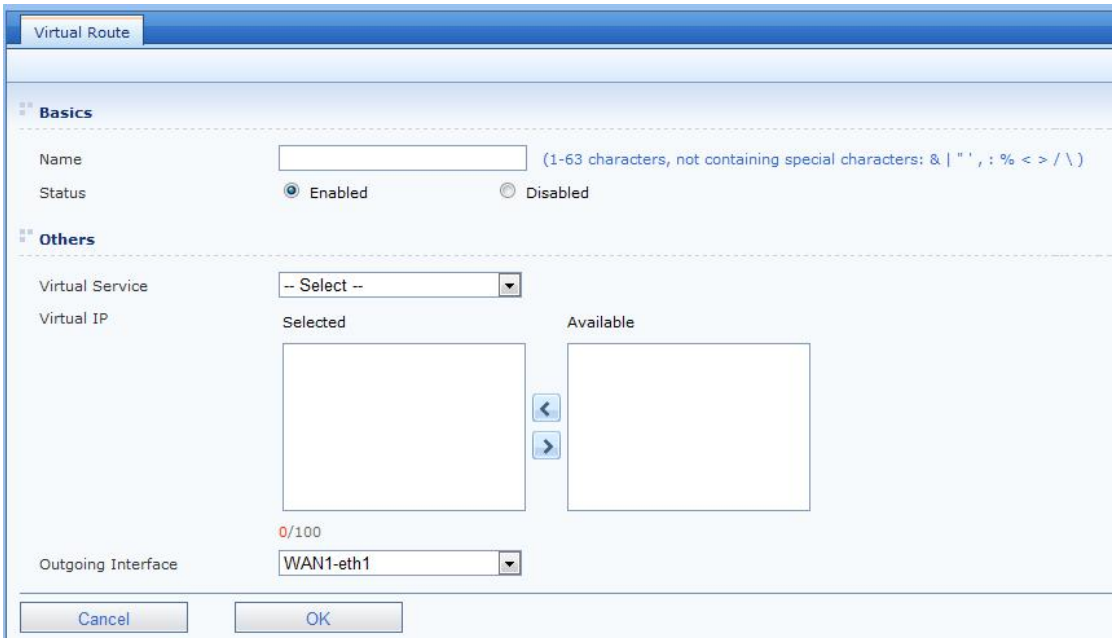
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

through a specified line by configuring virtual route. For example, there are two WAN links in customer network, Telecom and Unicom. The IP of the former is A, that of the latter is B. The IP group which has distributed virtual service are A and B. By configuring virtual route, when public IP accesses A, response packets must flow through Telecom, while public IP accesses B, response packets must flow through Unicom,



To remove the selected virtual route, click **Delete**.

To create a virtual route, click **Add** and configure the following fields:



Name: Specifies a distinguishable name.

Status: Select **Enabled** to make the virtual route configuration take effect.

Virtual Service: Select a virtual service and specify the virtual IP address through which external users can access that virtual service.

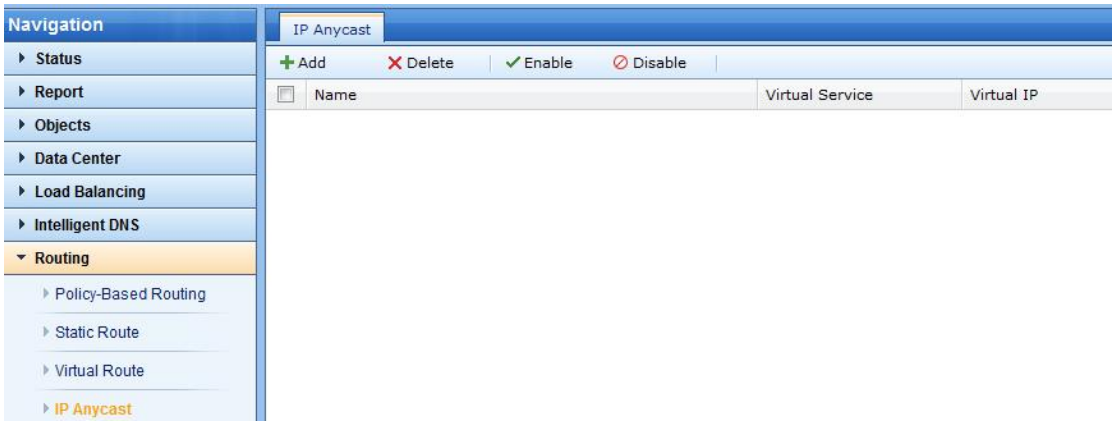
Virtual IP: Select a virtual IP address from **Available** box and add it to **Selected** box by clicking > arrow. The virtual route is applicable to the IP addresses in **Selected** box.

Outgoing Interface: Specifies an egress interface for the above virtual IP.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

9.4 IP Anycast

IP Anycast is used to configure globally distributed virtual service and corresponding route gateway. It can balance the loads on data centers.

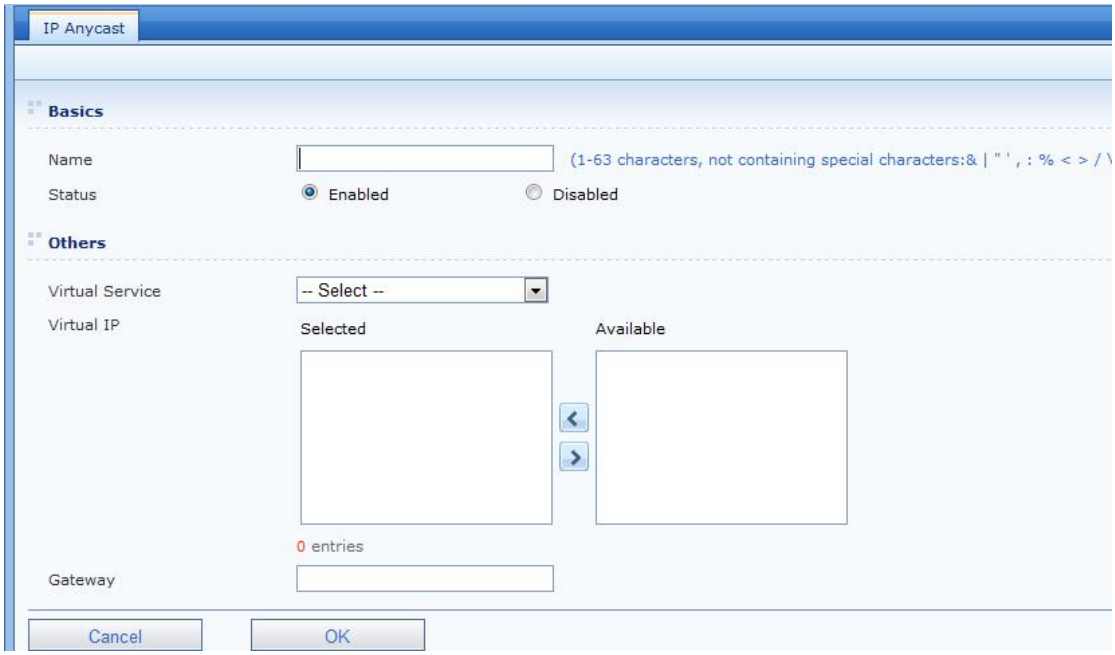


To enable the selected IP Anycast entry, click **Enable**.

To disable the selected IP Anycast entry, click IP **Disable**.

To remove the selected IP Anycast entry, click **Delete**.

To create a IP Anycast entry, click **Add** and configure the following contents:



Name: Specifies a distinguishable name.

Status: Specifies whether the IP Anycast is **Enabled** or **Disabled**.

Virtual Service: Select a virtual service and specify the virtual IP addresses through which external users can access that virtual service.

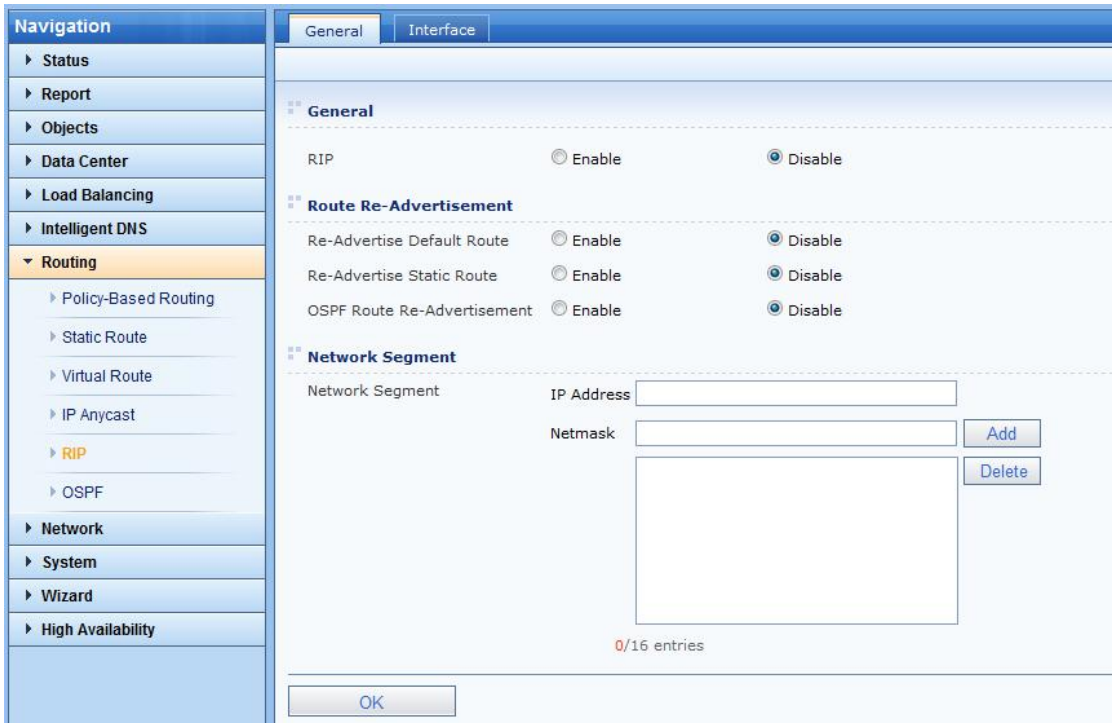
Virtual IP: Select a virtual IP address from **Available** box and add it to **Selected** box by clicking < arrow. The IP anycast is applicable to the IP addresses in **Selected** box.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Gateway: Specifies the next-hop address for the above virtual IP.

9.5 RIP

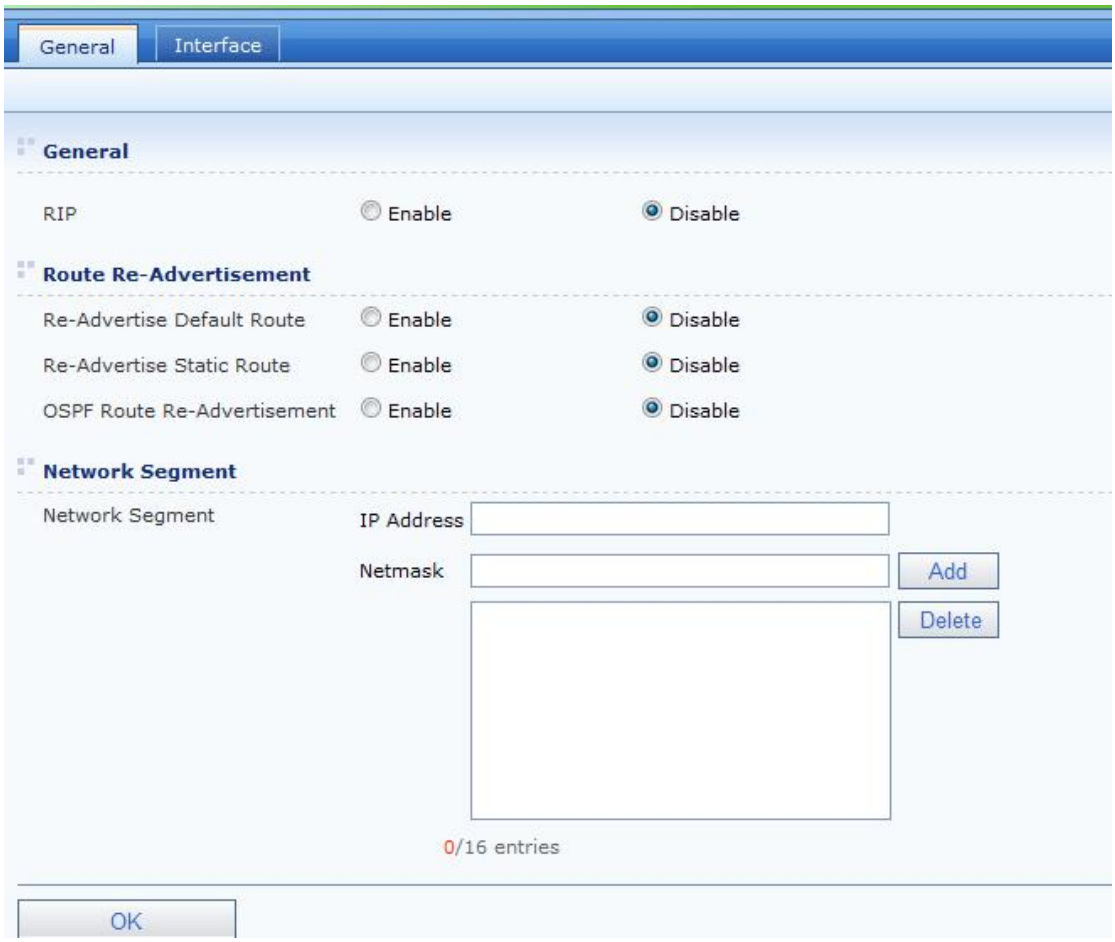
It's applicable to the network where the ADC is deployed and needs RIP to advertise routing information. To configure RIP, navigate to **Routing > RIP**, as shown below:



9.5.1 General Settings

It's used to configure the network which needs to be advertised through RIP and determine whether to allow RIP to advertise the routing information learned by other routing protocol.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Status: Select **Disable** to forbid devices using RIP.

Re-Advertise Default Route: Select **Enable** to allow RIP to broadcast default route, so that the adjacent

routers can reach the ADC based on the default route.

Re-Advertise Static Route: Select **Enable** to allow RIP to broadcast the static route configured on the device.

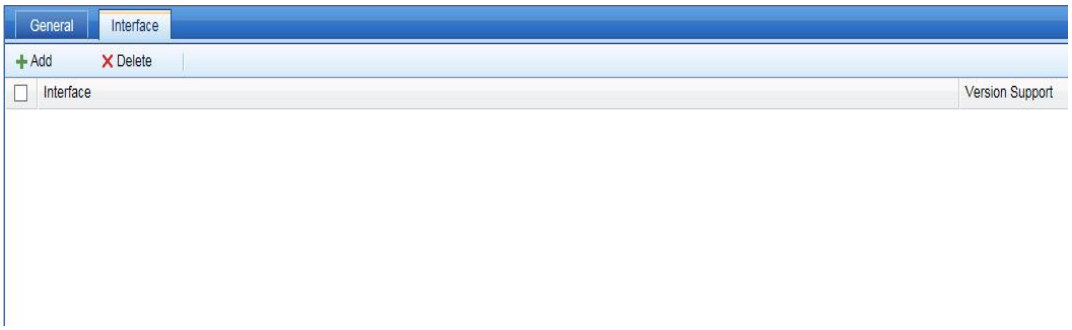
OSPF Route Re-Advertise: If **Enable** selected, OSPF route learned by the ADC can be broadcasted by RIP.

Network Segment: Specifies the network segment which is advertised to the peer device via RIP. Specify an IP address and netmask, and click **Add** to add these into network segment list.

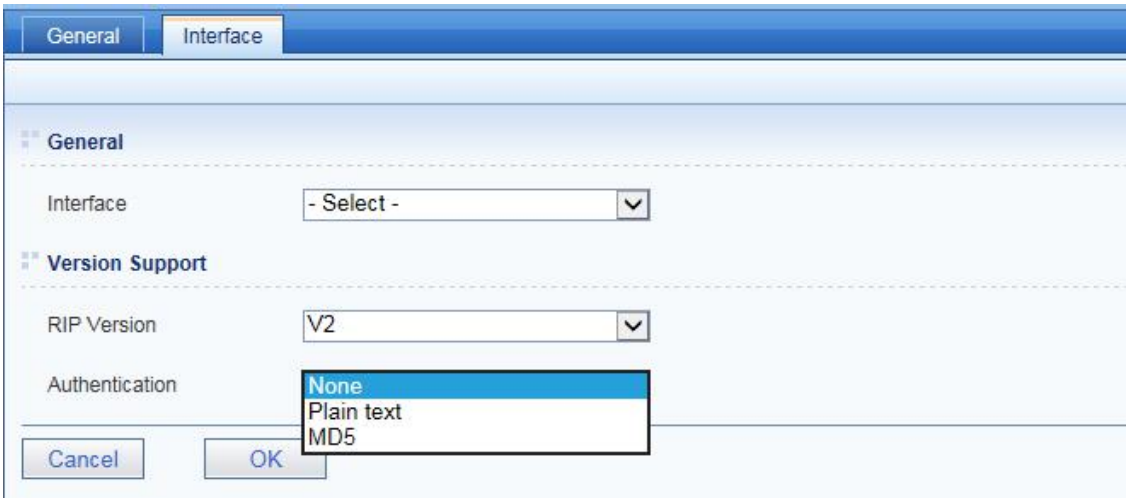
9.5.2 RIP Interface

It's configuration of interface which RIP runs on and version of RIP. By default, if the advertised network contains the network which the interface is located on, the interface will run RIP V2 and no need authentication.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Click **Add** to set version of RIP for the interface on which RIP runs, as shown in the following figure:



Interface: Specifies a interface for setting version information.

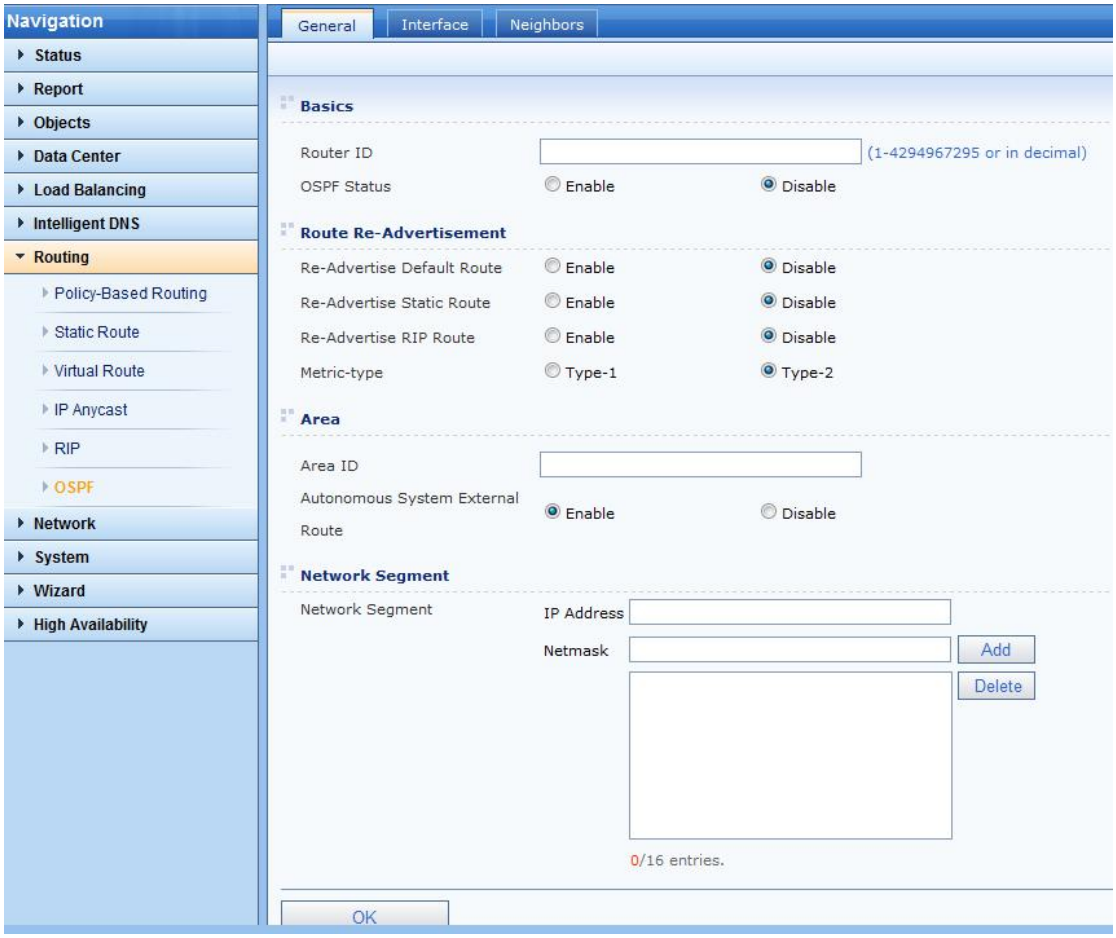
RIP Version: Specifies the version of RIP running on the interface, V1 or V2.

Authentication: Specifies an authentication method of RIP V2. Options are **None**, **Plain text**, and **MD5**. If select **Plain text**, you also need to specify **a**uthentication password; if select **MD5**, you should specify **a**uthentication key ID and **a**uthentication password.

9.6 OSPF

It's applicable to the network where the ADC is deployed and needs OSPF to advertise routing information.

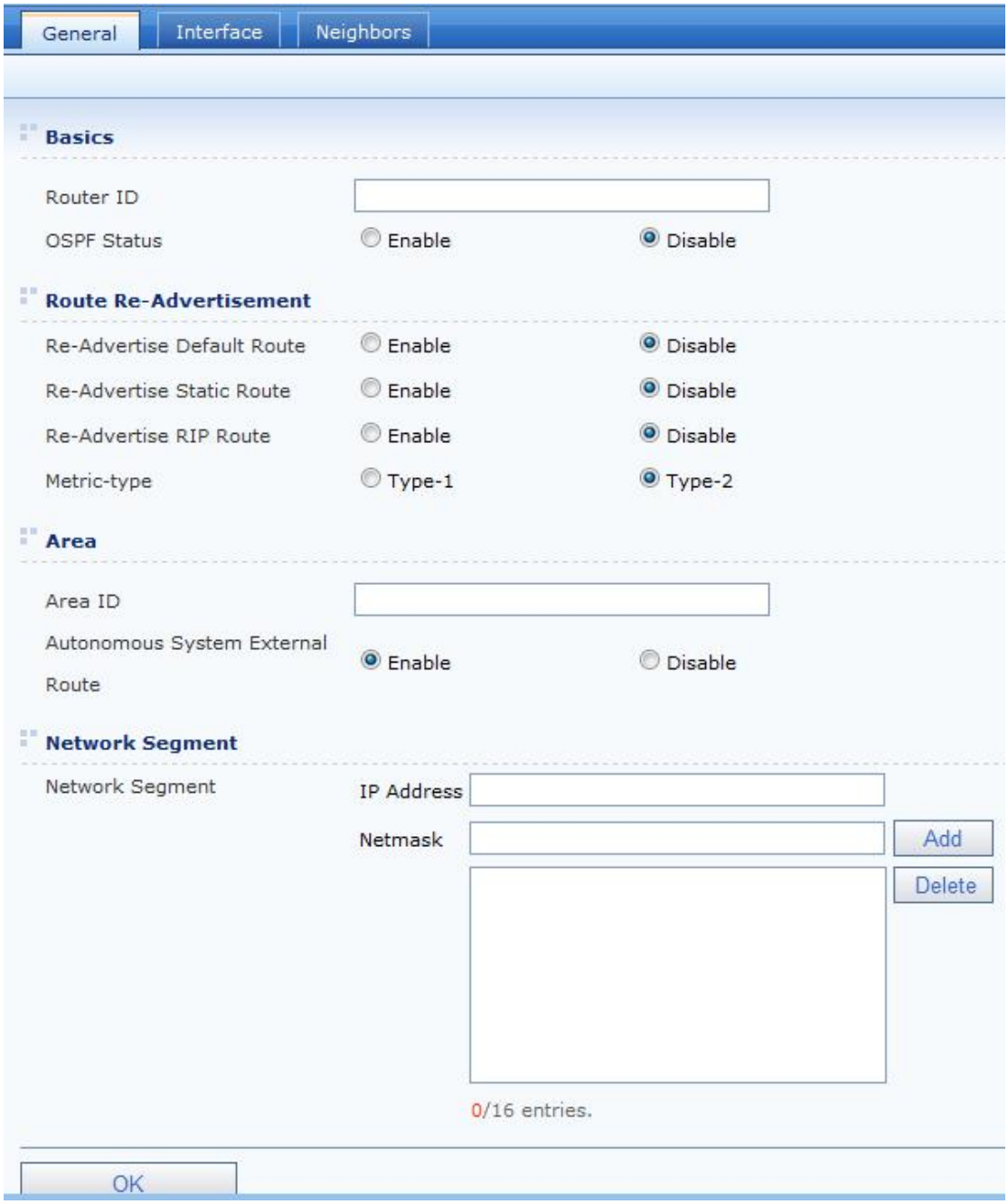
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



9.6.1 General Settings

It's used to configure the network which needs to be advertised through OSPF and determine whether to allow OSPF to advertise the routing information learned by other routing protocol.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Router ID: Specifies a distinguishable name for router. It can be expressed in decimal format (1- 4294967295) or in dot-decimal notation.

OSPF Status: Select **Enable** to allow device to run OSPF protocol.

Re-Advertise Default Route: Select **Enable** to allow OSPF protocol to broadcast default route, so that the adjacent routers can reach the ADC based on the default route.

Re-Advertise Static Route: Select **Enable** to allow OSPF protocol to broadcast the static route configured on the device.

Re-Advertise RIP Route: If **Enable** selected, RIP route learned by the ADC can be broadcasted by OSPF protocol.

Metric-type: Specifies a type for calculating OSPF path cost. If Type-1 selected, extended

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

field will be shown.

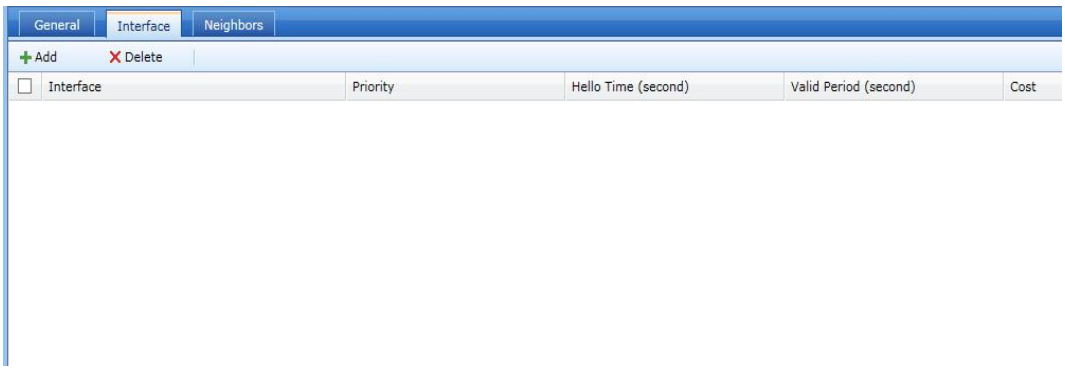
Area ID: Specifies an area ID for where the router is located.

Autonomous System External Route: Specifies whether to receive external link state notification from autonomous system. If select **Enable**, the router will receive state notification when route table on adjacent router has changed.

Network Segment: Specifies the network segment which is advertised to the peer device via OSPF protocol. Specify an IP address and netmask, and click **Add** to add these into network segment filed.

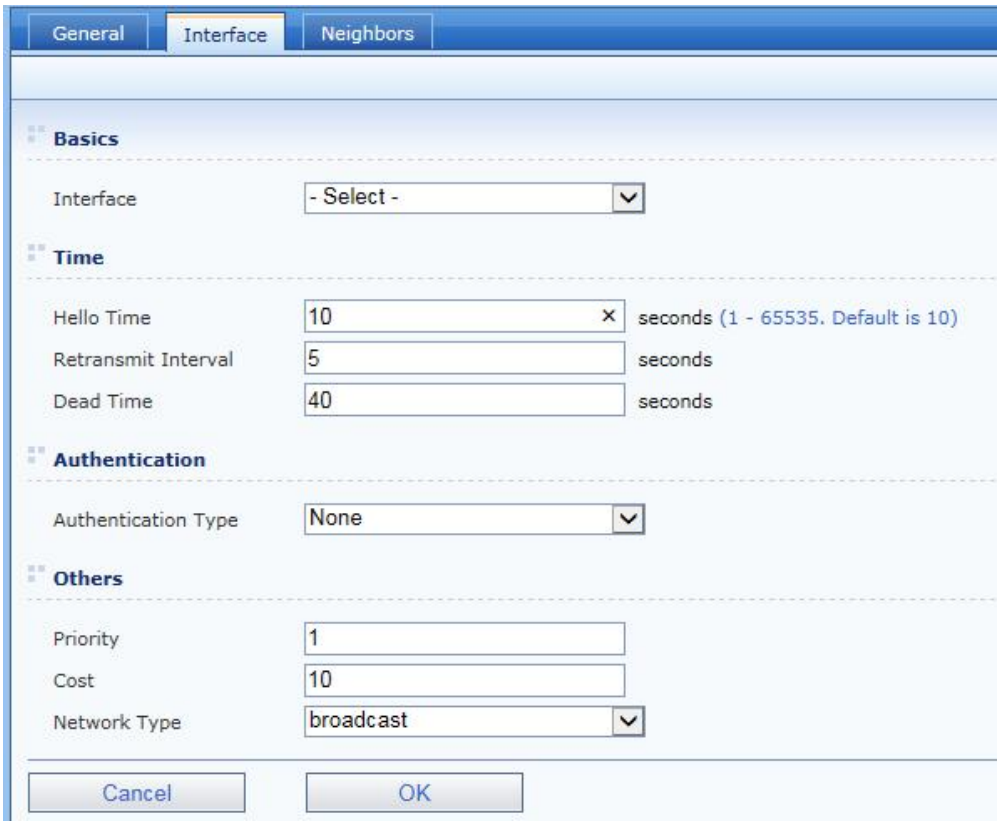
9.6.2 OSPF Interface

To configure the interface which OSPF protocol runs on, navigate to **Routing** > **OSPF** > **Interface**, as shown in the following figure:



To configure the interface which OSPF protocol runs on, click **Add** and configure the following fields:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Interface: Specifies an interface to apply OSPF protocol.

Hello Time: Specifies an interval of sending Hello packets by sender router.

Re-transmit Interval: Specifies the interval of re-sending link state notification by sender router.

Dead Time: Specifies a period. If sender router has not received Hello packets sent by peer device in that period, it will refuse to build neighbor relationship with peer device.

Authentication Type: Specifies an authentication method. It includes **None**, **Plaint text** and **MD5**. If select **Plaint text**, you also need to specify authentication password. If select **MD5**, you need to specify authentication key ID and authentication password.

Priority: Specifies the interface priority used for election of DR/BDR. Bigger the number you have entered, the priority is higher.

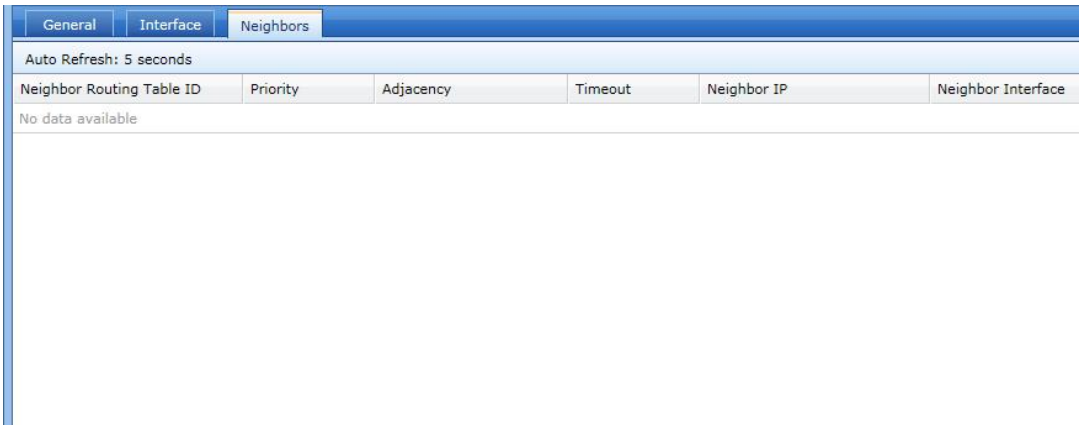
Cost: Specifies link cost of current interface. Bigger the number you have entered, the cost is higher.

Network Type: Specifies a network type for the current interface.

9.6.3 Neighbors

Yon can view which routers have built neighbor relationship with the ADC, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Neighbor Routing Table ID: Indicates the routing ID of neighbor router.

Priority: Indicates the interface priority of neighbor router.

Adjacency: Indicates the neighbor state.

Timeout: Indicates the timeout value of neighbor relationship. The value will begin countdown from 40 seconds. If the ADC has received packets from neighbor router in 40 seconds, that value will refresh. When the value turns to zero, and the ADC has not received packets, then the neighbor relationship will be deleted.

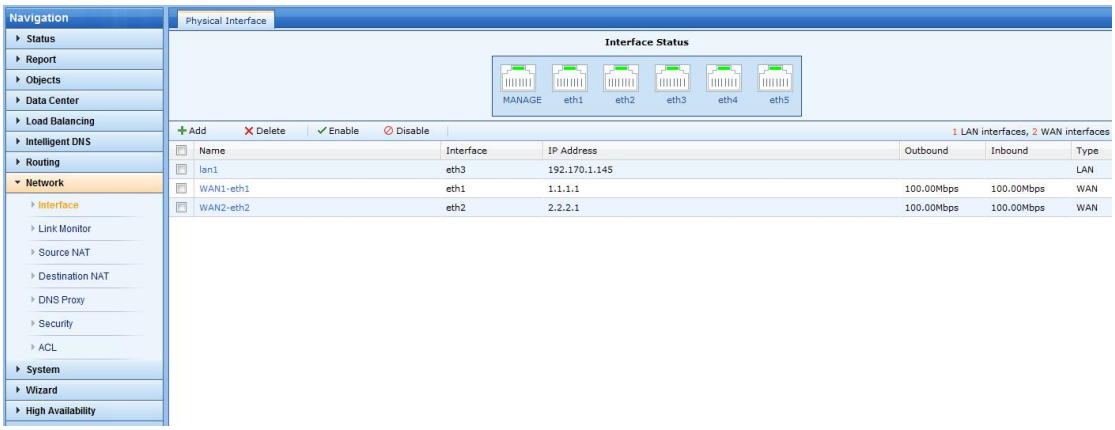
Neighbor IP: Indicates the IP address of the interface on neighbor router which is connected to ADC directly.

Neighbor Interface: Indicates the interface and its IP address of the neighbor router which is connected to ADC directly.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

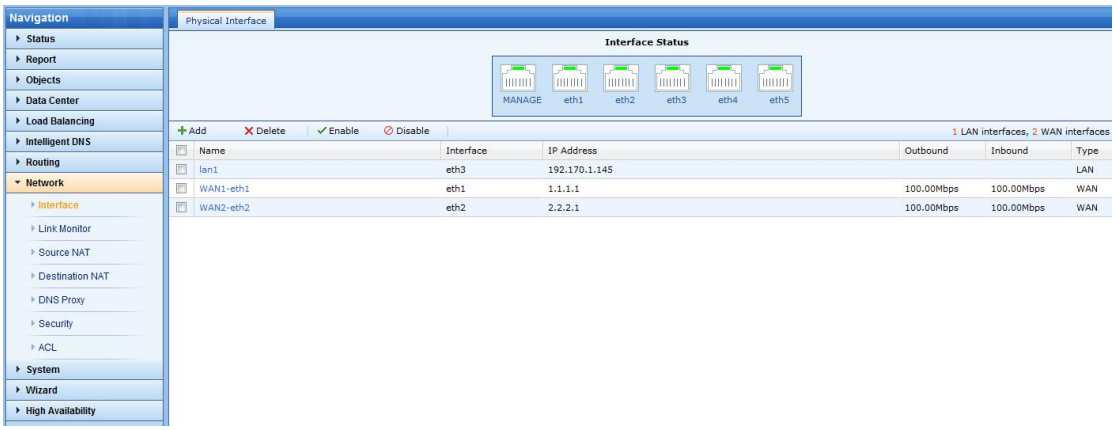
Chapter 10 Network

You can configure some relevant network parameters for the ADC. It includes **Interface**, **Link Monitor**, **Source NAT**, **Destination NAT**, **DNS Proxy** and **Security**, **ACL** as well, as shown in the following figure.



10.1 Interface

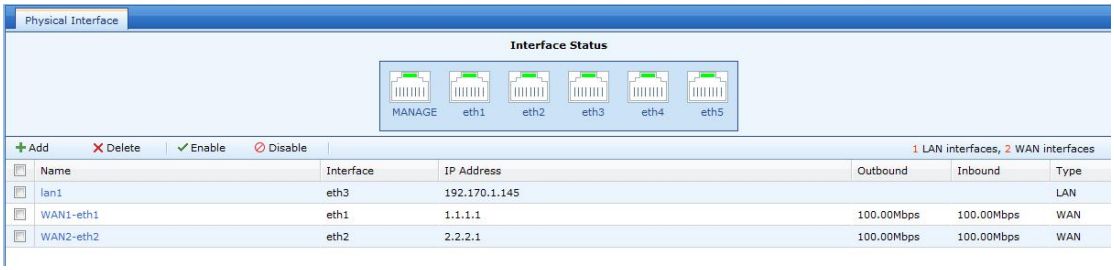
If yon want to use the interfaces except MANAGE interface to connect to SANGFOR ADC, you must configure MANAGE interface first. The default IP of MANAGE interface is 10. 252. 252/24 or 10. 254. 254. 254 /24.



10.1.1 Physical Interface

In **Network > Interface > Physical Interface**, you can configure interfaces on ADC, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

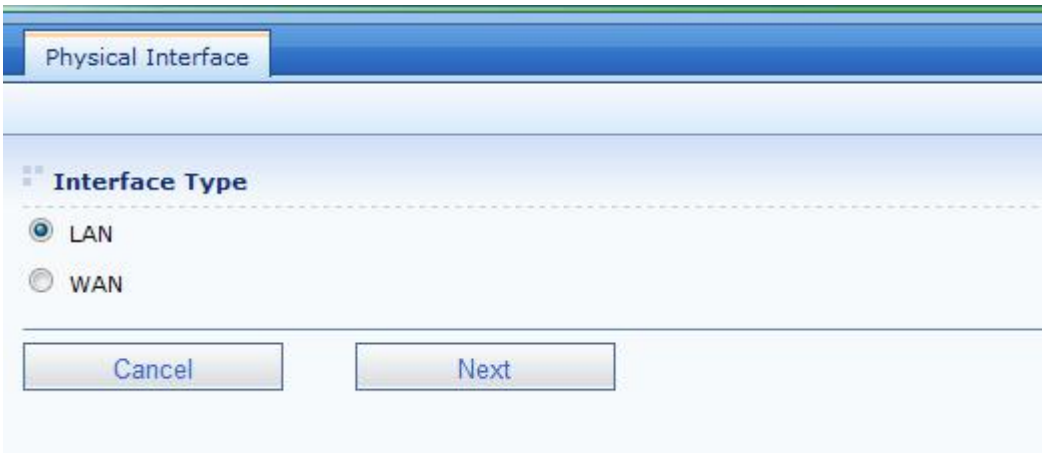


Interface Status: Indicates status of the interface which has been connected with network cable and can work normally.  indicates the interface has connected.  indicates the interface has not connected.

Click **Enable** to enable the selected interface; or click **Disable** to disable the selected interface.

Click **Delete** to remove the selected interface.

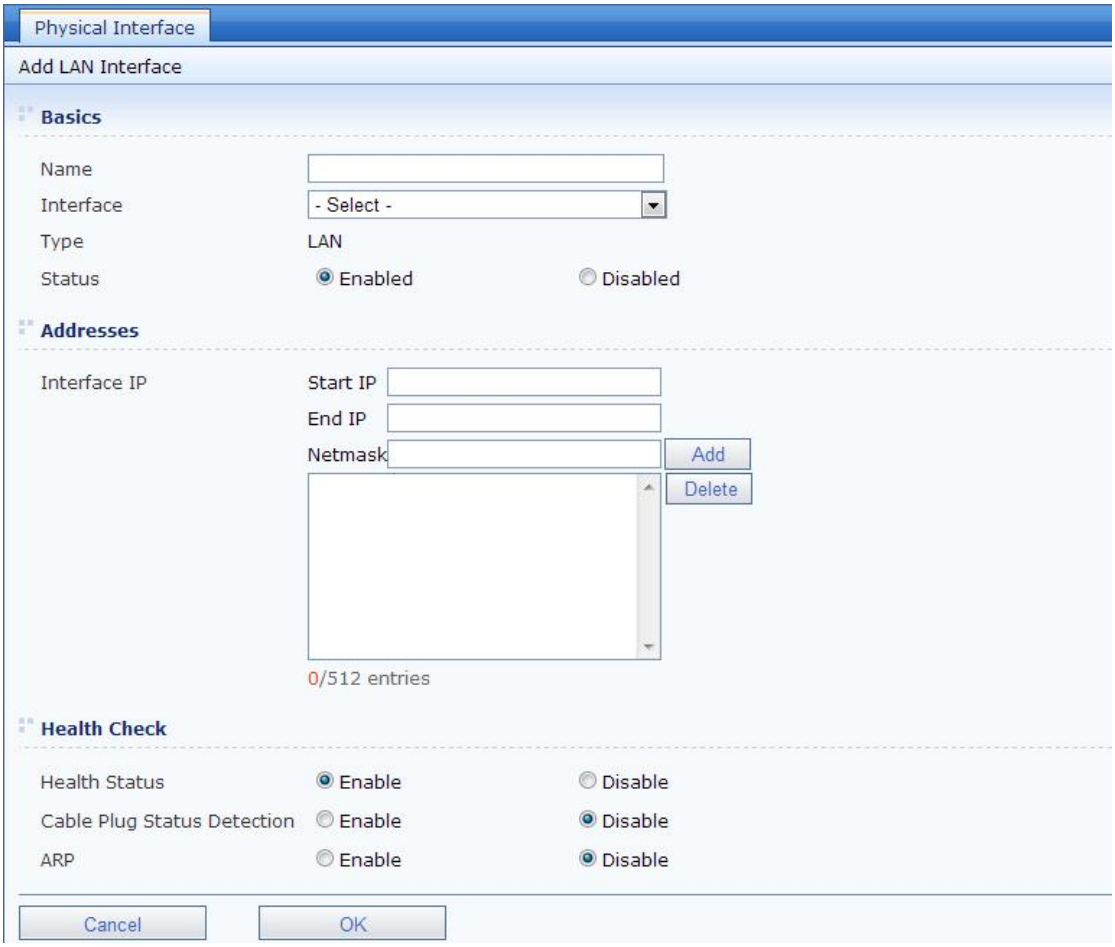
To create a physical interface, click **Add** to enter the following page:



Interface Type: Specifies an interface type, **LAN** or **WAN**. Select **LAN** to define an internal interface, or select **WAN** to define an external interface. And then click **Next** to continue, or click **Cancel** to give up configuration.

For **LAN** interface, you should configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Specifies a name for the LAN interface.

Interface: Specifies an interface.

Type: Indicates the type of the interface.

Status: Select **Enabled** to make all the configuration of the interface take effect.

Interface IP: Enter start IP, end IP and netmask. Mixture of IPV4 and IPV6 is supported.

Health Status: Select to enable or disable checking health status of LAN interface. Only IPV4 is supported.

Cable Plug Status Detection: Select **Enable** to check health status of LAN interface by detecting cable plug status.

ARP: Select **Enable** to check health status of LAN interface by obtaining the monitored IP address**.**



Click **Add** to add the IP address to interface IP field.

To save the settings, click **OK**; click **Cancel** to give up the the settings.

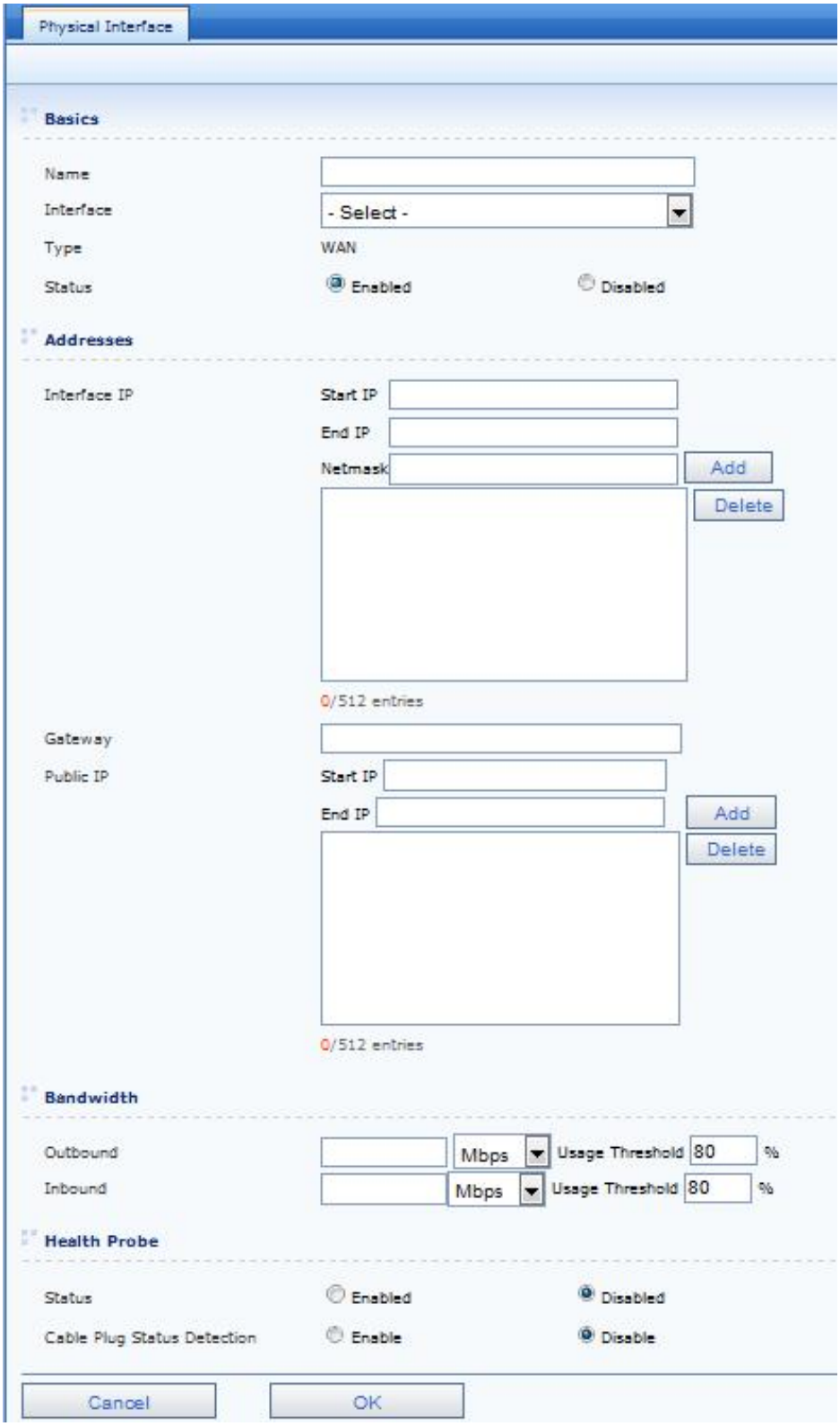
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

If you want to create a WAN interface, select **WAN**, as shown below:



Click **Next** to configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Specifies a name for the WAN interface.

Interface: Select an available interface.

Type: Indicates the interface type.

Status: Specifies whether all the configuration of the interface is **Enabled** or **Disabled**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Interface IP: Enter **Start IP**, **End IP** and **Netmask**, click **Add** to add them to Interface IP filed. You can also add multiple IP addresses or an IP segment, but the IP addresses must be the one that can be assigned to network adapter.

Gateway: Specifies a gateway IP address for the WAN interface.

Public IP: If the IP of the interface configured above belongs to public IP, this fieldis not required; otherwise, it's required, and the public IP must be corresponding to IP of the interface.



Bandwidth: Specifies bandwidth in order to manage and control bandwidth usage. If the traffic over the link exceeds the specified **Usage Threshold**, indicates the link is busy.

Outbound and **Inbound** are used to specify the bandwidth over public line. Unit can be **Kbps** or **Mbps**. The settings will be used in **Bandwidth Control** and **Link Load**.

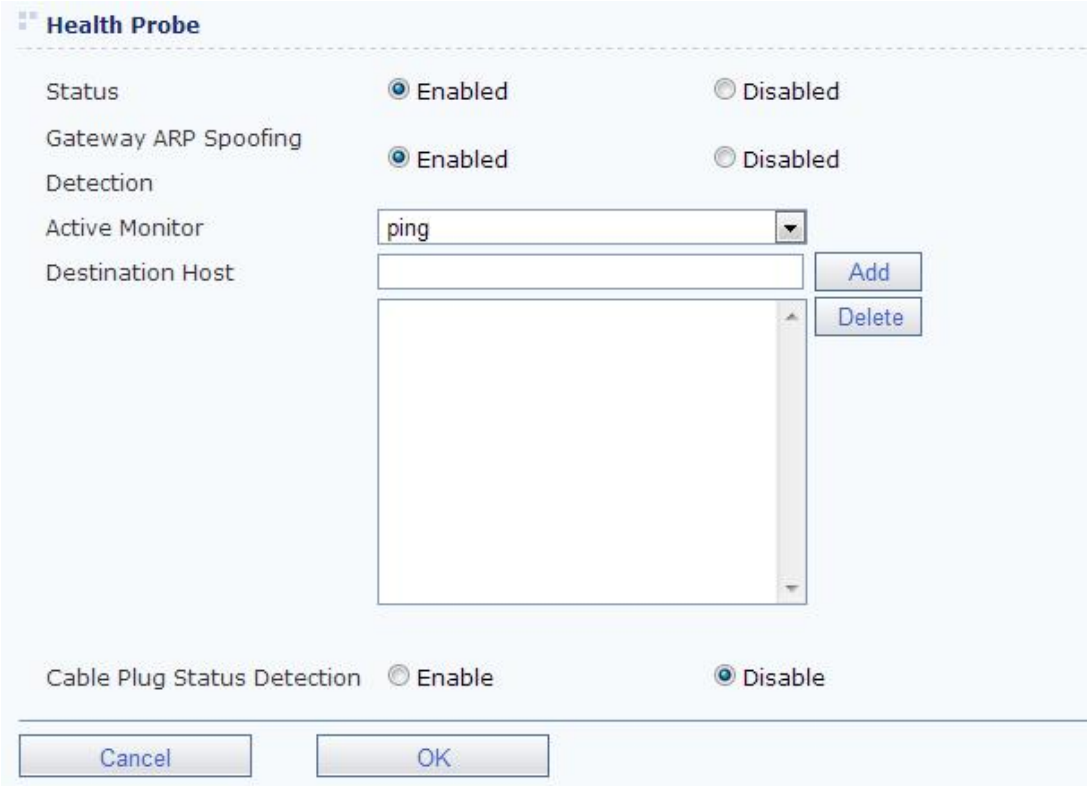
Usage Threshold: Specifies the threshold value. When bandwidth usage reached that value, the line status will show **Busy**.



1. To view the line status, navigate to **Status** > **Links** > **WAN Links**.
2. At most 512 IP addresses can be configured on each interface.
3. IPv4 address and IPv6 address can not co-exist on the same interface.

Health Probe: Specifies monitor link status, including **Status, Gateway ARP Spoofing, Detection**, **Active Monitor**, **Destination Host** and **Cable Plug Status Detection**. Click **Enabled** and specify the following expanded fields:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Status: Select **Enabled** to enable health probe.

Gateway ARP Spoofing: Specifies whether to check the link health status by detecting the gateway ARP If gateway ARP is unreachable, then the link is down.

Active Monitor: Specifies the monitors which you want to enable.

Destination Host: Enter the destination host name, IP address or DNS domain. Then click **Add** to add them to Destination Host filed.

Cable Plug Status Detection: Specifies whether to check connection state of interface. If the interface has not connected with cable, indicates there is a line fault. To enable **Cable Plug Status Detection**, select **Enable** or select **Disable** to disable **Cable Plug Status Detection**.

Floating IP address list: In HA mode, IP address is shared by several units. The floating IP works in which unit is decided by the group.

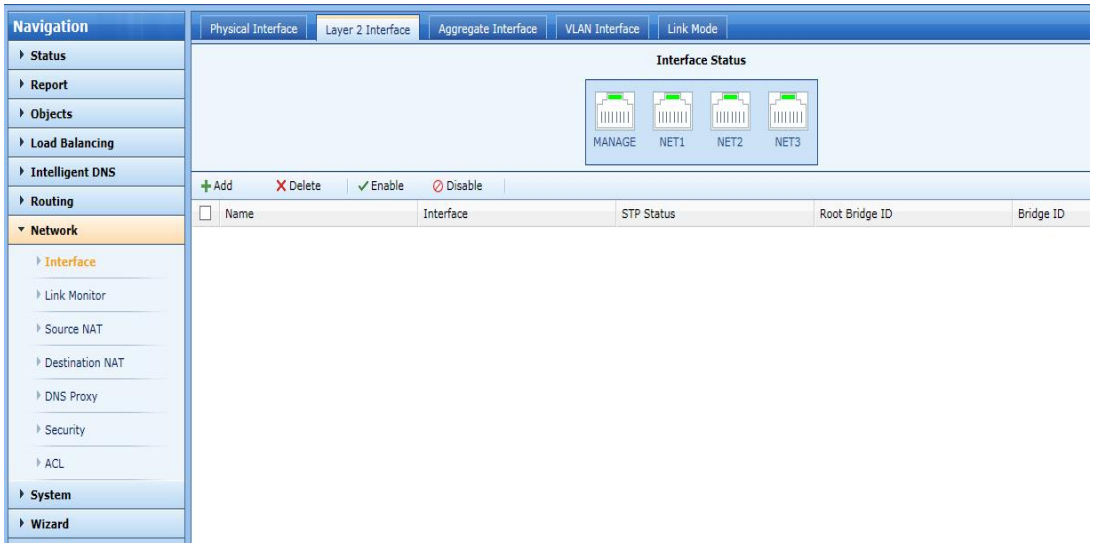
If interface configuration has changed, including Bandwidth, Usage Threshold, Gateway, Health Probe, Public IP, and adjusting the current IP address order, dynamic route process will not restart, avoiding dynamic route relearning which will lead to network interruption. If enable/ disable the interface, modify IP address of the interface, or change referenced interface, the dynamic route process will restart.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

10.1.2 Layer 2 Interface

To combine several interfaces on the ADC into a interface on layer 2 switch logically, navigate to **Network > Interface > Layer 2 Interface**. Then, each interface of ADC can be regarded as a layer 2 interface.

It's applied when the ADC is deployed at network exit, and firewall device is put behind it. To ensure high availability and high reliability of network, HA feature is enabled by firewall, that means two firewall devices with same configuration are used by a node. In case of not adding other nodes, such as switch, the layer 2 interface on the ADC can resolve the issues of active/standby switchover of firewall device, and implement the connection between ADC and firewall, and the connection between the firewalls as well.

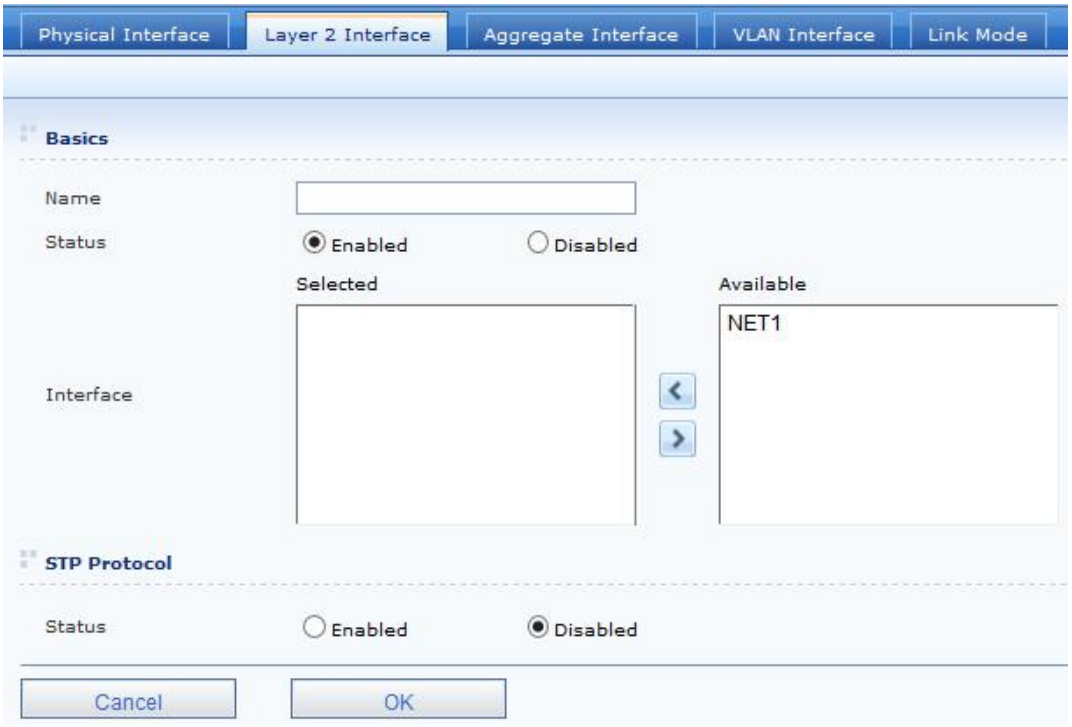


To make the selected layer 2 interface take effect, click **Enable**; or click **Disable** to disable the selected layer 2 interface.

To remove a layer 2 interface, click **Delete**.

To create a layer 2 interface, click **Add** to enter **t**he following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

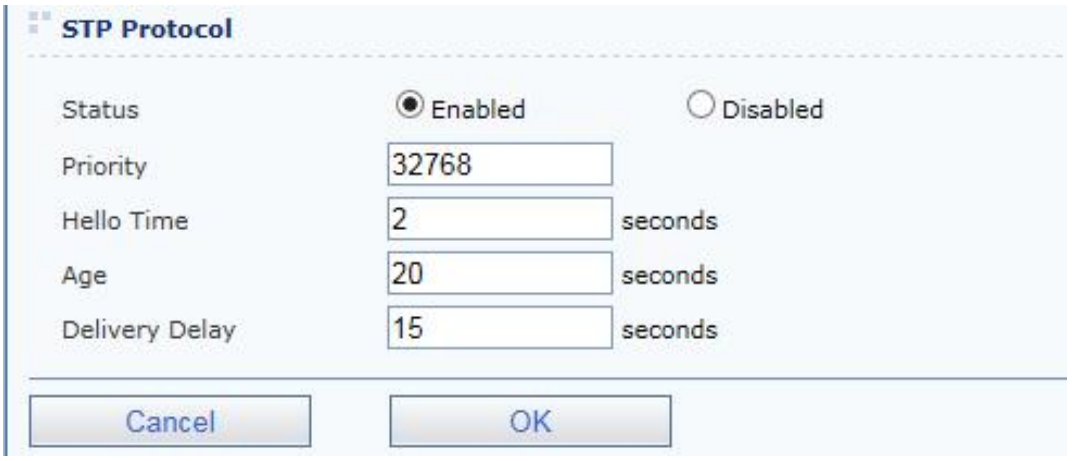


Name: Give it a distinguishable name.

Status: Specifies whether the layer 2 interface is **Enabled** or **Disabled**.

Interface: Specifies the interfaces to be combined into layer 2 interface. To add an interface, select the item and click the **<** arrow button to move it into the **Selected** box from the **Available** box. To remove an interface, select the item and click the **>** arrow button.

STP Protocol: It's used to configure **Priority**, **Hello Time**, **Age**, and **Delivery Delay**. Click **Enabled** and specify the extended fields:



Status: Specifies whether STP protocol on the layer 2 interface is **Enabled** or **Disabled**.

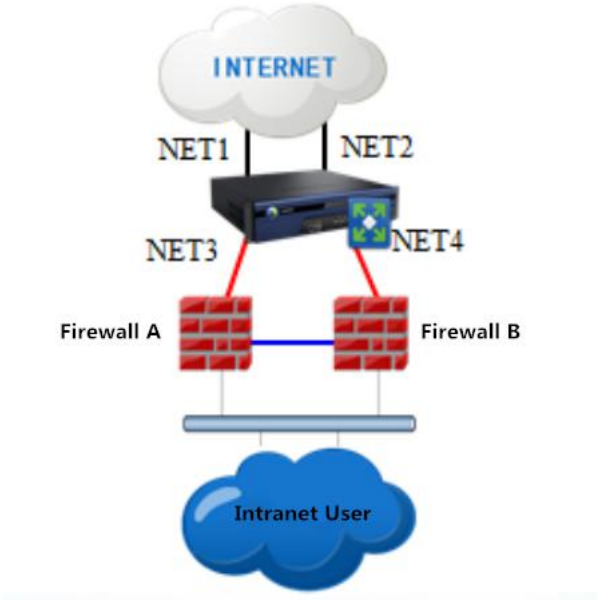
Priority: Specifies a protocol priority. Smaller the value, the possibility that the interface becomes root bridge is bigger.

Hello Time: Specifies, in seconds, how often the layer 2 interface sends BPDU. The sent BPDU will be forwarded by the switch or bridge which receives it.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

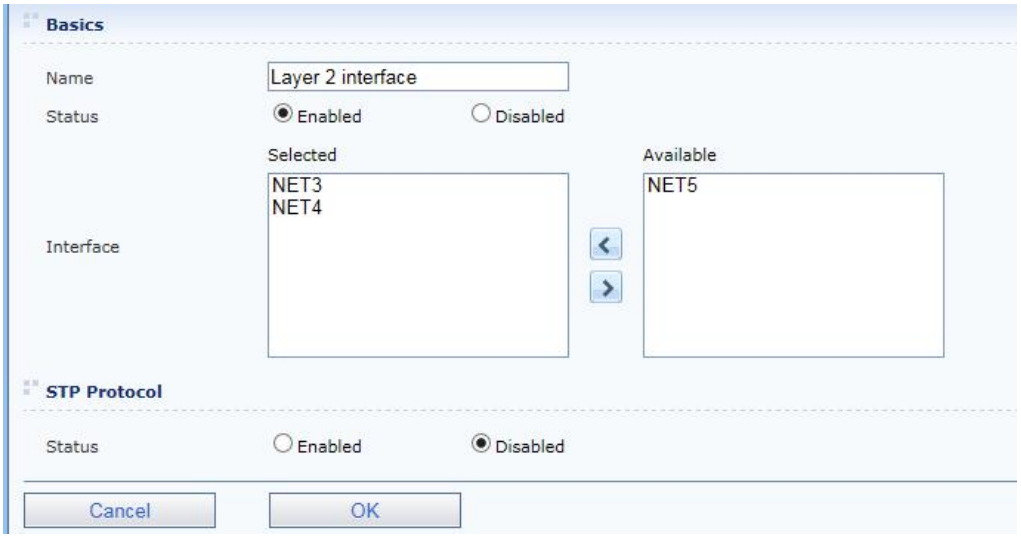
Age: Specifies how long it takes that the layer 2 interface determines if the topology has changed, in seconds. That value is always a multiple of Hello Time.

Delivery Delay: Specifies, in seconds, how long it takes that the interface status changes from congestion to forwarding. For example, there are two firewall devices, one as active device, the other one as standby device, in order to meet the need of high availability and high reliability. If the ADC is deployed at the network exit, the IP address of interface NET3 should be the same with that of interface NET4. Then, it seems that NET3 and NET4 are on the same VLAN, and the data sent by firewall, through interface NET3 or NET4, can communicate with the VLAN IP.



To combine NET3 and NET4 into a layer 2 interface, you should do:

1. Select NET3 and NET4, then click the < arrow button to move it into **Selected** box from **Available** box, and finally click **OK** to save the settings, as shown in the following figure:



2. Configure an IP address for the layer 2 interface. On the **Network** > **Interface** > **Physical**

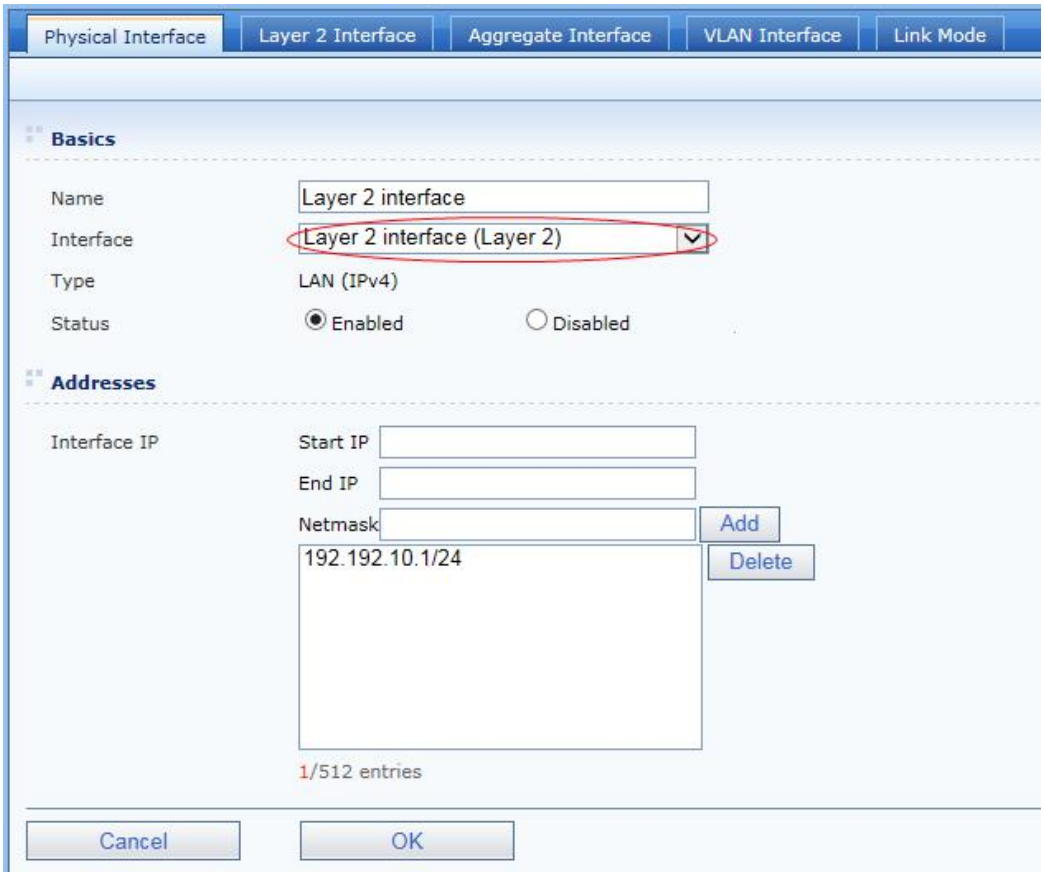
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Interface page, create a LAN interface. Clicking **Next**, you will view the layer 2 interface which you just created, and configure an IP address for it.

Note:

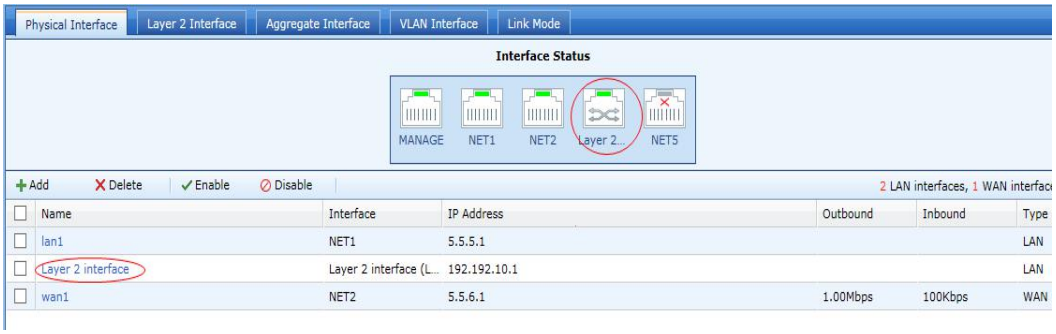
When you configure an IP address for the layer 2 interface, you can select the interface type as required, LAN or WAN, as shown in the following figure:





3. After configuring completed, you will see the following page:

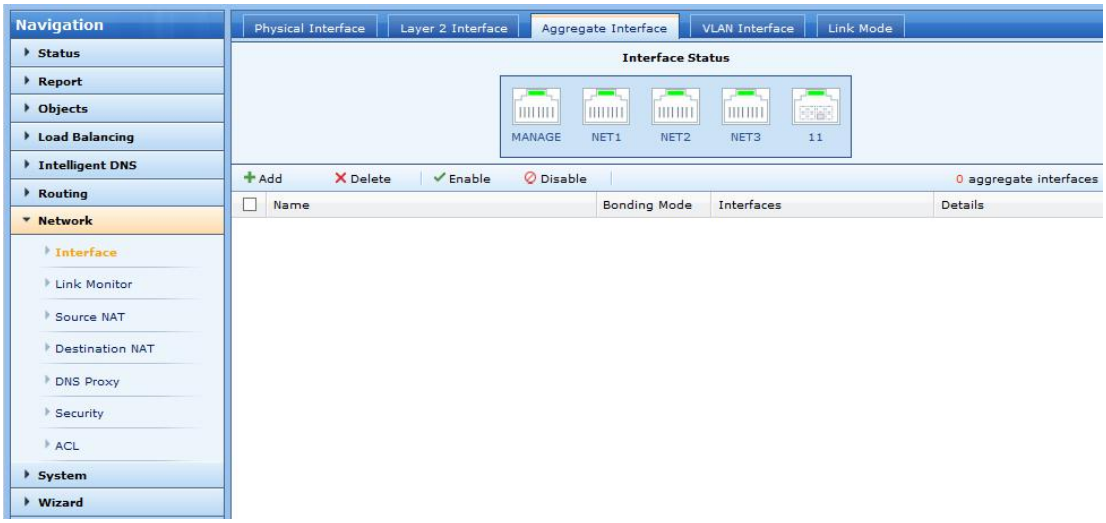
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



When select interfaces for combining into layer 2 interface, you can also select multiple interfaces, aggregate interface or other interfaces. For more about aggregate interface, refers to **Configuring Aggregate Interface**, following.

10.1.3 Aggregate Interface

In **Network > Interface > Aggregate Interface**, you can take several physical interfaces as a single logical interface. It allows several interfaces to connect parallelly and transmit data simultaneously, in order to provide higher bandwidth and throughput.

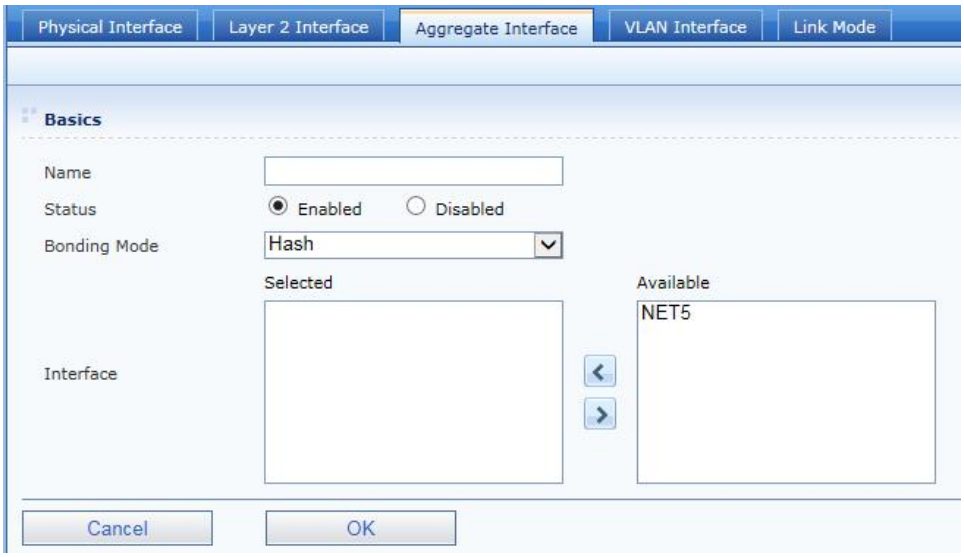


To make selected aggregate interface take effect, click **Enable**; or click **Disable** to disable an aggregate interface.

To remove selected aggregate interface, click **Delete**.

To create an aggregate interface, click **Add** and configure the following fields:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Status: Specifies whether the aggregate interface is **Enabled** or **Disabled**.

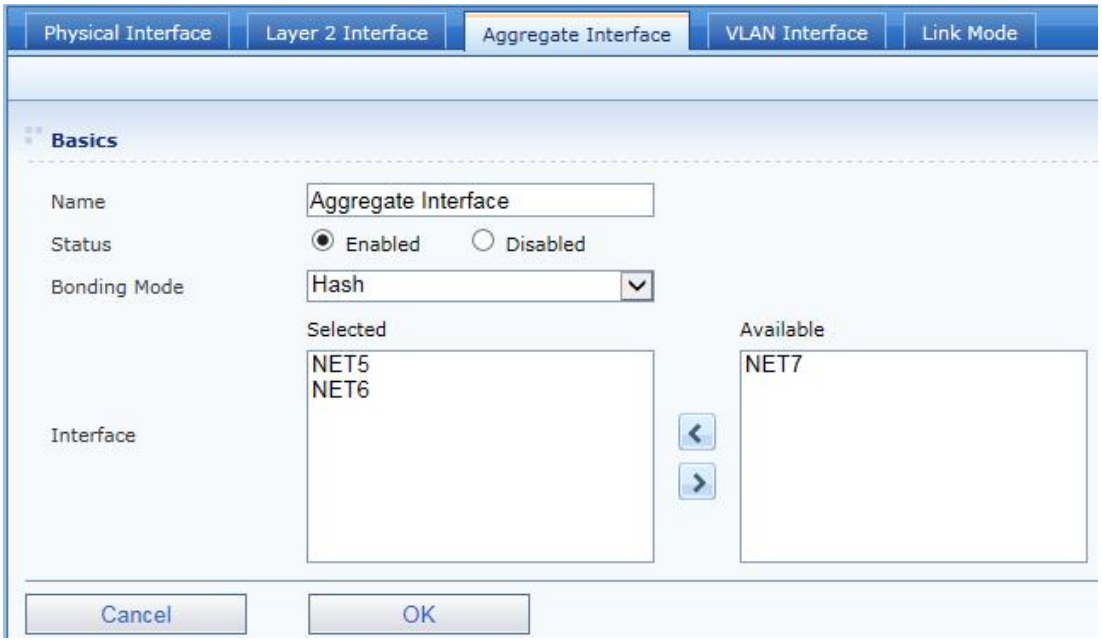
Bonding Mode: Select a work mode for the aggregate interface. Options are **Hash**, **Round robin**, **802**. **3ad** or **Dual NIC redundancy**. The following are brief introductions to each option:

- **Hash**: Select corresponding interface according to the hash value calculated based on the source IP address and target IP address.
- **Round robin**: Send packets to corresponding interface by turns.
- **802**. **3ad**: Select the link with maximum bandwidth as primary link automatically, others as secondary links. If the bandwidths are the same, send data based on hash algorithm.
- **Dual NIC redundancy**: Binds several physical interfaces into a logical interface, only one physical interface in active mode. When the active interface gets down, the standby interface can work continuously as the active interface.

Interface: Specifies the interfaces to be combined into aggregate interface. To add an interface, select the item and click **<** arrow button to move it into the **Selected** box from the **Available** box. To remove an interface, select the item and click the **>** arrow button.

For example, combine NET5 and NET6 into aggregate interface. Firstly, specify Hash as the bonding mode, select NET5 and NET6 and click the < arrow button to move them to **Selected** box from the **Available** box, and then click **OK** to save the settings, as shown in the following figure:

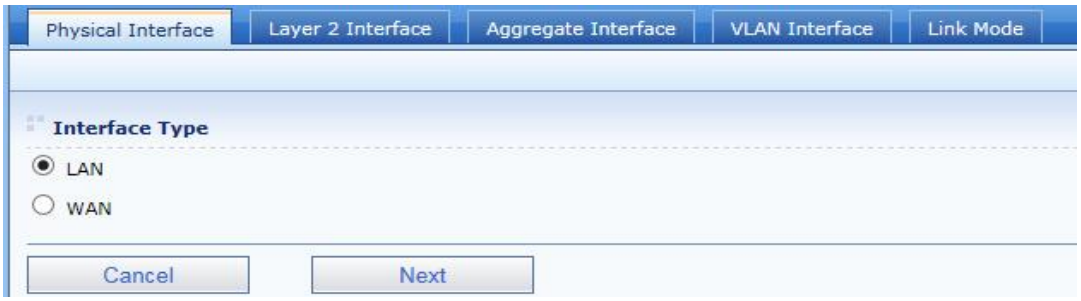
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



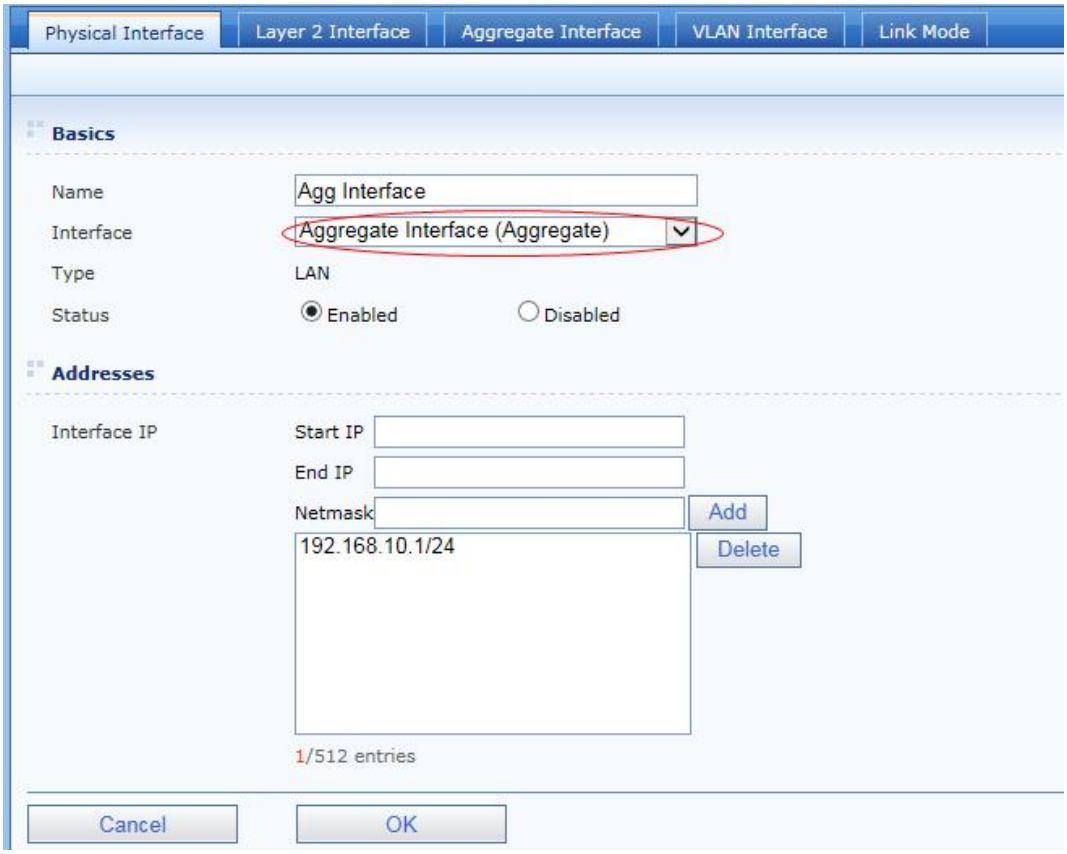
Next, configure an IP address for the aggregate interface. On the **Network > Interface > Physical Interface** page, create an LAN interface. Clicking **Next**, you can view the aggregate interface just created, and configure an IP address for it.

Note:

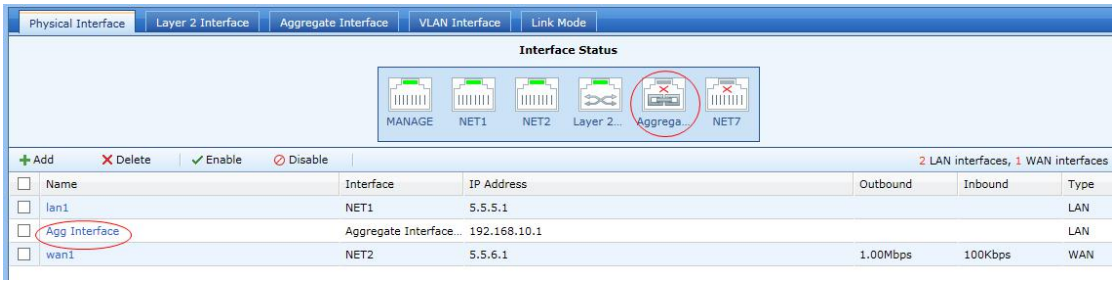
When you configure an IP address for the aggregate interface, options are **LAN** and **WAN**, as shown in the following figure:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



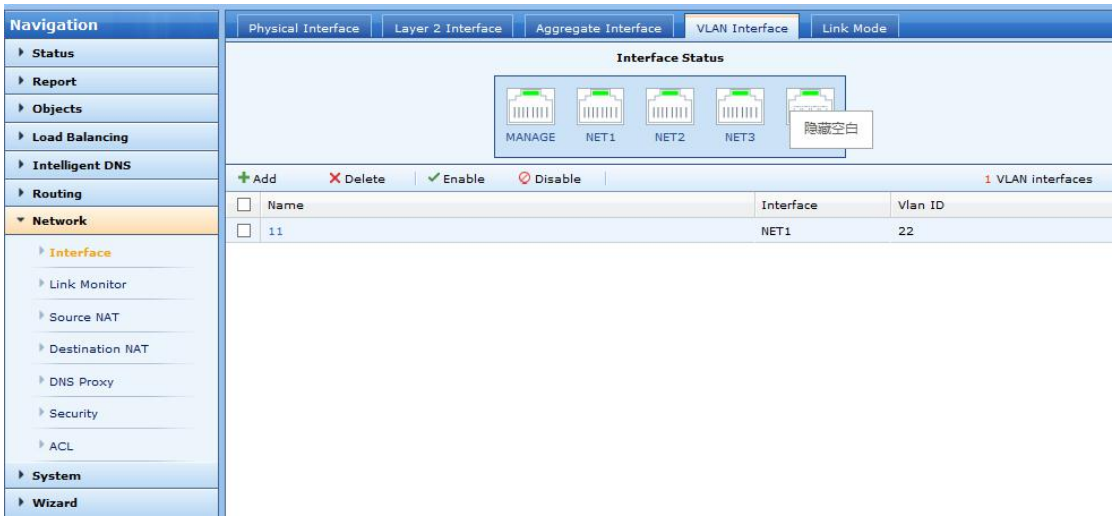
After configuring completed, you will see the following page:



10.1.4 VLAN Interface

In **Network** > **Interface** > **VLAN Interface**, the interface on the ADC can be separated into several virtual sub-interfaces to make virtual work group available.

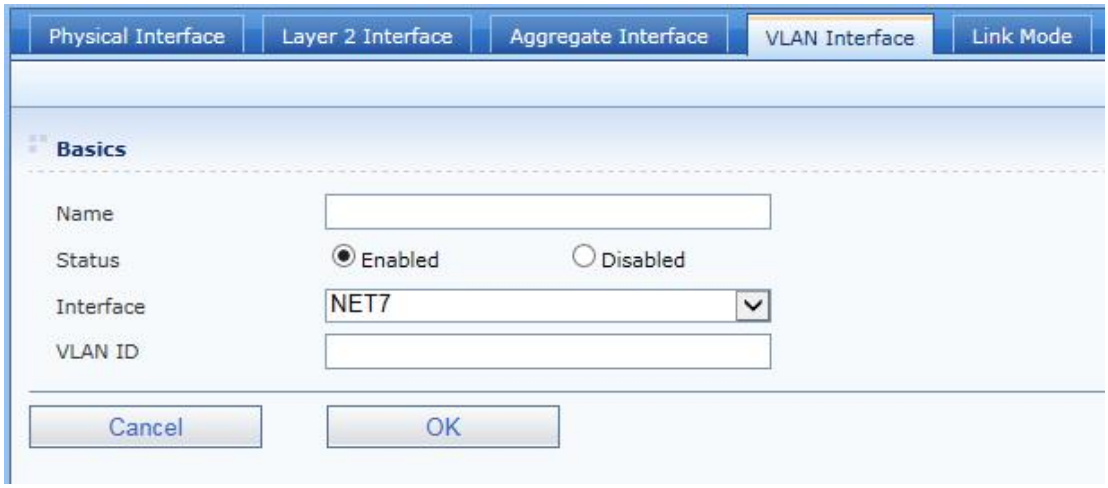
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To make the selected VLAN interface valid, click **Enable**; to make a VLAN interface invalid, click **Disable**.

To remove the selected VLAN interface, click **Delete**.

To create a VLAN interface, click **Add** and configure the following fields:



Name: Give it a distinguishable name.

Status: Specifies whether the VLAN interface is **Enabled** or **Disabled**.

Interface: Specifies a physical interface which you want to separate.

VLAN ID: Give an ID to the VLAN.

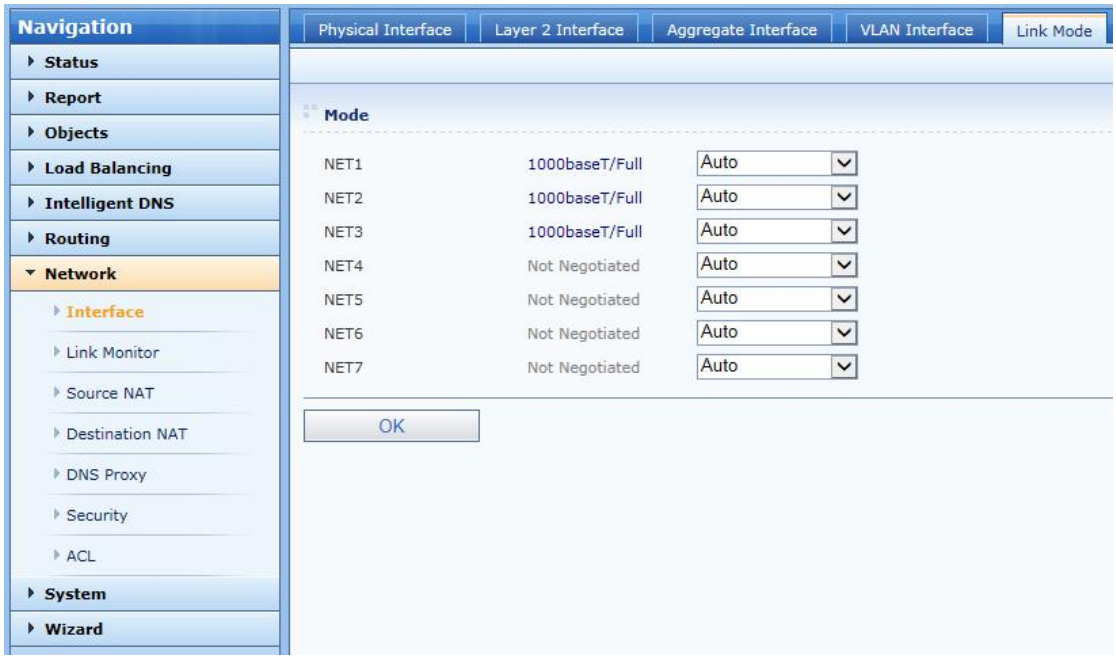
After configuring VLAN interface, create an interface in **Physical Interface**, and specify an IP address for the VLAN interface.

VLAN interface supports aggregate interface.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

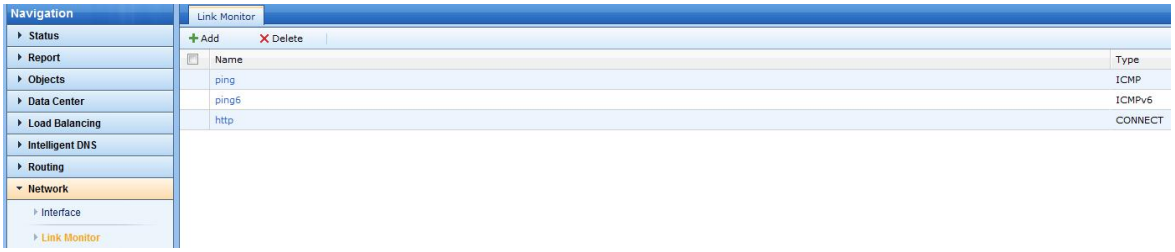
10.1.5 Link Mode

To set interface mode, navigate to **Network** > **Interface** > **Link Mode**, as shown in the following figure:



10.2 Creating Link Monitor

Link Monitor can monitor the status of the link that's used to release applications.

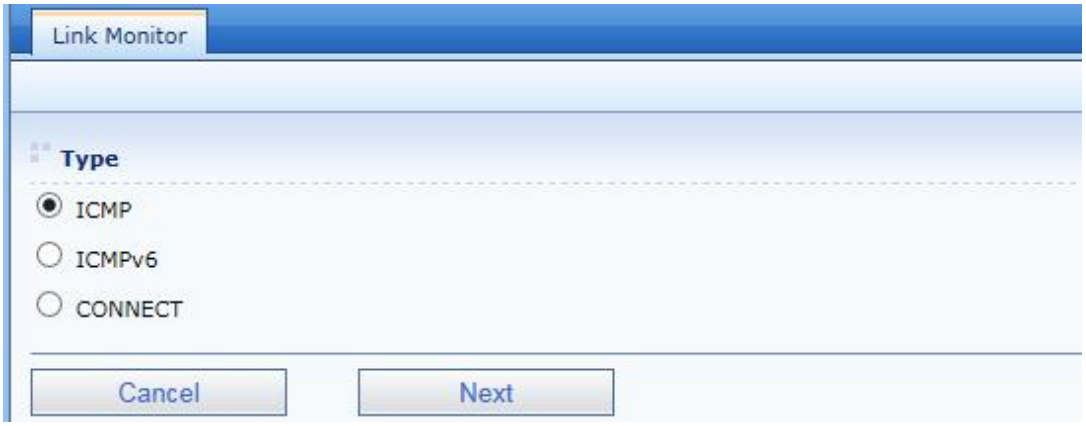


In **Link Monitor**, you can view the **Name** and **Type** of link monitors, including predefined and custom link monitors.

To remove a link monitor, click **Delete**. Please note that predefined monitors cannot be deleted.

To create a link monitor, click **Add** to enter the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

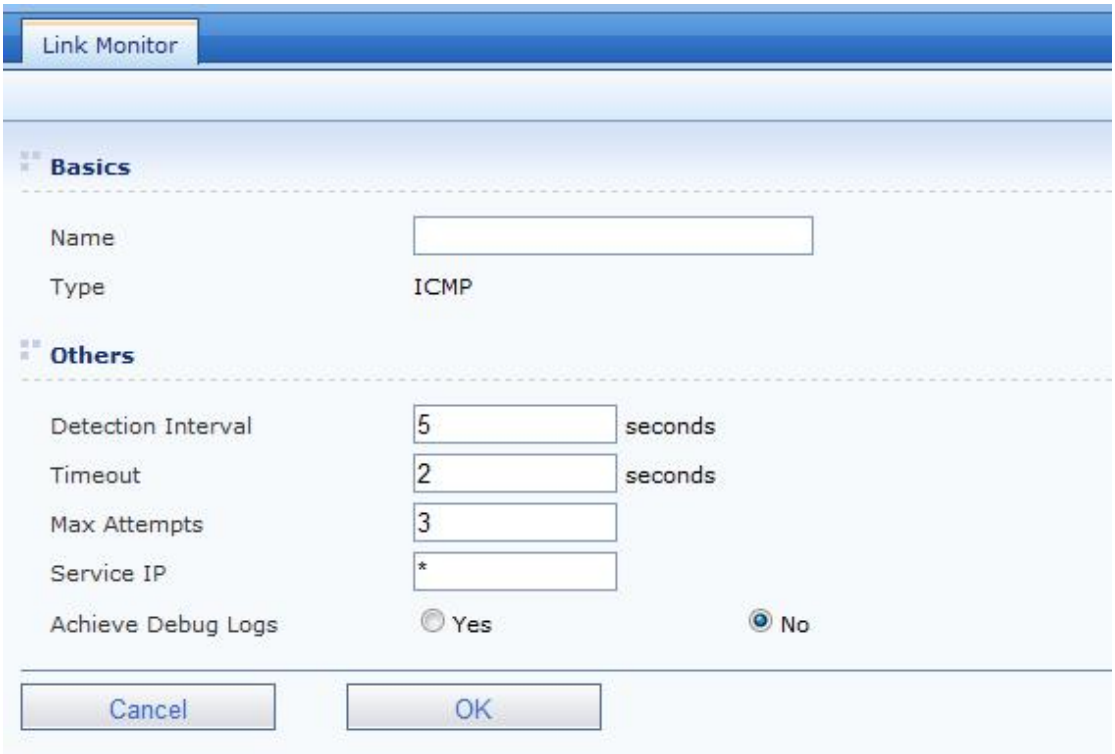


Type: Specifies a type of the link monitor.

To give up the setting, click **Cancel**.

Select a monitor type and click **Next**.

For **ICMP** or **ICMPv6**, the attributes are as follows:



Name: Give it a distinguishable name.

Type: Indicates the type of the link monitor.

Detection Interval: Specifies an interval of detecting link status. Unit is second.

Timeout: Specifies a timeout value of detection, in second.

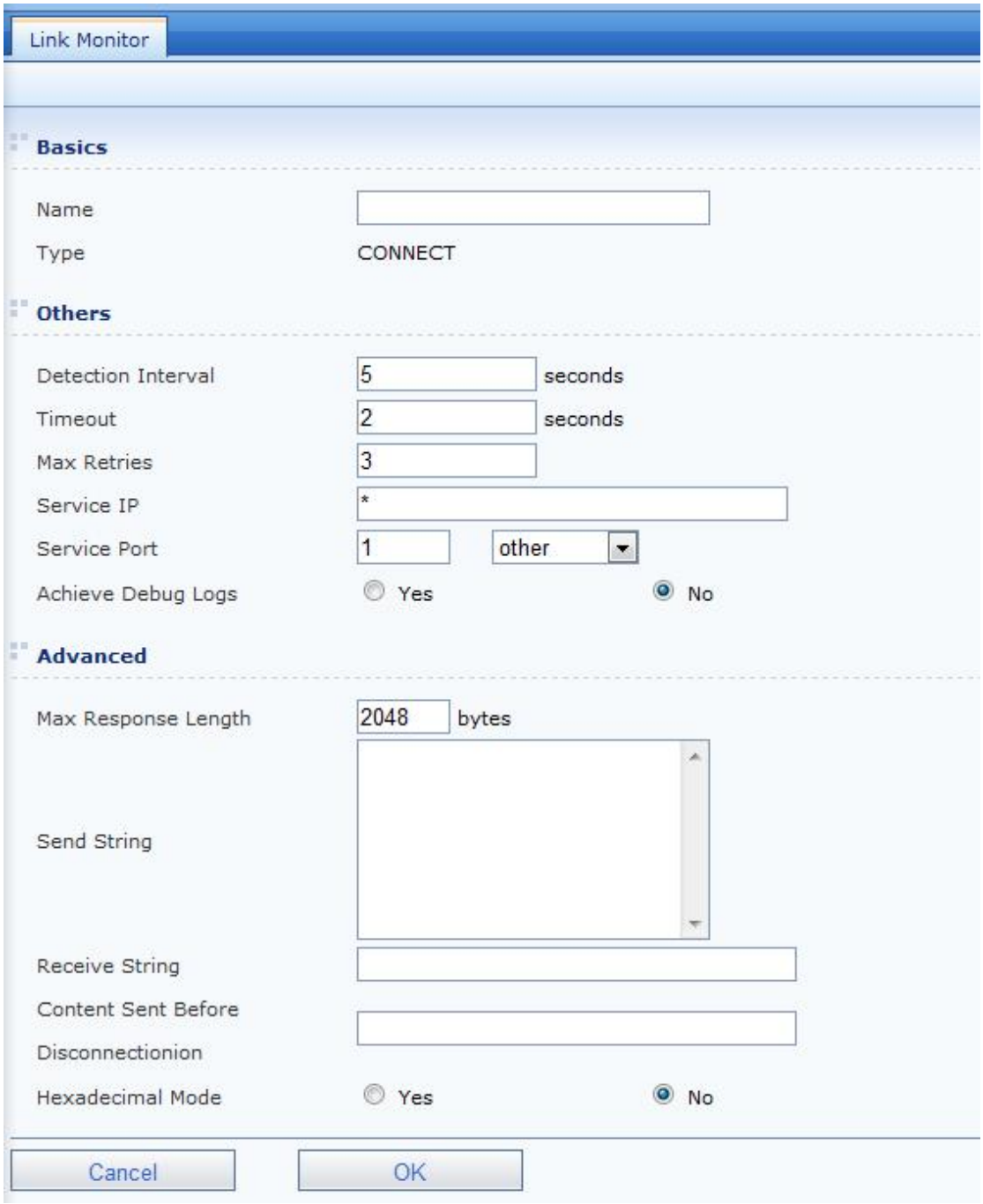
Max Attempts: Specifies maximum number of attempts for probing status of link after timeout value reached.

Service IP: Specifies the IP address to be monitored. * indicates all hosts.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Achieve Debug Logs: Specifies whether to archive debug log of ICMP-based link monitoring.

For **CONNECT-based** monitor, the attributes are as follows:



Name: Give it a distinguishable name.

Type: Specifies the type of the link monitor.

Detection Interval: Specifies an interval of detecting link status. Unit is second.

Timeout: Specifies a timeout value of detection, in second.

Max Retries: Specifies maximum number of attempts for probing status of link after timeout value reached.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Service IP: Specifies the IP address to be monitored. * indicates all hosts.

Service Port: Specifies the ports to be monitored. You can select **http**, **smtp**, **pop3**, **imap** to monitor the corresponding port, or select **other** to specify other port.

Achieve Debug Logs: Specifies whether to archive debug log of CONNECT-based link monitoring.

Max Response Length: Specifies the maximum length of contents in response, in byte.

Send String: Specifies the contents to be sent after connection setup.

Receive String: Specifies the contents which must be contained in received packets.

Content Sent Before Disconnection: Specifies the contents to be sent in the packet before connection is disconnected.

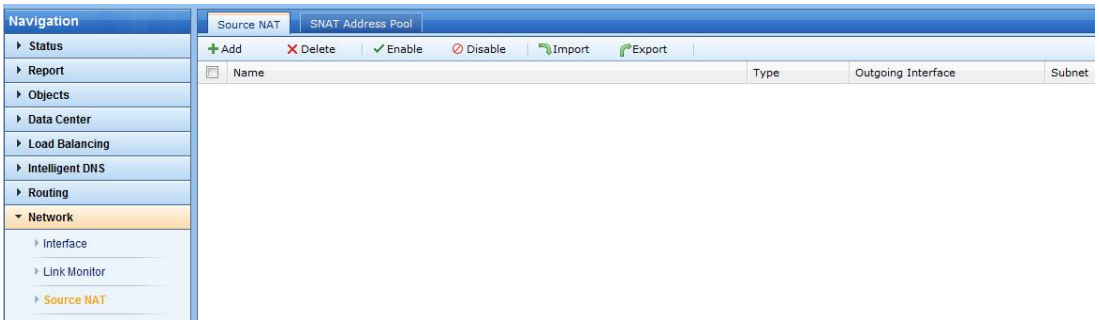
Hexadecimal Mode: Specifies whether contents to be sent and received is expressed in hexadecimal.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

10.3 Source NAT

10.3.1 Source NAT

Source NAT is used to translate the source IP address of the data going through the ADC. It's applicable to IPv4 and IPv6, and always used to proxy internal users to access the Internet.



To enable an NAT rule, click **Enable**; to disable an NAT rule, click **Disable**.

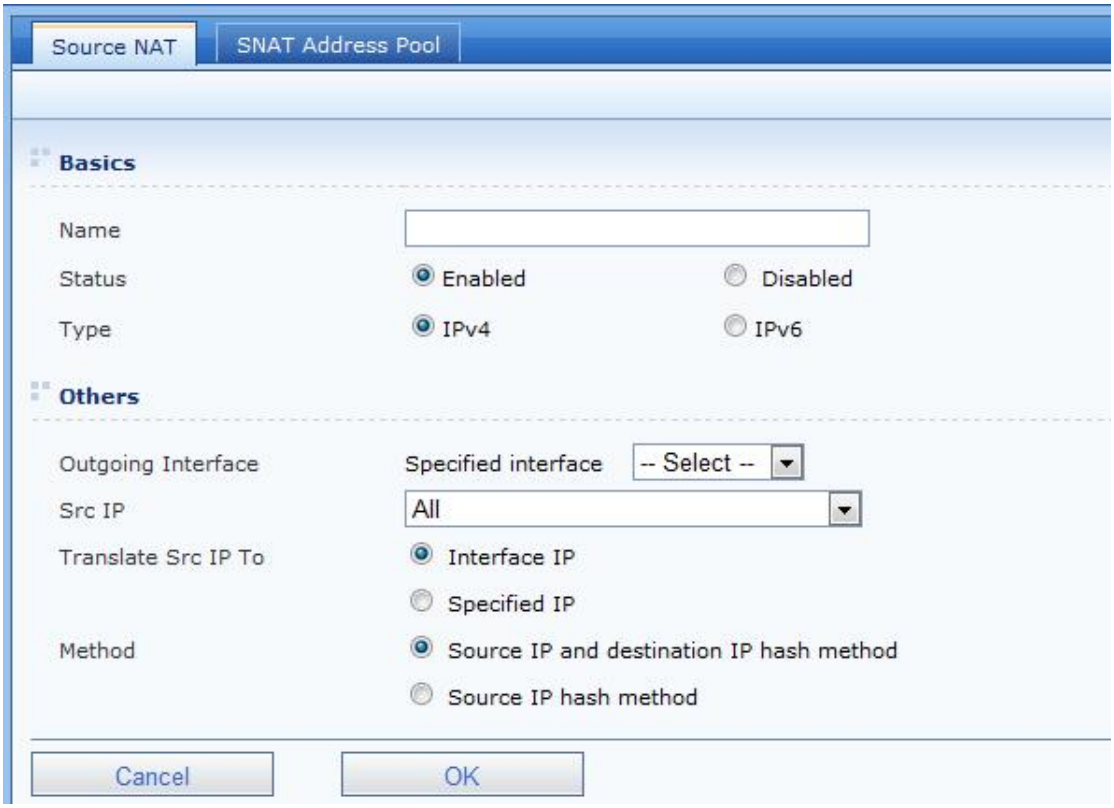
To remove an NAT rule, click **Delete**.

To move up the selected NAT rule, click  icon; or click  icon to move down the NAT rule NAT rule marches from top to button.

To duplicate the selected NAT rule, click  icon.

To create an NAT rule, click **Add** and configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

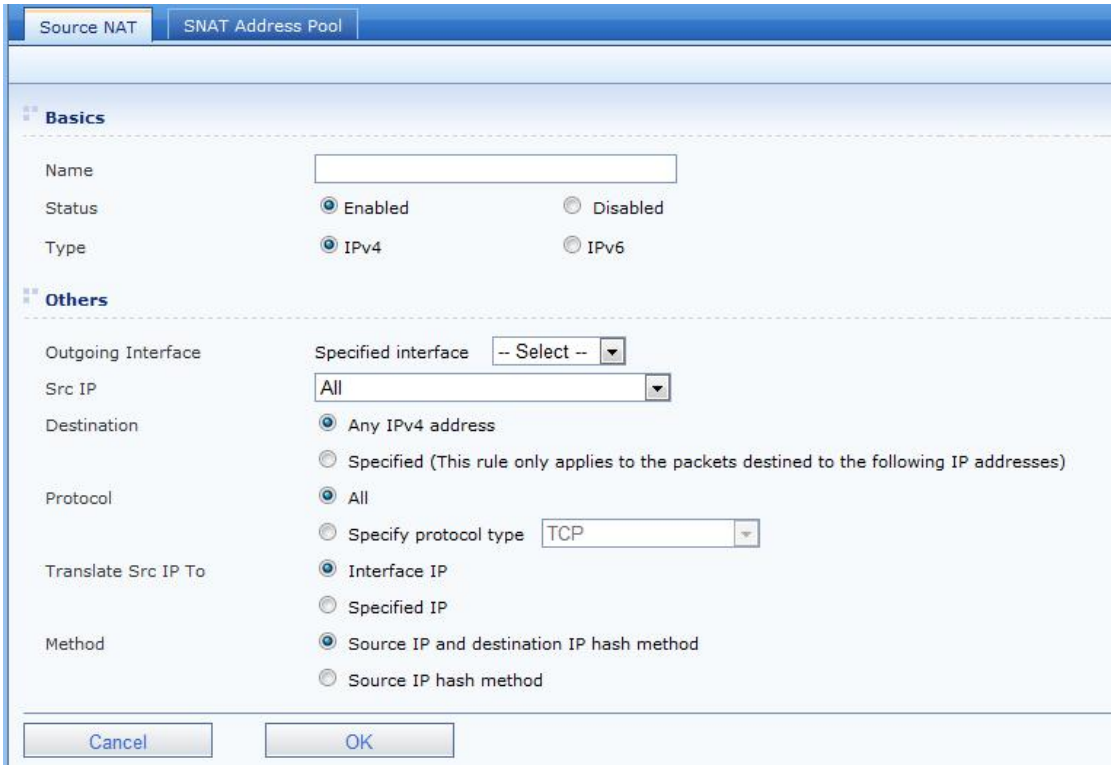


Tips:

1. Source IP address can be IPV4 and IPV6.
2. .Options for **Src IP** field can be **All, Subnet, IP range** and **local IP group**.

The above figure shows basic configuration information. For more information, you can click on **Advanced** on the upper-right corner to see the extended fields:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



For example, create an NAT rule to proxy all the internal user to access the Internet. The LAN segment is 192. 168. 1. 0/255. 255. 255. 0. You should configure the following fields:

Name: Specifies a distinguishable name.

Outgoing Interface: Specifies an egress interface for outbound data. Once the interface is specified, the rule only applies to the packets from the WAN or MANGE interface.

Src IP: Specifies an IP segment for source NAT. You can select **All** or **Specified**. In above example, select **Specified**, you need to enter 192. 168. 1. 0 as **IP Address** and 255. 255. 255. 0 as **Netmask**.

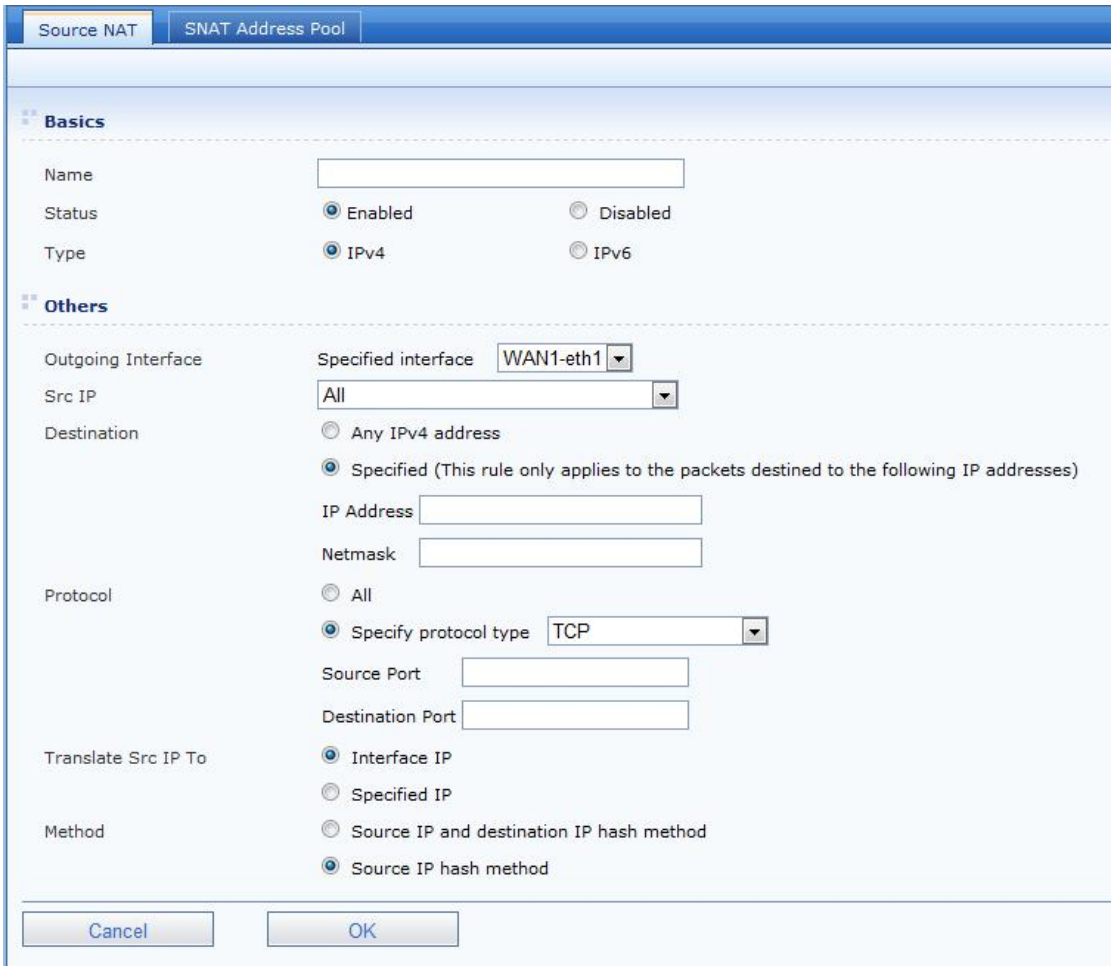
Destination: Specifies destination IP. Options are **All** and **Specified**. When the destination IP of data packet matches the specified dst IP address, the source IP address will be translated.

Protocol: Specifies a protocol. Options are **All** and **Specified**. **All** indicates all the protocols. For **Specified**, also need to specify protocol type and port. When the protocol of data packets matches the specified, the source IP address will be translated.

Translate Src IP To: Options are **Interface IP** and **Specified IP**. For **Specified IP**, you also need to specify start and end IP. In above example, you need to enter 202. 96. 137. 75 as public IP.

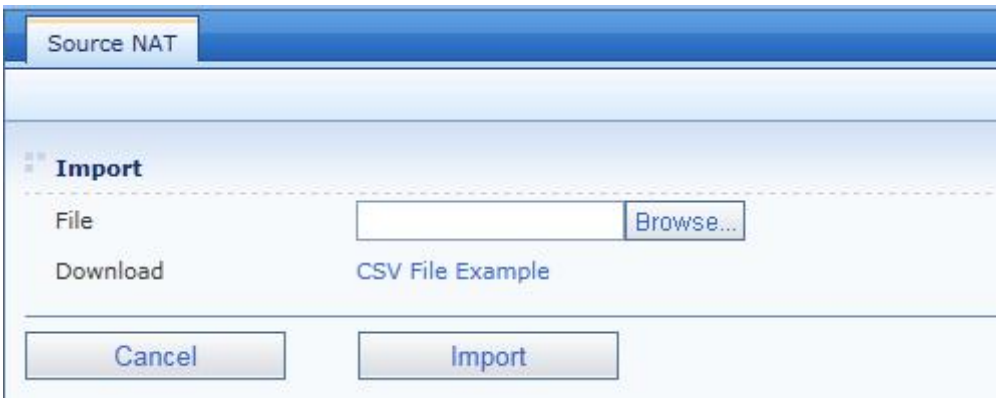
Method: Specifies a method for translating source IP address. For example, to translate two same source IP addresses to the same public IP address, you should select **Source IP hash method**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To save the settings, click **OK**; or click **Cancel** to give up the changes.

To import an NAT rule, click **Import**. The imported NAT rule file is custom file or the one exported from **Source NAT** list, click **Import** to enter the following figure:



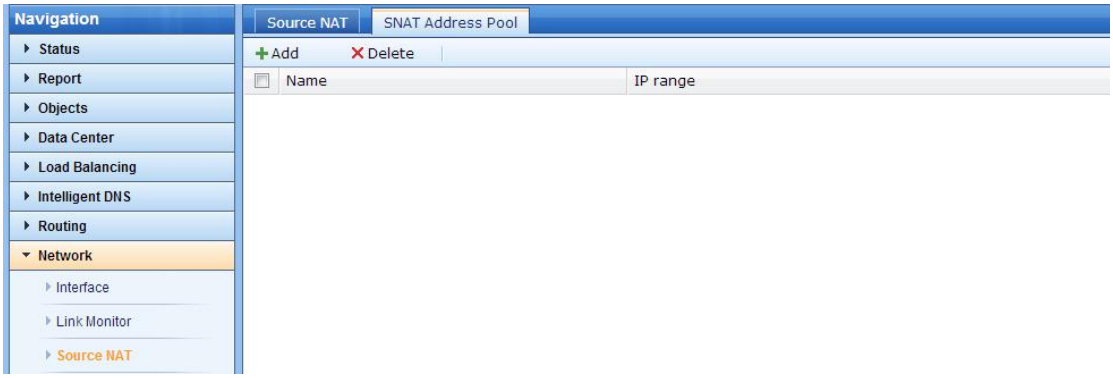
Click **Browse** to select local backup NAT rule or custom file, and click **Import** to import the file to the device; to give up the operation, click **Cancel**.

To download predefined template, click **CSV File Example**.

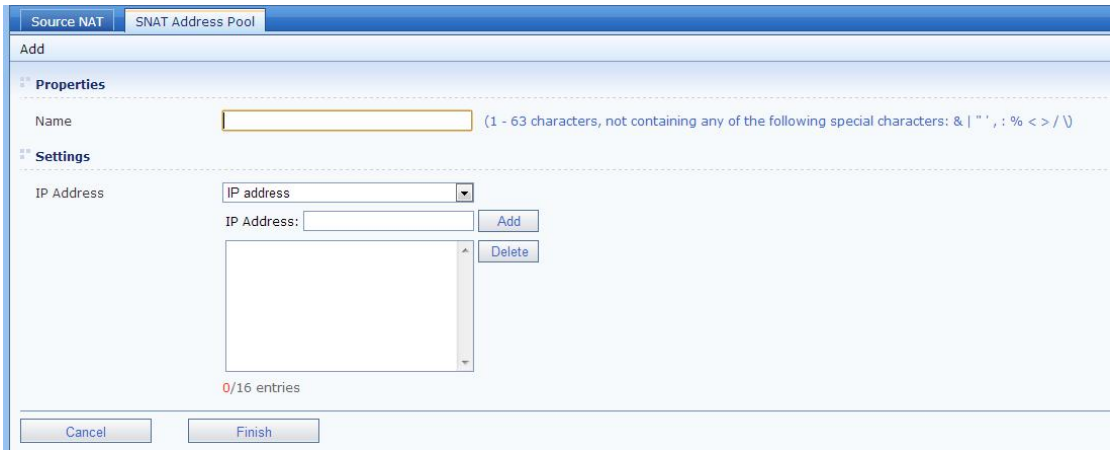
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

10.3.2 SNAT Address Pool

Navigate to **Network > Source NAT > SNAT Address Pool**, as shown in the following figure:



To create a new SNAT address pool, click **Add**, as shown in the following figure:



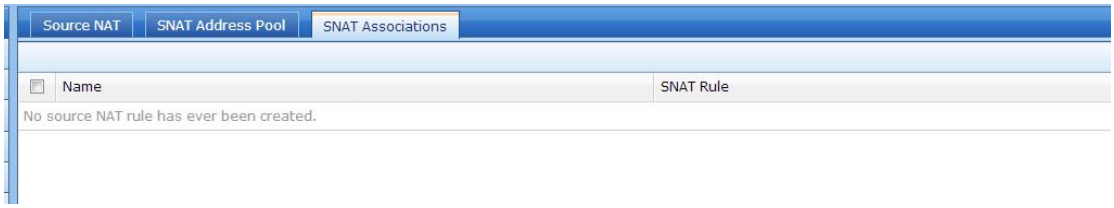
Name: Specifies the name of the SNAT address pool.

IP Address: Options can be IP address, IP range and subnet. IP ranges of the same SNAT address pool cannot overlap with each other, while IP ranges that belong to different SNAT address pools can overlap with each other. Mixture of IPV4 and IPV6 are supported.

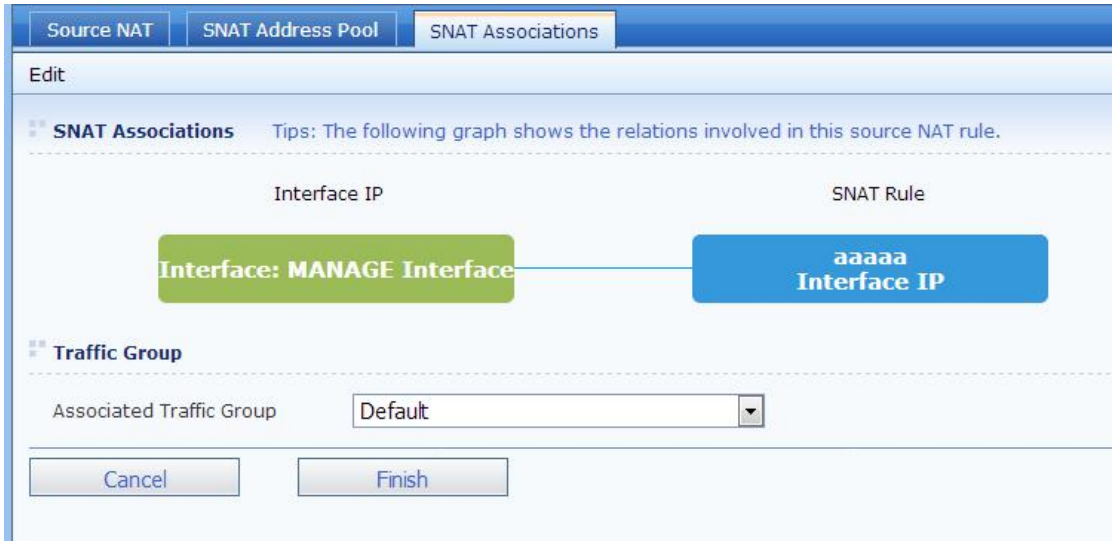
10.3.3 SNAT Associations

Navigate to **Network > Source NAT > SNAT Associations,** as shown in the following figure:
Note that this module is only available when high-availability cluster mode is enabled in **High Availability > HA Mode > Select HA Mode > High-availability cluster**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



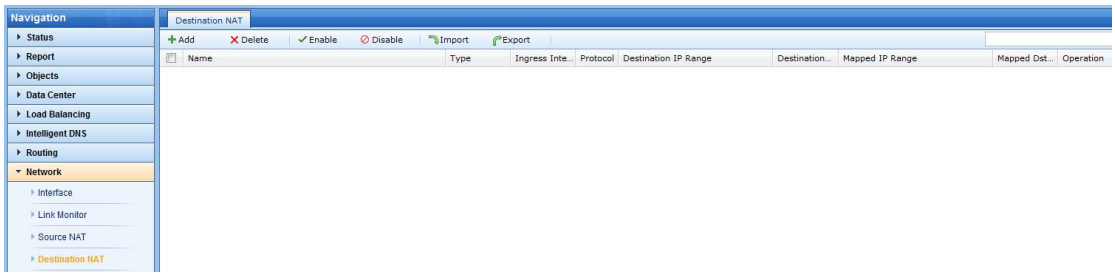
SNAT Associations: Source NAT rules will be put together and be associated, and the relations involved in this source NAT rule is shown below:



Associated Traffic Group: Specifies the traffic group to which the SNAT association group belongs. The policies in the association group will take effect on the device where the traffic group works.

10.4 Destination NAT

Navigate to **Network > Destination NAT**, you can launch the services provided by LAN servers. It's applicable to IPv4.

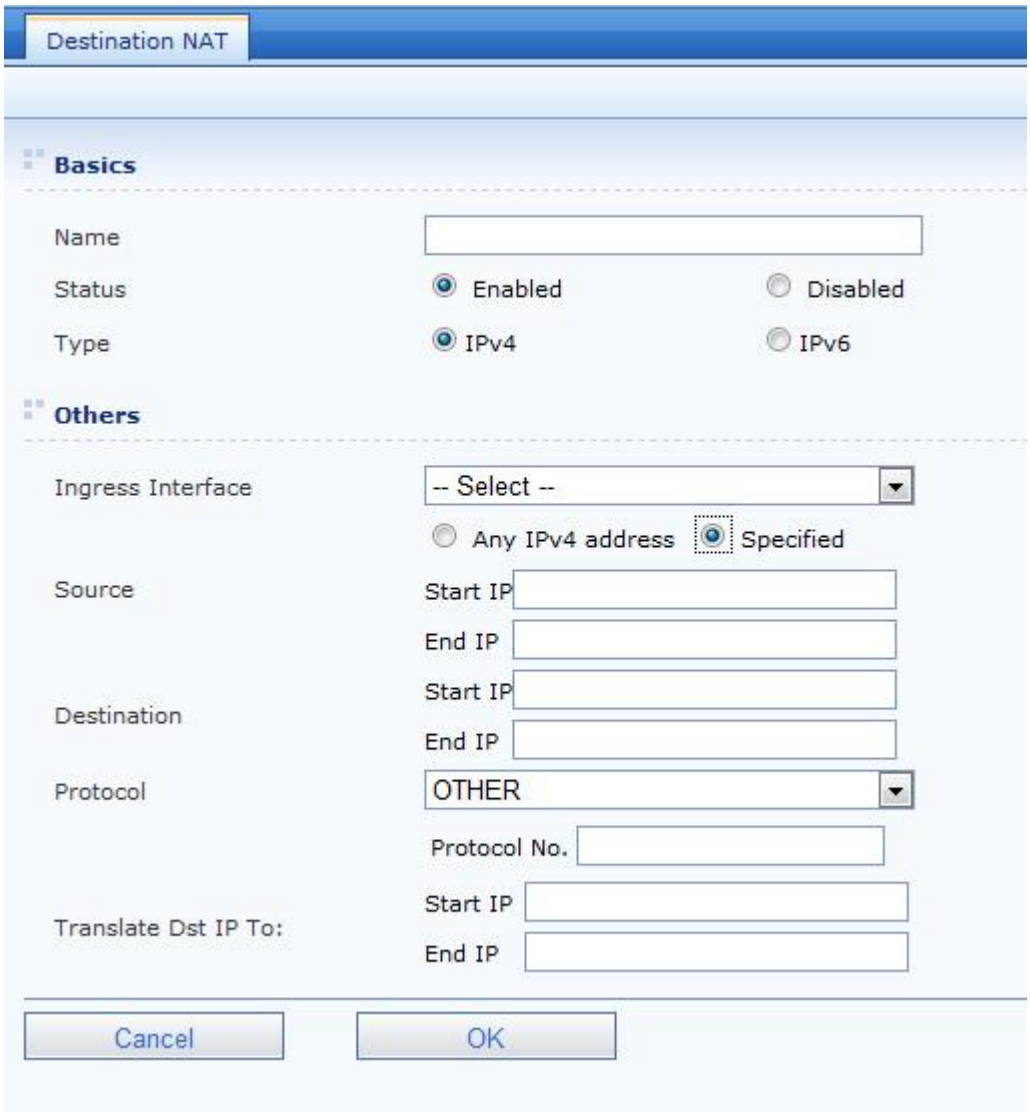


To enable a destination NAT rule, select the entry and click **Enable**; to disable a destination NAT rule, select the entry and click **Disable**.

To remove a destination NAT rule, select the entry and click **Delete**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

To create a destination NAT rule, click **Add** to enter the following page:



Name: Specified a name for the destination NAT rule.

Status: Specifies whether the destination NAT rule is **Enabled** or **Disabled**.

Type: Specifies the port type of the destination NAT rule, options are IPV4 and IPV6.

Ingress Interface: Specifies an interface to launch internal services.

Source: Options are **All** and **Specified**. For **All**, all the request packets will match the DNAT rule. For **Specified**, only when the the source IP of the request packets matches the specified one, it will match the DNAT rule.

Destination: Specifies a start and end IP. When the dst IP of the data packet matches the specified, it will match the DNAT rule.

Protocol: Specifies the service type launched by LAN server. Options are **ALL**, **TCP**, **UDP**, **ICMP** and **OTHER**. The following are brief introductions to each option:

- **ALL:** Indicates to launch all the services.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

- **TCP:** Indicates to launch TCP service, and you can specify the port to launch the service.
- **UDP:** Indicates to launch UDP service, and you can specify the port to launch the service.
- **ICMP:** Indicates ping service.
- **OTHER:** Specifies a protocol to launch the service.

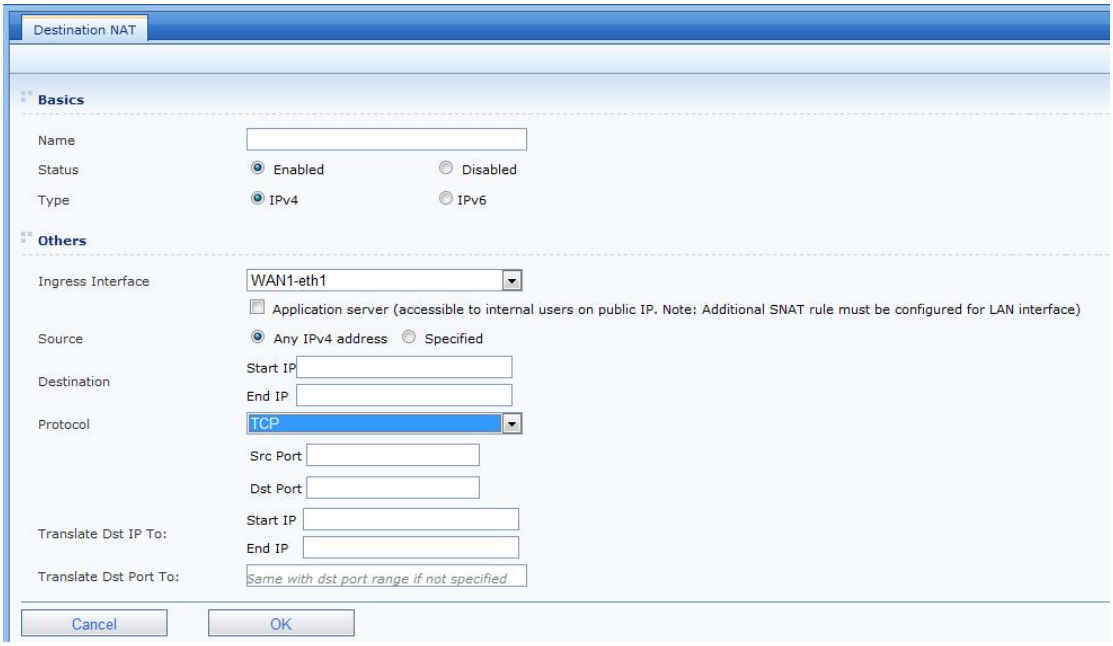
Translate Dst IP To: Optional, default values will be used. .

Association Traffic Group: This option is only available when high-availability cluster mode is enabled in **High Availability > HA Mode > Select HA Mode > High-availability cluster**. Select a traffic group to which the SNAT association group belongs. The policies in the association group will take effect on the device where the traffic group works.

To save the settings, click **OK**; to give up the changes, click **Cancel**.

For example, there is a computer on LAN whose IP is 192. 168. 100. 250 to provide Web service for external network. The IP address of WAN interface is 202. 96. 137. 75, and the port is 80.

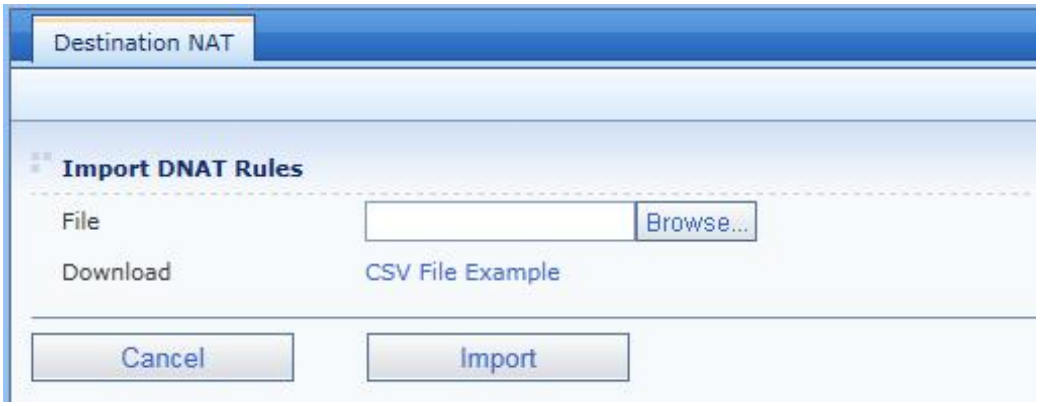
On the **Network** > **Destination NAT** page, click **Add** to configure the following contents:



To make the rule take effect, click **OK**. Then the Web service can be accessed by external users with the DNAT rule on the ADC.

To import a DNAT rule, click **Import**. The imported DNAT rule file is custom file or the one exported from **Destination NAT** list.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Click **Browse** to select local backup DNAT rule or custom file, and click **Import** to import the file to the device; to give up the operation, click **Cancel**.

To download predefined template for editing DNAT rule, click **CSV File Example.**

To back up the custom DNAT rule, click **Export**.

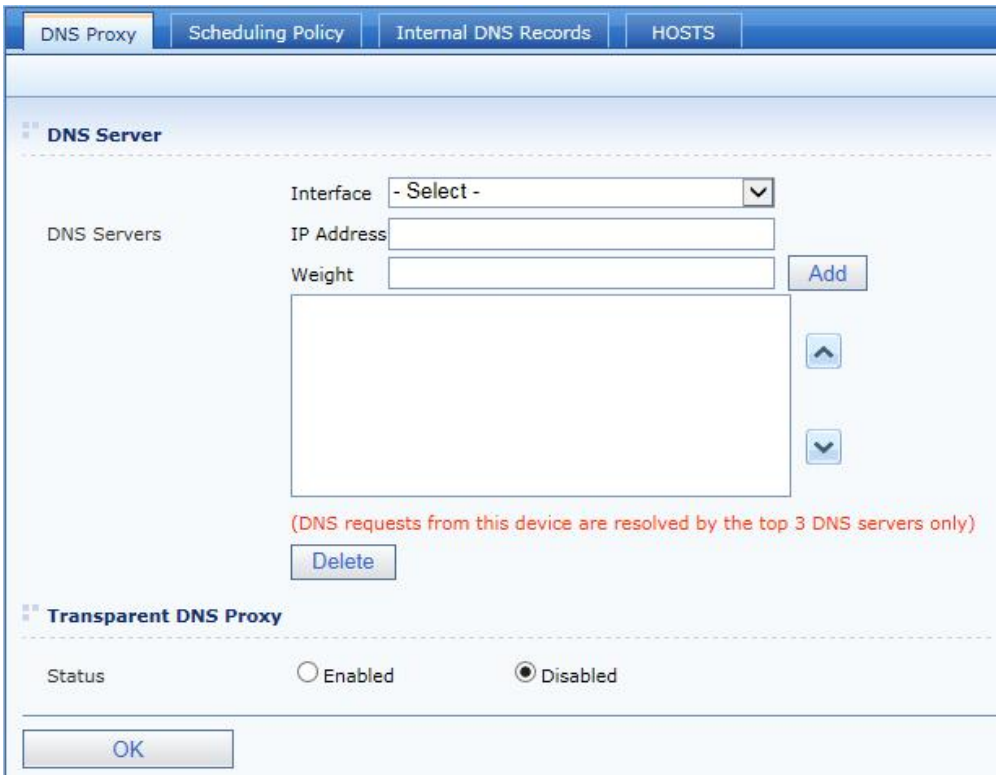
10.5 DNS Proxy

In **Network > DNS Proxy**, you can configure the following sections: DNS proxy, scheduling policy, internal DNS records and hosts.

10.5.1 DNS Proxy

To set DNS server address, navigate to **Network > DNS Proxy > DNS Proxy**. When the ADC needs to resolve domain name, it will reach to the DNS server with this IP address, and forward DNS request from internal hosts.

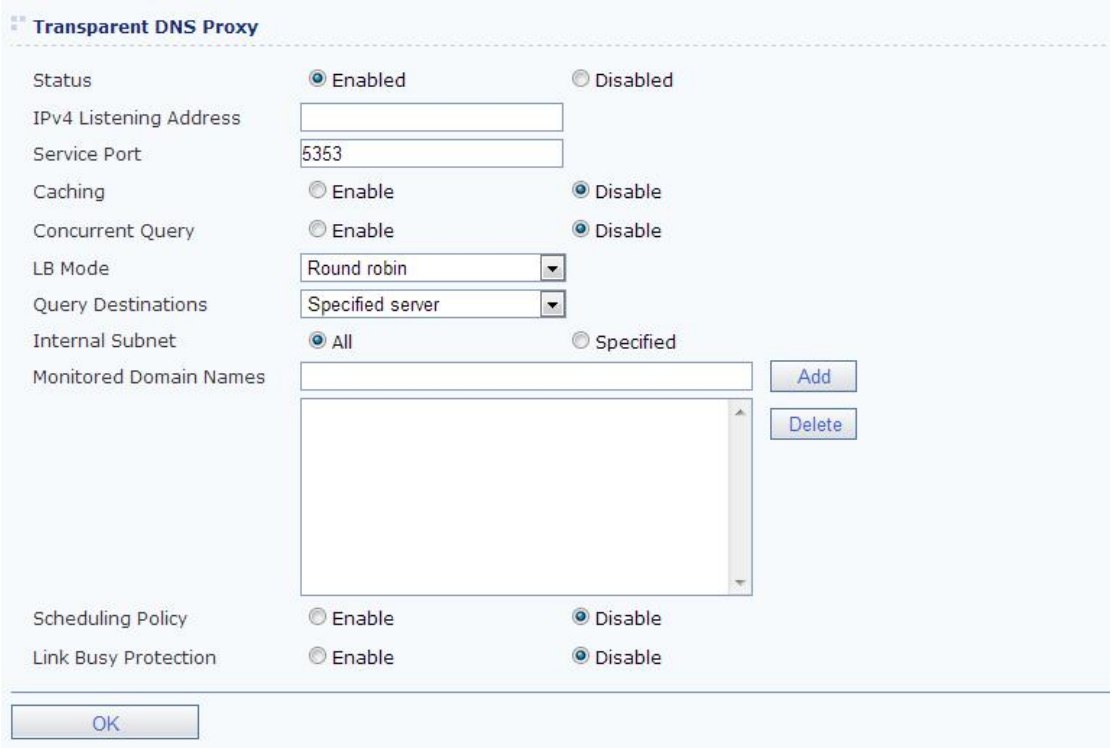
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



DNS Servers: Set an interface for the DNS server. You can configure **IP Address** and **Weight** of each DNS server for each WAN interface. The ADC only uses the top 3 DNS servers. Select an interface from **Interface** list and enter **IP Address** and **Weight** of DNS server. Click **Add** to add them to the **DNS Servers** list. To remove a DNS server, select the server and click **Delete**.

Status: Specifies whether the transparent DNS proxy is **Enable** or **Disabled**. If you select **Enabled**, the DNS request from internal hosts will be forwarded to the DNS server by the ADC, and configure the following expanded fields:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



IPv4 Service IP: Specifies a service IP address, DNS server address can be set as a service IP.

IPv6 Service IP: Specifies a service IP address, DNS server address can be set as a service IP.

Caching: Specifies whether to cache the DNS responses. Once enabled, cached contents will be used to respond to client when receiveing DNS queries.

Concurrent Query: Specifies whether to forward queries to all the available DNS servers and respond to client with the first valid response after receiving queries from the client**.** (The scheduling policy takes precedence over concurrent query.)

LB Mode: Select a LB mode for Transparent DNS Proxy. Options are **Round robin**, **Weighted round robin**, **Weighted least traffic** and **Priority**. The following are brief introductions to each option:

- **Round robin:** DNS server in the **DNS Servers** list will be selected by turns. Each server has equal chance.
- **Weighted round robin:** DNS server in **DNS Servers** list will be determined by their weight.
- **Weighted least traffic:** Select a DNS server based on the weight over the link with least traffic.
- **Priority:** Select the DNS server with the highest weight all the time. Only when the DNS server with highest weight is offline or busy, the DNS server with lower weight will be selected.

Query Destinations: Options can be **All DNS queries**, **Specified server** and **Specified domain name**. When **All DNS queries** is selected, **Internal Subnet** field should be specified, otherwise intelligent DNS is invalid. **Specified domain name** indicates the domain name

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

which has been configured in the scheduling policy.

Internal Subnet: Specifies a network segment where DNS proxy service is needed.

Listen Domain: Specifies the domain name to be listened, in order to determine the validity of DNS server. Only when the domain name is valid, the transparent DNS proxy will be performed.

To scheduled the request of special users to the specified server., click **Scheduling Policy**

Link Busy Protection: Specifies whether the link busy protection is **Enabled** or **Disabled**. If select **Enabled**, the busy link will not be scheduled; if all the links are busy, the DNS request will be scheduled to the DNS server bound by the links randomly.

To save the changes, click **OK**.

10.5.2 Scheduling Policy

Scheduling policy is used to schedule the request of special users to the specified server.



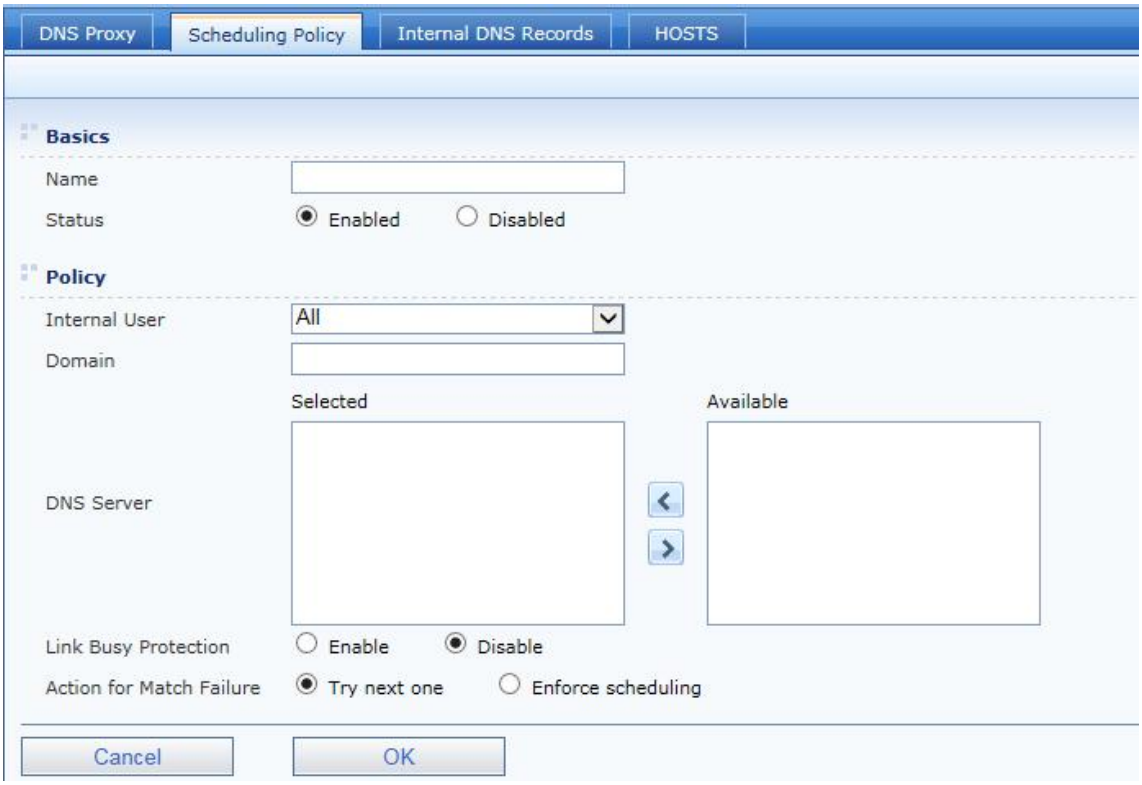
To make a scheduling policy take effect, select the policy and click **Enable**.

To disable a scheduling policy, select the policy and click **Disable**.

To remove the selected scheduling policy, click **Delete**.

To create a scheduling policy, click **Add** and configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Specifies a distinguishable name.

Status: Specifies whether the scheduling policy is **Enabled** or **Disabled**.

Internal User: Select an internal IP segment that the policy will apply to. Options are **All**, **IP range** and **Subnet**.

Domain: Specifies the target domain name to match the scheduling policy.

DNS Server: Specifies a DNS server to return results for this scheduling policy.

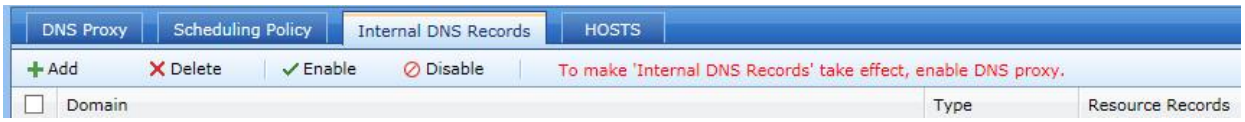
Link Busy Protection: Specifies whether to select links in accordance with link state.

Action for Match Failure: Specifies how to handle the issue when the DNS servers become invalid. Select **Try next one** to match next scheduling policy instead of the current one. Select **Enforce scheduling** to return the DNS server in **DNS Servers** all the time.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

10.5.3 Internal DNS Records

In **Network > DNS Proxy > Internal DNS Record**, you can add DNS items on the ADC for DNS resolution.



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

To make the selected internal DNS record take effect, click **Enable**.

To remove the selected internal DNS record, click **Delete**.

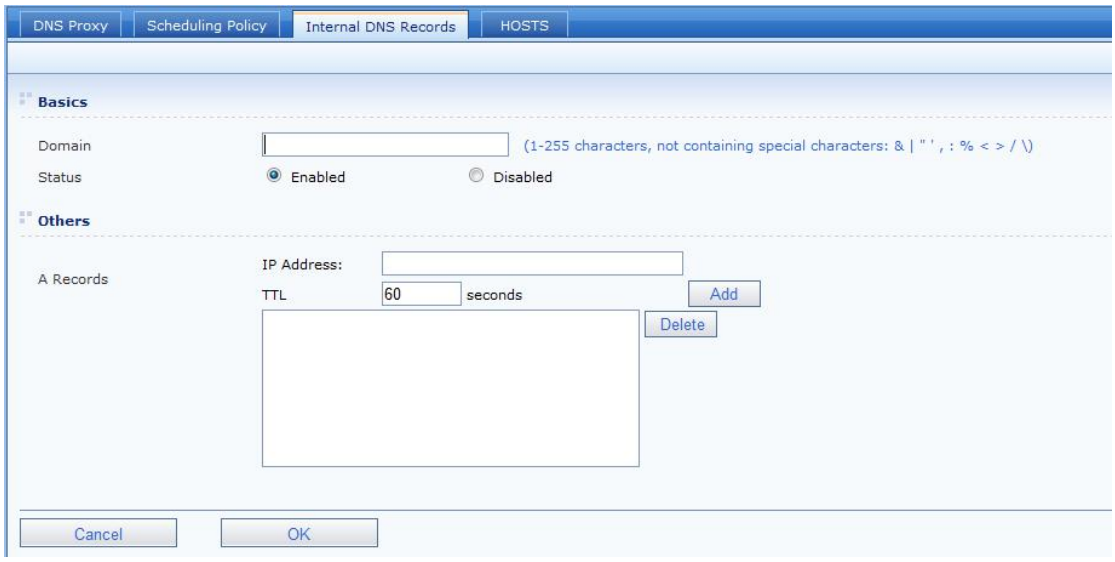
To create a DNS record, click **Add** to enter the following page:



Interface Type: Select an interface type for the DNS record. Options are **A records**, **AAAA records**, **MX records**, **CNAME records** and **TXT records**.

To give up the operation, click **Cancel**.

To create A records, select **A records** and click **Next**, as shown below:



Domain: Give it a domain name.

Status: Specifies whether the A records is **Enabled** or **Disabled**.

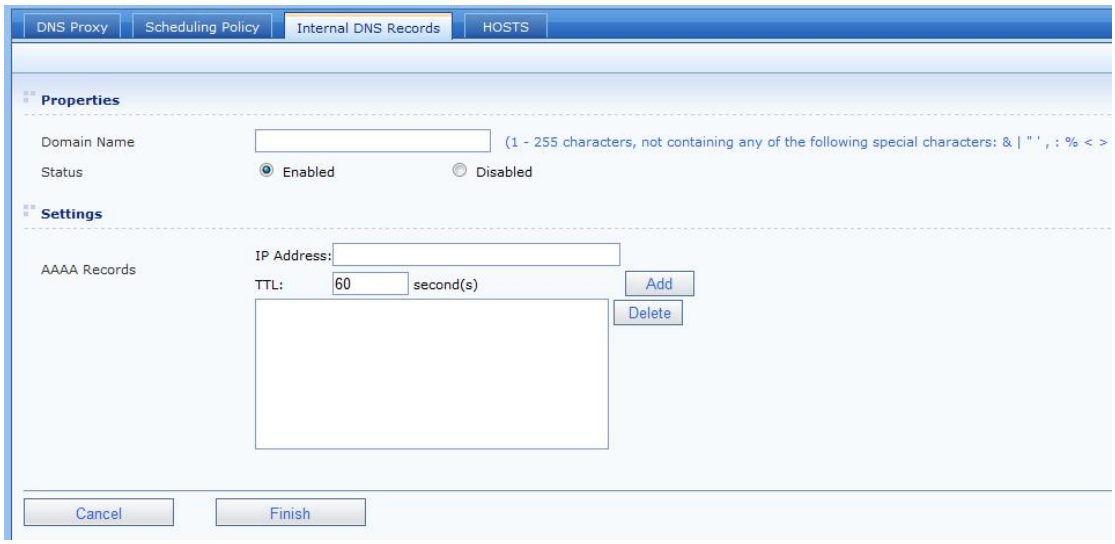
IP: Specifies an IP address corresponding to the domain name of A records.

TTL: Specifies time period how long the A records can be cached on local DNS server, in second.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

To create AAAA records, select **AAAA records** and click **Next**, as shown below:



Domain: Give it a domain name.

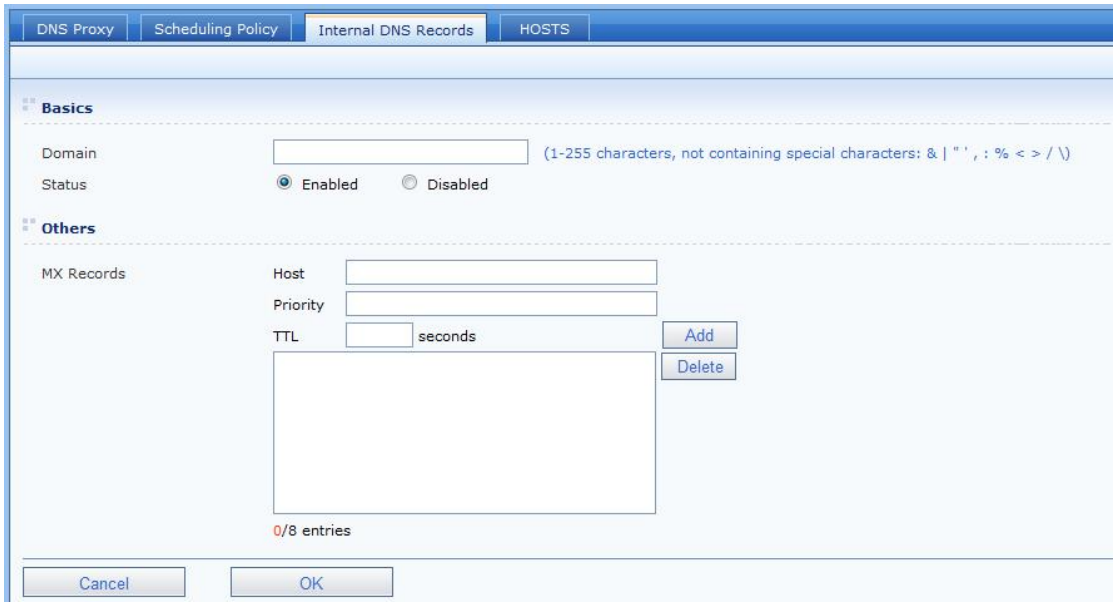
Status: Specifies whether the AAAA records is **Enabled** or **Disabled**.

IP: Specifies an IP address corresponding to the domain name of AAAA records.

TTL: Specifies time period how long the AAAA records can be cached on local DNS server, in seconds.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

To create MX records, select MX **records** and click **Next**, as shown below:



Domain: Give it a domain name.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Status: Specifies whether the MX records is **Enabled** or **Disabled**.

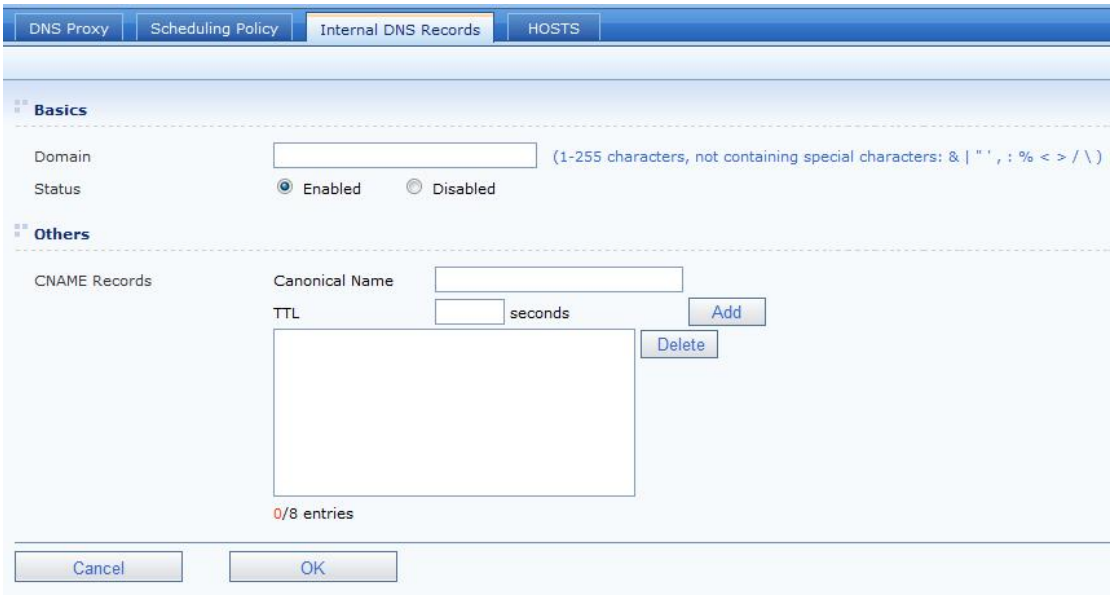
Host: Specifies an IP address or domain name for MX records.

Priority: Specifies a priority of MX records in **MX records** list.

TTL: Specifies time period how long the MX records can be cached on local DNS server, in seconds.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

To create CNAME records, select CNAME **records** and click **Next**, as shown below:



Domain: Give it a domain name.

Status: Specifies whether the CNAME records is **Enabled** or **Disabled**.

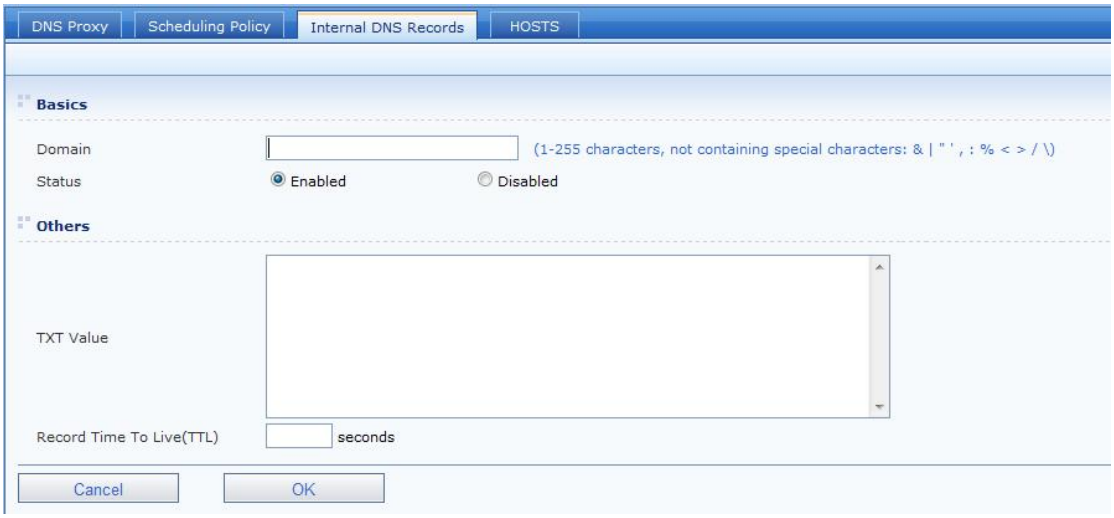
Canonical Name: Specifies a canonical name for CNAME records.

TTL: Specifies time period how long the CNAME record can be alive in Local DNS, in seconds.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

If select **TXT records** as the interface type, click **Next** and configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Domain: Give a domain name for TXT records.

Status: Specifies whether the TXT records is **Enabled** or **Disabled**.

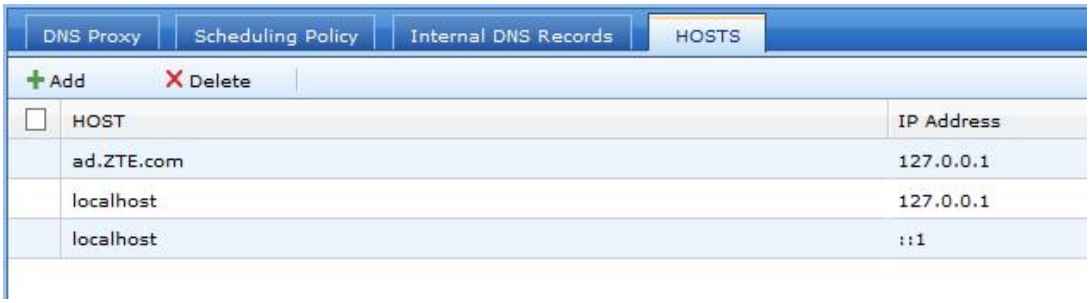
TXT Value: Specifies a TXT value corresponding to the domain of TXT records.

Record Time To Live(TTL): Specifies time period how long the TXT records can be cached on local DNS server, in seconds.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

10.5.4 HOSTS

It's applied when the ADC accesses a domain name. Navigate to **Network > DNS Proxy > HOSTS** to set HOST table.



To remove the selected HOST, click **Delete**.

To create a HOST, click **Add** to enter the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



HOST: Give it a host name or a domain name.

IP Address: Specifies a corresponding IP address for the host.

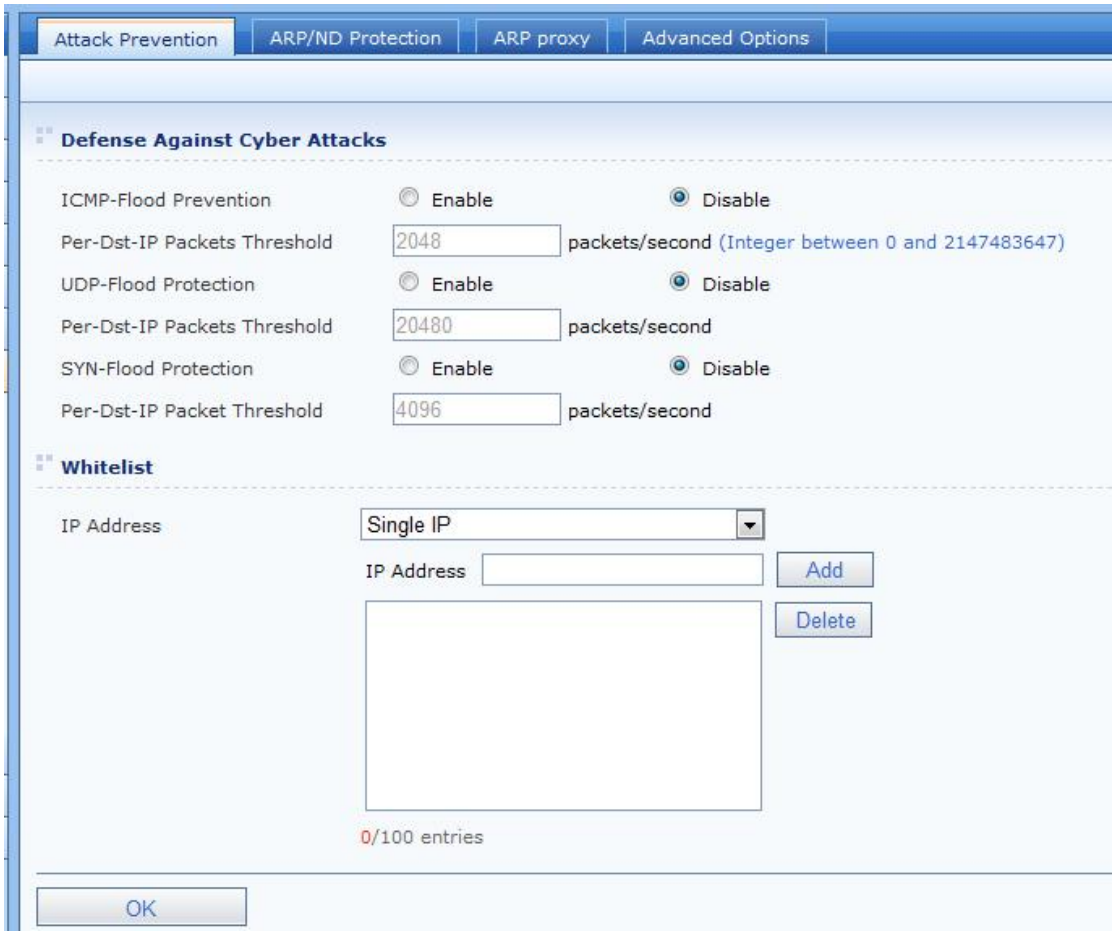
To save the settings, click **OK**; to give up the settings, click **Cancel**.

10.6 Security

10.6.1 Attack Prevention

DOS attack usually motives for consuming resources on servers and forcing the server to stop response. It can also cause congestion of server response by forging massive request data, so that the request from legal users cannot get response. The anti-DOS attack feature of SANGFOR ADC can prevent DOS attack from extranet and determine the attacker by its IP address.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



ICMP-Flood Prevention: Specifies whether the ICMP-Flood prevention is **Enabled** or **Disabled**.

UDP-Flood Protection: Specifies whether the UDP-Flood protection is **Enabled** or **Disabled**.

SYN-Flood Protection: Specifies whether the SYN-Flood protection is **Enabled** or **Disabled**.

Per-Dst-IP Packets Threshold: Specifies a maximum number of ICMP/UDP packets per second for protection module.

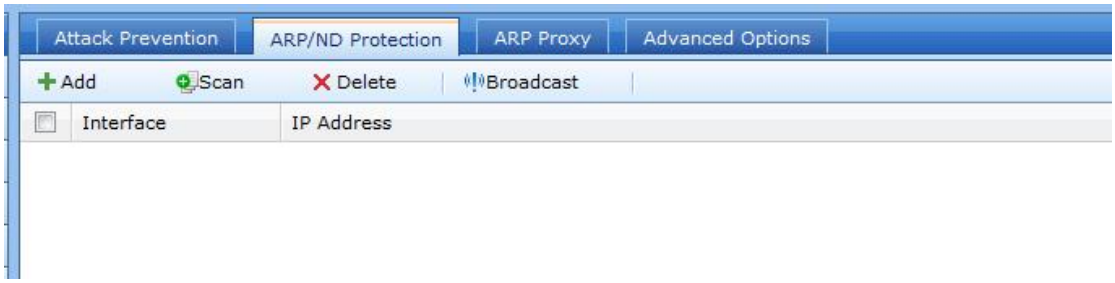
Per-Dst-IP Packet Threshold: Specifies a maximum number of SYN-Flood packets received by the WAN interface for protection module.

Whitelist: Specifies the unprotected IP addresses.

10.6.2 ARP/ND Protection

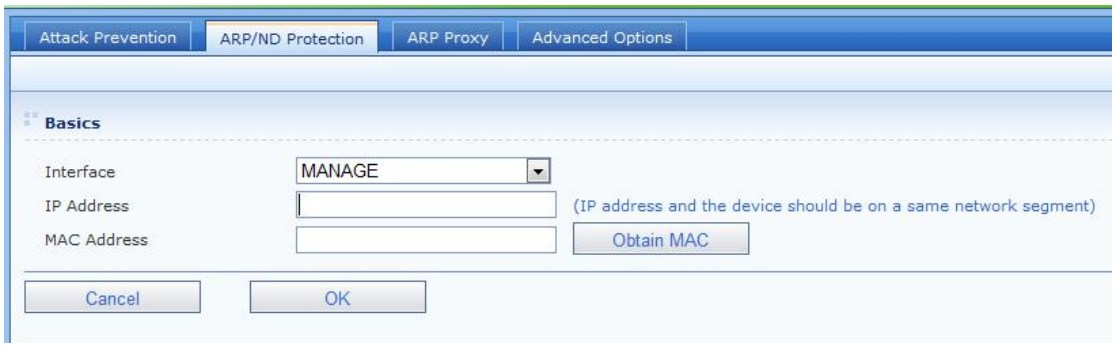
On the **Network > Security > ARP/ND Protectio**n page, you can set static ARP. It's always used to bind the ARP of critical device and server, in order to defend against internal ARP spoofing attacks.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To remove the selected ARP item, click **Delete**.

To create an ARP item, click **Add** to enter the following page:



Interface: Specifies an interface to bind IP/MAC.

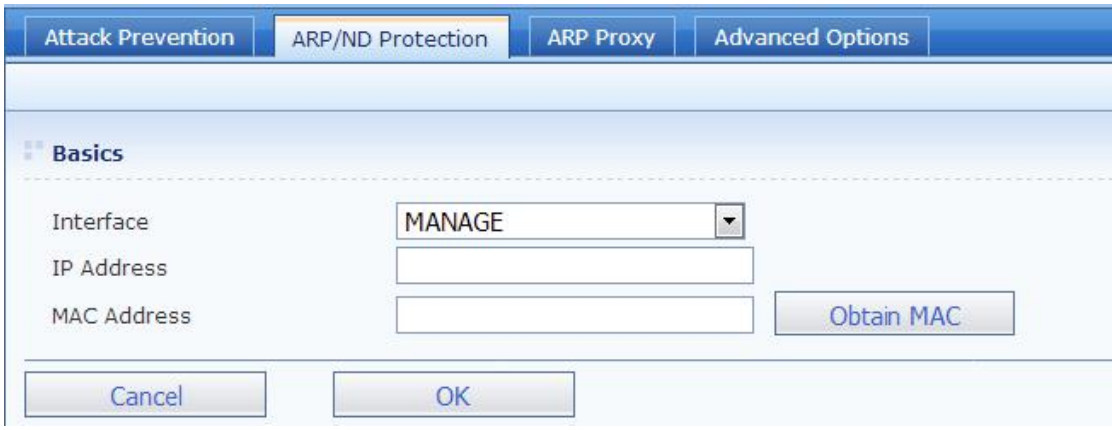
IP Address: Specifies an IP address for the interface.

MAC Address: Specifies a MAC address of IP address specified above.

Click **Obtain MAC** to get MAC address for the specified IP address automatically. If failed to get it, failure information will pop up.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

The ADC provides the feature of getting MAC address automatically. Click **Obtain** to get the MAC addresses corresponding to an IP range automatically, as shown in the following page:



Enter a start IP and end IP. Click **Obtain** and the ADC will get the corresponding MAC address by sending ARP broadcast.

MAC Address: Displays the ARP information after scanning completed.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Click **OK,** then the ARP information will be added to the ARP list automatically.

To give up searching ARP information, click **Cancel** to return to the default **ARP/ND Protection** page.

To broadcast MAC address of gateway proactively, click **Broadcast**.



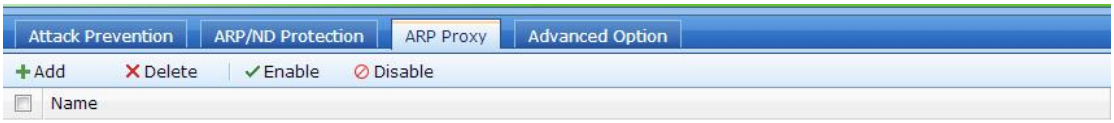
Broadcast Interval: Specifies how often the ADC sends a ARP broadcast packet, in minutes.

Click **Broadcast**, then the ARP information scanned automatically will be added to the ARP list.

To update the configuration, click **OK**; to give up the settings, click **Cancel**.

10.6.3 ARP Proxy

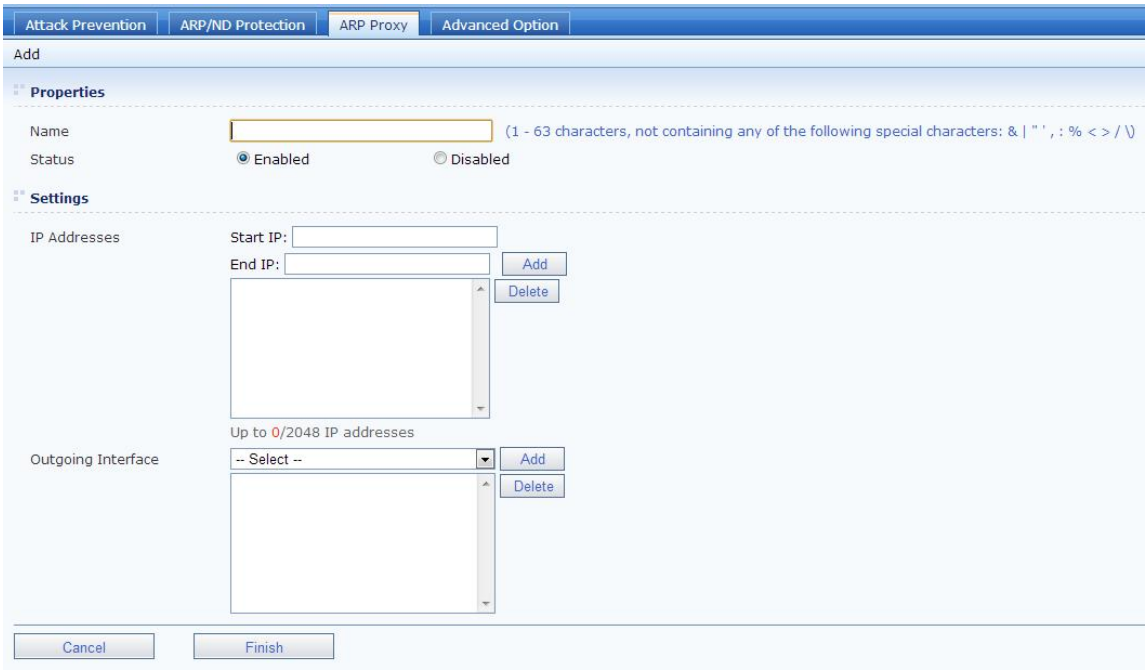
Navigate to **Network > Security > ARP Proxy,** as shown in the following figure:



To remove the selected ARP Proxy entry, click **Delete**.

To create an ARP proxy entry, click **Add** to enter the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Specifies the name of ARP Proxy.

Status: Specifies whether to enable or disable ARP Proxy.

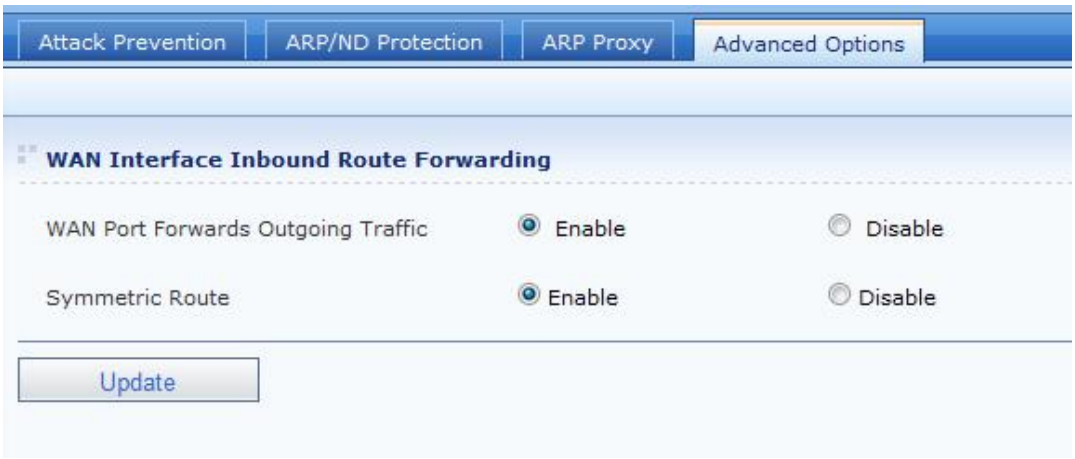
IP Address: Specifies IP addresses

Outgoing Interface: Specifies outgoing interfaces. Multiple outgoing interfaces can be selected for one policy. But if **Interface received request** is selected, other outgoing interfaces cannot be selected, and if other outgoing interfaces are selected, **Interface received request** can not be selected.

Interface received request: Specifies destination MAC address of ARP response according to the incoming interface of ARP request.

10.6.4 Advanced Options

To set route forwarding options, navigate to **Network > Security > Advanced Options**.



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

WAN Port Forwards Outgoing Traffic: Select **Enable** to forward the data packets received by the WAN interface; or select **Disable** to drop the data packets. If select **Disable**, the data can not transmit between WAN and LAN interface, except for that of **Virtual Service**, **DNS**, **Source NAT**, **Destination NAT**, **Remote logging**, and **Policy-based Routing** or **Static Route**. All the data can transmit until **Enable** is selected.

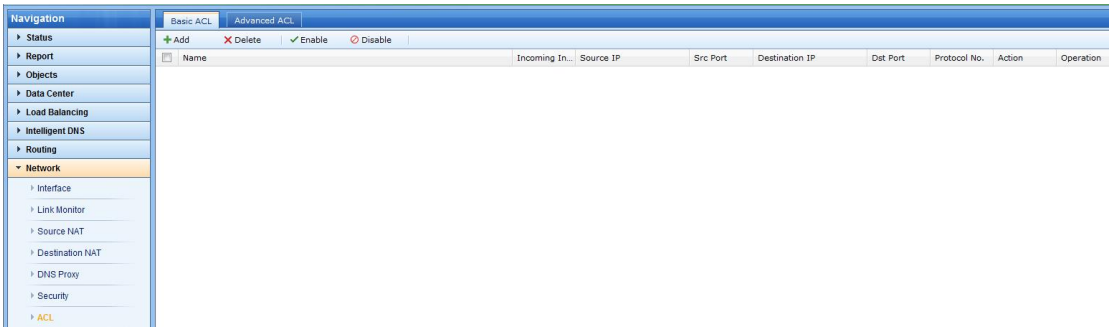
Symmetric Route: Select **Enable** to enable symmetric route; or select **Disable** to enable asymmetric route. Default is symmetric route.

10.7 ACL

It provides link-based access control policy and that based on virtual service.

10.7.1 Basic ACL

Navigate to **Network > ACL > Basic ACL**, you can configure access control policy based on protocol and IP.



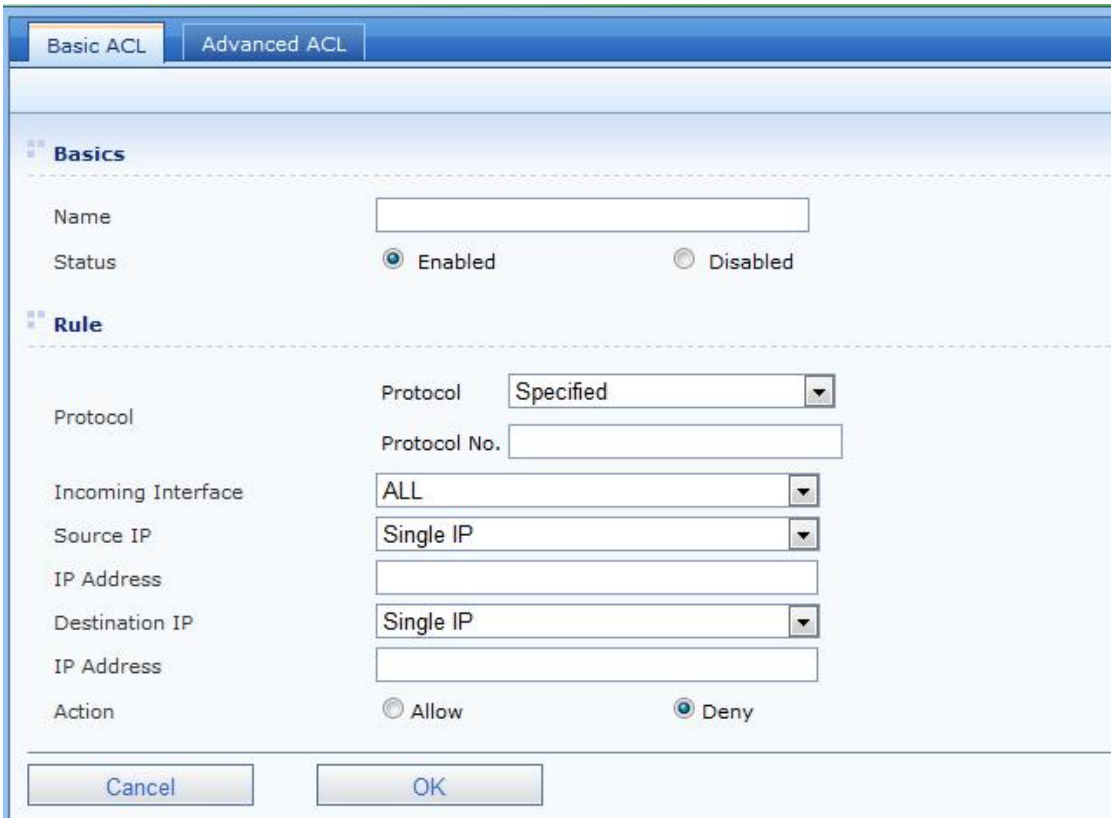
To enable the selected ACL rule, click **Enable**; or click **Disable** to disable the selected ACL rule.

To remove the selected ACL rule, click Delete.

To move up an ACL rule, click icon; to move down an ACL rule, click icon. The ACL rules match from top to button.

To create an ACL rule, click **Add** to configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Protocol: Specifies a protocol number. When the protocol used in the communication is consistent with the specified protocol number, the ACL rule will be matched. 0 represents all the protocol.

Incoming Interface: Specifies incoming interface. You can select ALL and specify incoming interfaces..

Source IP: Specifies an IP segment. When the source IP address complies with the IP segment, the current ACL rule will be matched.

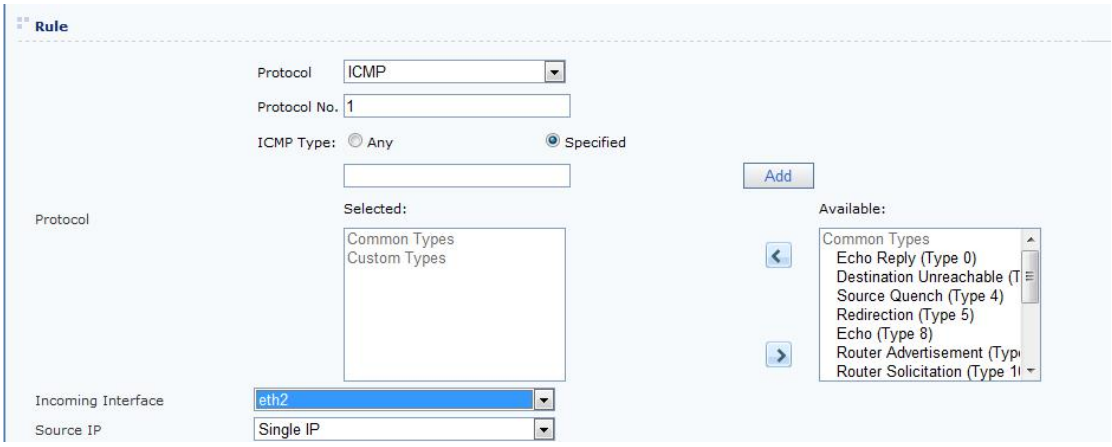
Destination IP: Specifies an IP segment. When the destination IP address complies with the IP segment, the current ACL rule will be matched.

Action: When the above criteria are matched, then the **Action** will be performed.

- **Allow:** when the above criteria are matched, allow this access request.
- **Deny:** When the above criteria are matched, deny this access request.

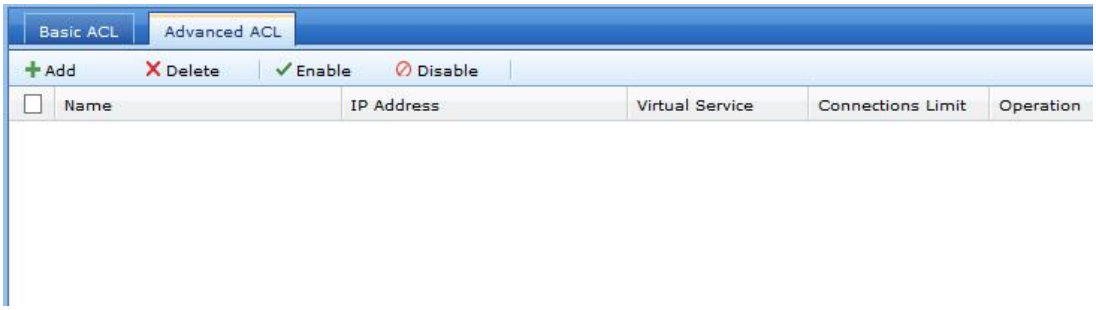
Tips: When ICMP protocol is selected, you can select **Common Types** for ICMP Type, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



10.7.2 Advance ACL

To configure ACL for virtual service, navigate to **Network > ACL > Advanced ACL**, as shown in the following figure:



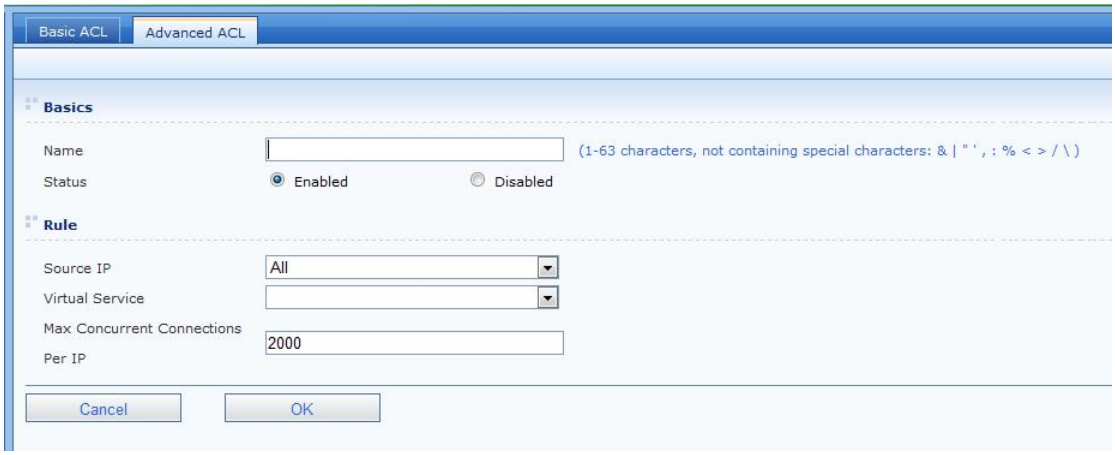
To enable the selected ACL rule, click **Enable**; or click **Disable t**o disable the selected ACL rule.

To remove the selected ACL rule, click **Delete**.

To move up an ACL rule, click icon; or click icon to move down an ACL rule. The ACL rules match from top to button.

To create an ACL rule, click **Add** to configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Source IP: Specifies an IP segment. When the source IP address belongs to the IP segment, the current ACL rule will be matched.

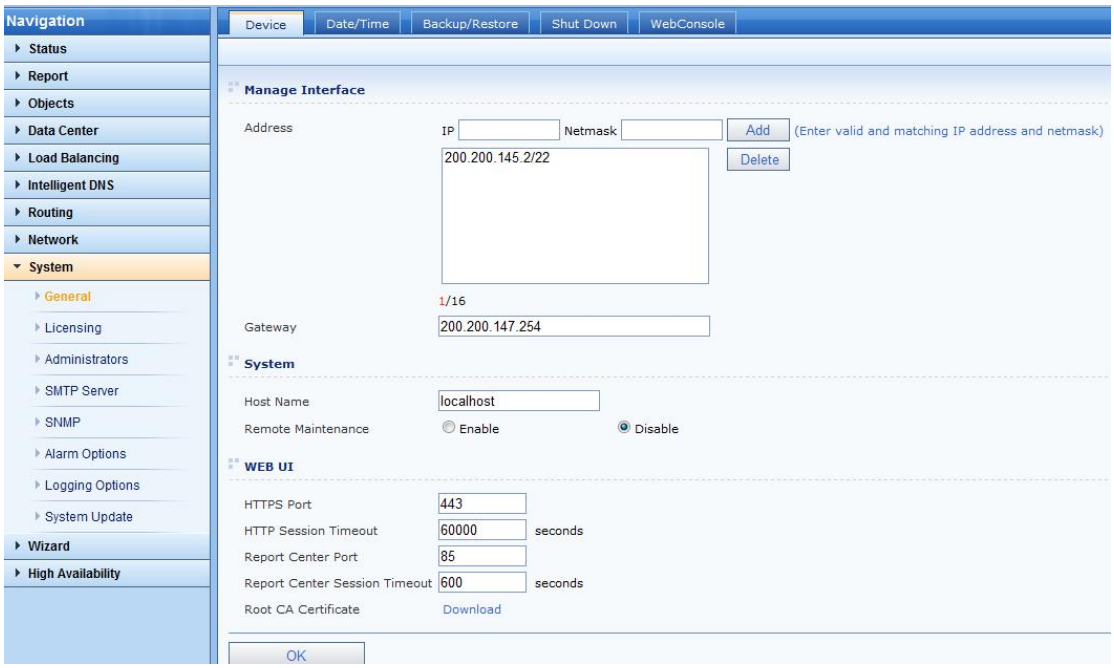
Virtual Service: Specifies a virtual service to apply the ACL rule.

Max Concurrent Connections Per IP: Specifies the max number of concurrent connections to virtual service on public IP. When the number of concurrent connections reaches the maximum, the new connection will de denied.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 11 System

It's used to configure the system of the ADC, including **General**, **Administrators**, **SMTP Server**, **SNMP**, **Alarm** and **High Availability**, as shown in the following figure:

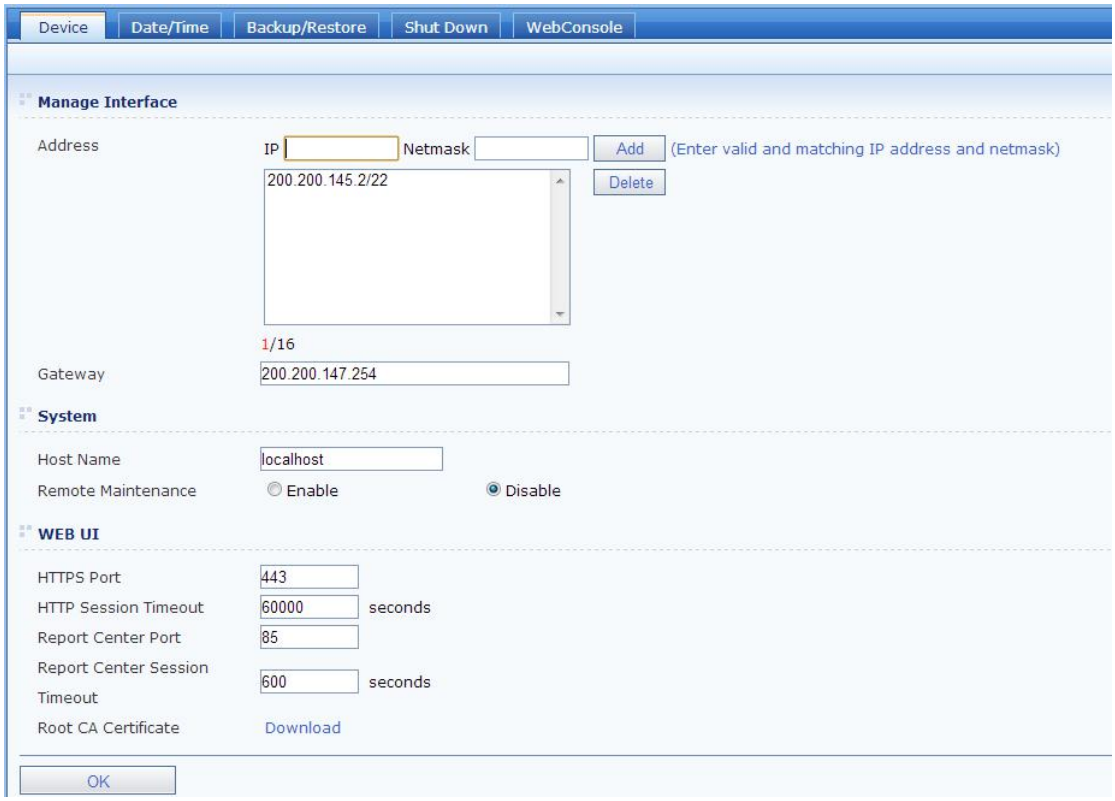


11.1 General Settings

11.1.1 Device

In **System > General > Device**, you can configure Manage interface and other information, including host name and the settings about **WEB UI**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Manage Interface: It's for setting related parameters of Manage interface.

Address: Specifies an **IP** and **Netmask**, and click **Add** to add the IP into the address list; click **Delete** to remove the selected address.

Gateway: Specifies gateway IP address of manage interface.

Host Name: Specifies a host name of the ADC. It's recommended that enter the DNS host name which has been applied for.

Remote Maintenance: Specifies whether to enable remote maintenance. If select **Enable**, administrator can access the ADC and manage it via WAN interface.

HTTPS Port: Specifies a port to log into administrator console of ADC. The default port is 443.

HTTP Session Timeout: Specifies the timeout value. After that period, the current session will be logged out.

Report Center Port: Specifies a port to connect to report server. The default port is 85.

Report Center Session Timeout: Specifies the timeout value. If user who has logged in Report Center has not any operation during that period, related session will be cleared and he/she needs to login again.

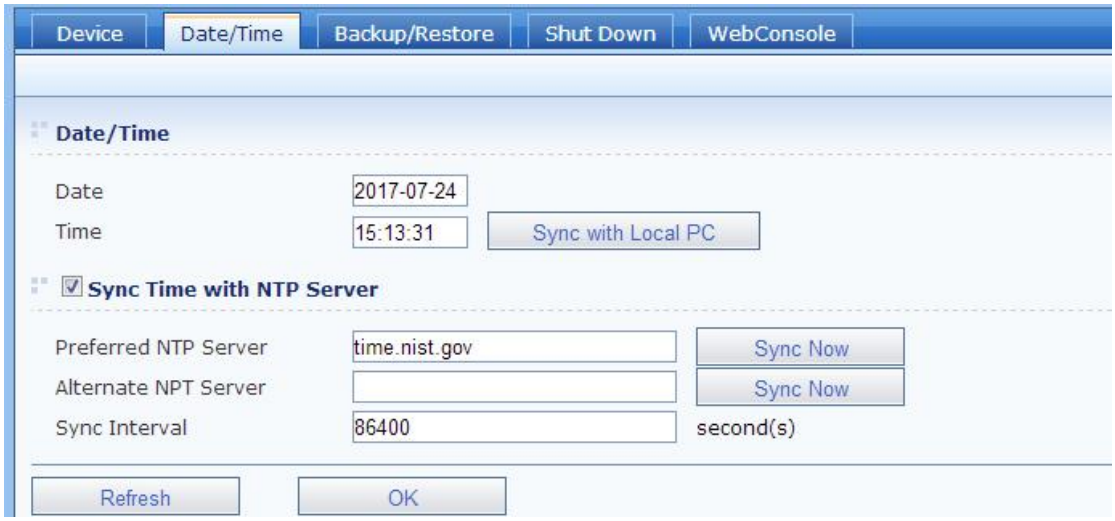
Root CA Certificate: Click **Download** to download root CA certificate and import it to browser, then no tip will pop up informing you that certificate is invalid when you log into the Web admin console of ADC.

To update the settings, click **OK**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

11.1.2 Date/Time

To set system time of the ADC, navigate to **System > General > Date/Time**, as shown in the following figure:



Refresh: It's used to refresh the time settings.

Sync with Local PC: Specifies whether to sync time with that of the local computer.

Sync Time with NTP Server: If it is selected, the system time will synchronize with NTP server automatically.

Preferred NTP Server: Specifies an NTP server.

Alternate NTP Server: Specifies a standby NTP server.

Sync Interval: Specifies the interval of synchronizing system time with NTP server. Integer can be between 1 and 604800s. Default is 86400s.

Click **Sync Now** to make the system time synchronize with NTP server instantly.

Click **Refresh** to update the settings.

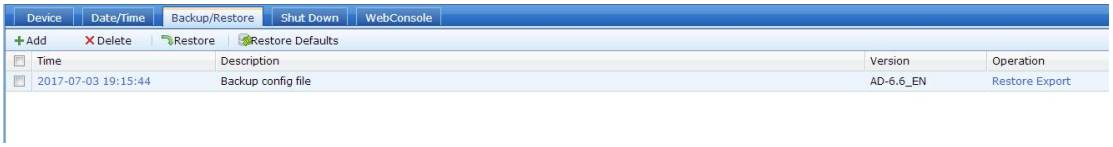


If the updated time is after original time, the data in the period between the current time and the original time will not be recorded. If the updated time is before original time, the view by minute and hour in report will show latest data, while the view by day and month in report will show the result after data overlap.

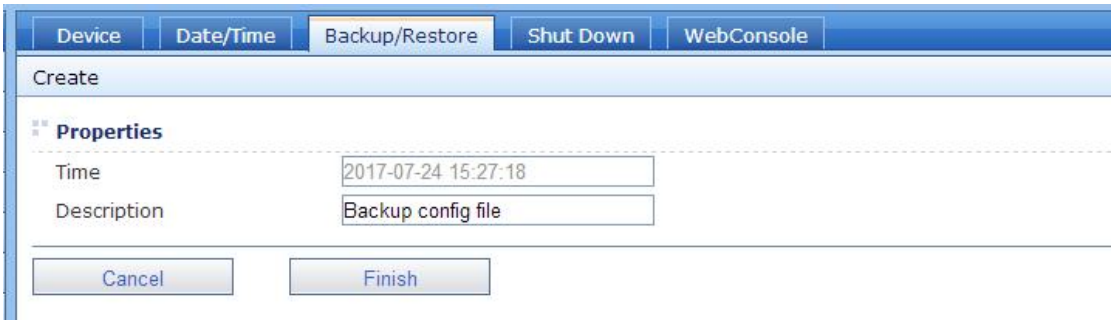
11.1.3 Backup/Restore

Go to **System > General > Backup/Restore**, you can back up and restore configuration.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

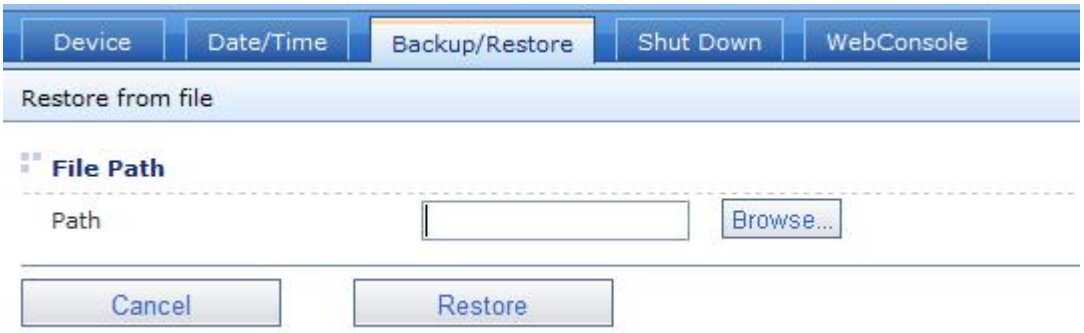


To back up the current configurations, click **Add** to configure the following contents:

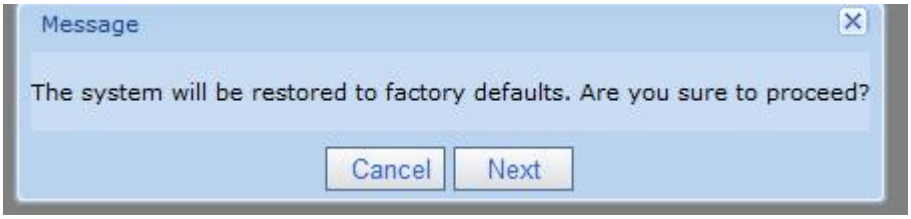


To restore the configurations of selected backup, click **Restore**.

To restore from file, click  to upload file, as shown below:



To restore to factory defaults, click  to configure the following contents:





1. Restoring configuration from backup will lead to restarting device automatically.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

2. Configurations will be automatically backed up before ADC is joined to cluster.

11.1.4 Shut Down

In **System > General > Shut Down**, you can perform the operation of restarting the ADC, as shown in the following figure:



To shut down the device, click **Shut Down**.

To restart the device, click **Restart Device**.

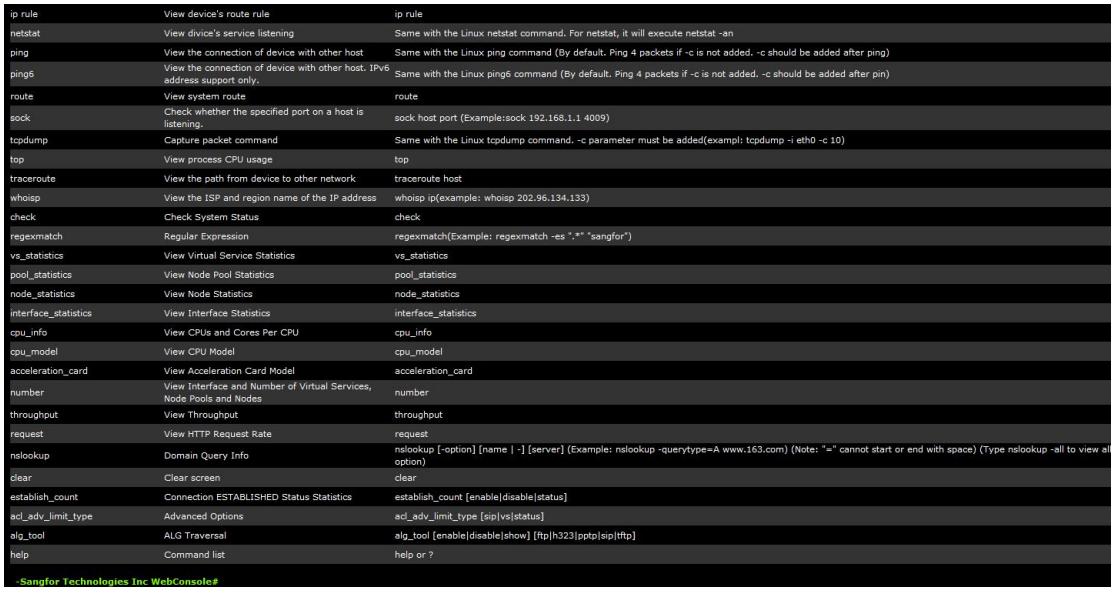
To restart all the services on the ADC, click **Restart Service** and device will not restart.

11.1.5 WebConsole

In **System > General > WebConsole**, you can view some basic information with command line on this page, as shown in the following figure:



Command Help List: Lists the commands supported by WebConsole and its usage. Enter command " help " behind " Sangfor Technologies Inc Webconsole# " on the bottom of the page, and press **Enter** key to view corresponding information about system, as shown in the following figure:



ip rule	View device's route rule	ip rule
netstat	View divice's service listening	Same with the Linux netstat command. For netstat, it will execute netstat -an
ping	View the connection of device with other host	Same with the Linux ping command (By default. Ping 4 packets if -c is not added. -c should be added after ping)
ping6	View the connection of device with other host. IPv6 address support only.	Same with the Linux ping6 command (By default. Ping 4 packets if -c is not added. -c should be added after pin)
route	View system route	route
sock	Check whether the specified port on a host is listening.	sock host port (Example:sock 192.168.1.1 4009)
tcpdump	Capture packet command	Same with the Linux tcpdump command. -c parameter must be added(exampl: tcpdump -i eth0 -c 10)
top	View process CPU usage	top
traceroute	View the path from device to other network	traceroute host
whoisp	View the ISP and region name of the IP address	whoisp ip(example: whoisp 202.96.134.133)
check	Check System Status	check
regexmatch	Regular Expression	regexmatch(Example: regexmatch -es ".*" "sangfor")
vs_statistics	View Virtual Service Statistics	vs_statistics
pool_statistics	View Node Pool Statistics	pool_statistics
node_statistics	View Node Statistics	node_statistics
interface_statistics	View Interface Statistics	interface_statistics
cpu_info	View CPUs and Cores Per CPU	cpu_info
cpu_model	View CPU Model	cpu_model
acceleration_card	View Acceleration Card Model	acceleration_card
number	View Interface and Number of Virtual Services, Node Pools and Nodes	number
throughput	View Throughput	throughput
request	View HTTP Request Rate	request
nslookup	Domain Query Info	nslookup [-option] [name | -] [server] (Example: nslookup -querytype=A www.163.com) (Note: "=" cannot start or end with space) (Type nslookup -all to view all option)
clear	Clear screen	clear
establish_count	Connection ESTABLISHED Status Statistics	establish_count [enable|disable|status]
acl_adv_limit_type	Advanced Options	acl_adv_limit_type [sip|vs|status]
alg_tool	ALG Traversal	alg_tool [enable|disable|show] [ftp|h323|pptp|sip|tftp]
help	Command list	help or ?

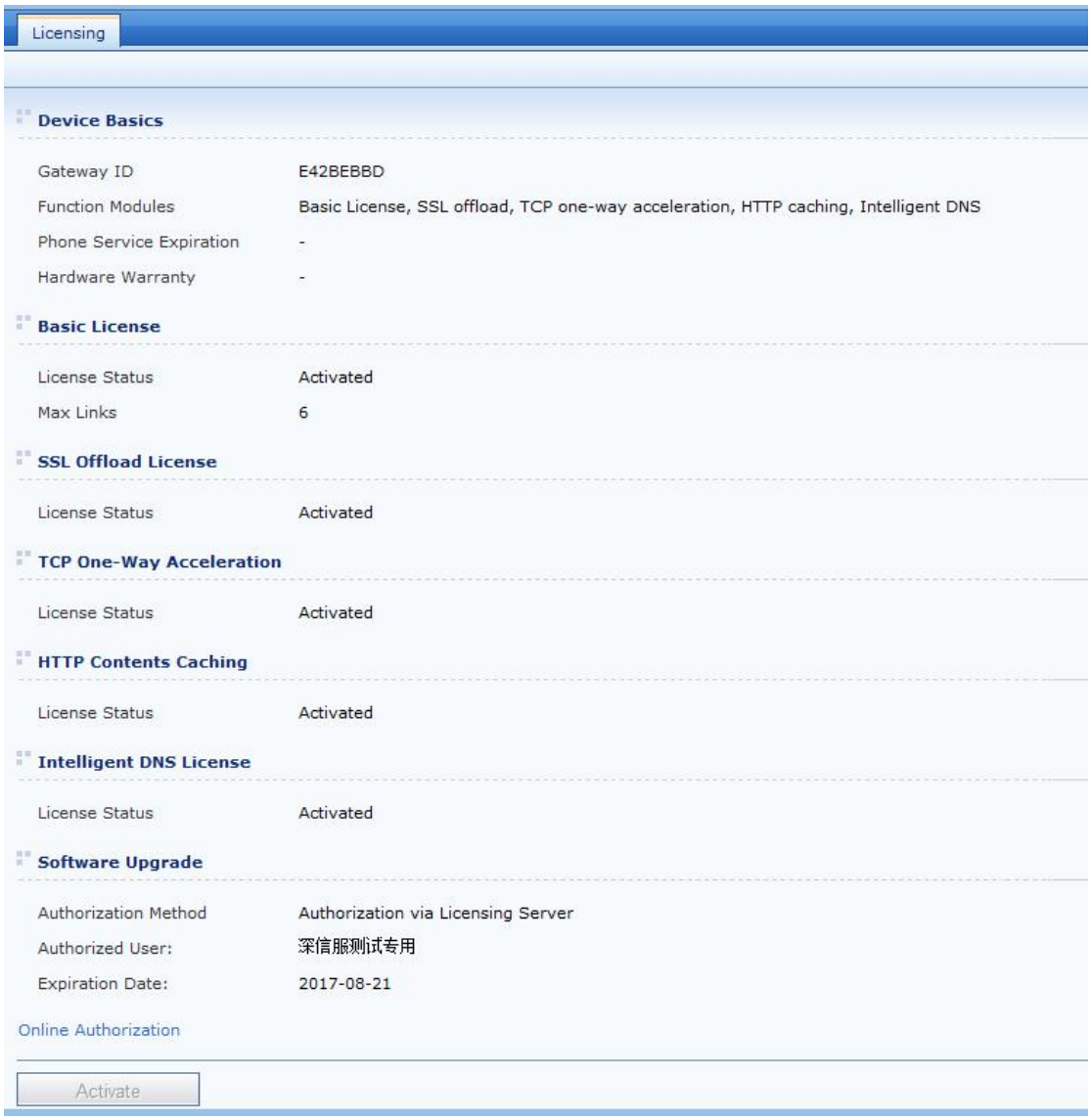
-Sangfor Technologies Inc WebConsole#

11.2 Licensing

Licensing includes **Device Basics, Basic License**, **SSL Offload License**, **TCP One-Way Acceleration**, **HTTP Contents Caching**, **Intelligent DNS License**, **App Analytics, Security Analytics** and **Software Upgrade**. **Device Basics** shows **Gateway ID, Function Modules**, **Phone Service Expiration** and **Hardware Warranty.**

Navigate to **System > Licensing**, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Device basics: Specifies **Gateway ID, Function Modules**, **Phone Service Expiration** and **Hardware Warranty**.

Basic License: The basic license should be activated, otherwise, other main features such as load balancing and link Load cannot be used.

License Status: Specifies the status of the license. When the license has not been configured or is invalid, the device will be in inactivated status.

Max Links: Specifies the max number of WAN links supported by the ADC.

SSL Offload License: SSL offload license should be activated, or else virtual service related to SSL cannot be configured.

TCP One-way Acceleration: TCP one-way acceleration license should be activated, or else this feature is not available.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

HTTP Contents Caching: HTTP contents caching license should be activated, or else HTTP caching and HTTP compression of the acceleration policy is not available.

Intelligent DNS License: Intelligent DNS license should be activated, or else global functions such as configuration backup and restoration, etc., wil not be available.

App Analytics: App analytics license should be activated, or else performance and resource usage analysis on WebLogic, Oracle, SQL Server databases will not be available.

Security Analytics: Security analytics license should be activated, or else realtime vulnerability analysis will not be available.

Software Upgrade: Software upgrade license is valid within a period of time.

Multi-Tenant License: Multi-tenant license should be activated, or else virtual ADC cannot be created or started. The number of virtual ADCs that can be created is restricted by the license.

11.3 Administrators

11.3.1 Administrators

Navigate to **System > Administrators**, you can view the already-configured administrators and their roles, and manage them via the console.

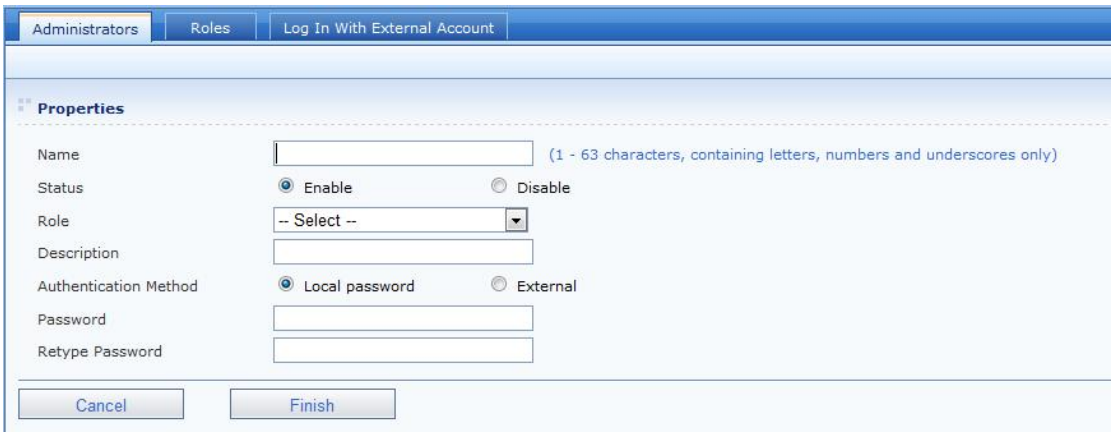


To enable the selected administrator, click **Enable**; or click **Disable** to disable the selected administrator.

To remove the selected administrator, click **Delete**. Please note that the administrator whose username is 'admin ' cannot be deleted.

You can change settings about administrator by clicking on **Username** of the administrator.

To create an administrator, click **Add** and configure the following contents:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Name: Give it a name.

Status: Specifies whether the administrator is **Enabled** or **Disabled**.

Role: Specifies a role for the administrator.

Description: Enter a brief description for the administrator.

Authentication Method: Options are **Local password** and **External**.

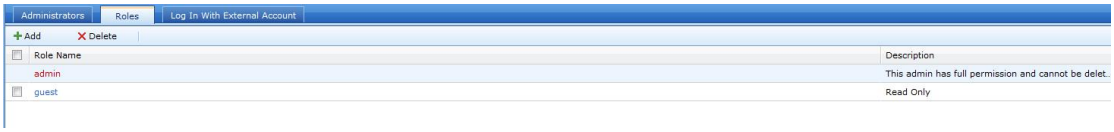
Password: Specifies a login password for the administrator.

Retype Password: Enter a password which must be the same as that entered in **Password** filed.

To save the settings, click **OK**; to give up the settings, click **Cancel**.

11.3.2 Roles

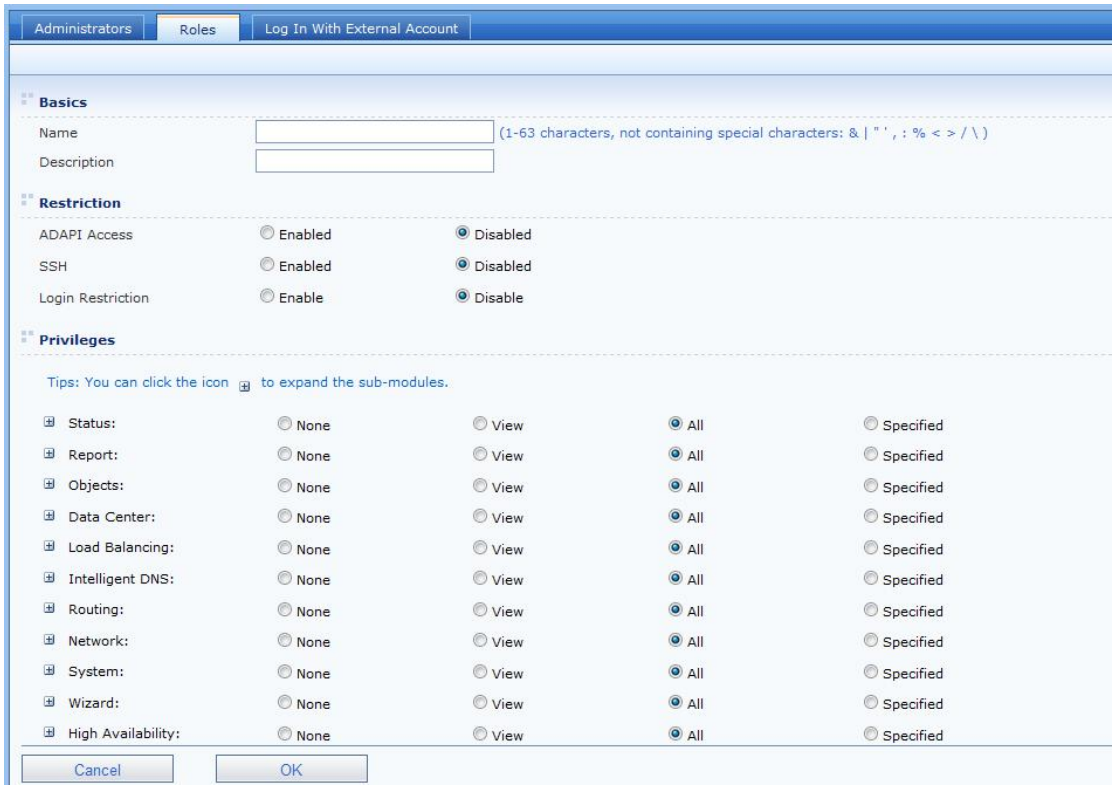
In **System > Administrators > Roles**, you can view the role of already-configured administrator.



To remove the selected administrator, click **Delete**. Please note that the role whose role name is " admin " cannot be deleted. The administrator has all privilege and its default password is " admin ".

Before creating a administrator, you need to make sure the role of the administrator. on **Roles** configuration page, you can configure different control privilege and others. To create a role, click **Add** and configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Name: Give it a distinguishable name.

Description: Enter some brief description to the role.

SSH: Select **Enabled** to allow the user associated with the roles to have access to back end command lines. Command lines function to import or export all the configurations of SSL, virtual service, network, routing, system, etc.

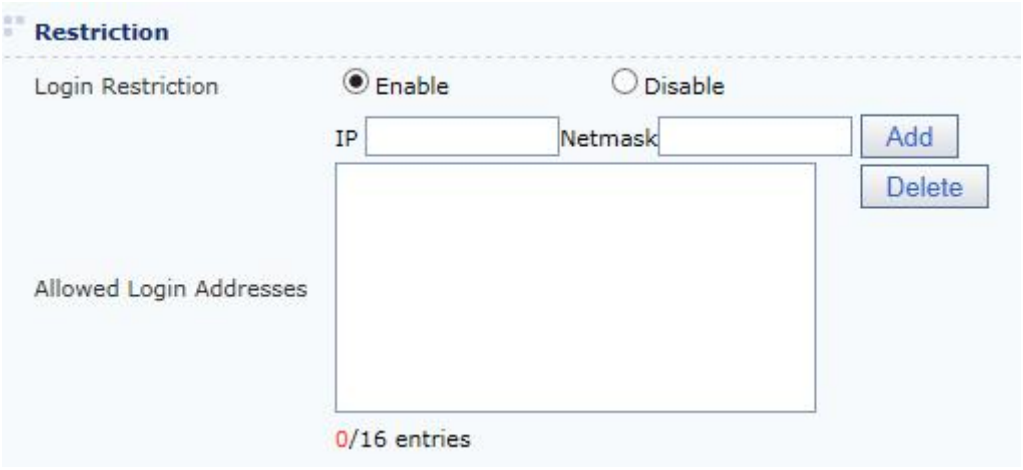
Scenario: A great many ADC devices have similar configurations and can be configured at the same time. Take rewriting HTTP header for example. You can configure it only on one device through WebUI, export configurations via SSH, and then execute the commands via SSH on other devices.

Export virtual service configuration commands, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

```
[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}
```

Login Restriction: Specifies whether to allow the IP address of the administrator to login with this role. Select **Enable** to configure the expanded fields:



Allowed Login Addresses: Enter an IP address and netmask, and click **Add** to add it to Allowed Login Address list.

Privileges: Specifies the privileges of roles based on modules, including **Status**, **Report**, **Objects**, **Load Balancing**, **Intelligent DNS**, **Routing** and **Network**, **System** and **Wizard**.

The available privileges are as follows:

- **None**: Indicates there is no privilege to view each module, nor to edit it.
- **View**: Indicates there is the privilege to view module, but cannot edit it.
- **All**: Indicates there is the privilege to view and edit each module.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

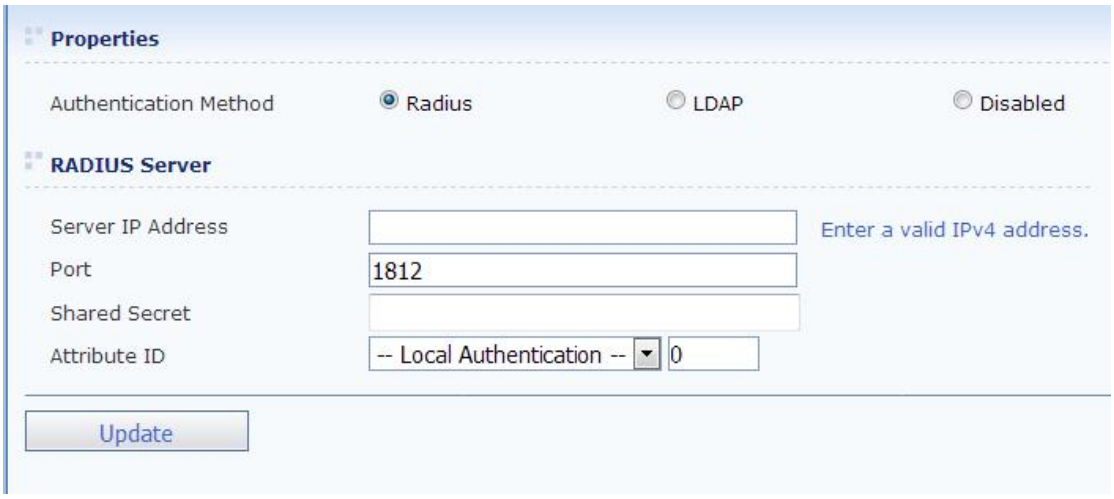
- **Specified**: Specifies the privilege of viewing or editing each module.

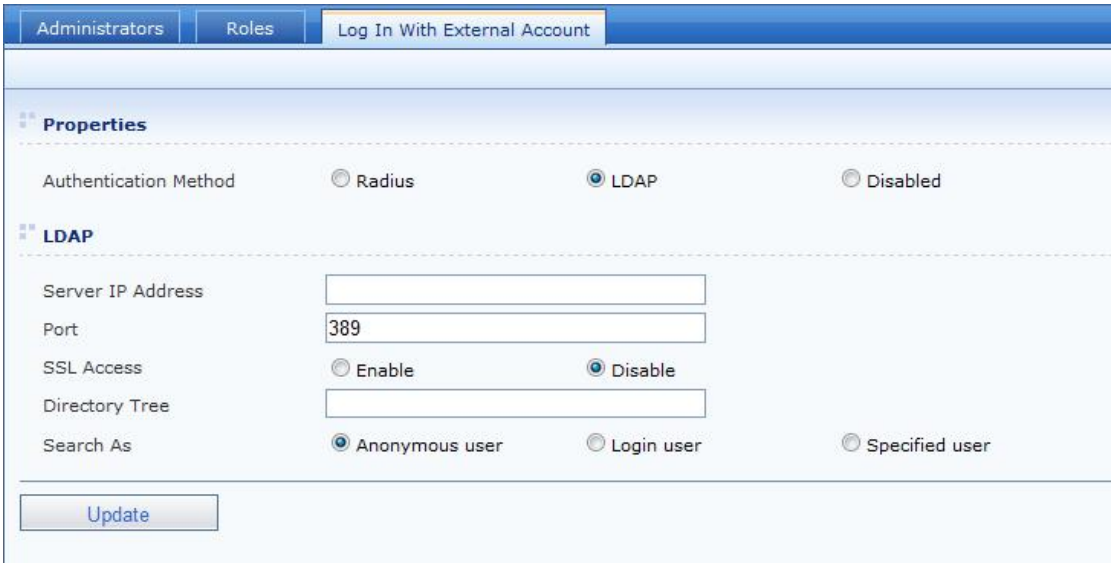
To save the settings, click **OK**; to give up the settings, click **Cancel**.

Note: If the device has been upgraded and you want to grant command line permission to previous users, you have to change the password of previous users.

11.3.3 Log In With External Account

Log In With External Account is used to configure external authentication. Options are **Radius**, LDAP and **Disabled**.





Authentication Method: Specifies the type of external authentication server. Default option is **Disabled**.

Server IP Address: Specifies server IP address.

Port: Specifies the server port.

Shared Secret: Specifies shared secret of communication between server and client when authentication method is **Radius**.

Attribute ID: Obtain role name of login account via specified attribute(STRING type) carried by Radius response when authentication method is **Radius**. Local Authentication is required to create user(External Authentication) and associate with certain roles.

SSL Access: Specifies whether to enable or disable SSL Access. Default option is **Disabled**.

Directory Tree: Specifies AD domain server file location in authentication database.

Search As: Specifies the way of initiating the first request to server, . Dfault option is **Anonymous user**.

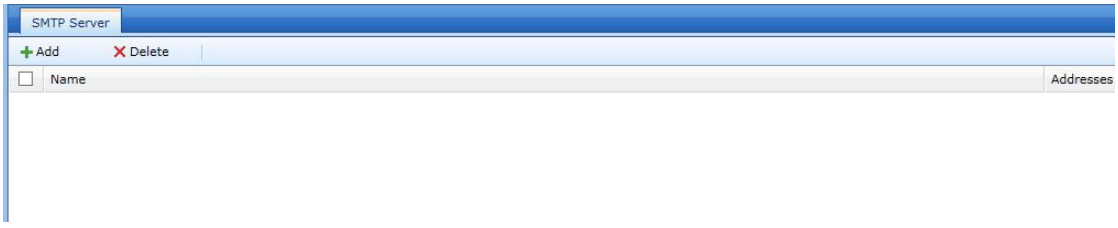
Username Extension: This field should be configured this when searching as an login user. For example, if you input ${user}@sangfor. com, username upon login will be changed to ${user}.

DN: Specifies a specific username, with which, user information on LDAP can be accessed. Make sure that the user has relevant permissions, for example, you may input admin account of LDAP. Remember to input complete user name. But MS Active Directory is an exeption, you can input user name in the form of user@domain.

Password: Specifies the password of the user.

11.4 SMTP Server

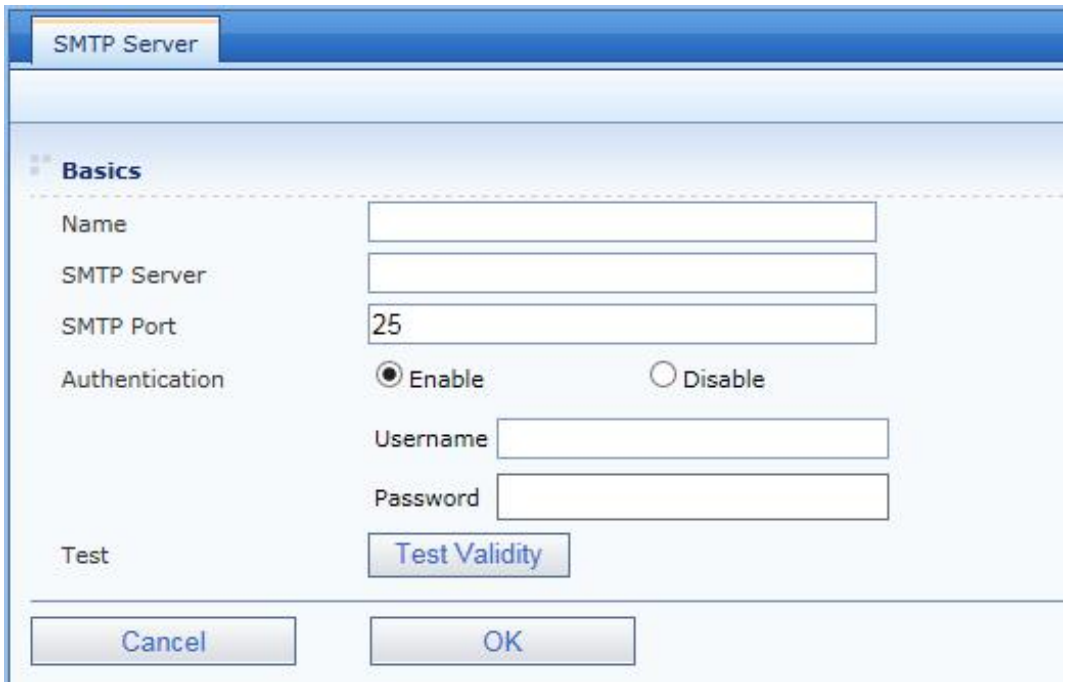
Navigate to **System > SMTP Server**, you can configure SMTP server. It's mainly used in **Email Alarm** and **Subscription**.



To remove the selected SMTP server, click **Delete**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

To create a SMTP server, click **Add** and configure the following contents:



Name: Give it a distinguishable name.

SMTP Server: Enter an address of SMTP server. It can be an IP address or domain name.

SMTP Port: Specifies a port for SMTP. The default port is 25.

Authentication: If SMTP server needs to authenticate username and password, you should select **Enable** and enter username and password then.

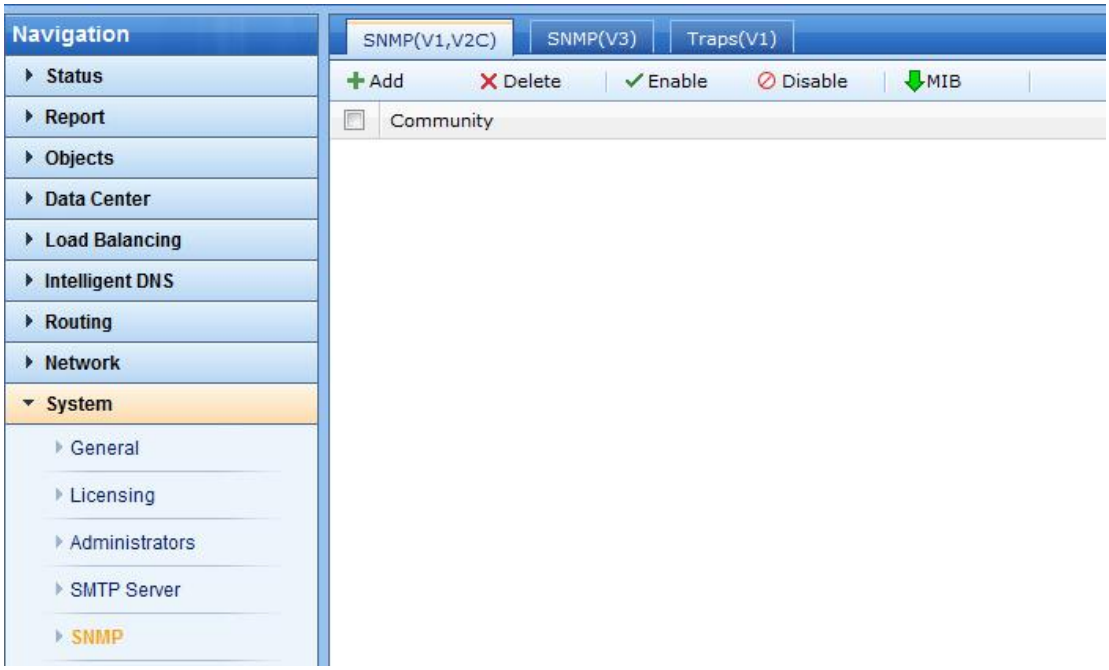
Test: It's used to test the validity of the newly- configured SMTP server. The accuracy of the test will be higher under well network condition. To begin the test, click **Test Validity**.

To save the settings for SMTP server, click **OK**; or click **Cancel** to give up the changes.

11.5 SNMP

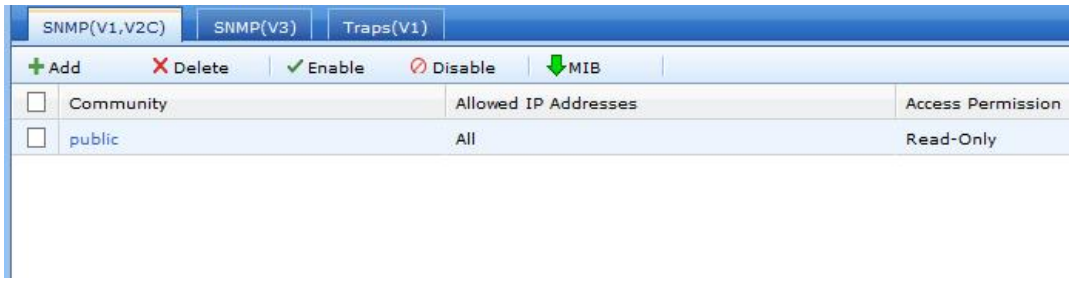
Navigate to **System > SNMP**, you can configure SNMP. It's mainly used for network management device to obtain some status information about the ADC with SNMP, such as CPU usage, memory and interface status.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



11.5.1 SNMP (V1, V2C)

In **System > SNMP > SNMP (V1, V2C)**, you can configure SNMP version 1(SNMPv1) and SNMP version 2 (SNMPv2) to get the parameters of the ADC, as shown in the following figure:



To remove the selected item, click **Delete**.

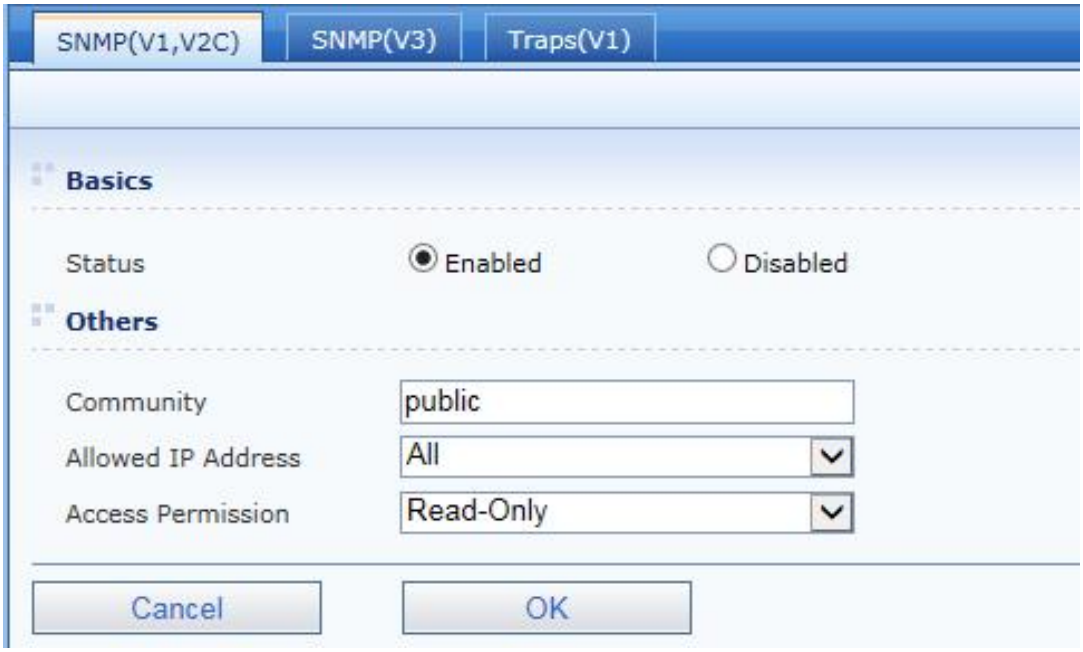
To enable the selected item, click **Enable**.

To disable the selected item, click **Disable**.

To download a MIB file, click **MIB** and save it on local computer.

To create a SNMP (V1, V2C), click **Add** and configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Community: Specifies a private key which should be same as that of peer device.

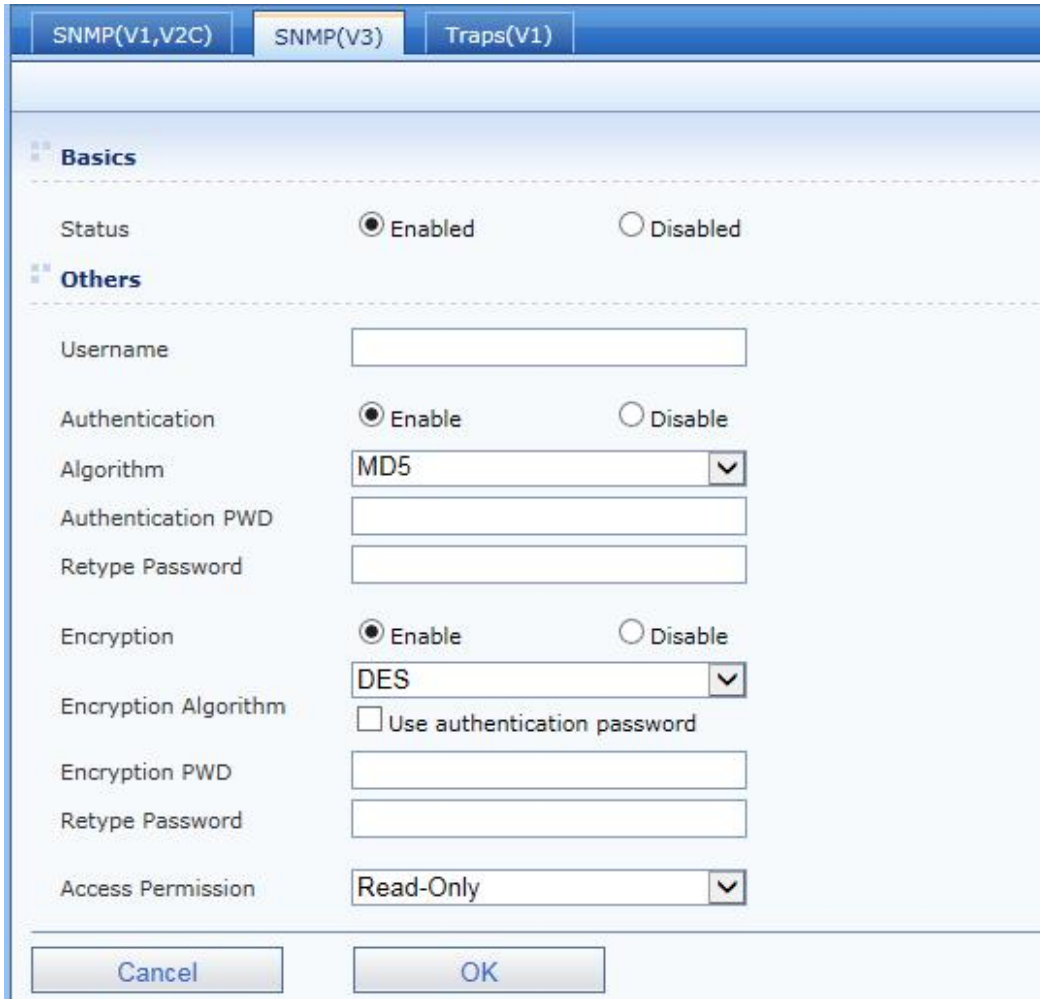
Allowed IP Address: Specifies the IP address allowed to get information about the ADC with SNMP. Options are **All**, **Single IP** and **Subnet**.

Access Permission: Specifies the permission of peer device to access the ADC with SNMP. Options are **Read-Only** and **Read/Write**.

11.5.2 SNMP (V3)

In **System > SNMP > SNMP (V3)**, you can configure SNMP version 3(SNMP V3) to get the parameters of the ADC for network management devices. To create a SNMP(V3), click **Add** and configure the following contents:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Username: Specifies a name for the ADC.

Authentication: Select **Enable** to enable authentication mechanism of SNMP (V3).

Algorithm: Specifies authentication algorithm and password same as those configured on peer device.

Encryption: Select **Enable** to enable encryption mechanism of SNMP (V3).

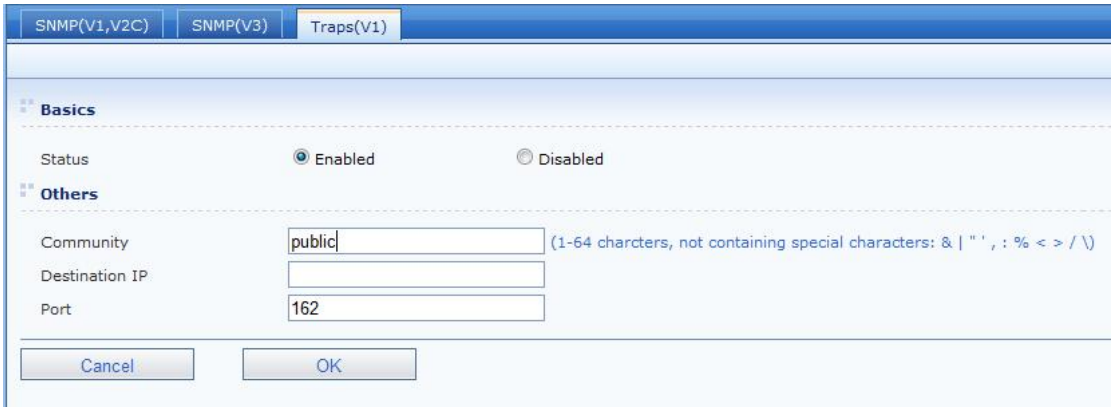
Encryption Algorithm: Specifies encryption algorithm and encryption password same as those configured on peer device.

Access Permission: Specifies the permission of peer device to access the ADC with SNMP. Options are **Read-Only** and **Read/Write**.

11.5.3 Traps(V1)

In **System > SNMP > Traps(V1)**, you can configure the ADC to send its status information to one IP address proactively. Click **Add** to enter the following page:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Community: Specifies a private key same as that set on peer device.

Destination IP: Specifies an IP address which the ADC will send its status information to.

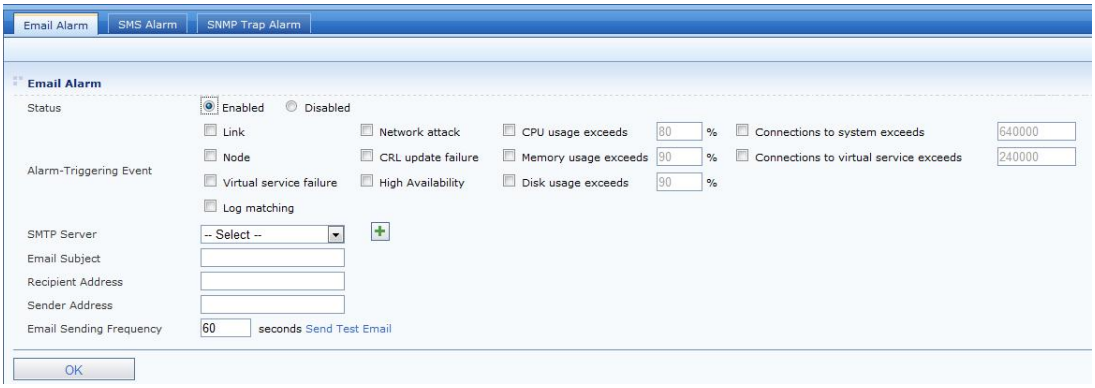
Port: Specifies a listening port of peer device.

11.6 Alarm Options

Navigate to **System > Alarm**, you can configure the ADC to send alarm via Email, SMS or SNMP Trap.

11.6.1 Email Alarm

In **System > Alarm Options > Email Alarm**, you can configure the ADC to send alarm email automatically, as shown in the following figure:



To enable **Email Alarm**, select **Enabled**, and the ADC will send alarm email automatically.

To disable **Email Alarm**, select **Disabled**.

Alarm-Triggering Event: Specifies an event. When it happens, alarm email will be triggered to send. The events include the following:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

- **Link:** When any link status changes, alarm will be triggered.
- **Node:** When any node status changes, alarm will be triggered.
- **Virtual service failure:** When all the links or nodes status change, alarm will be triggered.
- **Network attack:** When there is illegal HTTP request or flooding attack which cannot be identified, alarm will be triggered.
- **CRL update failure**: When failure occurred during updating CRL, alarm will be triggered.
- **High Availability:** When active-standby mode or cluster is enabled, alarm will be triggered when switching modes.
- **CPU usage exceeds**: When the CPU usage exceeds the threshold, alarm will be triggered.
- **Memory usage exceeds**: When the memory usage exceeds the threshold, alarm will be triggered.
- **Disk usage exceeds**: When the disk usage exceeds the threshold, alarm will be triggered.
- **Connections to system exceeds**: When the connections exceeds the threshold, alarm will be triggered.
- **Connections to virtual service exceeds:** When the virtual service connections exceed the threshold, alarm will be triggered.
- Log matching: When logs in ADC match the specified logs, alarm will be triggered.

SMTP Server: Specifies a SMTP server to send alarm email. For how to configure SMTP server, please see Chapter 10, **Configuring SMTP Server** or click "+**"** button to redirect to SMTP Server configuration page.

Email Subject: Specifies an email subject.

Recipient Address: Specifies a mailbox to receive alarm emails.

Sender Address: Specifies a mailbox to send alarm emails. The mailbox is usually the one corresponding to the selected SMTP server.

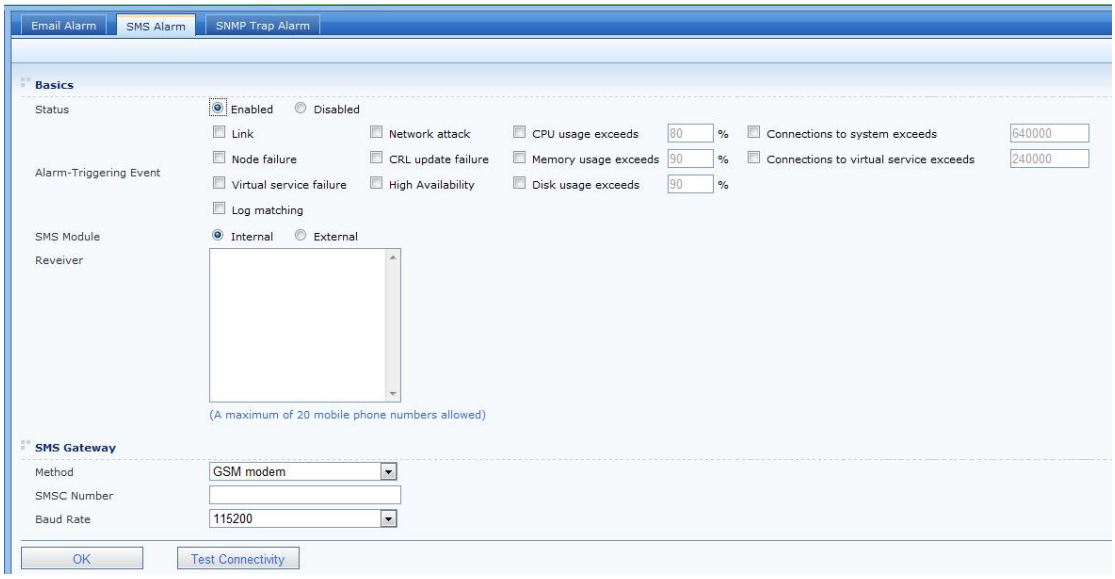
Email Sending Frequence: Specifies how often alarm email is sent, in seconds.

To update the settings, click **OK**.

11.6.2 SMS Alarm

In **System > Alarm Options > SMS Alarm**, you can configure the ADC to send message to mobile phone automatically, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To enable **SMS Alarm**, click **Enabled**, so that the ADC can send messages to mobile phones automatically.

To disable **SMS Alarm**, click **Disabled**, so that the ADC cannot send messages to mobile phones automatically.

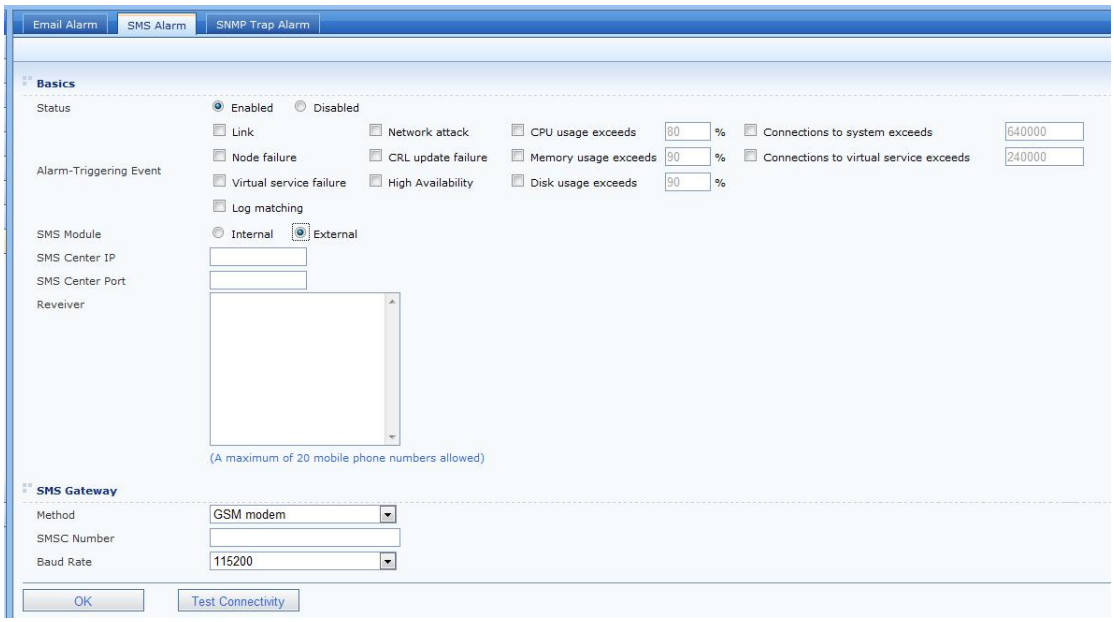
Alarm-Triggering Event: Specifies an event. When it happens, the corresponding alarm SMS will be sent. The events include the following:

- **Link :** When the link status changes, alarm will be triggered.
- **Node failure:** When the node status changes, alarm will be triggered.
- **Virtual Service failure:** When all the links or nodes status change, alarm will be triggered.
- **Log matching**: When logs in ADC match the specified logs, alarm will be triggered.
- **Network attack:** When there is illegal HTTP request or flooding attack which cannot be identified, alarm will be triggered.
- **CRL update failure**: When failure occurred during updating CRL, alarm will be triggered.
- **High Availability**: When active-standby mode or cluster is enabled, alarm will be triggered when switching modes.
- **CPU usage exceeds**: When the CPU usage exceeds the threshold, alarm will be triggered.
- **Memory usage exceeds**: When the memory usage exceeds the threshold, alarm will be triggered.
- **Disk usage exceeds**:When the disk usage exceeds the threshold, alarm will be triggered.
- **Connections to system exceeds**: When the connections to system exceeds the threshold, alarm will be triggered.
- **Connections to virtual service exceeds:** When the connections to virtual service exceeds the threshold, alarm will be triggered.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

SMS Module: Specifies a SMS module to send SMS. If select **Internal**, SMS modem must be connected to the ADC. If select **External**, the ADC must be connected to SMS gateway.

For **External**, you need to specify an IP address and port for SMS center, as shown below:



Receiver: Specifies mobile phone numbers to receive alarm message.

Method: Specifies a method of sending SMS message. The options are **GSM Modem**, **China mobile V2**, **China mobile V3** and **China Unicom**.

For **GSM modem** method, you also need to specify SMSC number and baud rate; for other methods, such as **China Mobile V2**, **China Mobile V3** or **China Unicom**, you need to configure the following fields:



SMS Gateway IP: Specifies an IP address of SMS gateway.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

SMS Gateway Port: Specifies a port of SMS gateway.

Corporate Code: Enter corresponding code as the SMS provider provides.

Service Code: Enter related code as the SMS provider provides.

SP Number: Enter related SP number as the SMS provider provides.

Gateway Number: Enter corresponding gateway number as the SMS provider provides.

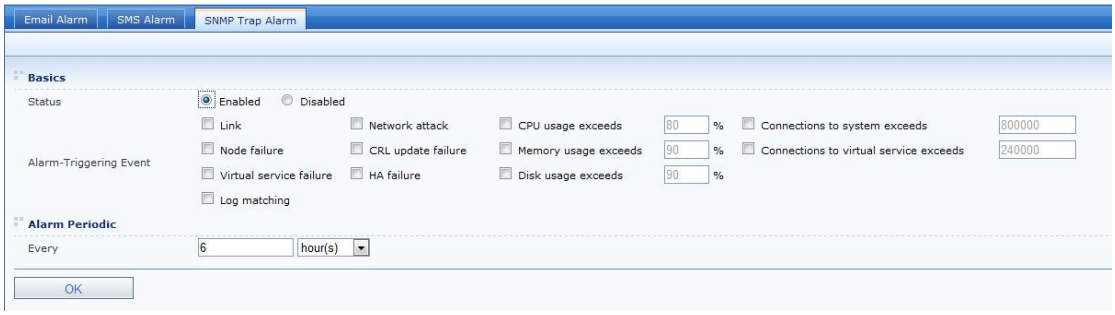
Login Account: Enter a login account as the SMS provider provides. For **China Mobile** method, the login account is its corporate code.

Password: Enter corresponding password as the SMS provider provides.

Retype Password: Enter the same password you entered in **Password** field.

11.6.3 SNMP Trap Alarm

In **System > Alarm > SNMP Trap Alarm**, you can configure the ADC to send alarm log via SNMP Trap, as shown in the following figure:



Select **Enabled** to enable **SNMP Trap Alarm**, so that the ADC can send alarm messages to mobile phone through SNMP Trap.

Select **Disabled** to disable **SNMP Trap Alarm**, so that the ADC cannot send alarm messages to mobile phones through SNMP Trap.

Alarm-Triggering Event: Specifies an event when it happens, the corresponding alarm SMS will be sent. The events include the following:

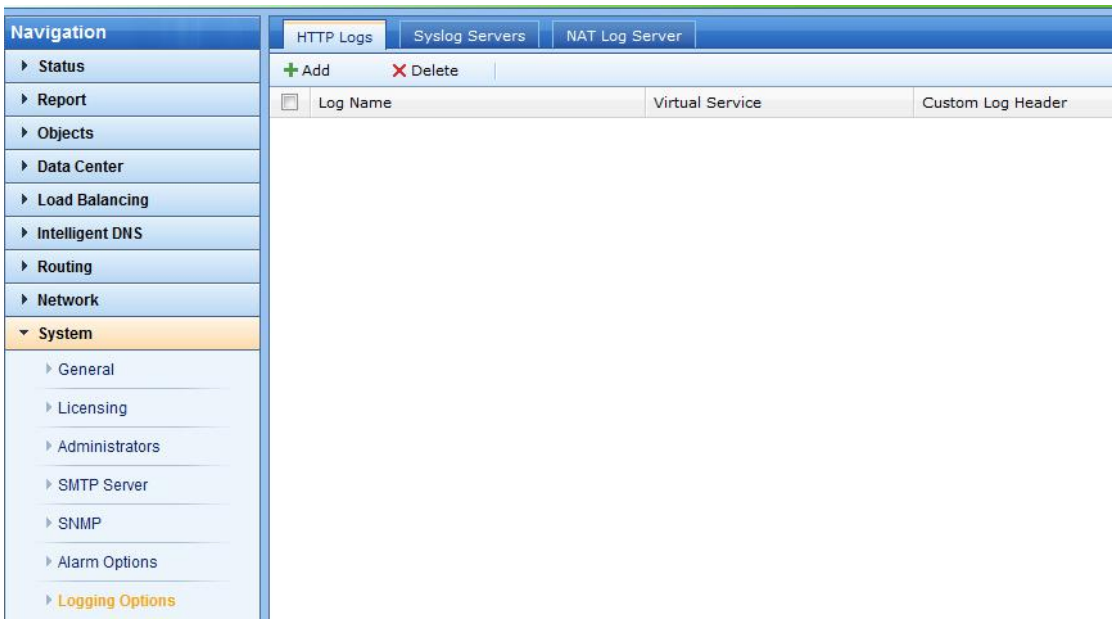
- **Link :** When any link status changes, alarm will be triggered.
- **Node failure:** When any node status changes, alarm will be triggered.
- **Virtual Service Breakdown:** When the all the links or nodes status change, alarm will be triggered.
- **Log matching**: When logs in ADC match the specified logs, alarm will be triggered.
- **Network attack:** When there is illegal HTTP request or flooding attack which cannot be identified, alarm will be triggered.
- **CRL update failure**: When failure occurred when updating CRL, alarm will be triggered.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

- **High Availability:** When active-standby mode or cluster is enabled, alarm will be triggered when switching modes.
- **CPU usage exceeds**: When the CPU usage exceeds the threshold, alarm will be triggered.
- **Memory usage exceeds**: When the memory usage exceeds the threshold, alarm will be triggered.
- **Disk usage exceeds**:When the disk usage exceeds the threshold, alarm will be triggered.
- **Connections to system exceeds**: When the connections to system exceeds the threshold, alarm will be triggered.
- **Connections to virtual service exceeds:** When the connections to virtual service exceeds the threshold, alarm will be triggered.

11.7 Logging Options

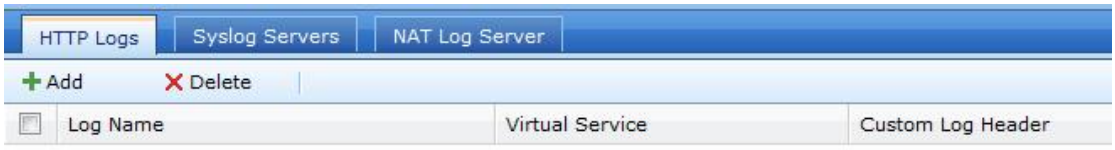
Navigate to **System** > **Logging Options**, it includes **HTTP Logs, Syslog Servers** and **NAT Log Server**, as shown in the following figure:



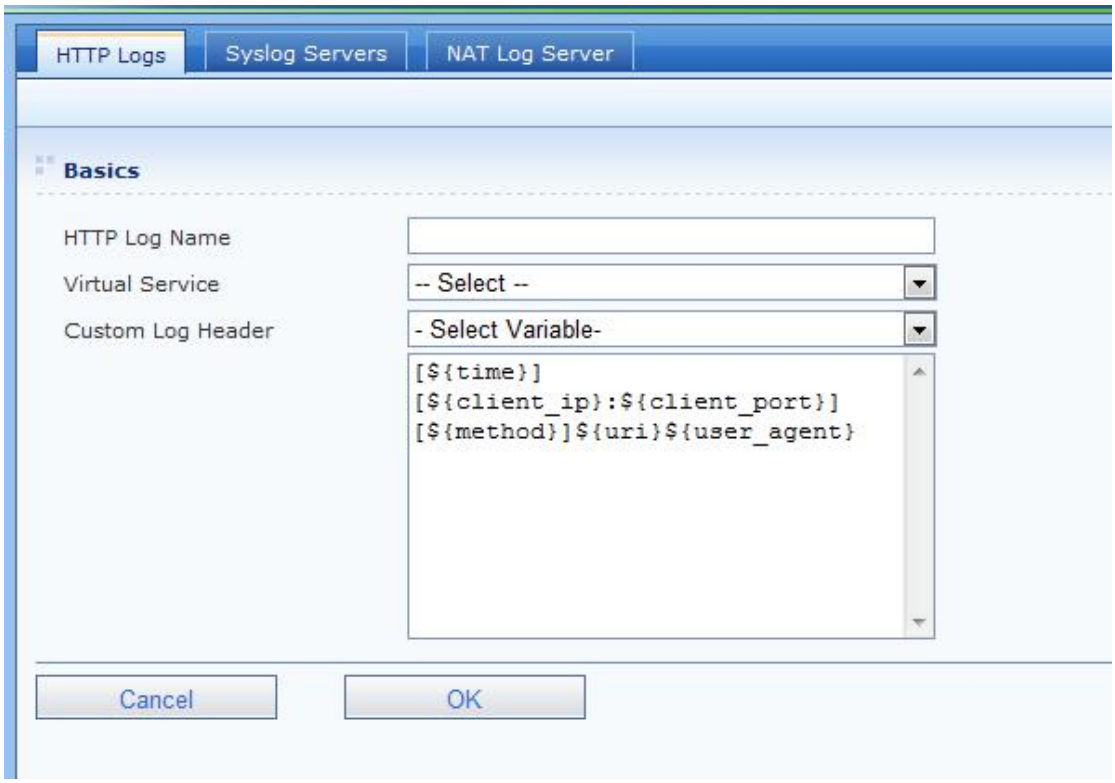
11.7.1 HTTP Logs

Navigate to **System** > **Logging Options > HTTP Logs**, you can configure log variables of virtual service and send through Syslog servers, as shown in the below figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To add an HTTP log, click **Add**, as shown in the below figure:

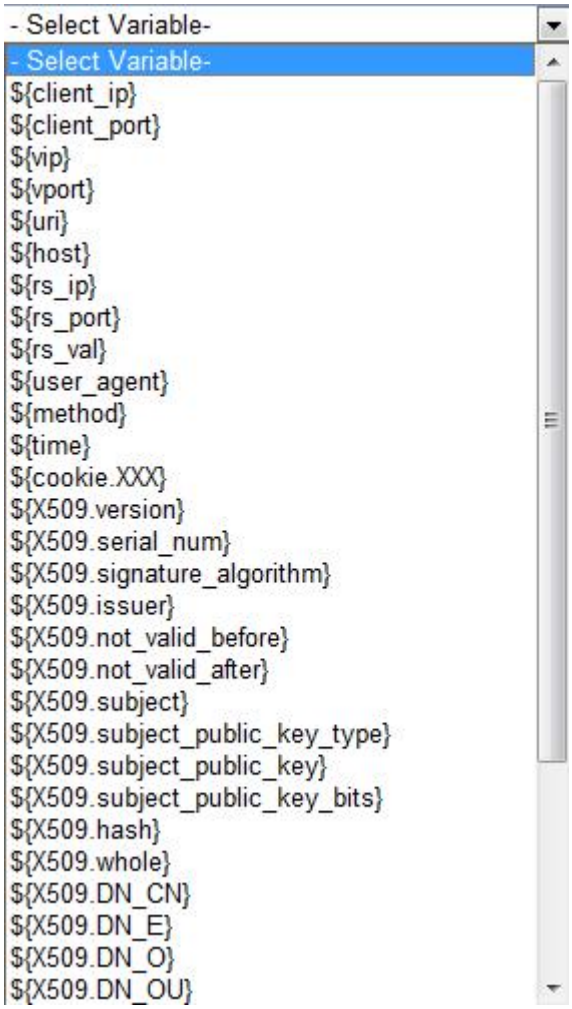


HTTP Log Name: Specifies the name of HTTP logs.

Virtual Service: Options can be HTTP and HTTPS, and a virtual service can only be added once.

Custom Log Header: To select variable of logs, click the drop-down box. Options are shown as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



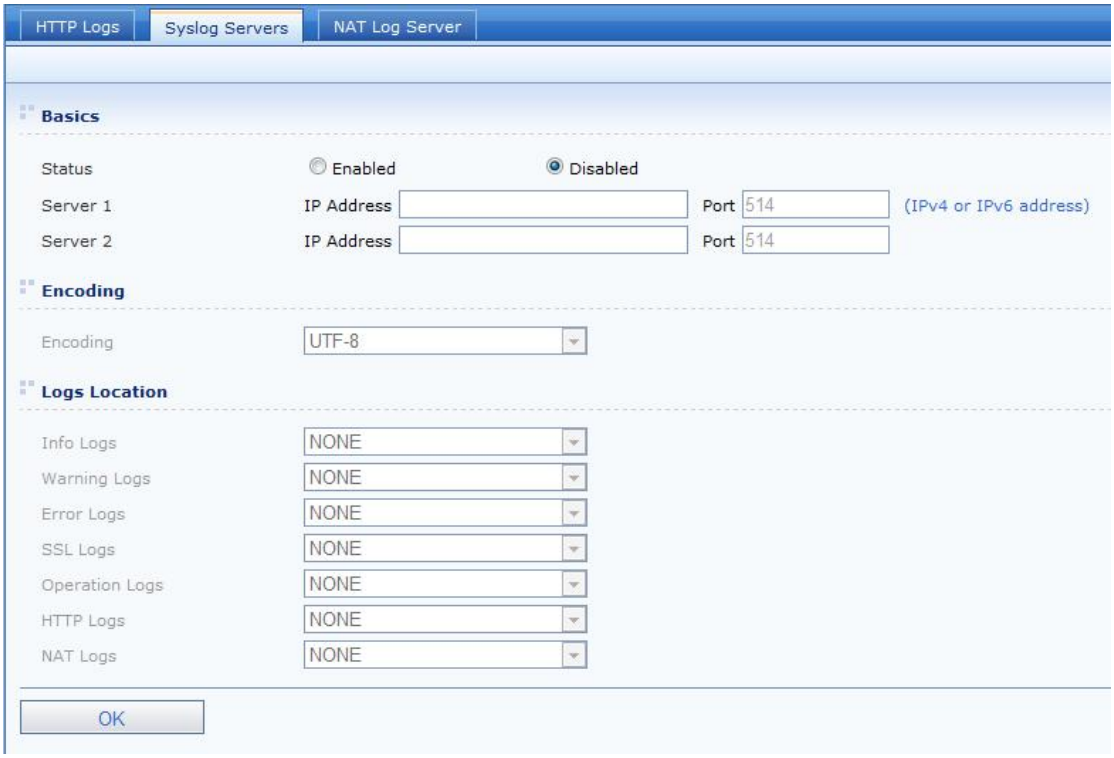
Descriptions of the variables:

Customized variable	**Description**	**Customized variable**	**Description**
${client_ip}	Client IP	${ rs_ip }	Server IP
${ client_port }	Client port	${ rs_port }	Server Port
${ vip }	Virtual service IP	${ user_agent }	Browser Version
${ vport }	Virtual service port	${ method }	Request Method
${ uri }	Request URL	${ time }	Request Time
${ host }	Request host		

11.7.2 Syslog Servers

Navigate to **System** > **Logging Options > Syslog Servers**, you can configure to send logs on ADC to specific Syslog server. Two syslog servers sending logs at the same time is supported, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Status: Specifies whether to enable or disable sending logs to Syslog server.

IP Address: Specifies IP address of Syslog server.

Port: Specifies port of Syslog server.

Encoding: Specifies encoding of logs, options are **UTF-8, GBK, GB2312.** Select as per your need.

Logs Location: It contains I**nfo Logs, Warning Logs, Error Logs, SSL Logs, Operation Logs, HTTP Logs** and **NAT Logs.** Logs are classified into different categories and are sent to Syslog server. Options are from **LOCA0** to **LOAC7**, **NONE** indicates not sending logs to Syslog server.

11.7.3 NAT Log Server

Navigate to **System** > **Logging Options** > **NAT Log Server,** you can configure to send logs to NAT server, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Status: Specifies whether to enable or disable sending logs to NAT server.

IP Address: Specifies IP address of NAT server.

FTP Port: Specifies FTP port of NAT server.

Username: Specifies username of NAT server.

Password: Specifies password of NAT server.

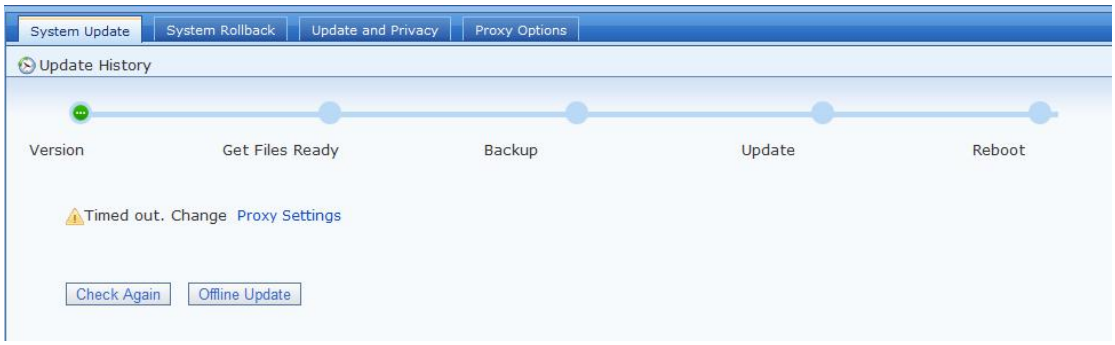
Path: Specifies path of NAT server.

11.8 System Update

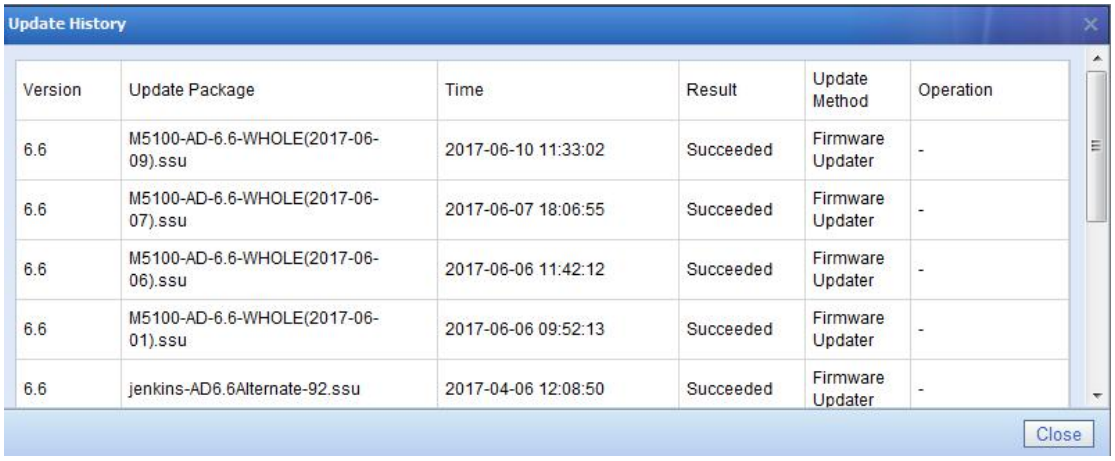
11.8.1 System Update

Navigate to **System** > **System Update > System Update** to update ADC, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



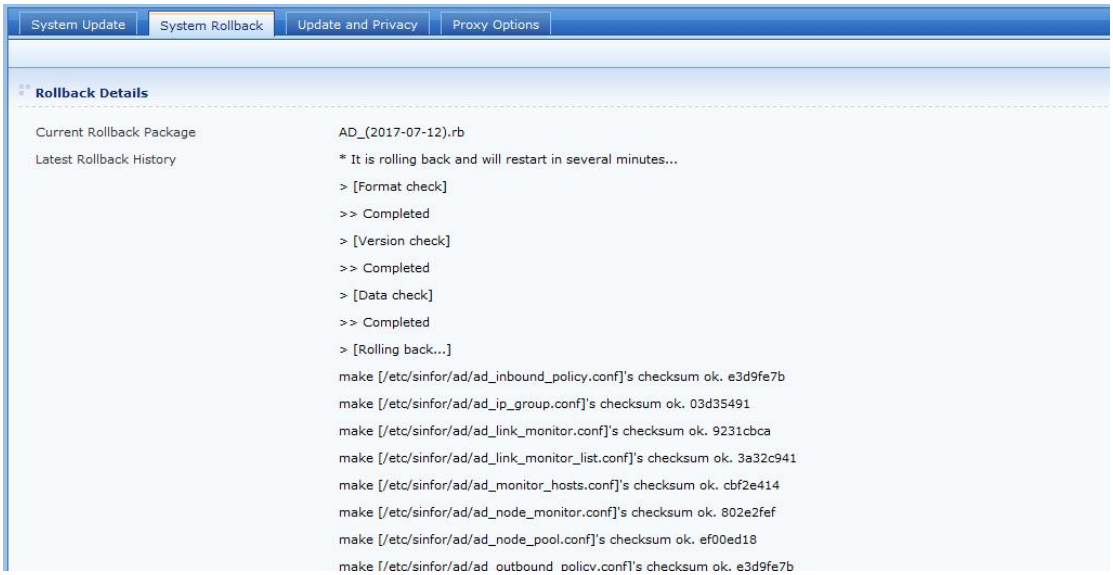
To check update history, click **Update History**.



11.8.2 System Rollback

Navigate to **System > System Update > System Rollback** to rollback update package to downgrade, as shown in the following figure:

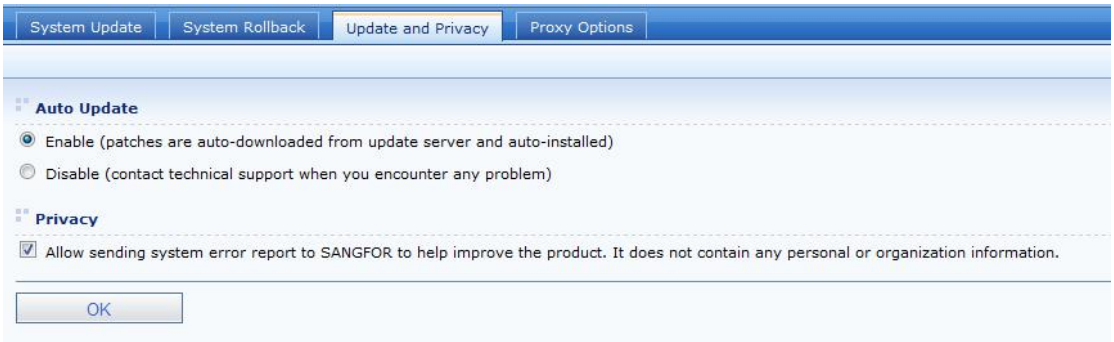
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Note: If the current rollback package is shown on this page, it indicates that this version can be rolled back. Click Rollback and refresh the page several minutes later.

11.8.3 Update and Privacy

System > **System Update > Update and Privacy,** you can configure related information about update and privacy here, as shown below:



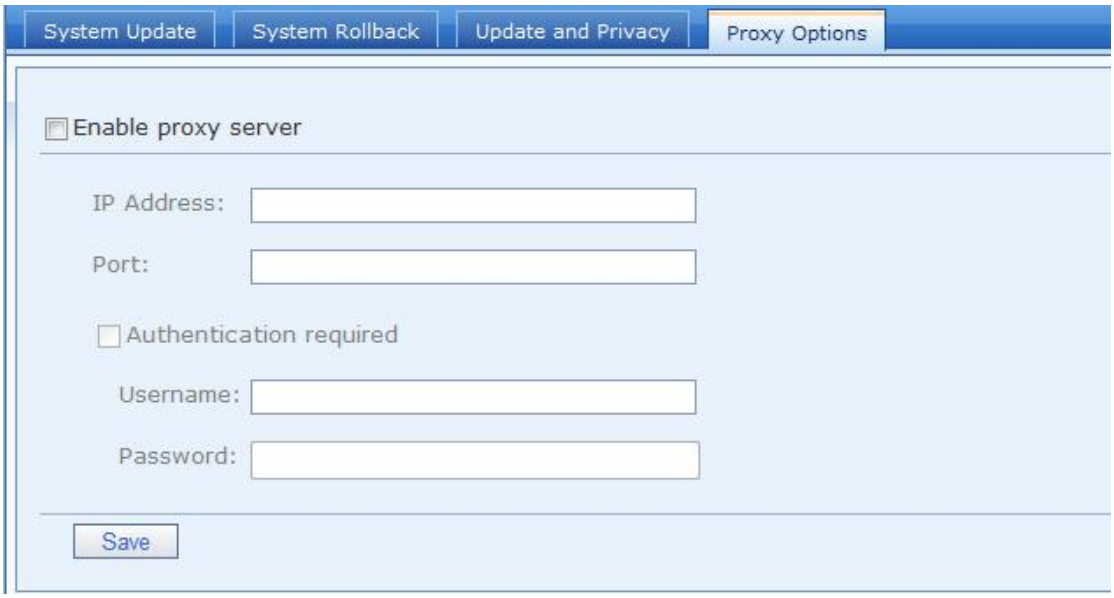
Auto Update: If select **Enabled**, patches will be downloaded from Sangfor official website and installed automatically.

Privacy: Specifies whether to send system error report to Sangfor.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

11.8.4 Proxy Options

Navigate to **System** > **System Update > Proxy Options**, as shown below:



Enable proxy server: Make sure that the proxy server supports HTTP and HTTPS. Once enabled, the proxy server will be used to obtain latest configurations.

IP Address: Specifies IP address of proxy server**(IPV4 address only).**

Port: Specifies port of proxy server**(Integer between 1 and 65535).**

Authentication required: Specifies whether to enable authentication.

Username: Specifies username of proxy server.

Password: Specifies password of proxy server.

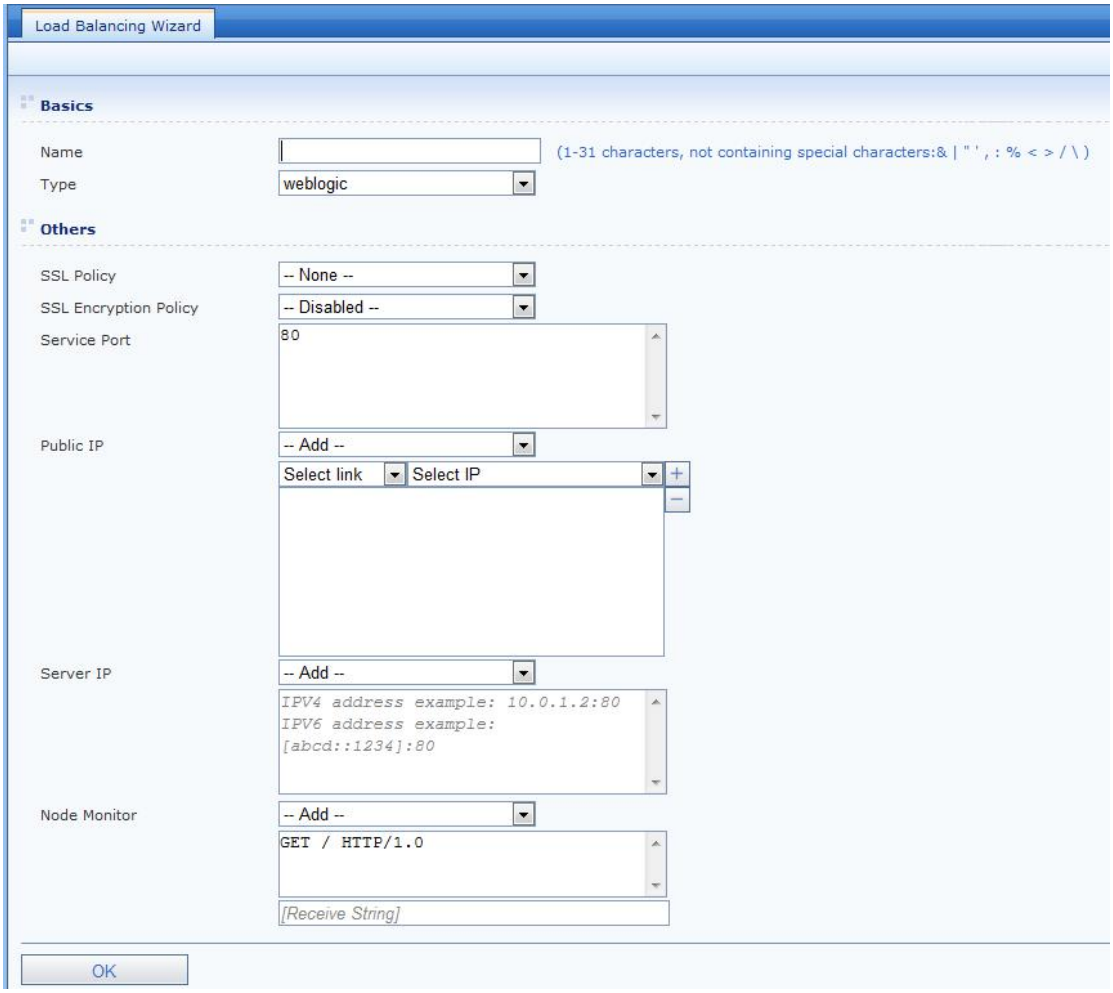
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 12 Wizard

With configuration wizard, you can configure load balancing and route quickly.

12.1 Load Balancing Wizard

On **Wizard > Load Balancing Setup** page, you can configure load balancing quickly, as shown below:



12.2 Routing Wizard

In **Wizard > Routing Setup**, you can configure policy-based routing quickly by completing the following steps:

Configuring link

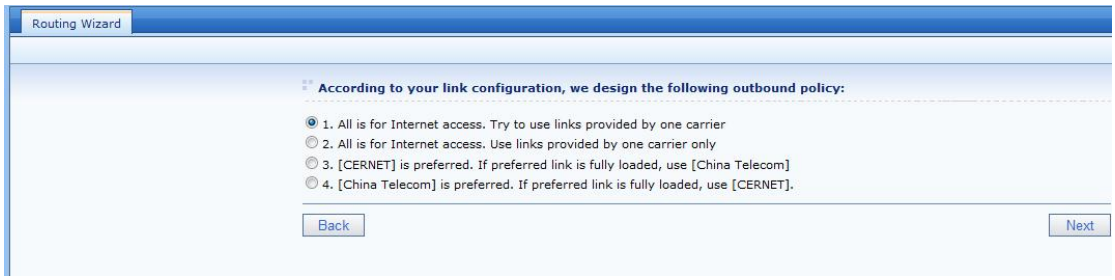
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Select an ISP address segment for each link. Then click **Next** to continue.

Configuring routing policy

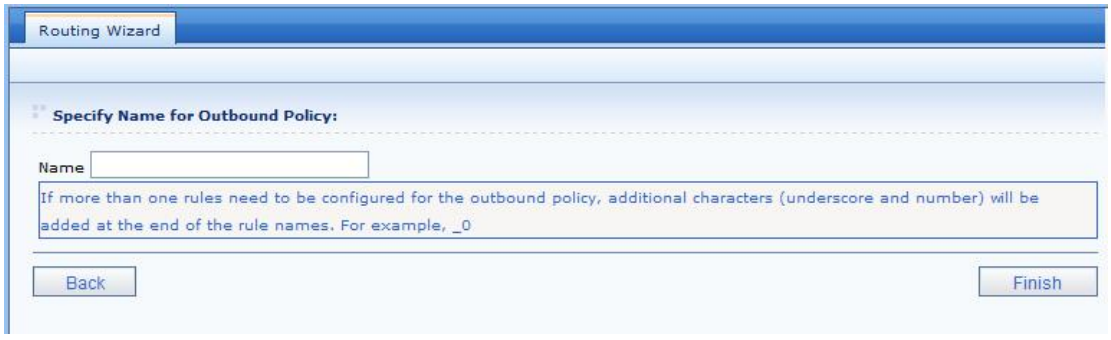
Select a outbound policy in accordance with your link configuration, as shown in following figure:



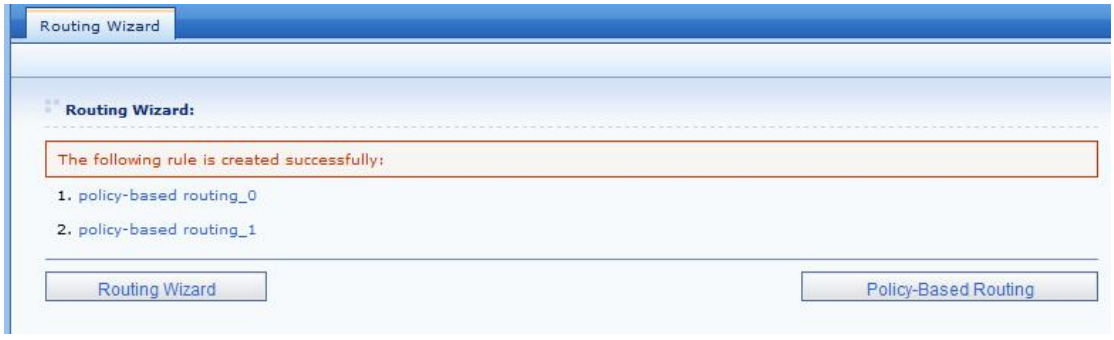
To return to previous step, click Back; or click **Next** to continue.

Configuring outbound policy

Specify a distinguish name for the outbound policy, as shown below:



To save the settings, click **Finish**. Then you will see the following page:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

As shown in the above figure, the ADC has added two policy-based routing automatically according to what has been set in the above configuration steps.

Click **Routing Wizard** to return to the homepage of routing wizard.

You will be redirected to **Routing > Policy-Based Routing** page by clicking **Policy-Based Routing**, as shown below:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 13 High Availability

You can configure different modes such as active-standby or high-availability cluster modes on several ADC devices to avoid single point of failure, which will bring about negative effects to network and application.

13.1 HA Mode

HA Mode: Options are **Active-standby** and **High Availability cluster.** Factory default is **Active-standby**.

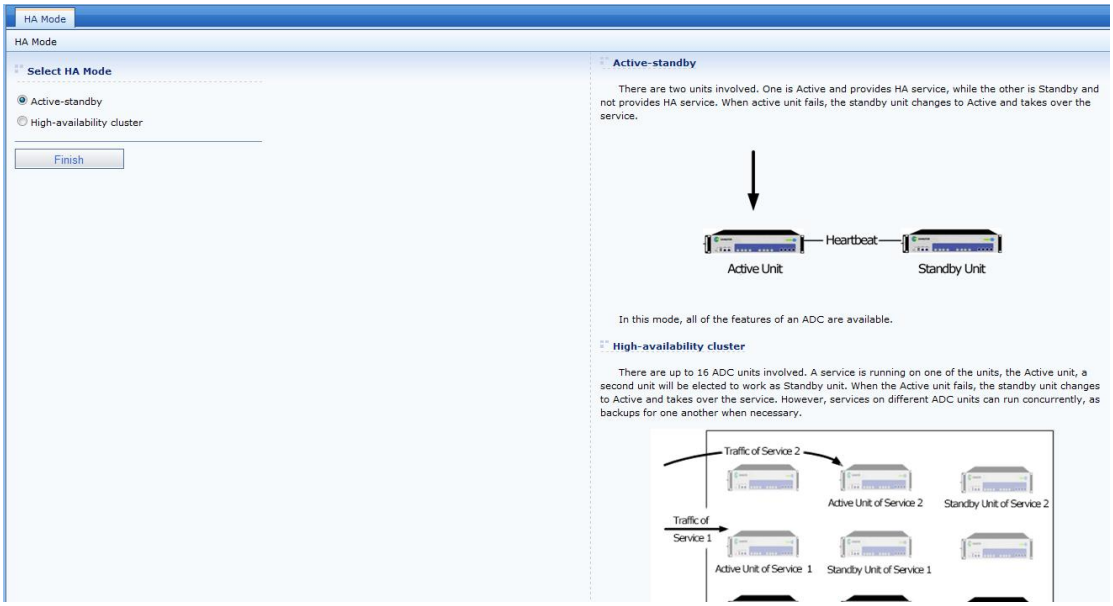
Active-standby: There are two units involved. One is Active and provides HA service, while the other is Standby and not provides HA service. When active unit fails, the standby unit changes to Active and takes over the service.



In this mode, all of the features of an ADC are available.

High availability cluster: There are up to 16 ADC units involved. A service is running on one of the units, the Active unit, a second unit will be elected to work as Standby unit. When the Active unit fails, the standby unit changes to Active and takes over the service. However, services on different ADC units can run concurrently, as backups for one another when necessary.

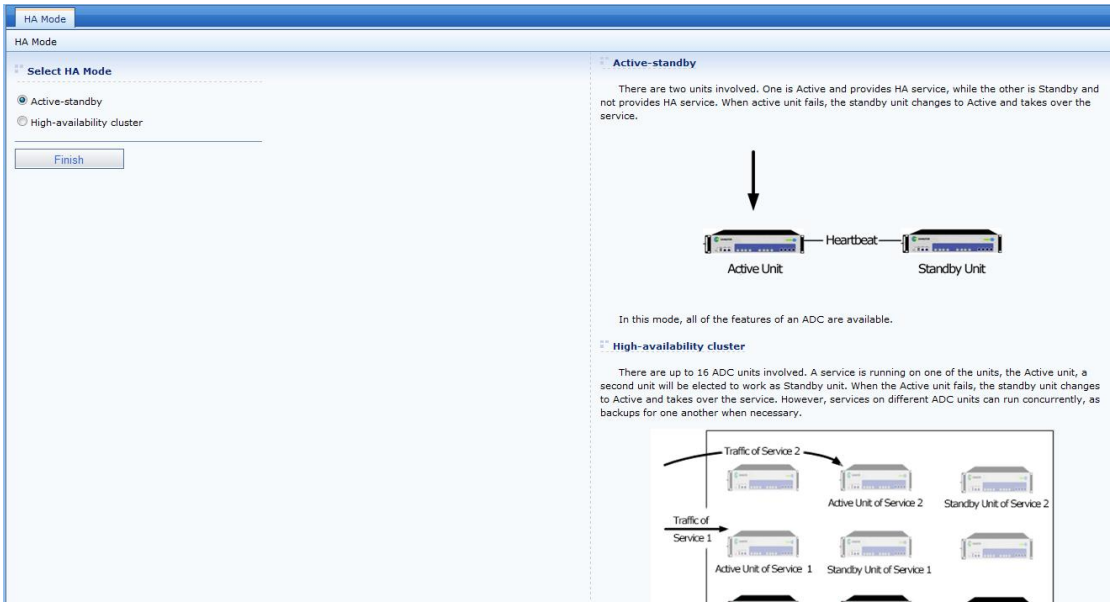
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



This mode is chosen for server load balancing, link load is not supported.

13.2 Active-standby

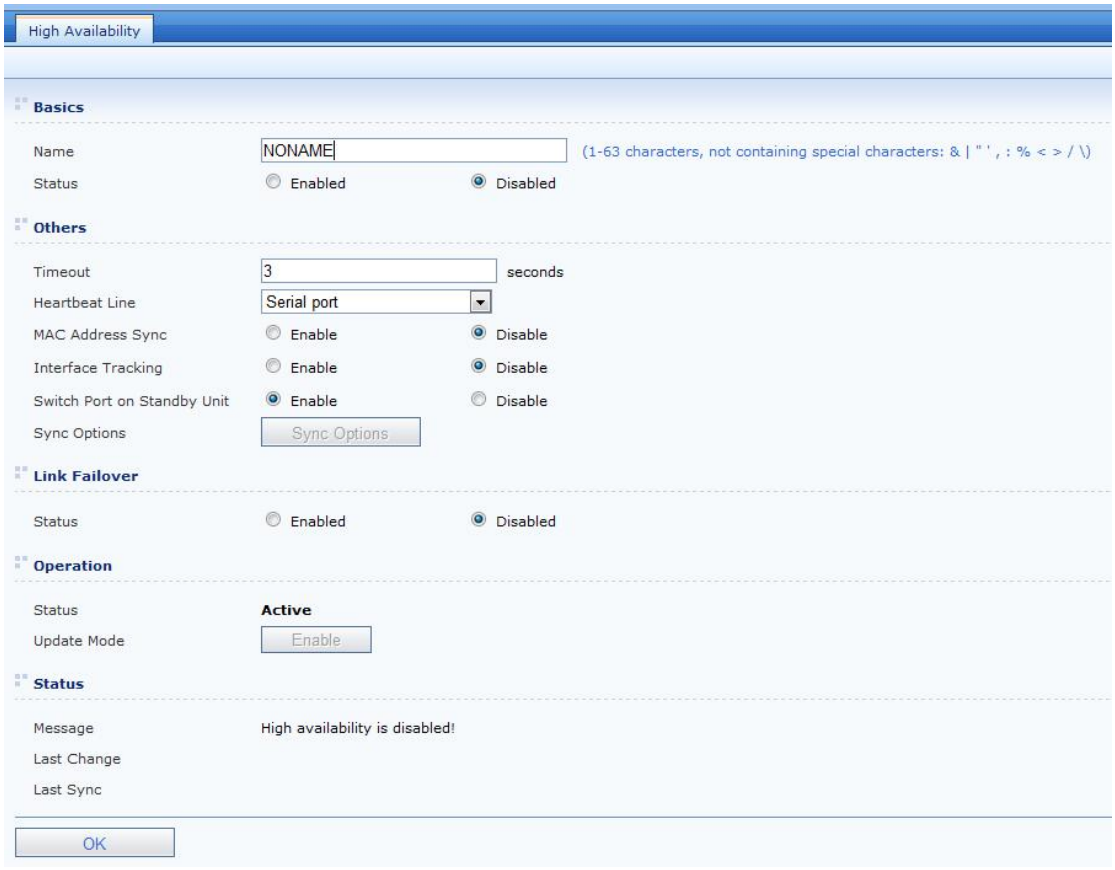
Navigate to **High Availability** > **HA mode** > **Active-standby**, as shown in the following figure.



Click **Finish** to switch mode and reboot device to log in again.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Active-standby includes two units, one is active unit and the other is standby unit, as shown in the following figure:



Name: Specifies the name of the unit, so as to distinguish which unit functions as an active unit.

Status: Specifies whether to enable or disable active-standby unit.

Timeout: Specifies the timeout period. If the standby unit cannot receive heartbeat packets from the active unit within the timeout period, then the standby unit will switch to be active unit automatically.

Heartbeat Line: Specifies the interface connecting two units. Options are serial port or other Ethernet ports. You need to configure an IP address for the selected port and the IP address should not conflict with other IP addresses. Ethernet port is recommended because it takes less time in switching units and supports synchronzing sessions.

MAC Address Sync: Specifies whether to sync MAC address when switching two units.

Interface Tracking: Specifies whether to check the status of the peer device through data packets, so as to avoid IP address conflict when both of the two units are active unit. The interfaces of the two devices should be in the same broadcast domain. You can select an interface that is already in use or select an idle interface and configure an IP address for the

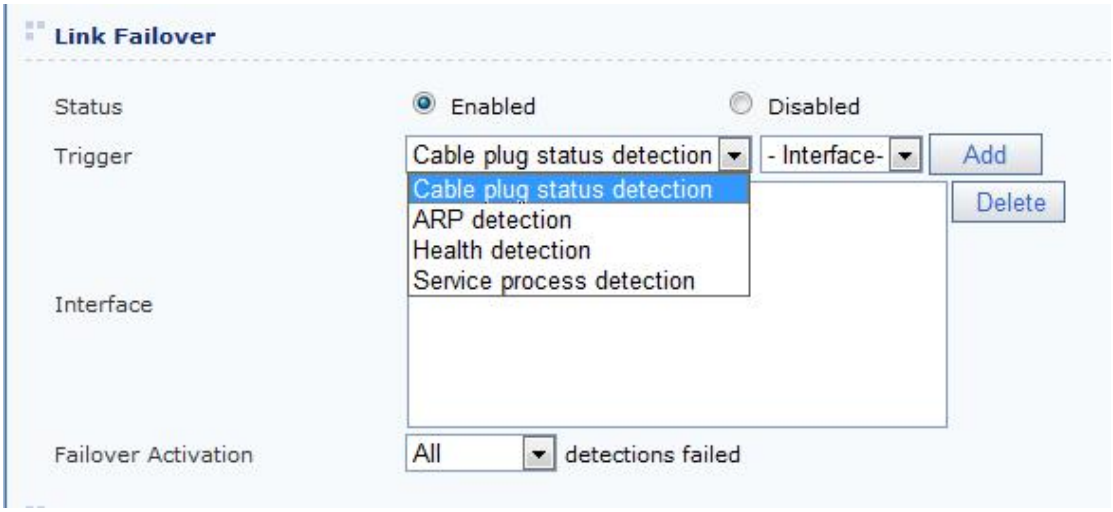
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

idle interface.

Switch Port on Standby Unit: Select **Enable** to enable switch port on standby unit.

Sync Options: Click **Sync Options** to synchronize configurations to standby unit.

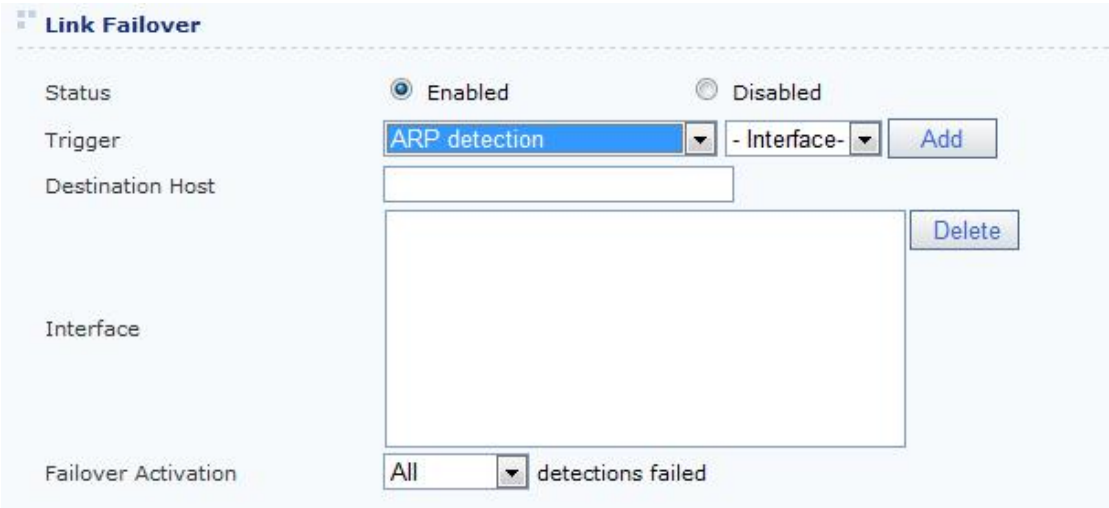
Select **Enabled** for **Status** in **Link Failover,** as shown the following figure:



Status: Specifies whether to enable failover. Options are **Cable plug status detection, ARP detection** and **Health detection**. Click **Add** to add multiple detection factors and click **Delete** to delete the detection factor.

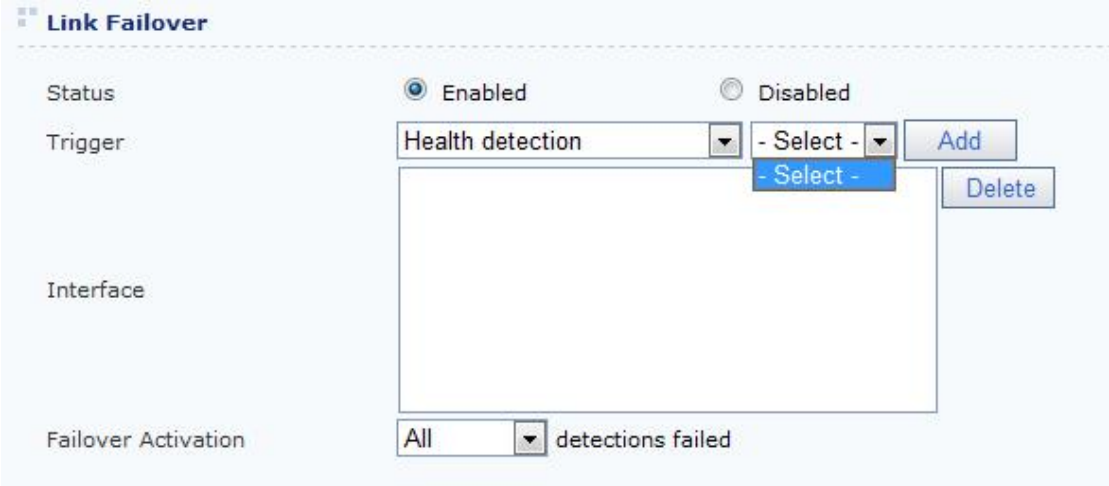
Cable plug status detection: Detects status of interface and switches when the interface is not connected correctly.

ARP detection: ADC sends ARP broadcast to selected interface. If the destination host responds to the request, it indicates that the host is normal. The IP address of the destination host should be on the same network segment with that of ADC interface, as shown in the following figure:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Health detection: Select **Health detection** to check health status of links, as shown in the following figure:



Operation: Options are **Active** and **Standby,** as shown below:



Update mode: Once enabled, units will not be switched and configurations will not be synchronized. Please update under customer service's guidance.

Status: Displays the status of the two units.
Last Change: Specifies the time of the last switch of the two units.
Last Sync: Specifies the last time configurations are synchronized.

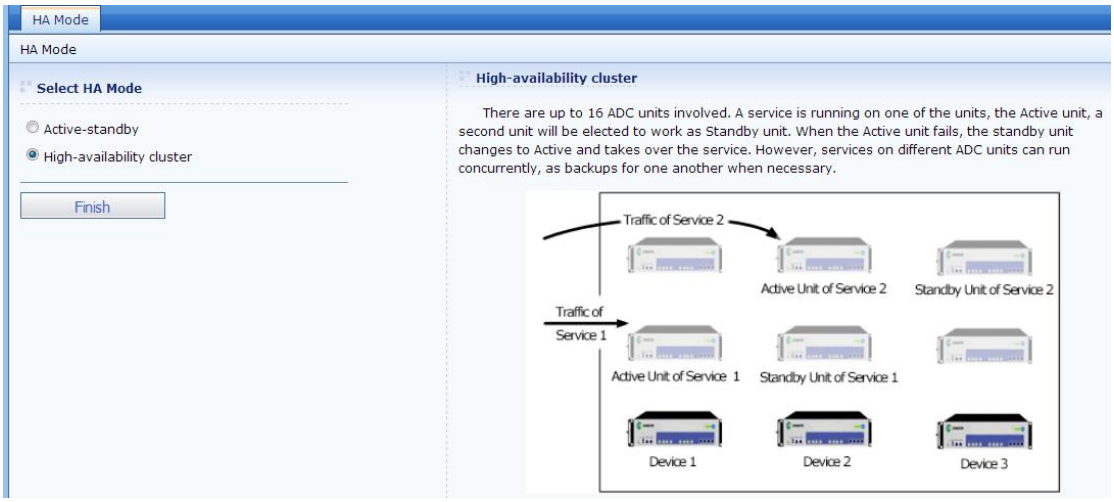
13.3 Cluster

Cluster includes **High-availability cluster.**

13.3.1 High-availability Cluster

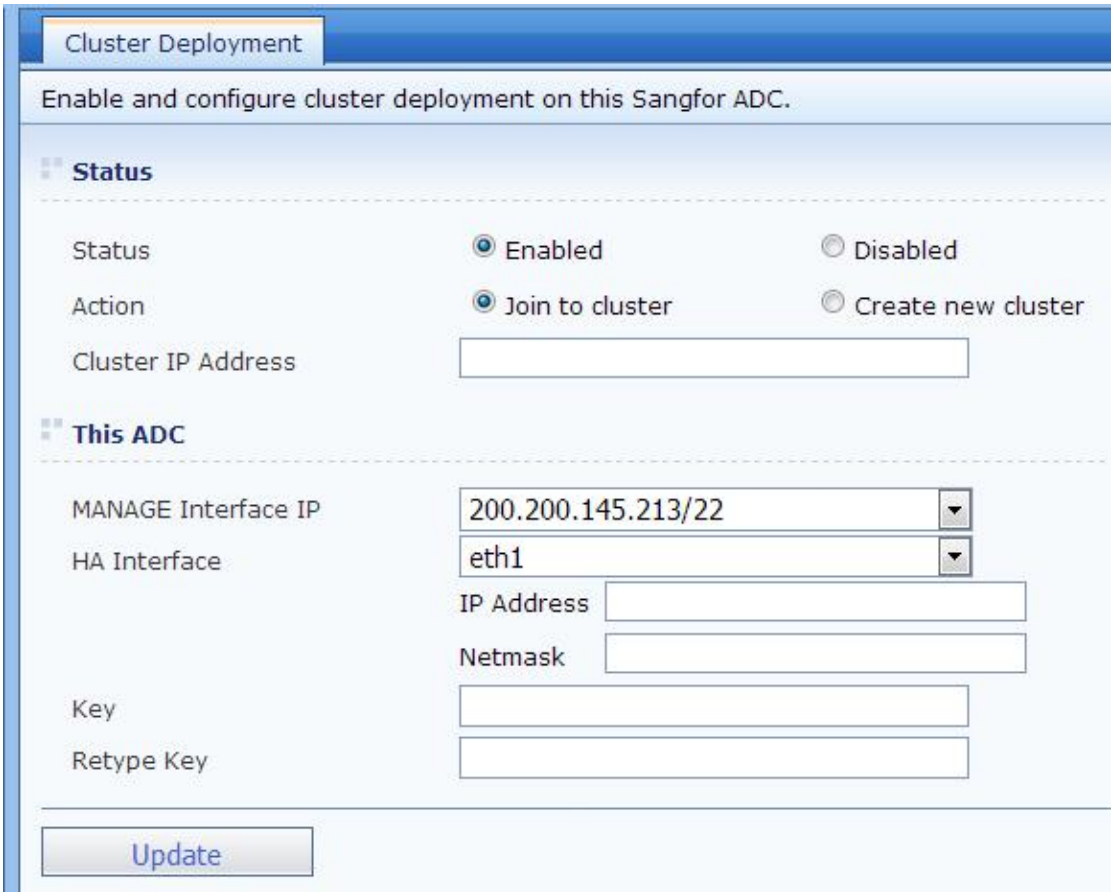
Navigate to **High Availability** > **HA mode** > **High-availability cluster,** select High-availability cluster and click **Finish**, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



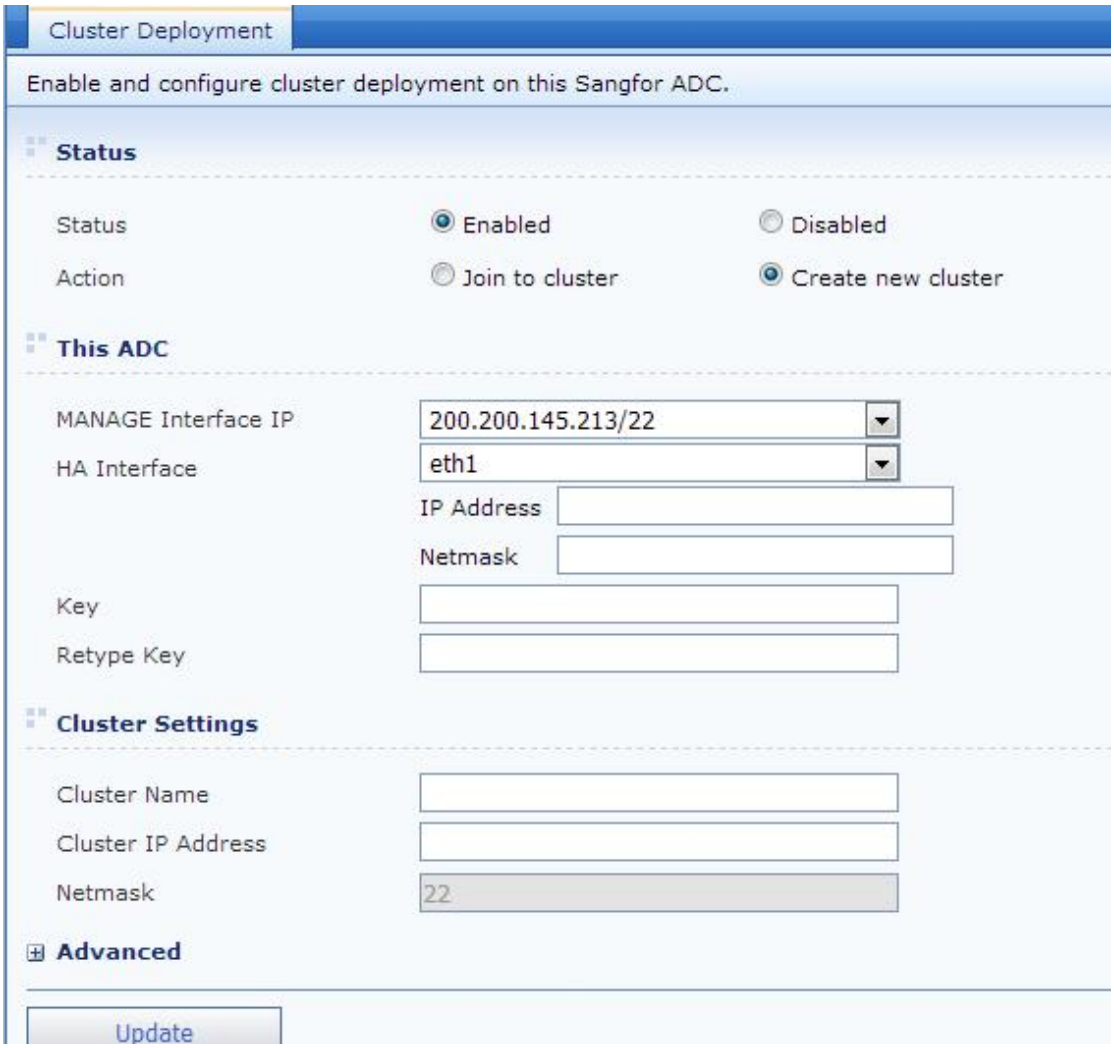
Cluster

Navigate to **High Availability > Cluster**, as shown in the following figure:



Status: Specifies whether to enable or disable cluster feature.
Action: Options are **Join to cluster** and **Create new cluster**. Select **Create new cluster** for the first device, or else other devices cannot be joined to cluster, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Manage Interface IP: Specifies IP address of the MANAGE interface through which, cluster controller sends heartbeats to other devices and manages other units.

HA Interface: The interface is used to send heartbeats, synchronize sessions and track connections. HA interface of the devices must be the same, or else the devices may not be able to join to cluster.

IP Address and **Mask**: Specifies IP address and mask of the HA interface. HA interface IP address of devices in the cluster must be on the same network segment, but should not on the same network segment with that of other interfaces.

Key: Specifies key for devices to join to cluster. Input the same key, or else failure may occur when joining to cluster.

Retype Key: Retype the key in the previous step.

Cluster Name: Specifies name of the cluster.

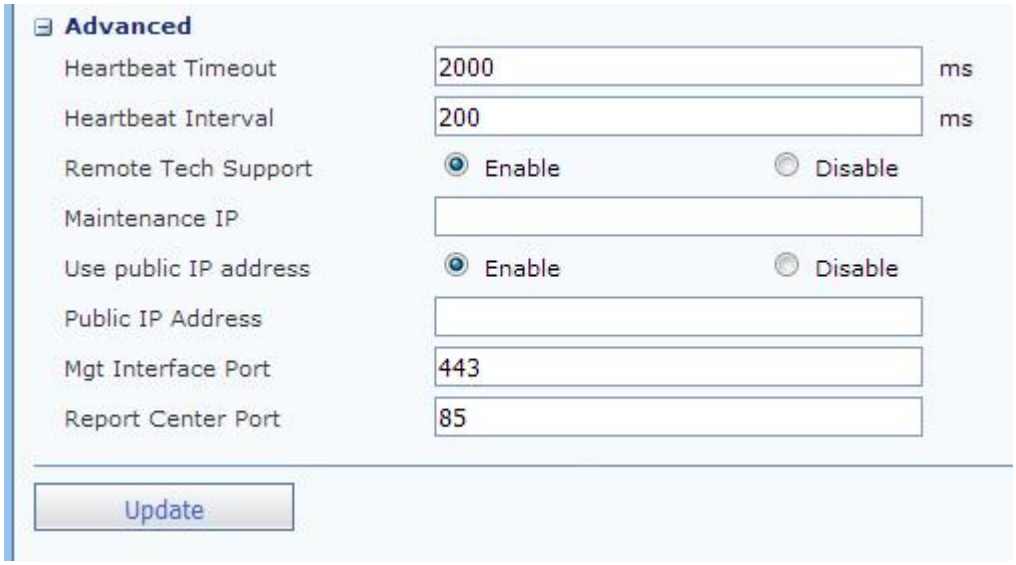
Cluster IP Address: Specifies an IP address to manage, configure cluster and log in to the cluster controller. Once devices are joined to cluster, they can only be managed via the cluster IP address.

Netmask: Specifies netmask of cluster IP address.

Heartbeat Timeout: If the unit in the cluster receives no heartbeat from other units within

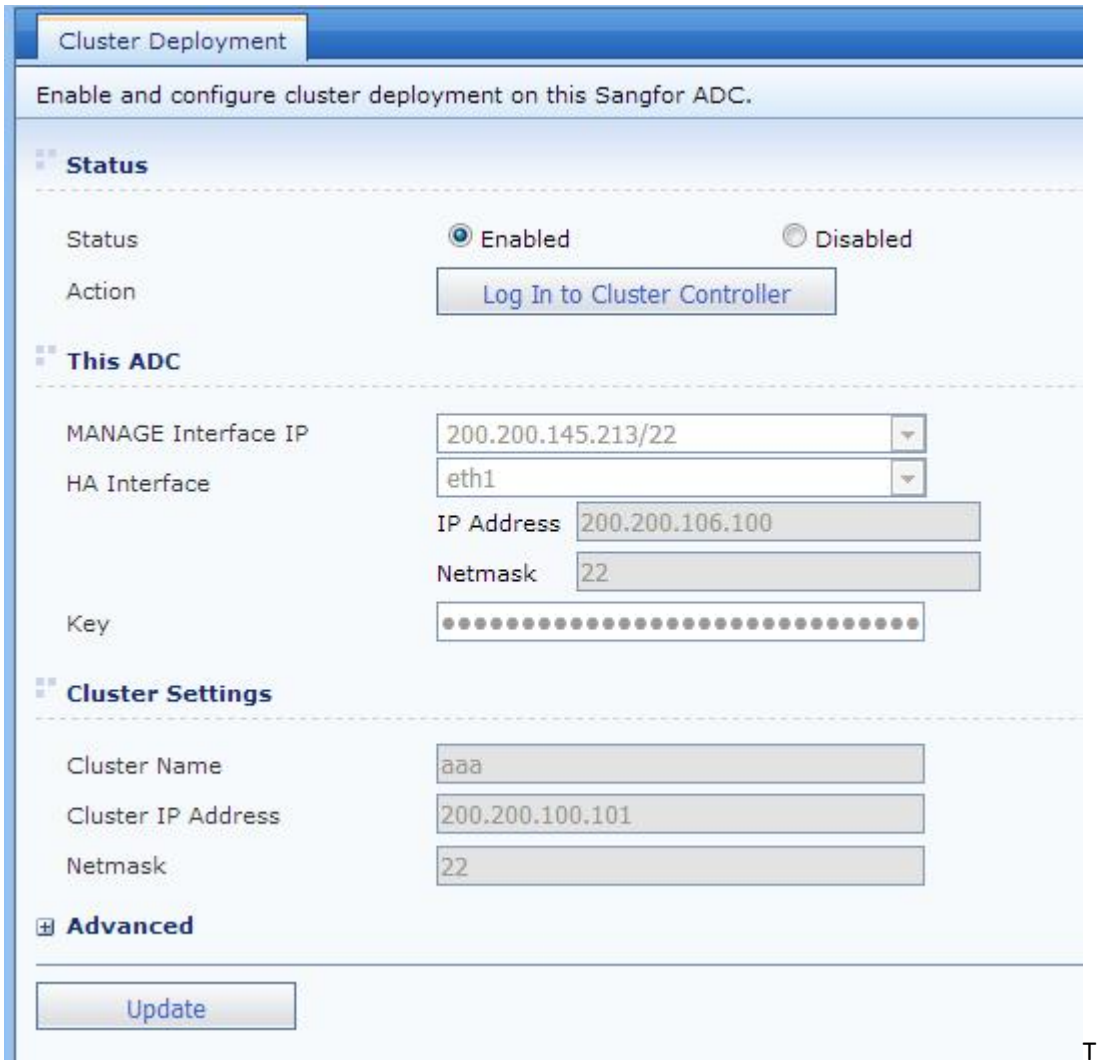
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

the timeout, the other units are thought as offline and then take over work from the unit.
Heartbeat Interval: Specifies interval of sending heartbeat package.
Remote Tech Support: Specifies whether to enable logging in to devcie with maintenance IP, as shown in the following figure:



Maintenance IP: Specifies floating IP address of WAN port.
Use public IP address: Specifies whether to log in to device with public IP address.
Internet IP**:** Specifies internet IP of WAN port.
Mgt Interface Port: Specifies port of the Web admin console.
Report Center Port: Specifies port of the Report Center.
Click **Update** to save the changes, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



T

Click **Log In to Cluster Controller** to enter the following, as shown in the following figure:

Cluster IP Address: Specifies Management IP when create a cluster which only supports IPV4 and mask.

MANAGE Interface IP: Specifies IP address of the MANAGE port. Support IPV4 only.

HA Interface: Specifies an HA interface which should be the same with that of other units in the cluster. Support IPV4 only.

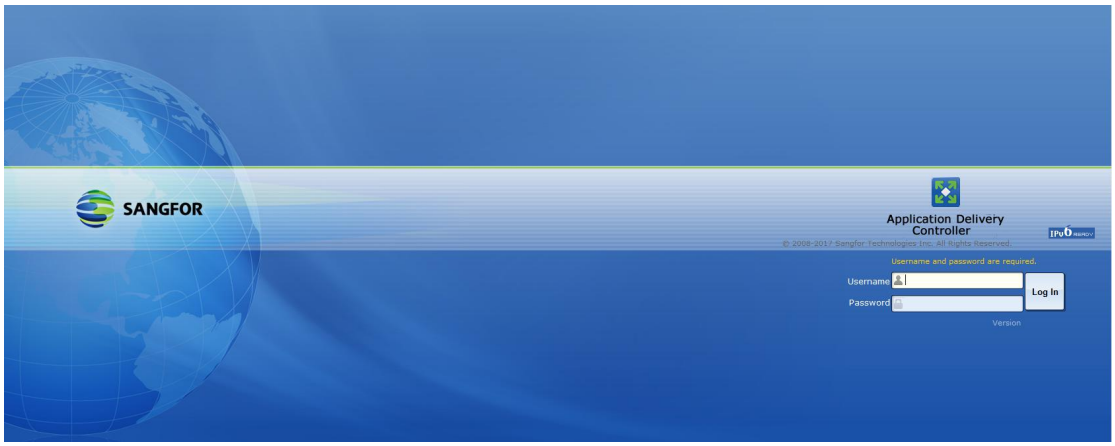
IP Address and **Mask**: Specifies IP address and mask of HA interface. IP address of HA interfaces in the cluster must be in the same network segment.

Secret Password: Specifies the secret password to join the cluster.

Click **Update**, save and activate configuration.

Click to jump to the login page of cluster management system, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



The default password is cluster. After joining the cluster, you can only configure the device by cluster management system.
Login by cluster management IP:

Status includes Disable, join the cluster and create a cluster. If you want to create a cluster, access the first device and choose to create a cluster, then join other units to the cluster in the unit management page.

Device management IP: Specifies IP address of device management port for establishing the cluster control connection and monitoring on units' heartbeat.

HA interface indicates a physical interface(Usable port aggregation) and requiring configuring IP address for establishing data connection and monitoring on units' heartbeat.

To cluster authentication and transmission encryption. Click **Secret Password**. All units with the same secret password can join the cluster.

Cluster Name: Specifies the name of cluster.
To manage IP address of all the cluster and login cluster management page with this IP, click **Cluster Management IP.**
Heartbeat Timeout: If unit in the cluster receive no heartbeat from other units within the timeout, the other units are thought as offline and then take over work from the unit.
Heartbeat Interval: Specifies the interval of broadcasting heartbeat package to other units.
Cluster Remote Maintenance: When it enables, you can login cluster console or each units' consoles by remote maintenance IP address to manage.

To prevent the breakdown caused by the heartbeat failure of cluster nodes, click **Heartbeat Line Detection**. (when it enables, if you modify the service port you need to synchronously modify the physical port referenced by service port.)

Unit Management

Navigate to **High Availability > Unit Management**

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Click **Add** to add a new unit
Name: Specifies the name of the joining cluster

To manage, deploy cluster and login cluster control center, click **Device management IP.** After joining the cluster, you can only configure the device by cluster management IP.

Application Group Management

Navigate to **High Availability > Application Group Management**

Click **Add** to add a new application group.

Name: Specifies the name of application group.
Session Sync: When it enables, the activated units in the group will synchronize session to backup units. If activated units break down, the backup units will become activated units to continue the existing connection.
Default unit has the highest priority to be selected as activated unit.
Preemption: If it enables, when the default unit of the application group is healthy, it will become activated unit automatically and the previous activated unit becomes backup of the application unit.
Failure Detection: Click to select the link associated with application group. If a activated unit's associated link failure, then switch to other unit in the application group. Otherwise the unit cannot become activated unit when the activated unit breaks down.
Virtual MAC: If it configures a virtual MAC address in one link for application group, all IP addresses of the application group in this link will connect with extern by the fake4 MAC. And if it failovers, new activated unit will work the same way.
Weight: If application activates in one unit, the unit's load will increase according to the application group weight. When application switches in the cluster, it will select unit based on the unit's load.
Information of Application Group**:** A series of configuration enable the application group to issue service contained in the application group including float IP, virtual service and NAT rule.

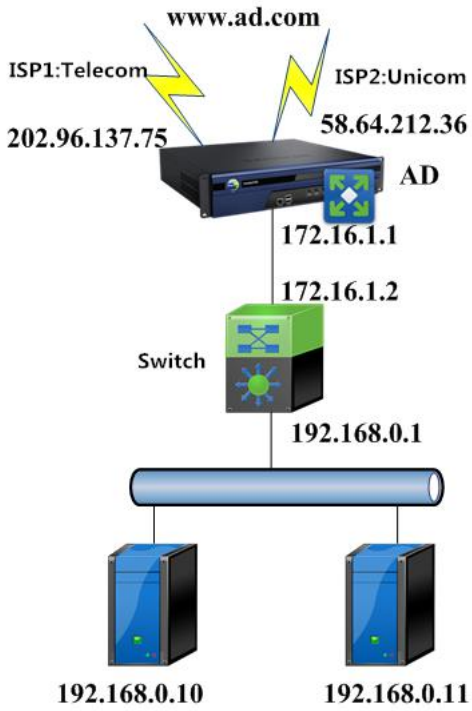
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Chapter 14 Cases Study

14.1 Deployment and Configuration

14.1.1 Scenario 1: Deploying Device in Route Mode

The advantage of route mode is that it can load balances the links and servers. The topology diagram of route mode is as shown below:



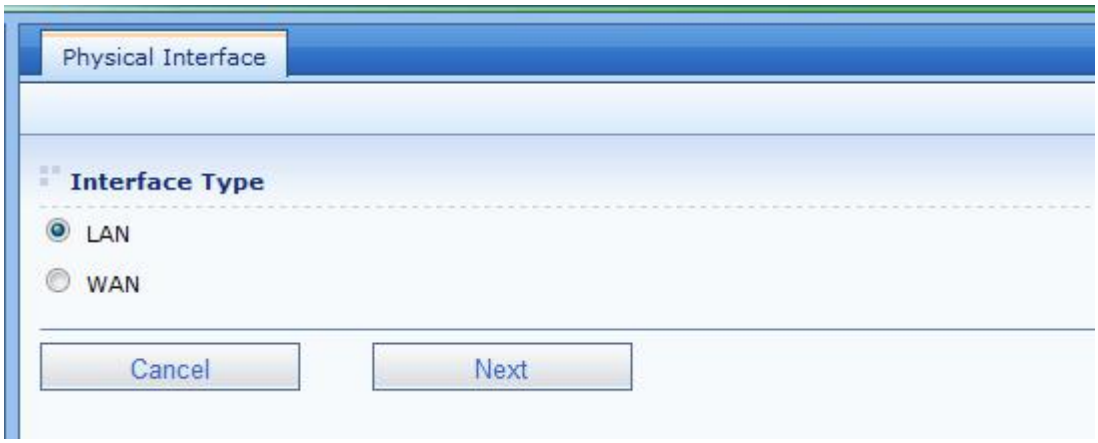
As shown in the figure above, the ADC is deployed as a router, and it acts as a gateway to proxy internal users to access internet. There are two WAN links: Telecom and Unicom. Their IP are 202. 96. 137. 75 and 58. 64. 212. 36 respectively, and the two IP addresses map to the same domain name: www. ad. com. The IP address of LAN interface on ADC is 172. 16. 1. 1. Layer 3 switch is placed behind the ADC. The IP address of the interface on the switch connecting to the ADC is 172. 16. 1. 2, while that of the interface on the switch connecting to intranet is 192. 168. 0. 1. There are two LAN servers which provide same Web services. Their IP addresses are 192. 168. 0. 10 and 192. 168. 0. 11 respectively.

Requirements: The ADC can load balances the WAN links and the two servers.

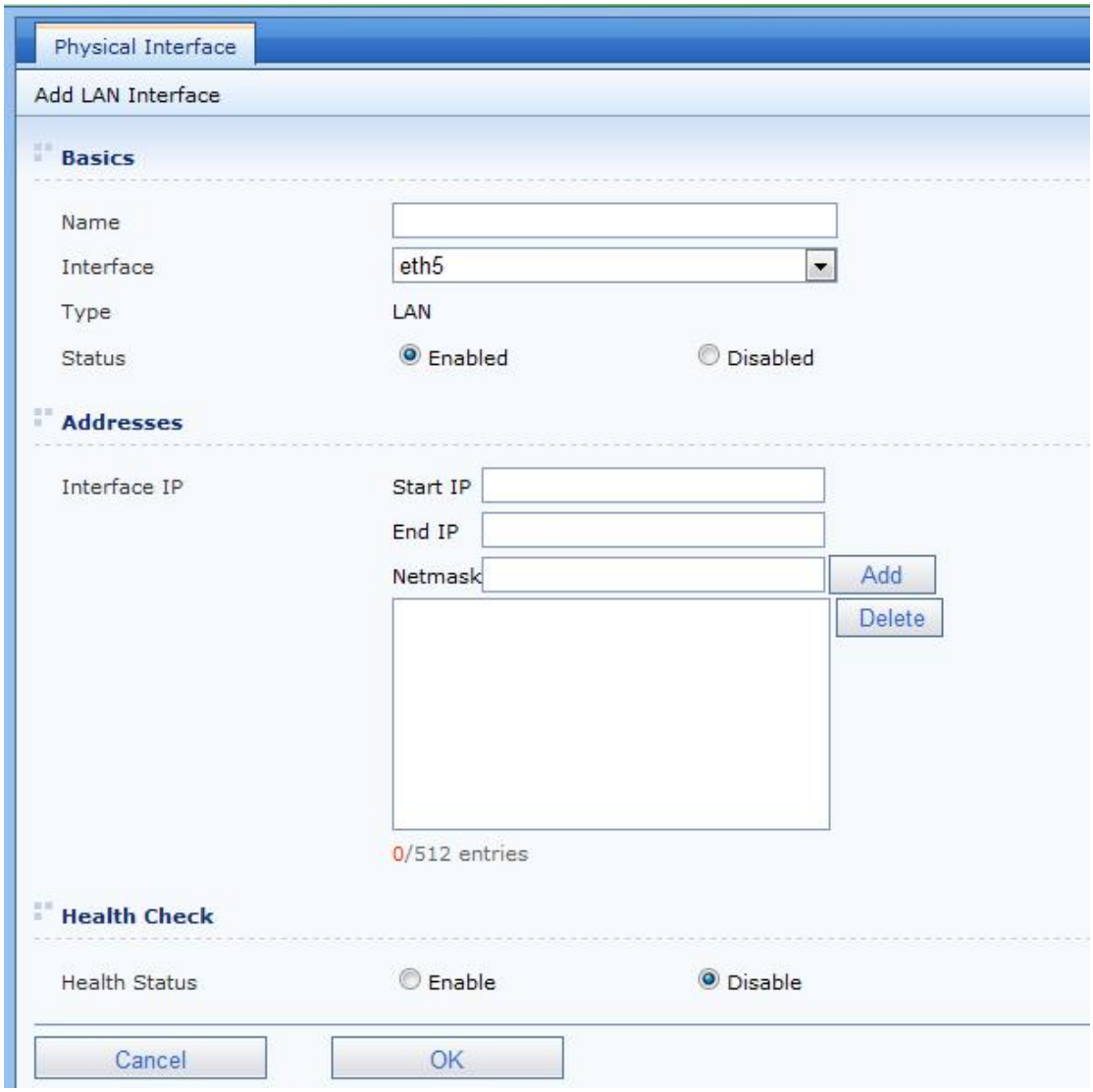
The configuration steps are as follows:

1. Go to the **Network > Interface > Physical Interface** page, and add a LAN interface, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

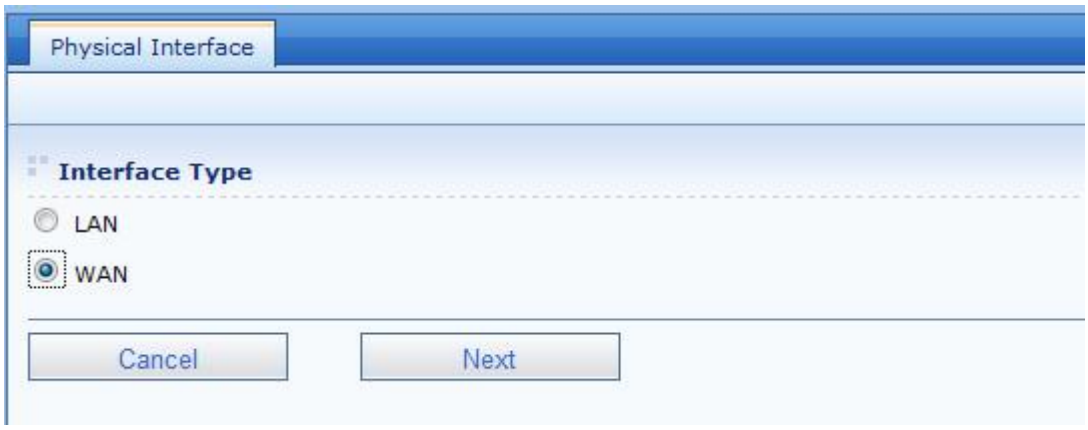


Select **LAN** and click **Next** to enter the following page:

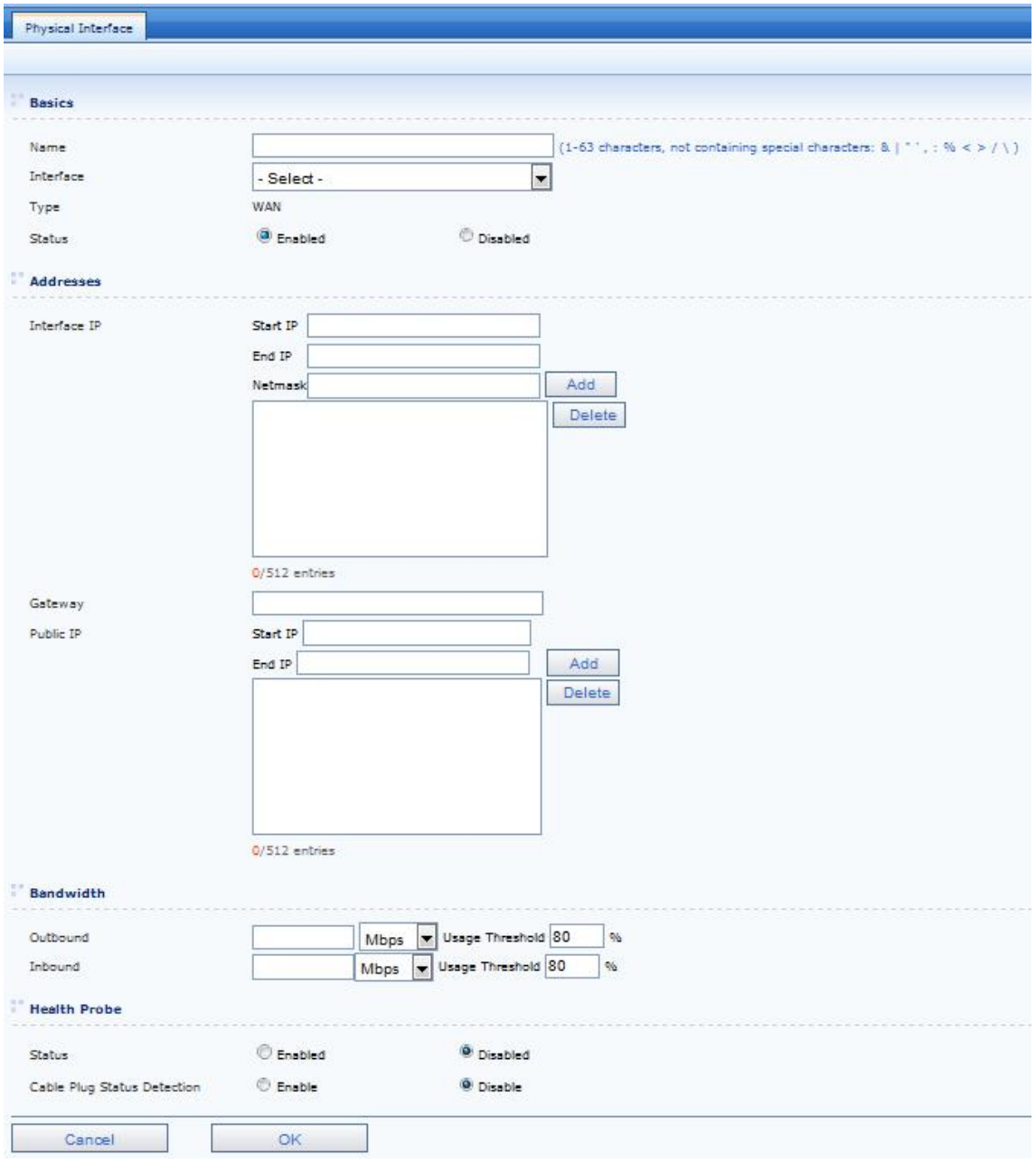


2. Add a WAN interface for telecom link on **Network > Interface > Physical Interface** page, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Select **WAN** and click **Next** to enter the following page:



3. Add a WAN interface for Unicom link on **Network > Interface > Physical Interface** page,

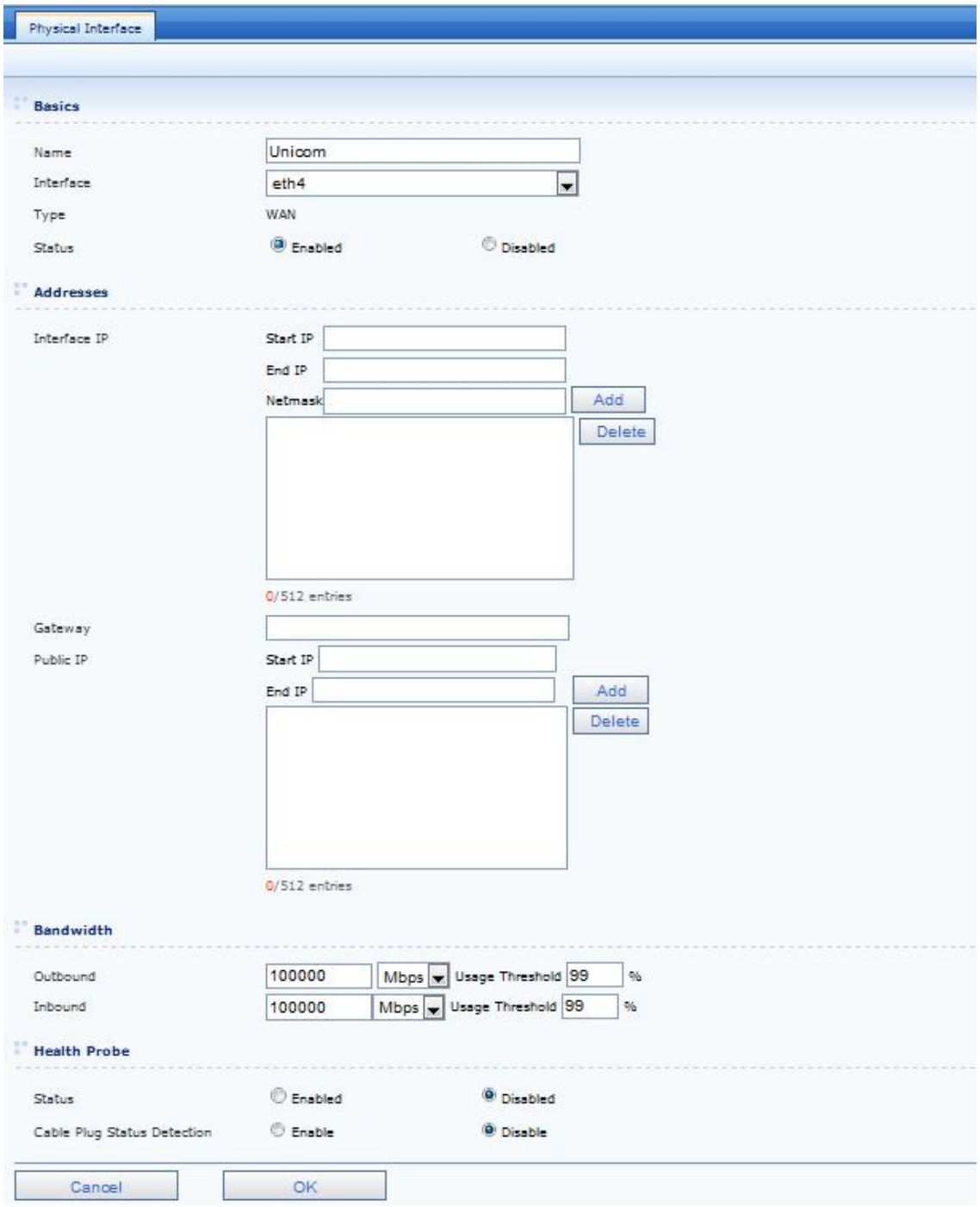
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

as shown below:

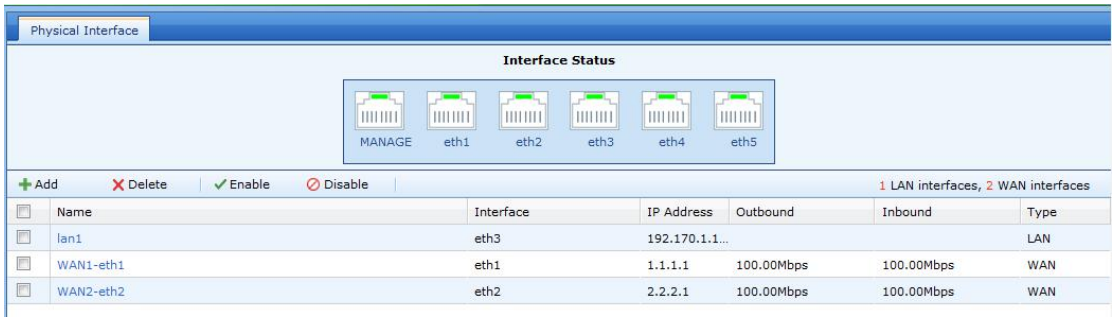


Select **WAN** and click **Next** and configure the following contents, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

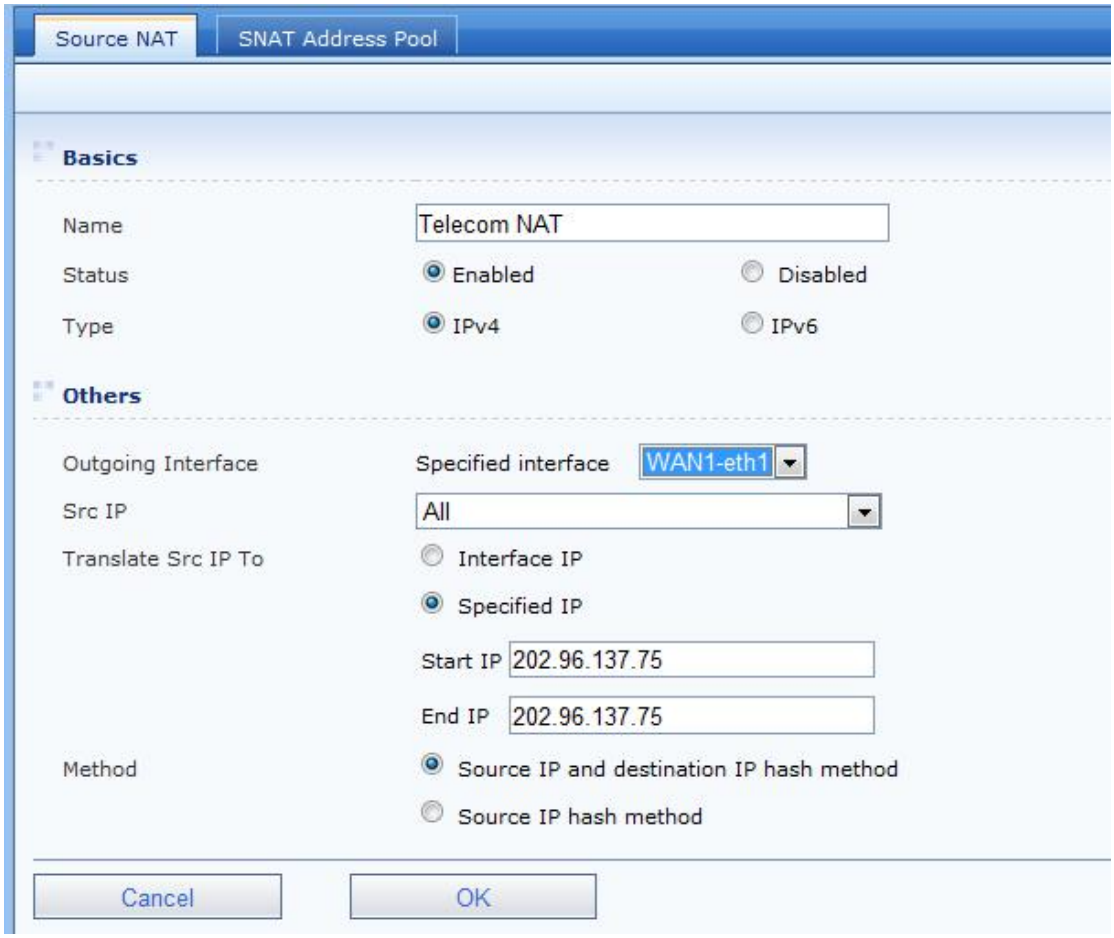


4. After completing the above configuration steps, you can view the following figure:



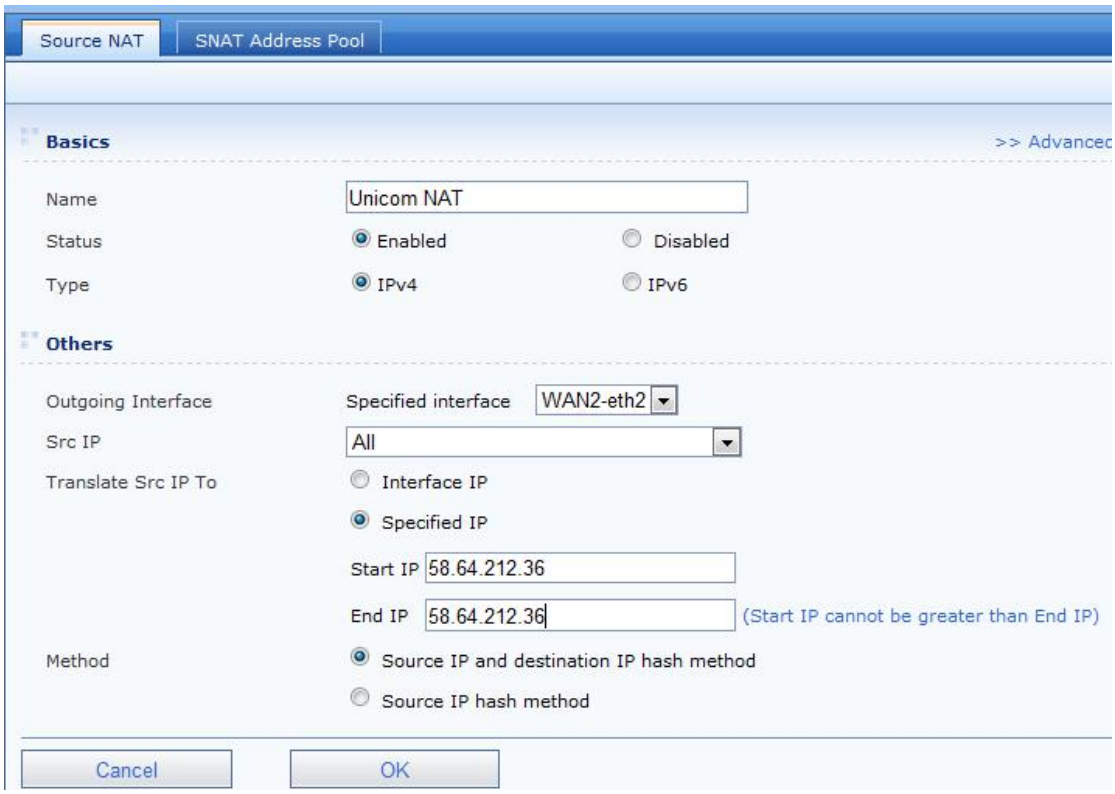
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

5. Go to the **Network > Source NAT** page, and configure source NAT policy. To make the traffic from intranet go through the telecom link, configure as shown below:



To make the traffic from intranet go through the Unicom link, configure as shown below:

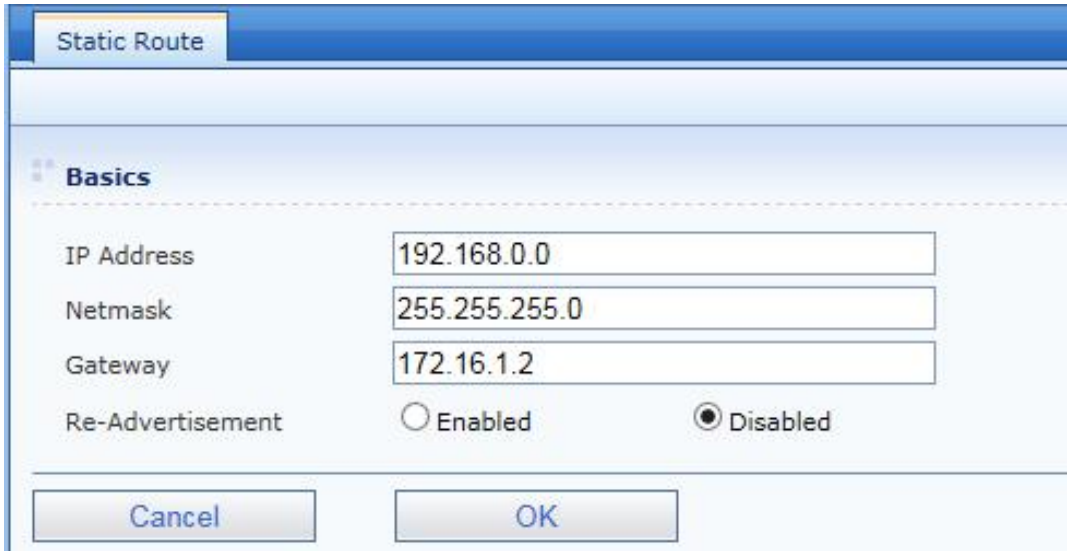
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



To save the settings, click **OK**. Then you can view the following figure:



6. Go to the **Routing > Static Route** page, and add a route on the ADC, as shown in the following figure:

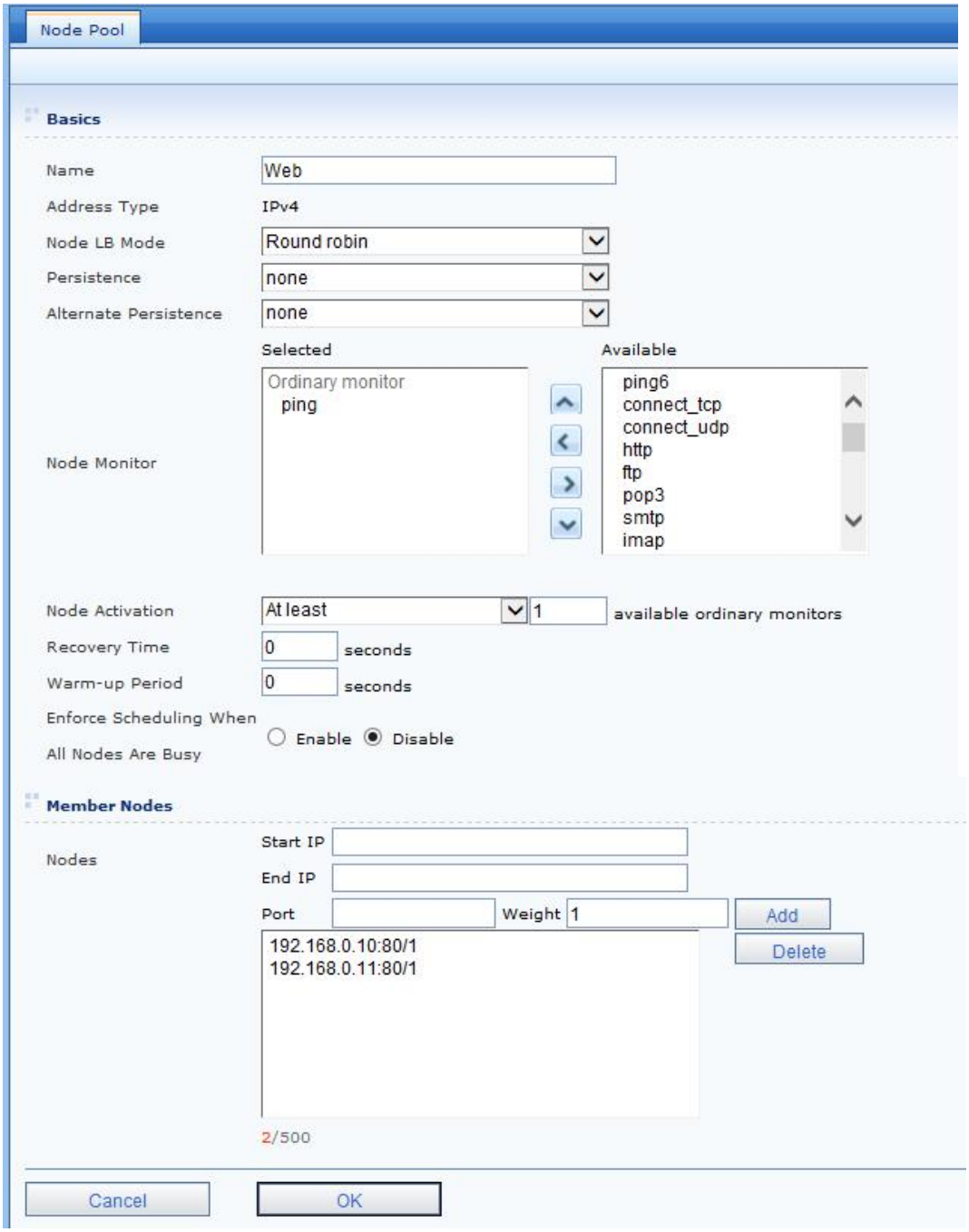


7. Go to the **Load Balancing > Service** page, and create a service. This step can be ignored, for there is HTTP service on the ADC by default.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

8. Go to the **Load Balancing > WAN Link** page, create a WAN link and then add the WAN links from the **Available** box into the **Selected** box.

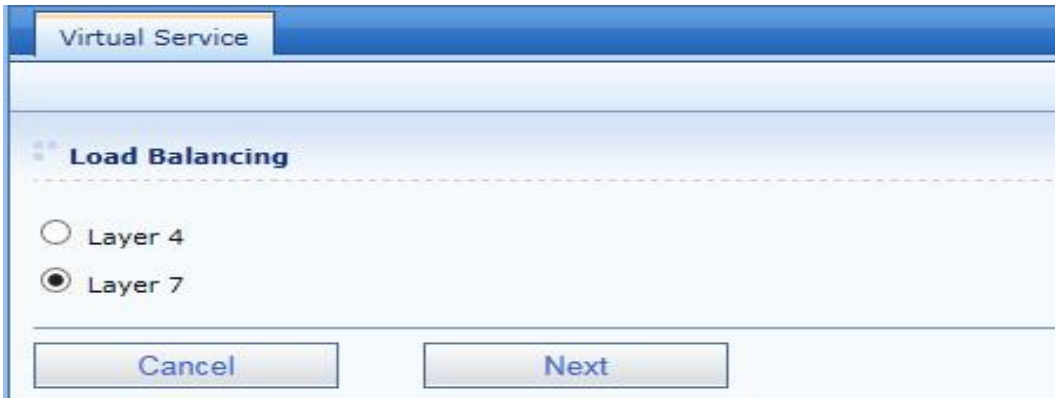
9. Go to the **Load Balancing > Node Pools** page, create a node pool, and then add the IP address of the server into the node pool, and specify a node monitor and session persistence method (there is no session persistence method on the ADC by default. If you need to schedule node based on session persistence, you can configure the session persistence method before). In **Node LB Mode** field, you can select **Round robin**, as shown below:

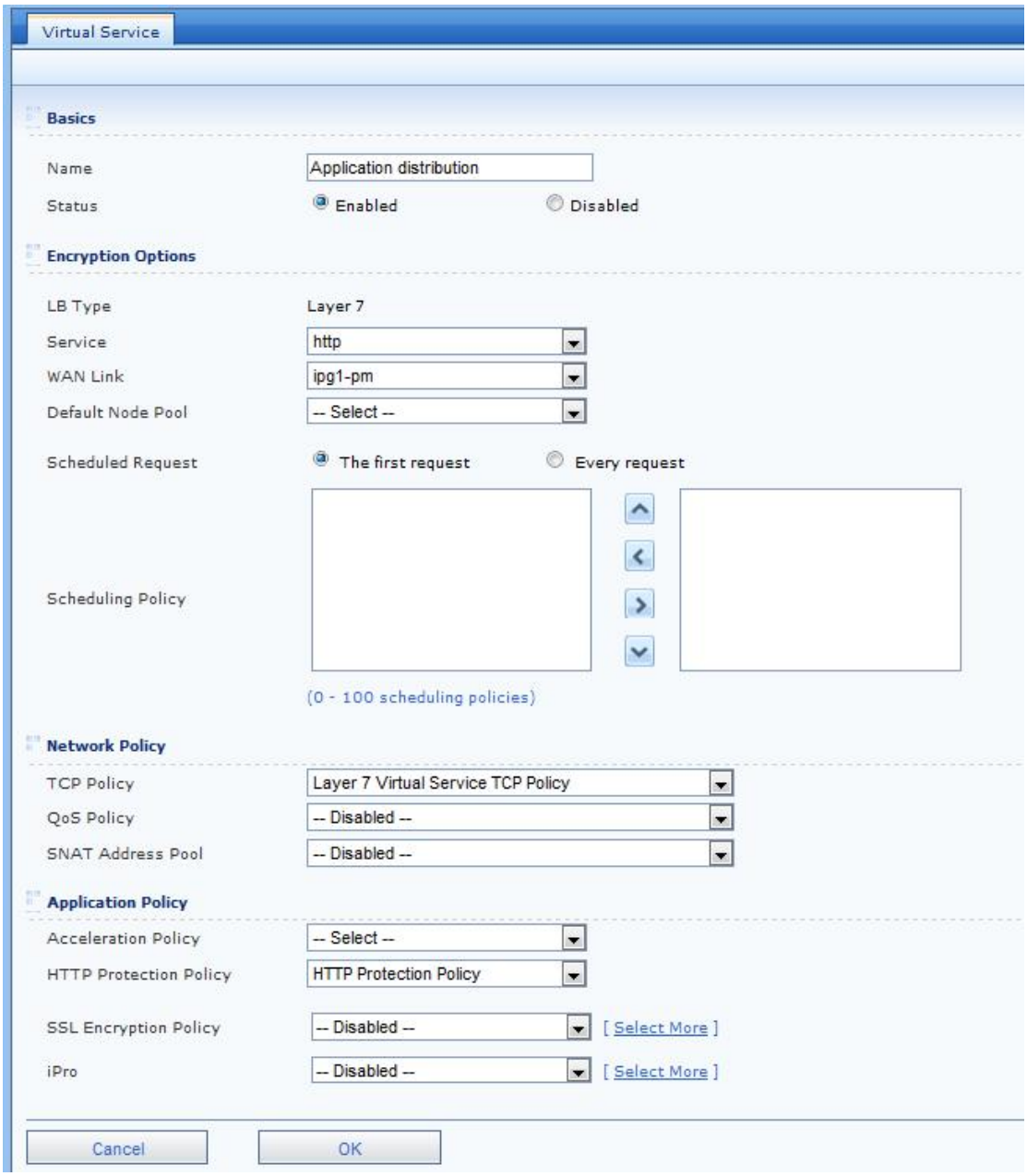


10. Go to the **Load Balancing > Virtual Service** page, and create a layer 7 virtual service, and

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

associate the configured options as well, as shown below:





Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

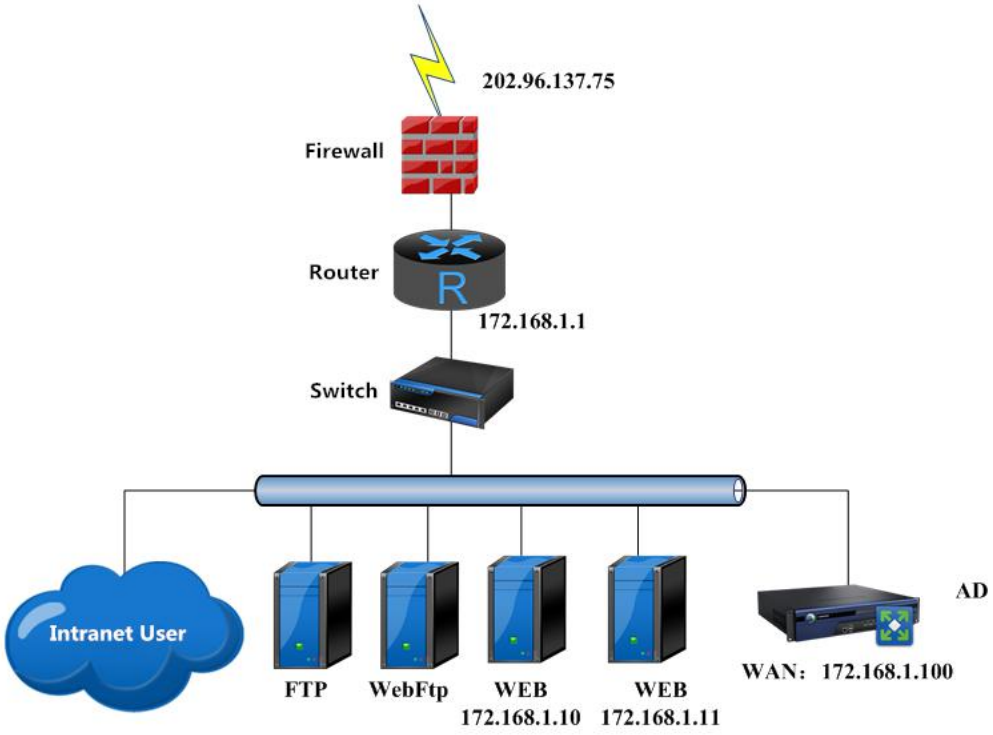
14.1.2 Scenario 2: Deploying Device in Bypass Mode

The ADC deployed in bypass mode can send and receive data via single port, while deployed in other modes, multiple pairs of interfaces must be used to receive and send data by the ADC.

Advantages: The newly-added ADC can be configured directly without need to change previous network topology.

Features: The internal users can access the server through the ADC instead of accessing the servers directly, so that the load on the servers can be balanced by the ADC. And it can also implement load balancing when the LAN servers distribute applications. The ADC can load balances the inbound links of intelligent DNS as well.

Figure 2: Network Topology



The IP address of the egress interface on the firewall device is 202. 96. 137. 75. The IP of the LAN interface on the router is 172. 168. 1. 1. The layer 2 switch is used to connect to all the devices located on intranet. The ADC is deployed in bypass mode, and its IP address is 172. 168. 1. 100. There are two LAN servers which provide same Web services. Their IP addresses are 172. 168. 1. 10 and 192. 168. 1. 11 respectively.

Requirements: The ADC can load balances the two Web servers.

Notes:

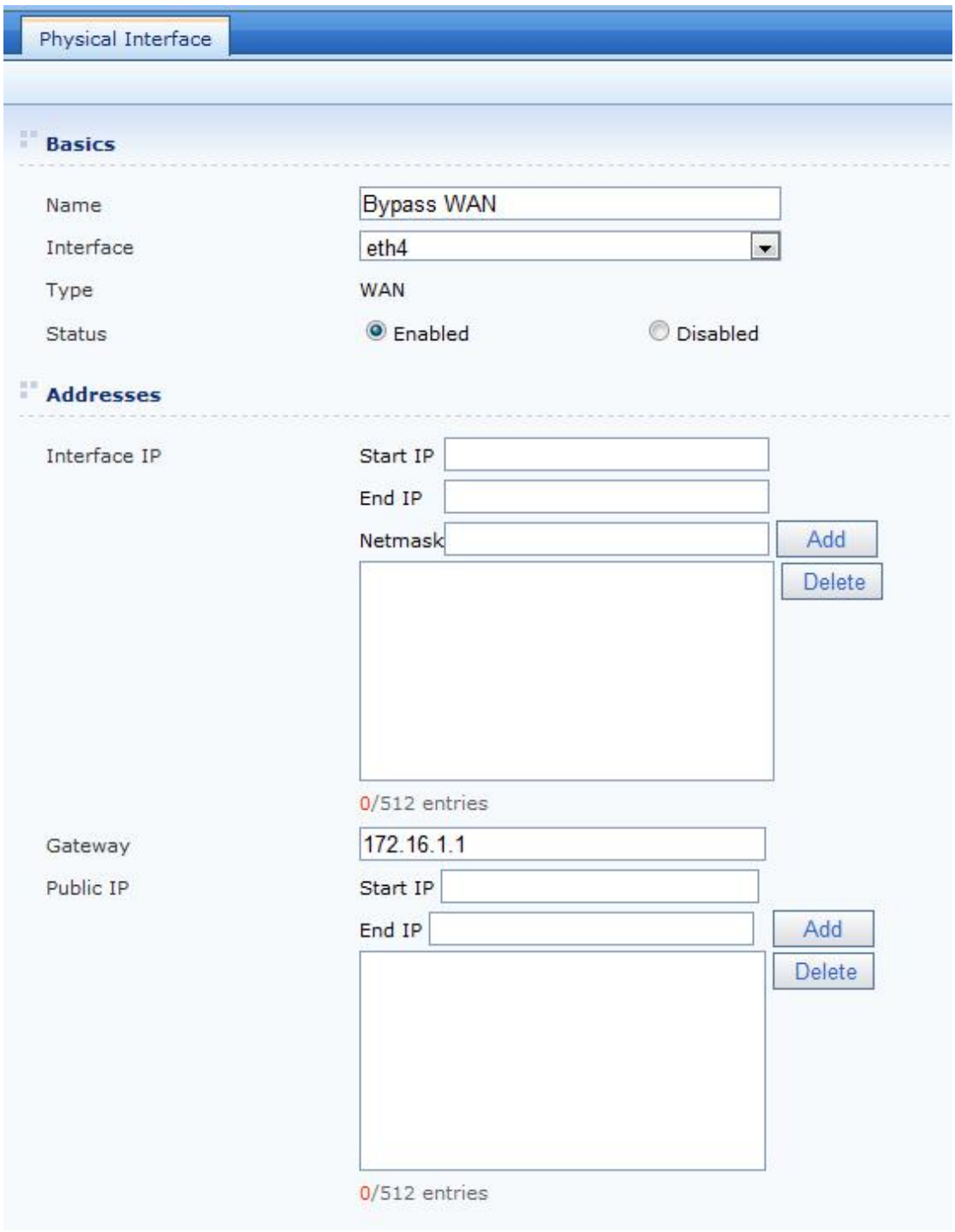
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

1. The WAN interface on ADC is on the same subnet as the servers.
2. The gateway of ADC is the same as that of servers, all directing to the front-end router.
3. Configure destination NAT policy on the firewall device located at the network egress to make the destination port mapped to the WAN interface on the ADC.

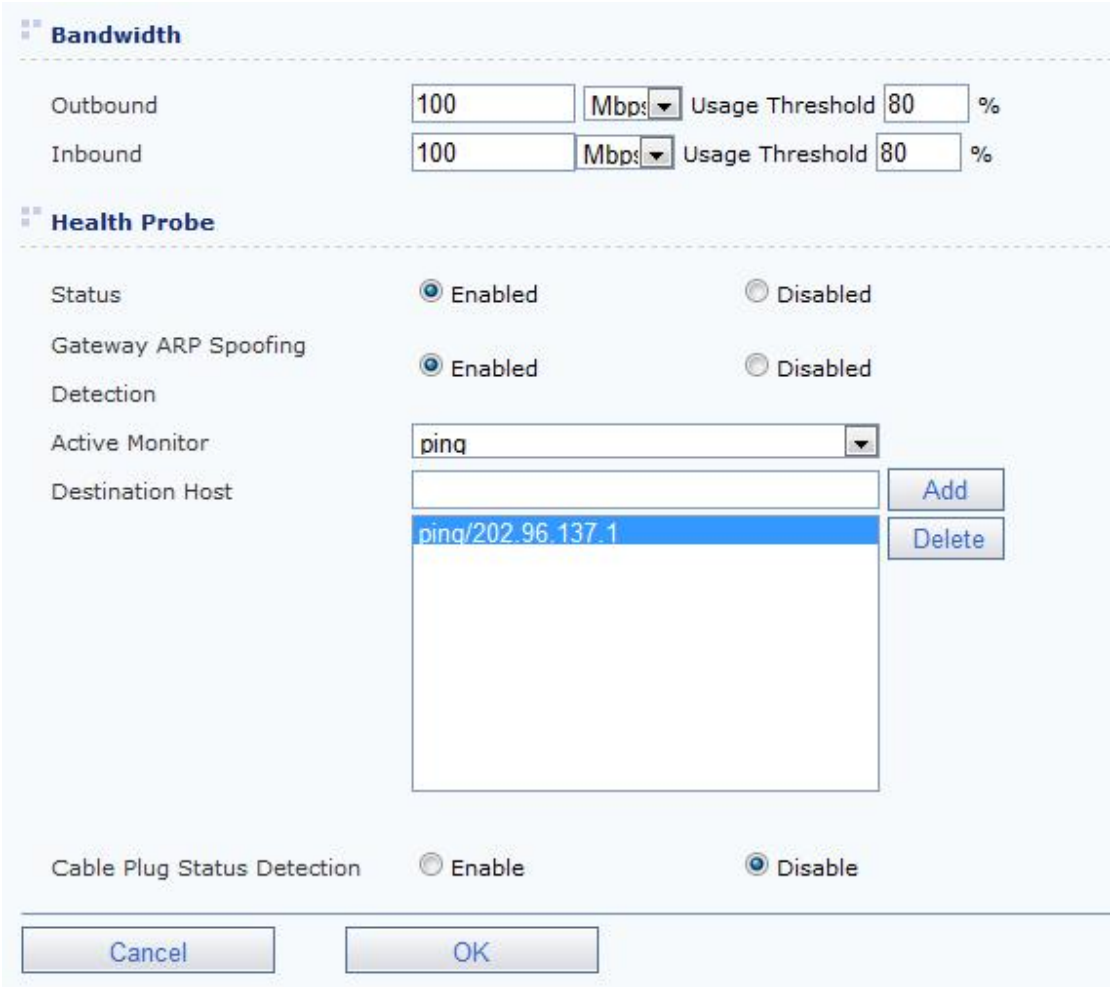
The detailed configuration steps are as follows:

1. Go to the **Network > Interface > Physical Interface** page, add a WAN interface as bypass WAN interface, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

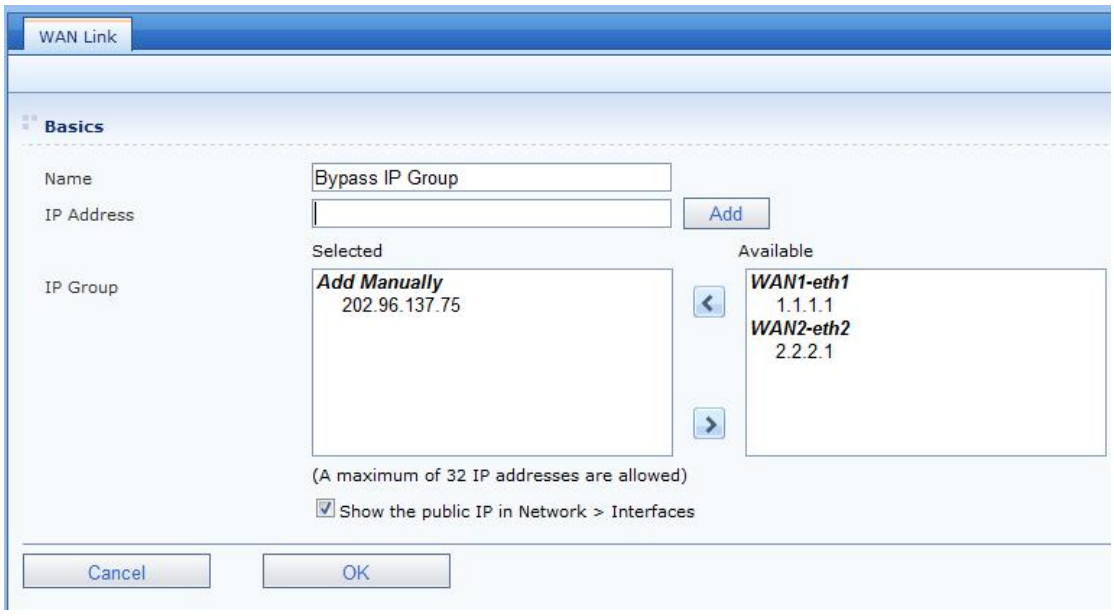


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



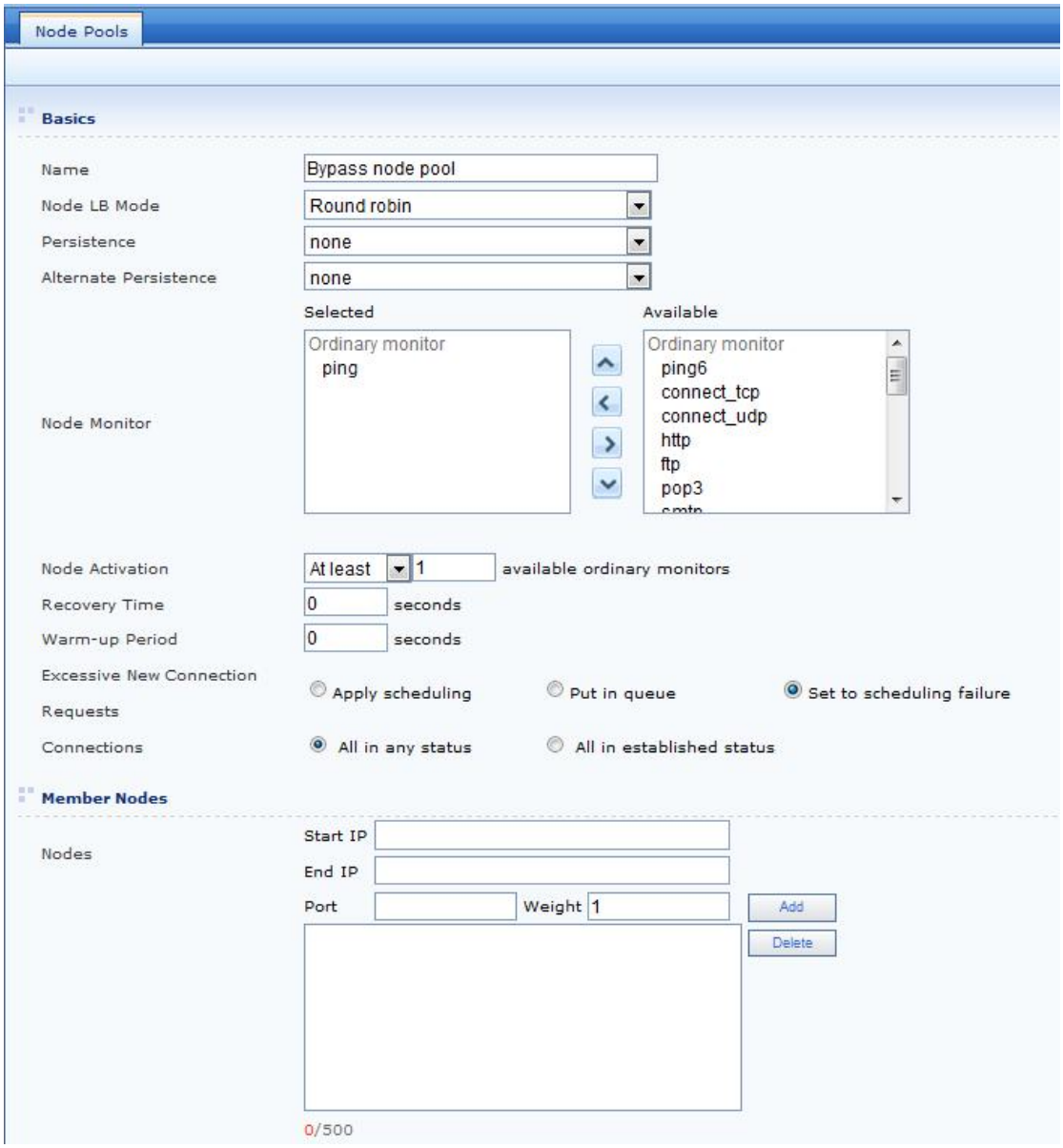
2. Go to the **Load Balancing > Service** page, and create a service. This step can be ignored for there is HTTP service on the ADC by default.

3. Go to the **Load Balancing > WAN Link** page, create a WAN link and then add the WAN links into the WAN link, as shown below:



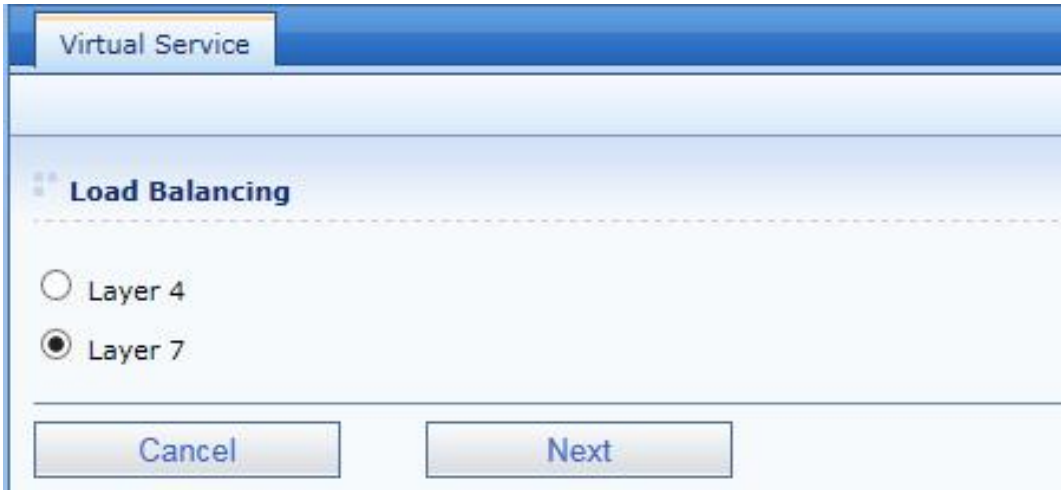
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

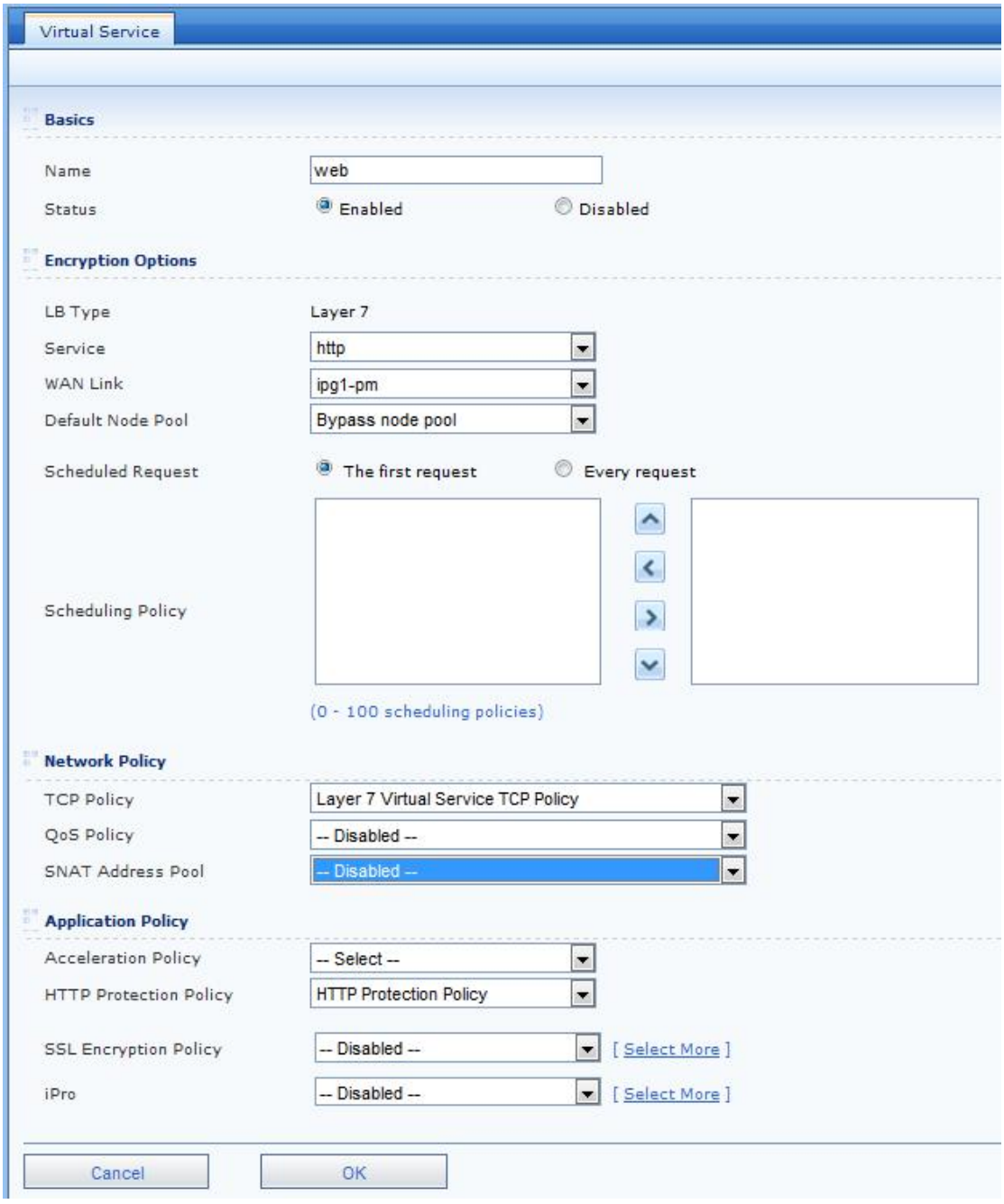
4. Create a node pool on the **Load Balancing > Node Pools** page.



5. Go to the **Load Balancing > Virtual Service** page, create a layer 7 virtual service, and associate the configured options as well, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

6. Go to the **Network > Source NAT** page, and set a source NAT policy to make the response packets from server flow through the ADC.

To save the changes, click **OK**.



When the ADC is deployed with bypass mode, the WAN interface on ADC does not need to be on the same subnet as the LAN server.

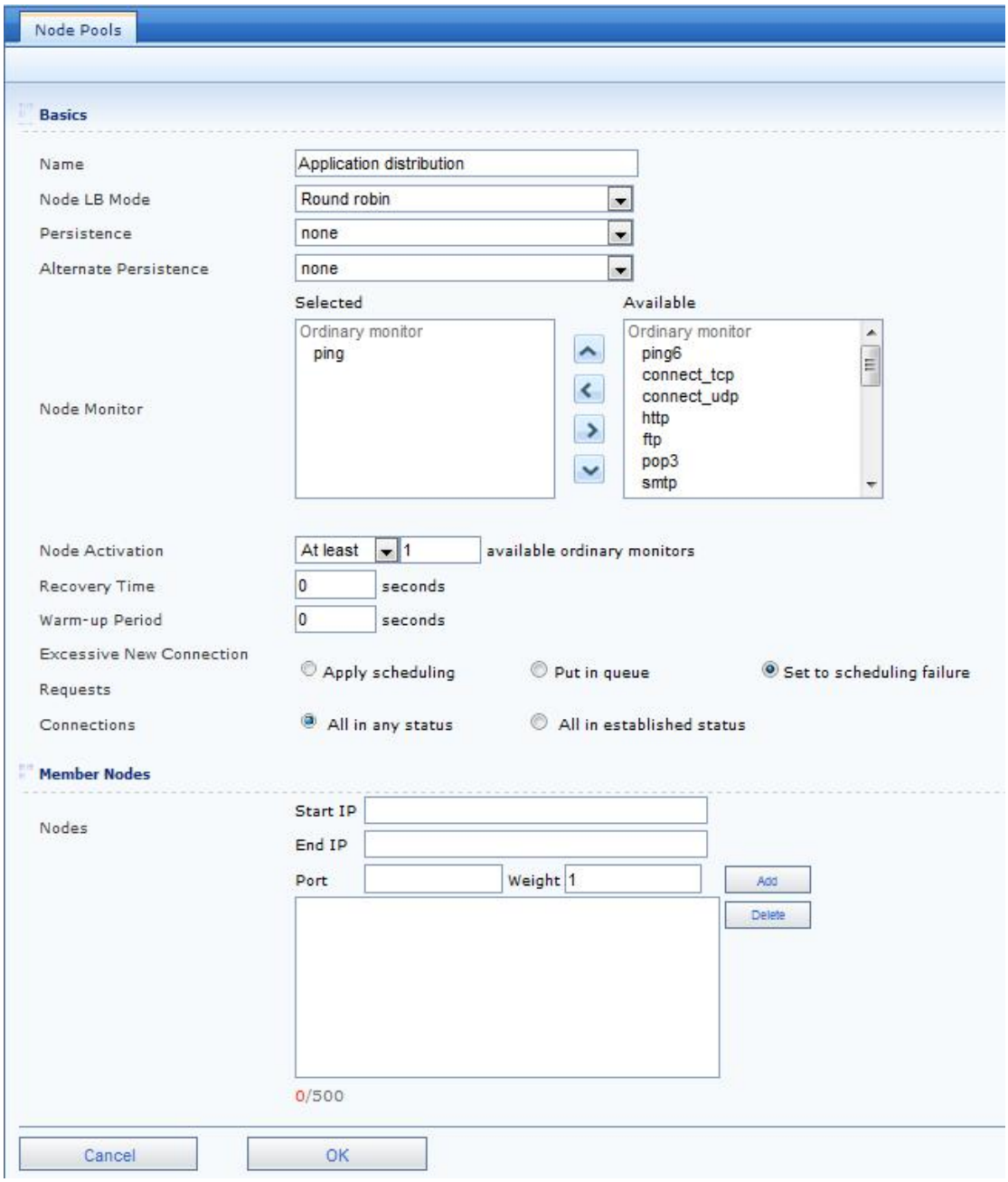
14.2 Server Load Balancing

Background: The ADC is deployed at the network egress in customer network. There are two LAN Web servers, and their access port are both 80. The ADC needs to load balances the servers with round robin method.

To load balances server, you can configure as follows:

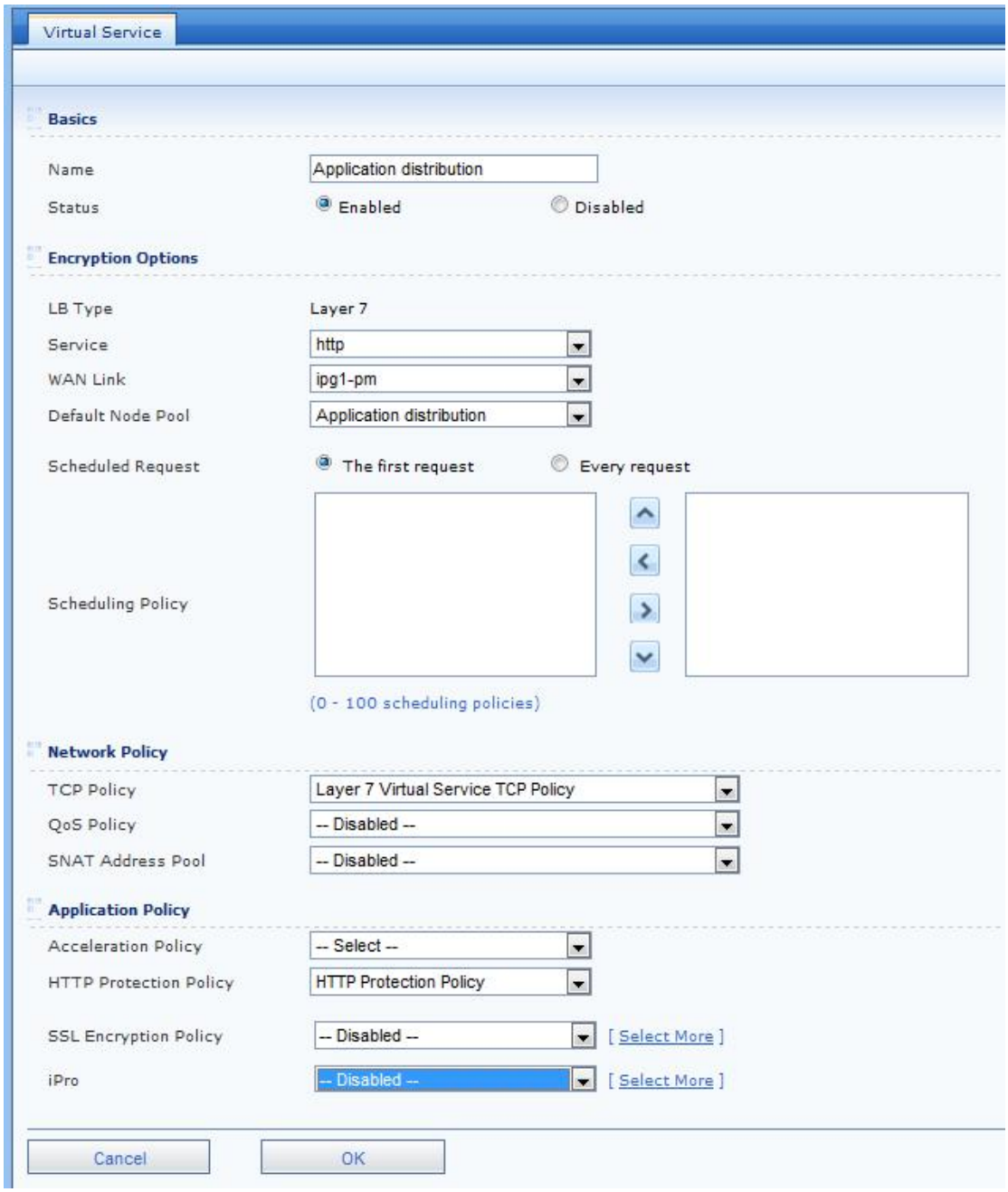
1. Refer to Chapter 7, **Configuring Service** for creating a service. This step can be ignored for there is HTTP service on the ADC by default.
2. Create a WAN link and add the WAN links to **IP Group** list. For how to configure the WAN link, please see Chapter 6, **Configuring WAN Link**.
3. Refer to Chapter 6, **Configuring Node Pool** for creating a node pool. Then add the IP address of the server into the **Nodes** list, and specify a node monitor and session persistence method (there is no session persistence method on the ADC by default. If you need to schedule node based on session persistence, you can set a session persistence method before). In **Node LB Mode** field, you can select **Round robin**, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



4. Go to the **Load Balancing > Virtual Service** page, and create a layer 7 virtual service, and associate the configured options as well, as shown below:

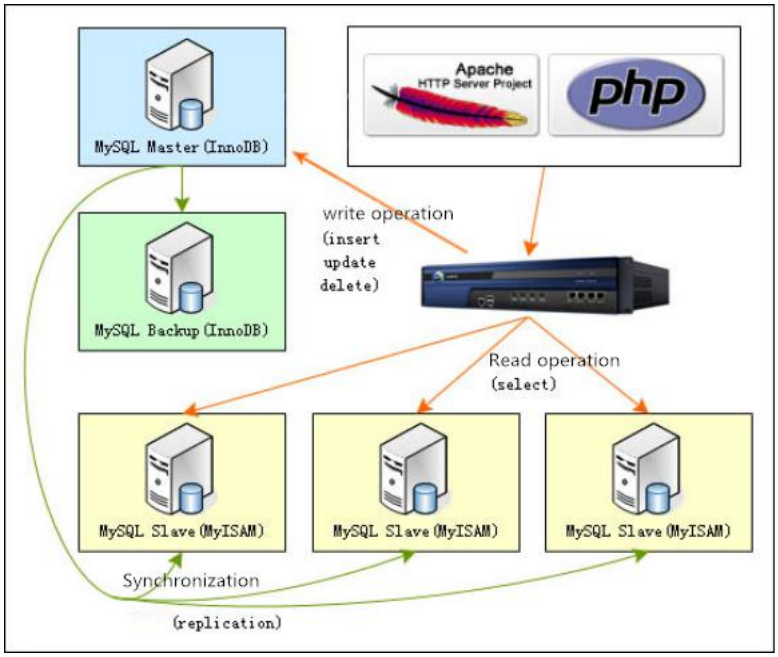
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



14.3 MySQL Database Load balance

Background: An active unit with several standby units, server version requires [5. 0, 5. 6]. The authentication is default authentication of MySQL. An additional function in AD6. 3 is load the database to improve the throughout concurrent of user servers. You can load the database by increasing devices but not modify the application structure to improve the throughout and concurrent.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



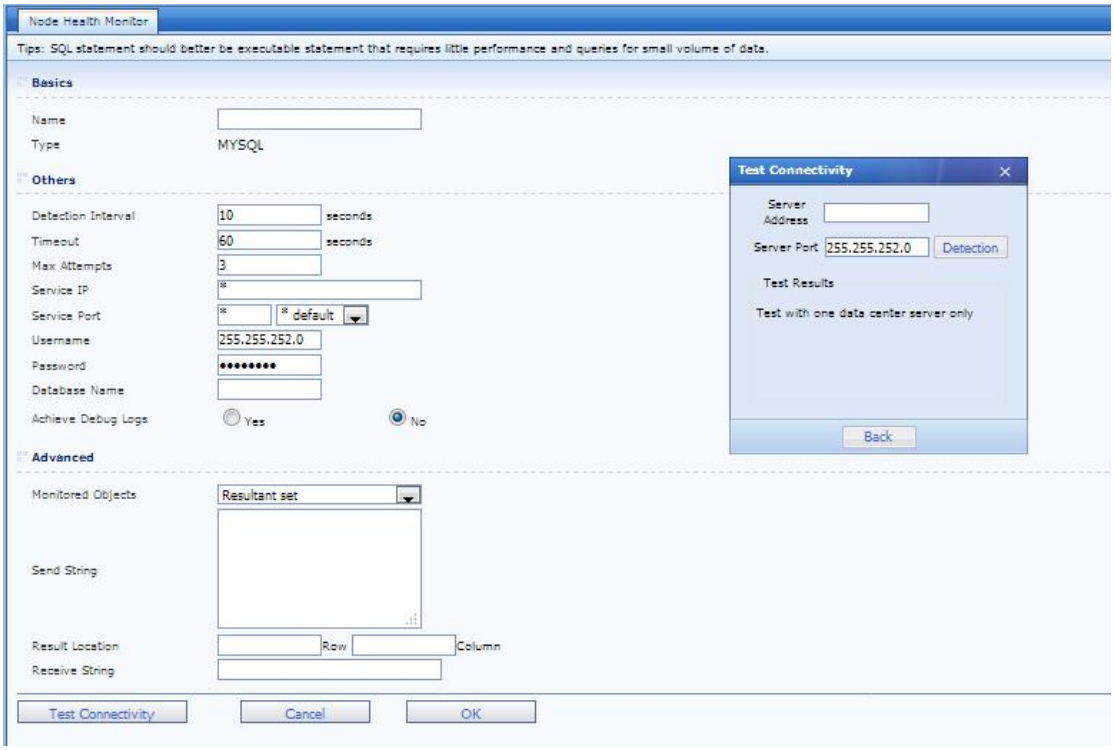
To load MySQL Database, you can configure as follows:

Management IP of ADC: 10. 252. 252. 68

Database Host IP: 10. 250. 66. 12

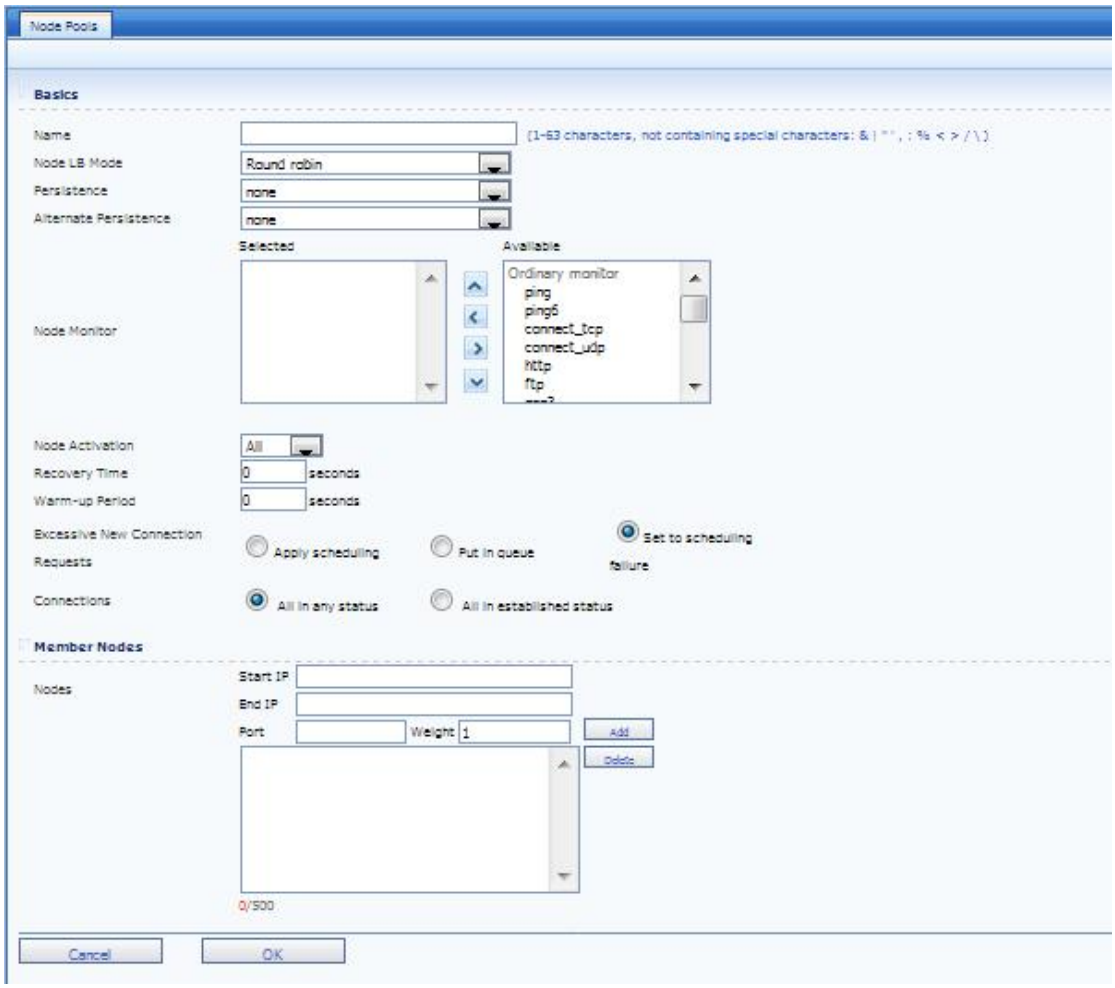
Database Host IP: 10. 250. 66. 13

1. Configure master node monitor



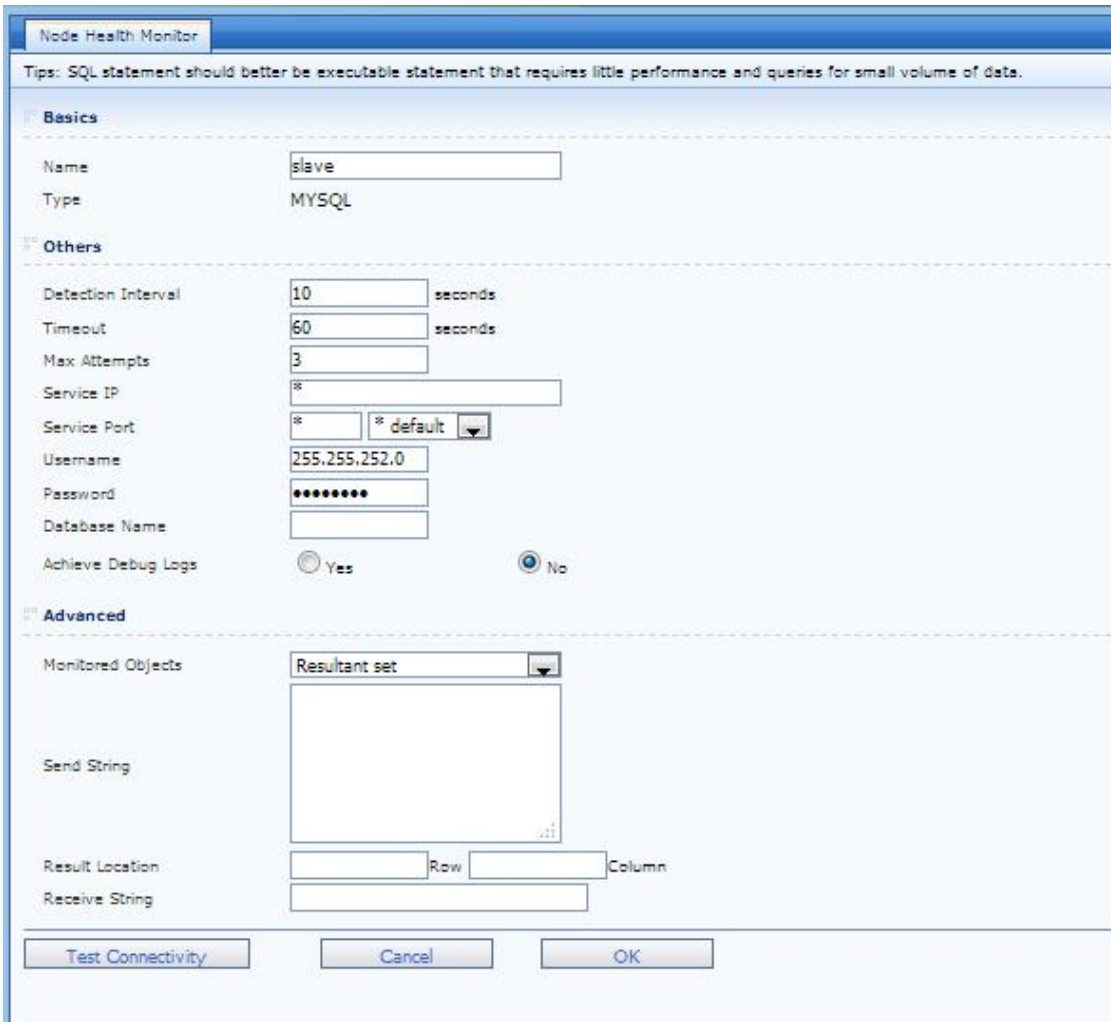
2. Configure master node pool

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



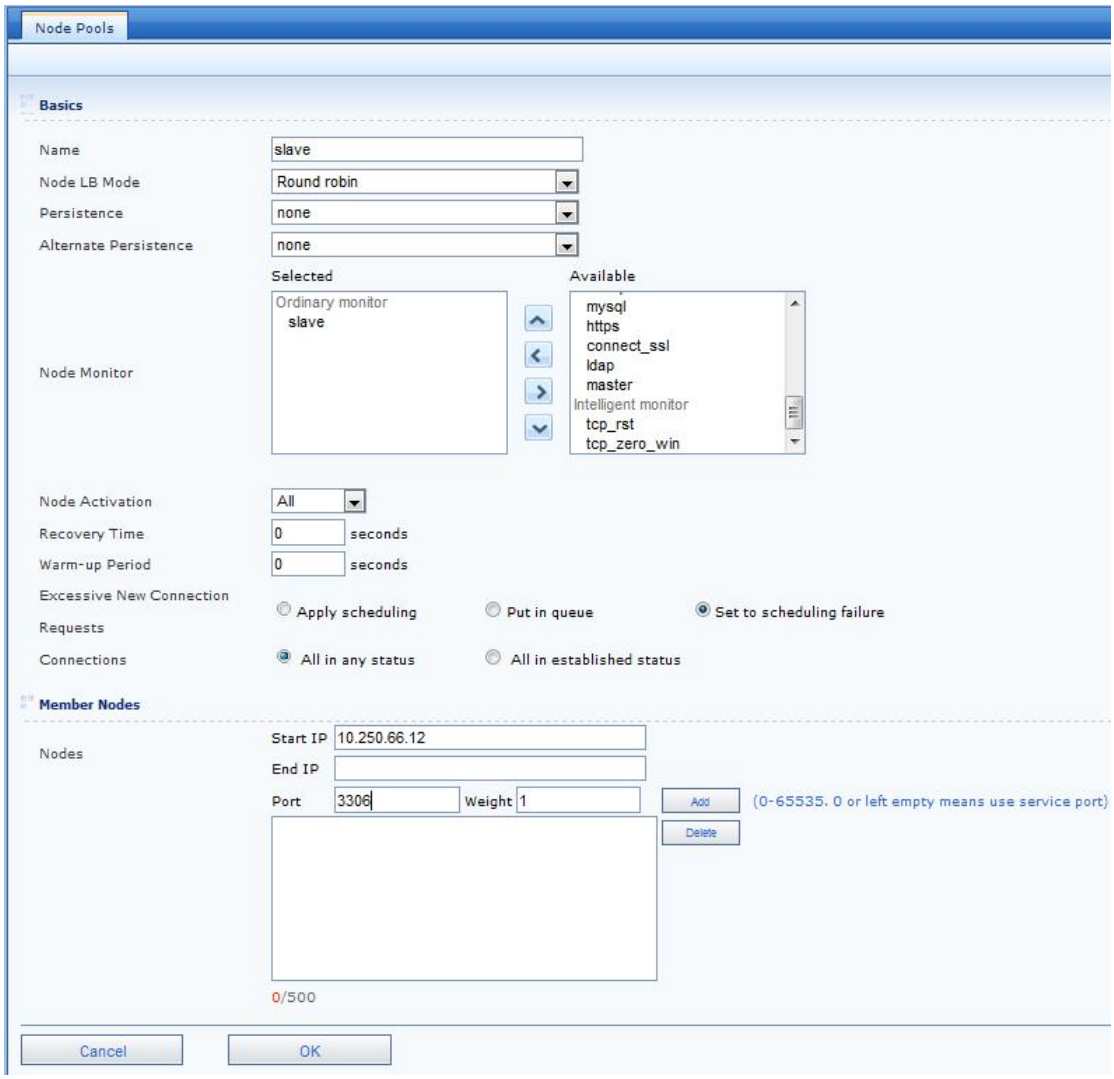
3. Configure slave node modifier

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



4. Configure slave node pool

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



5. Configure WAN interface and LAN interface

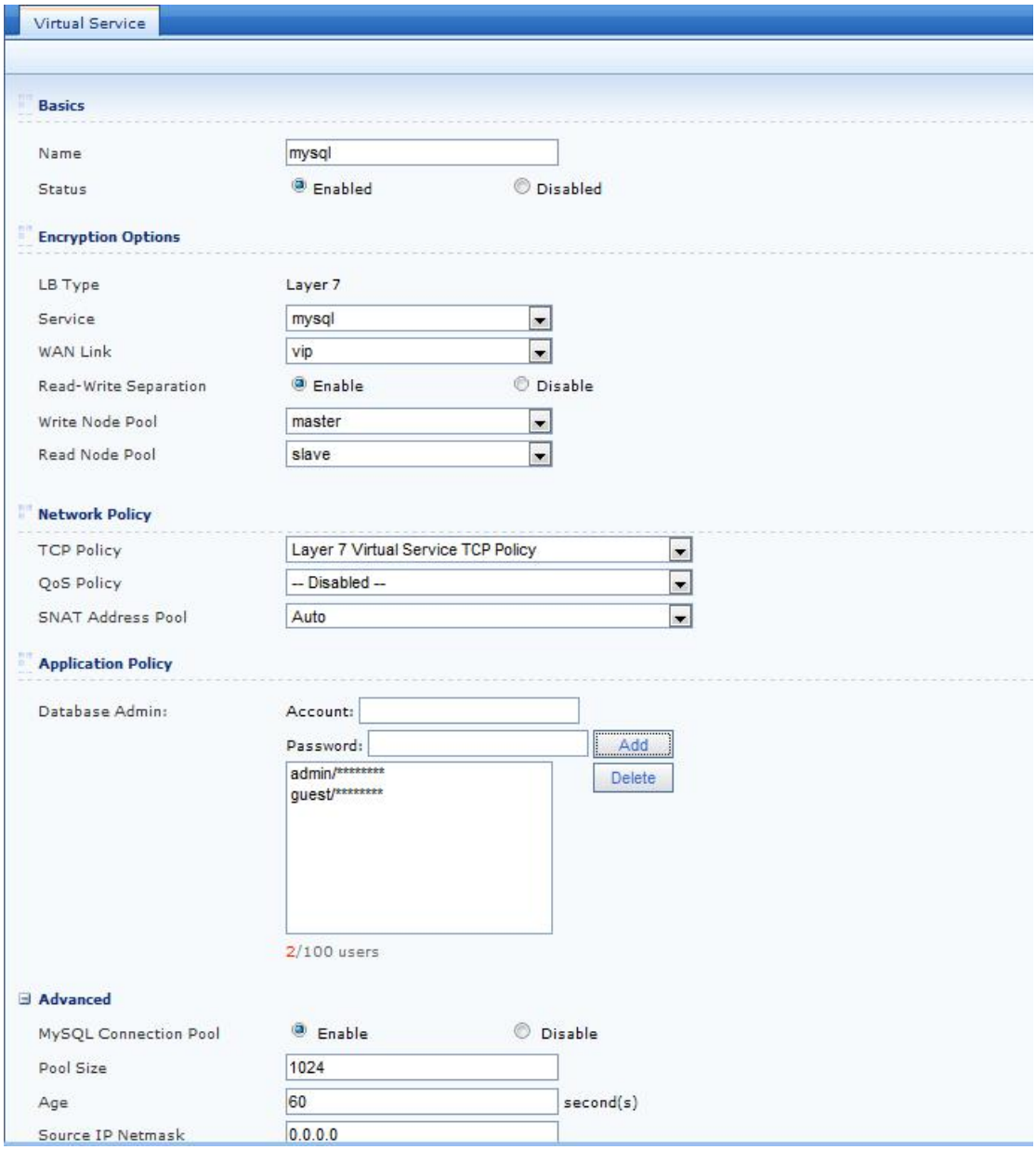
Name	Interface	IP Address	Outbound	Inbound	Type
lan1	eth3	192.170.1.145			LAN
WAN1-eth1	eth1	1.1.1.1	100.00Mbps	100.00Mbps	WAN
WAN2-eth2	eth2	2.2.2.1	100.00Mbps	100.00Mbps	WAN

6. Create vip

Name	Interface	IP Address
vip	eth3	10.250.67.89

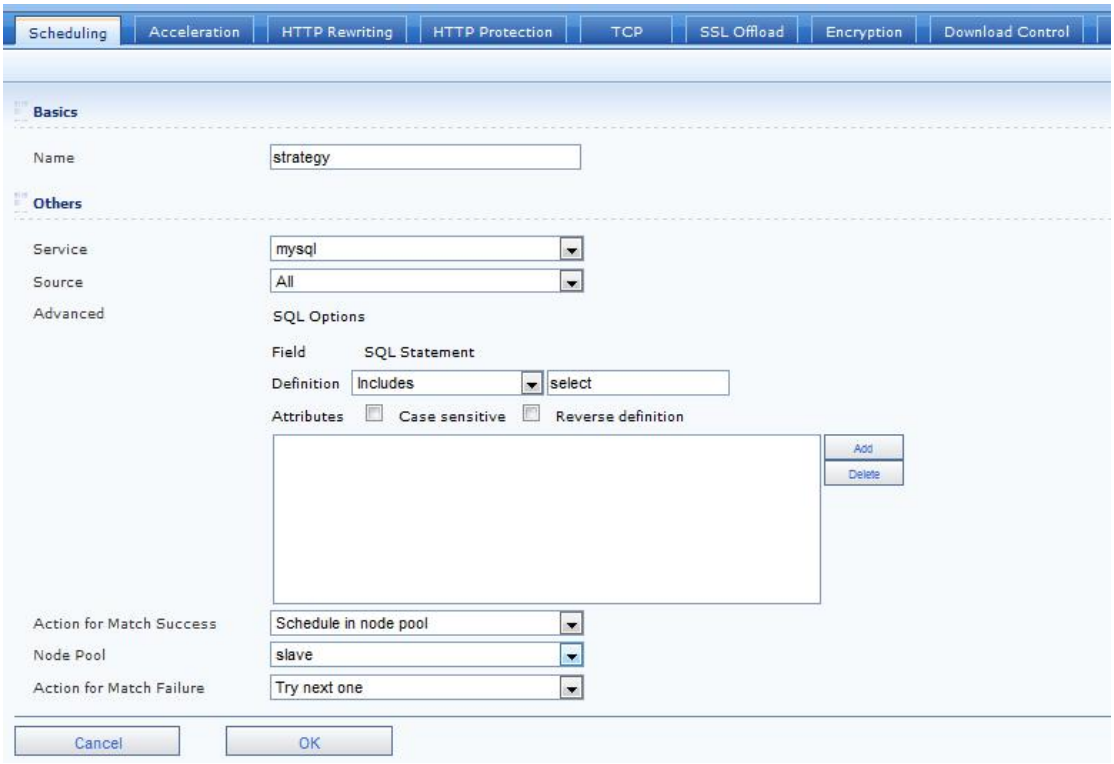
7. Configure virtual service

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



8. Separate read and write using scheduling policy

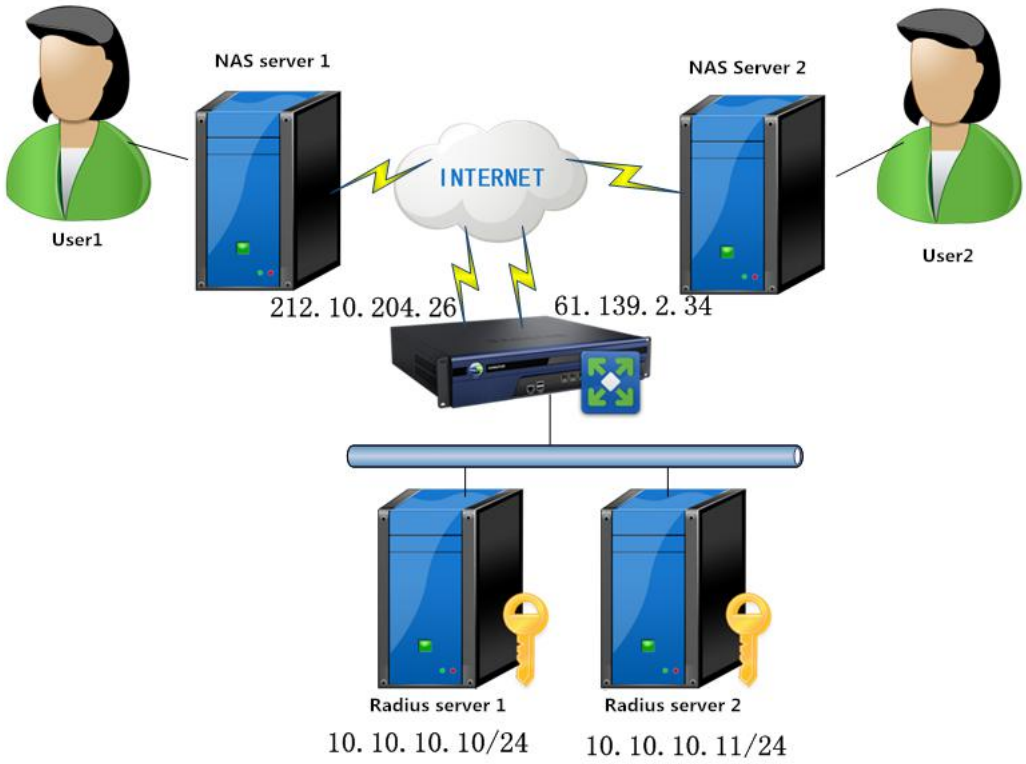
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



14.4 Radius Server Load Balance

Background: There are a few Radius servers in customer network. When authenticating users, the authentication request will be forwarded to NAS and then sent to Radius server. The ADC will achieve session persistence based on NAS-IP-ADDRESS in the request. If the NAS-IP-ADDRESS is IP1, the request should be scheduled to NAS server 1; If the NAS-IP-ADDRESS is IP2, the request should be scheduled to NAS server2.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Configuration steps are as follows:

1. Go to the **Load Balancing > Service** page, and create a Radius authentication service, including specifying service type and service port. This step can be ignored, due to the existence of Radius authentication service on ADC by default.

Service

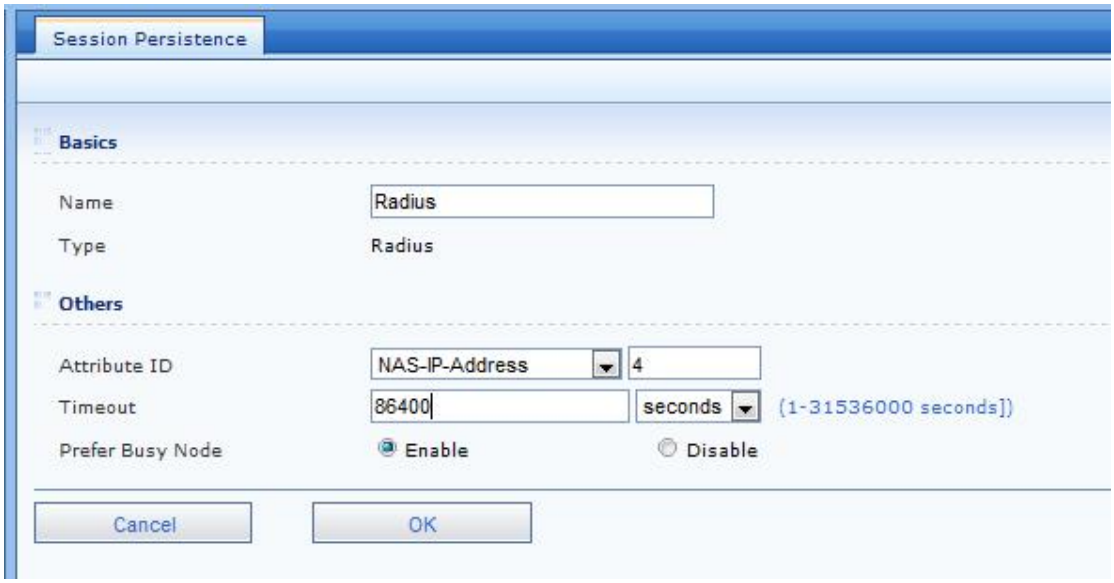
Add Delete

Name	Type	Port
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

2. Go to the **Load Balancing > WAN Link** page, create a **WAN Link** and move the WAN links from **Available** box into **Selected** box, as shown below:

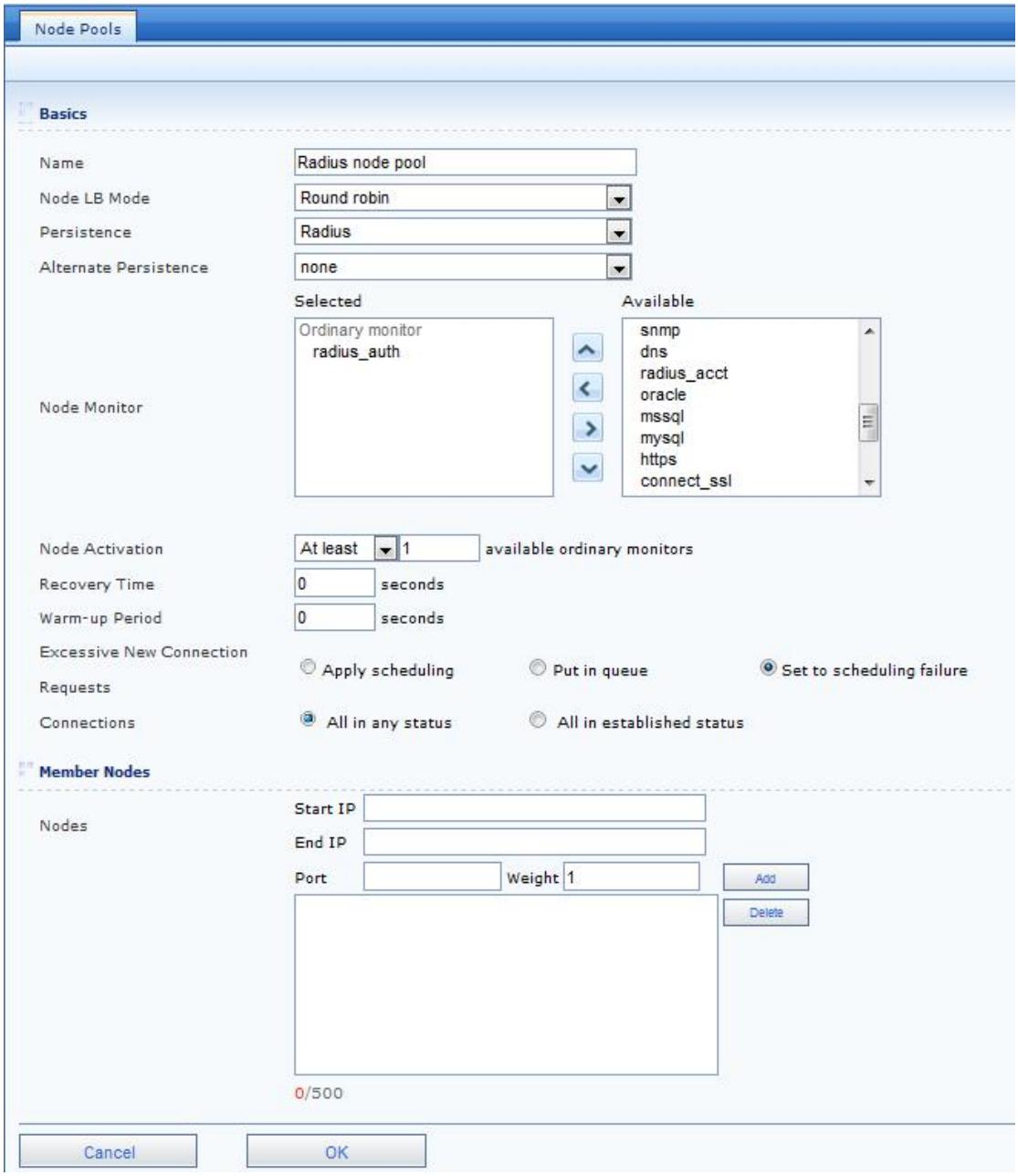
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

3. Go to **Load Balancing > Persistence > Session Persistence** page, and create a session persistence based on **Radius**, as shown in the following figure:



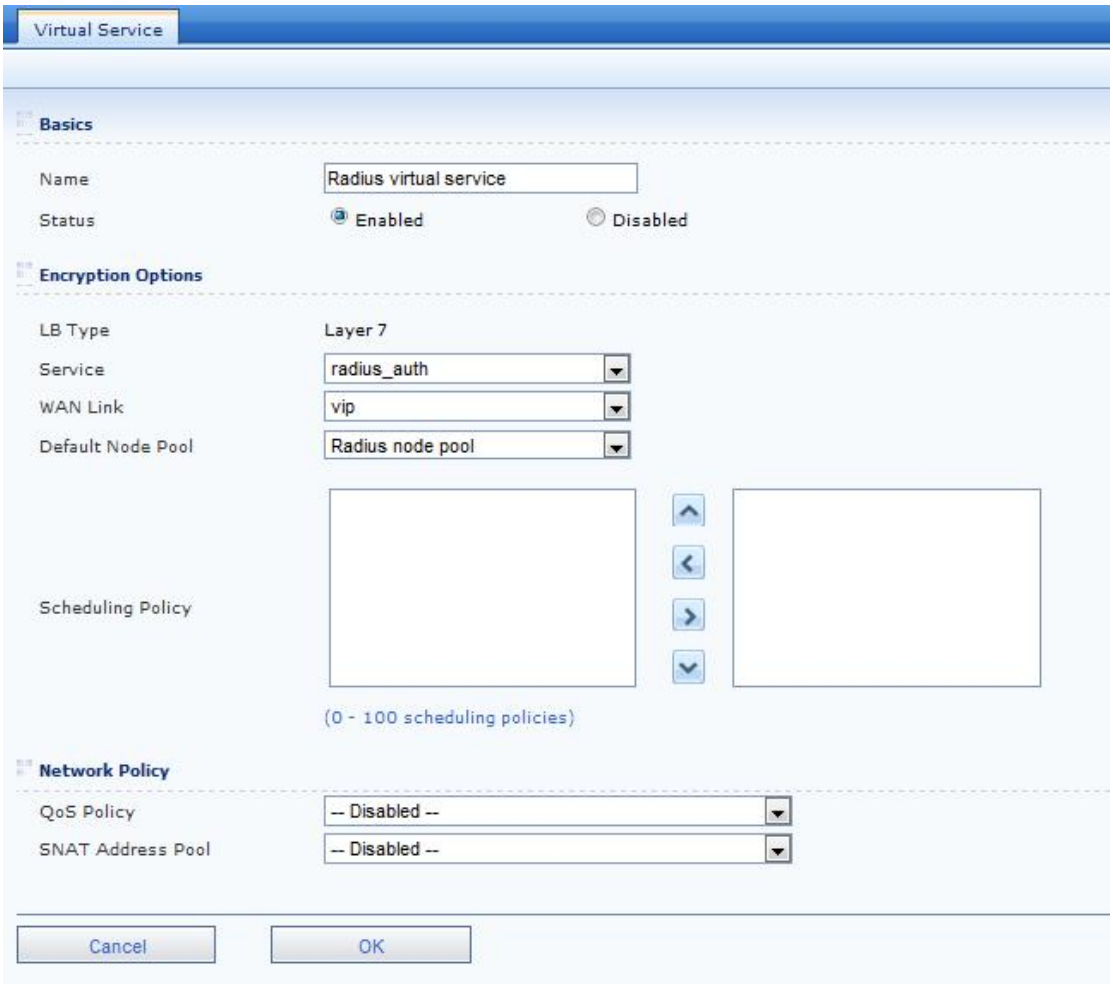
4. Create a node pool on the **Load Balancing > Node Pools** page, and then add the IP addresses of the servers into the node pool, and specify a node monitor and session persistence method. In **Node LB Mode** field, you can select **Round robin**, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



5. Go to the **Load Balancing > Virtual Service** page, create a layer 7 virtual service, and associate the configured options as well, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





If you want to configure a virtual service for accounting RADIUS, please create a radius_acct virtual service as the above configuration steps again. Please note that when configure that virtual service, the session persistence method and node pool should be the same as the the one configured above.

14.5 Get Client IP

Background: The ADC is deployed in bypass mode. There are two LAN Web servers, and their access port are both 80. The ADC needs to load balances the servers by round robin method, and optimize the access to client. Web server needs to obtain the source IP address of real client.

Configuration steps are as follows:

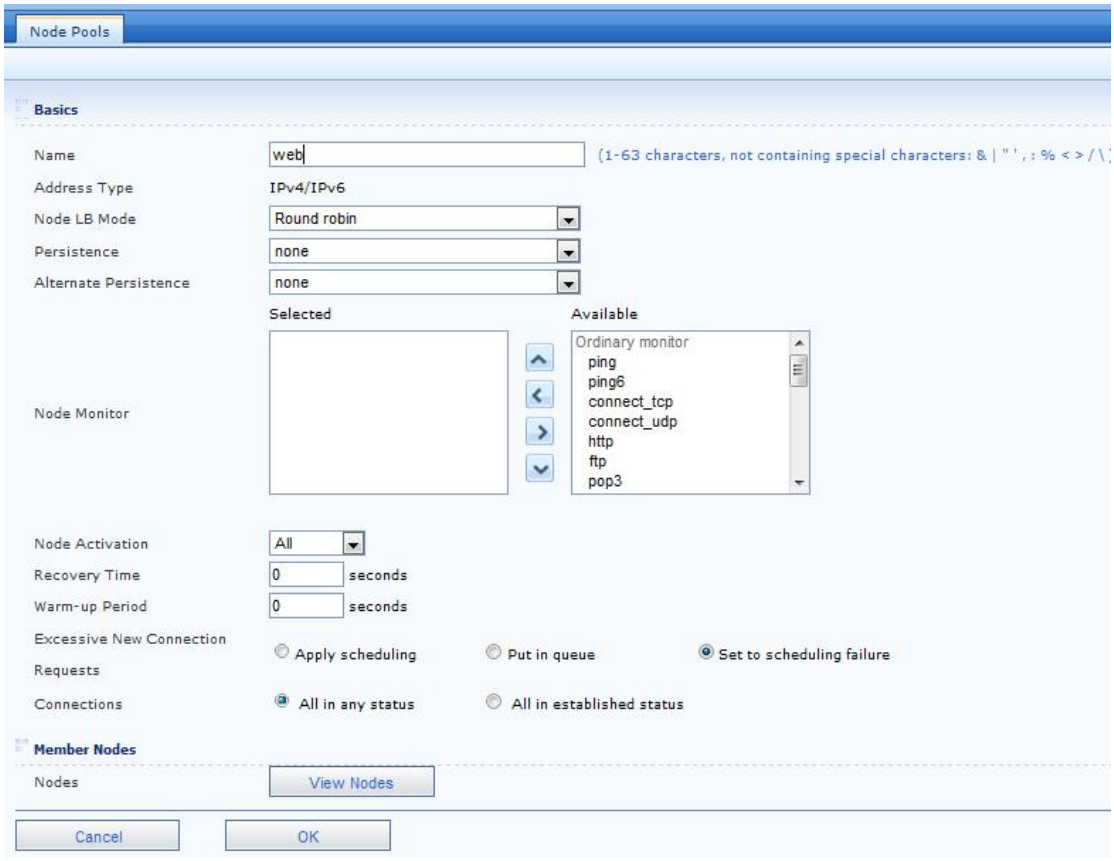
1. Refer to Chapter 7, **Configuring Service** for creating a service. This step can be ignored

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

for there is HTTP service on the ADC by default.

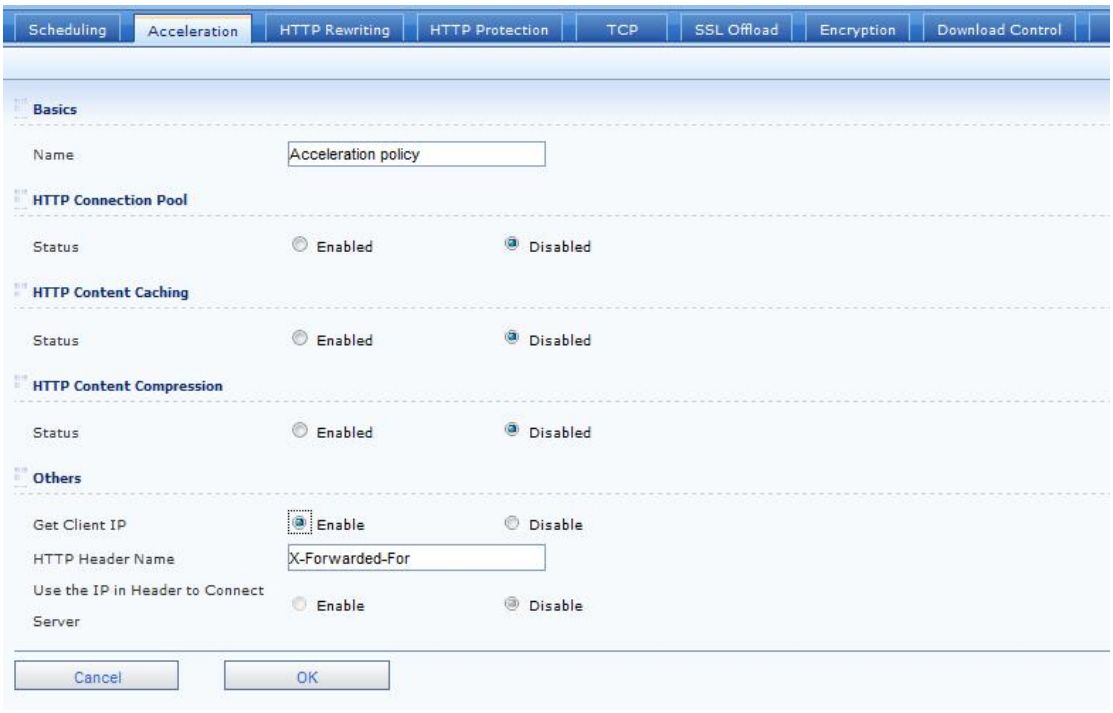
2. Create a WAN link and add the WAN links to **IP Group** list. For how to configure the WAN link, please see Chapter 6, **Configuring WAN Link**.

3. Refer to Chapter 6, **Configuring Node Pool** for creating a node pool. Then add the IP address of the server into the **Nodes** list, and specify a node monitor. In **Node LB Mode** field, you can select **Round robin**, as shown below:



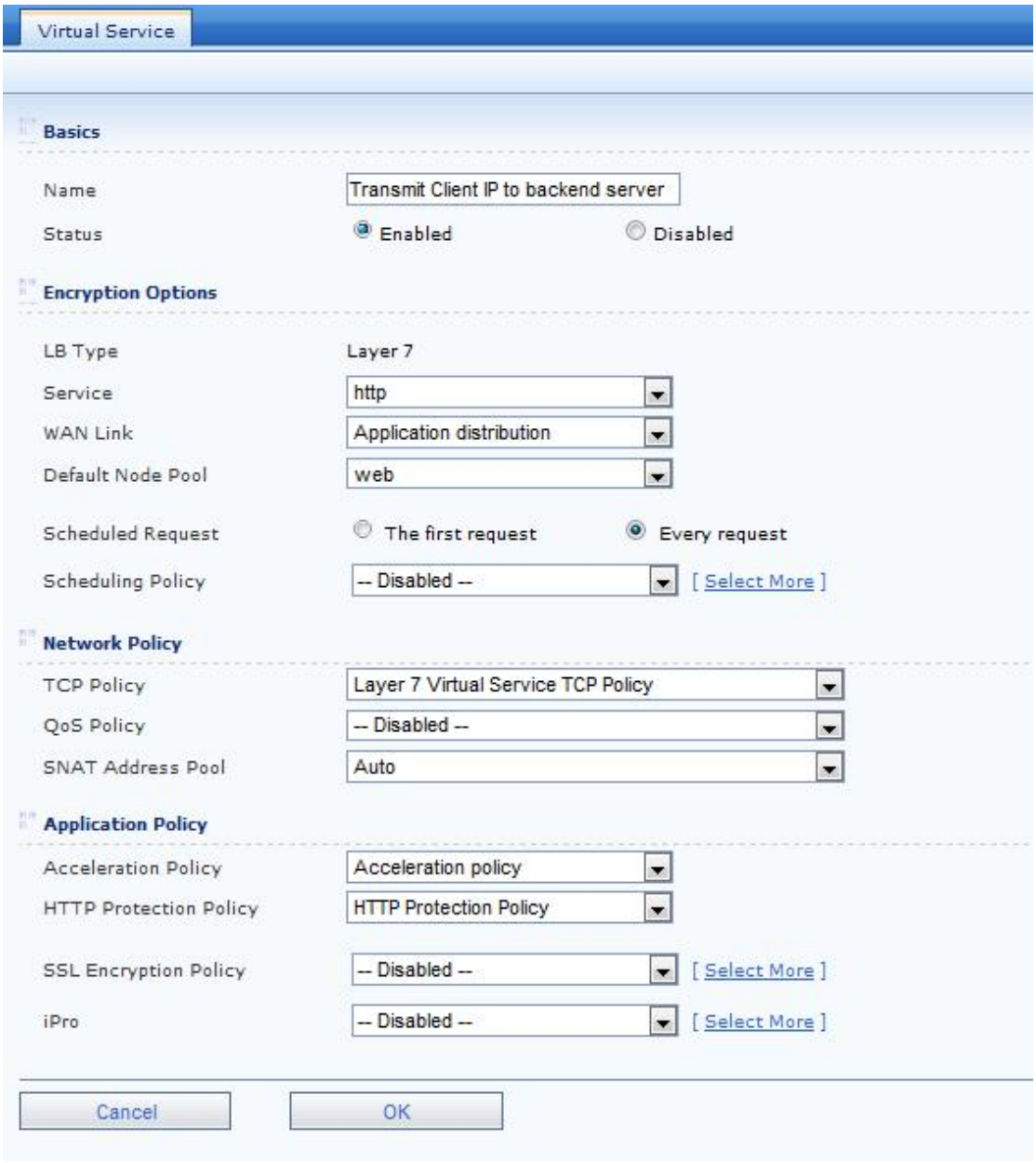
4. Refer to Chapter 6, **Configuring Acceleration Policy** for creating a acceleration policy and and enable **Get Client IP** option, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



5. Refer to Chapter 6, **Configuring Virtual Service** to create a layer 7 virtual service, and associate the configured options, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



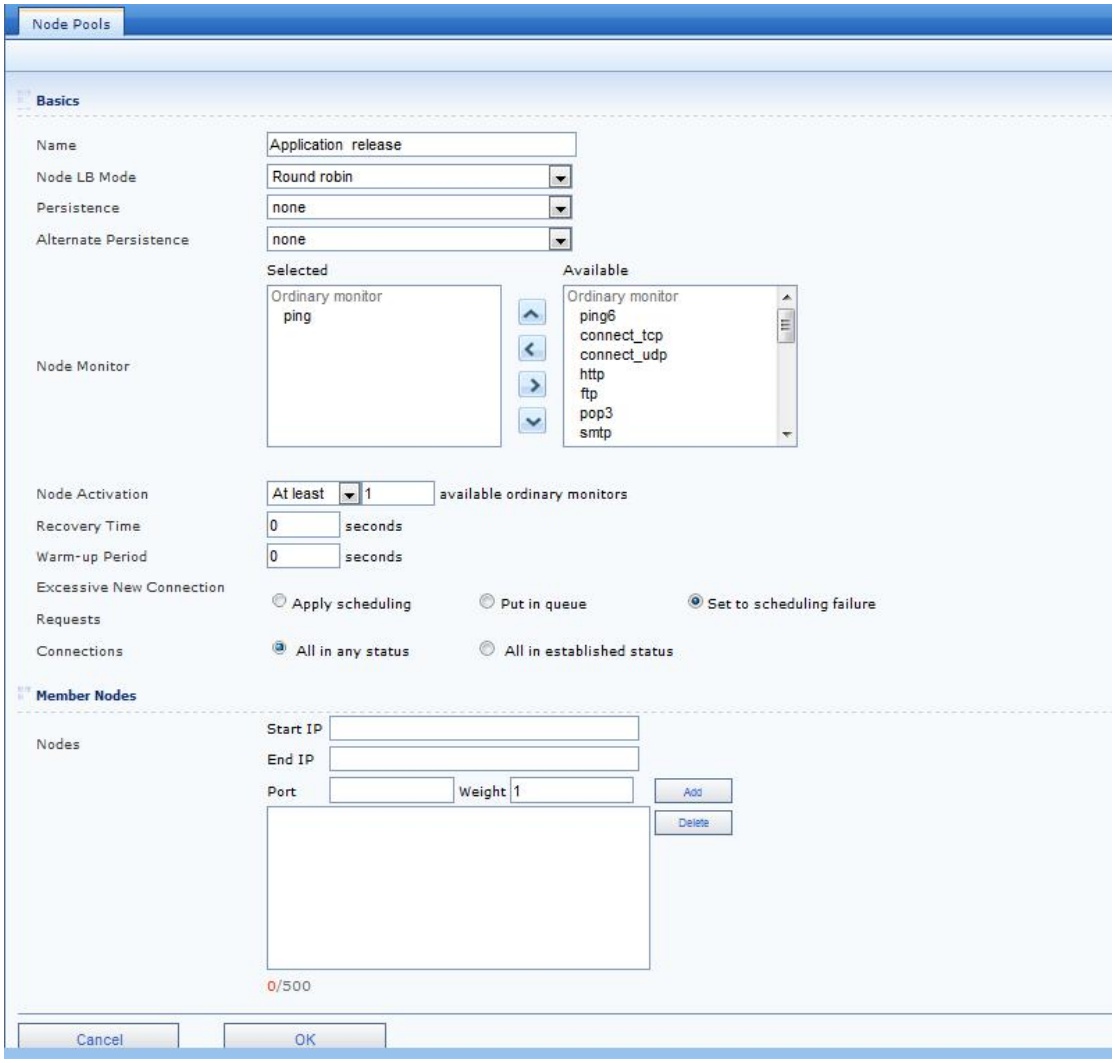
14.6 Inbound Scheduling Policy

Background: There are two LAN Web servers: A and B, which provide the same domain name service, and their access port are both 80. The domain name is sangfor. com. The ADC can load balances the servers with round robin method. The performance of serve A is higher than that of server B. The requests from special IP address 202. 96. 130. 36 need to be scheduled to server A always.

Configuration steps are as follows:

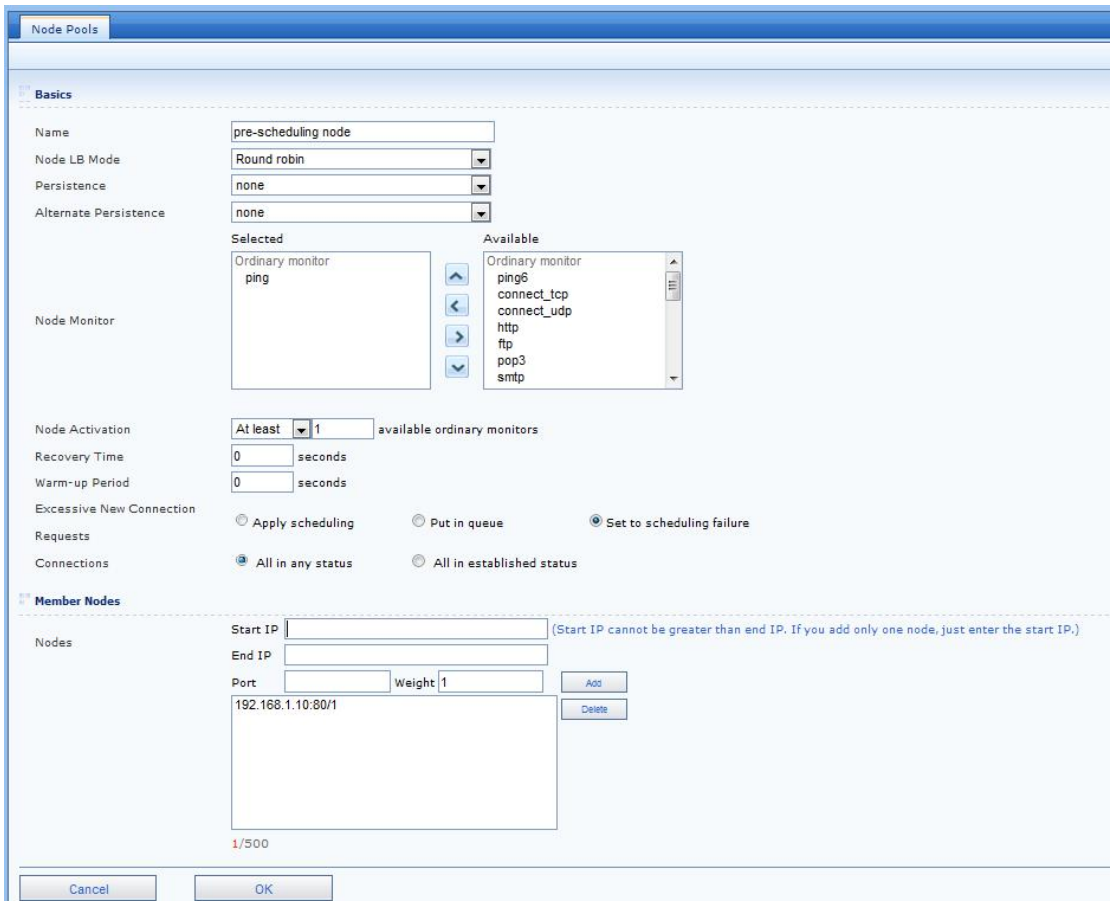
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

1. Refer to Chapter 6, **Configuring Service** to create a service. This step can be ignored for there is HTTP service on the ADC by default.
2. Create a WAN link and add the WAN links to **IP Group** list. For how to configure the WAN link, please see Chapter 6, **Configuring WAN Link**.
3. Refer to Chapter 6, **Configuring Node Pool** for creating a node pool. Then add the IP address of the server into the **Nodes** list, and specify a node monitor. In **Node LB Mode** field, you can select **Round robin**, as shown below:



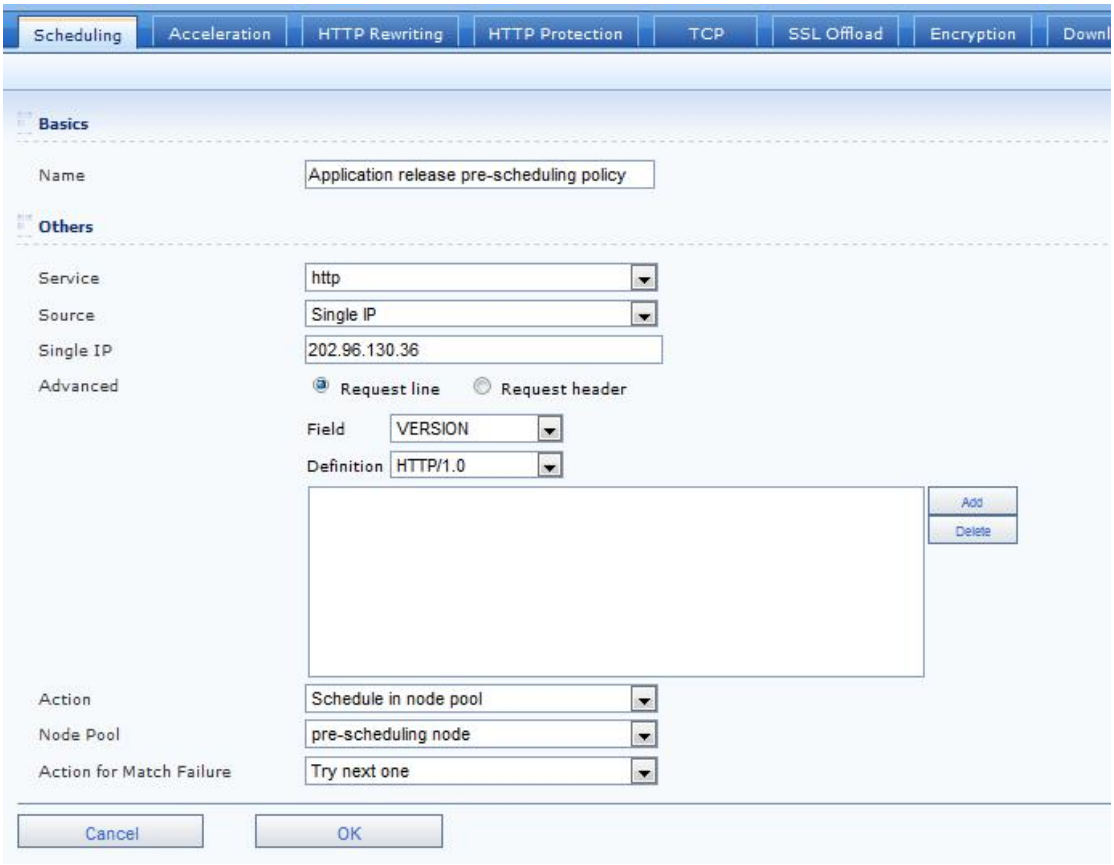
4. See Chapter 6, **Configuring Node Pool** to create a node pool. Then add the IP address of the server A into the node pool, and specify a node monitor. In **Node LB Mode** field, you can select **Round robin**, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



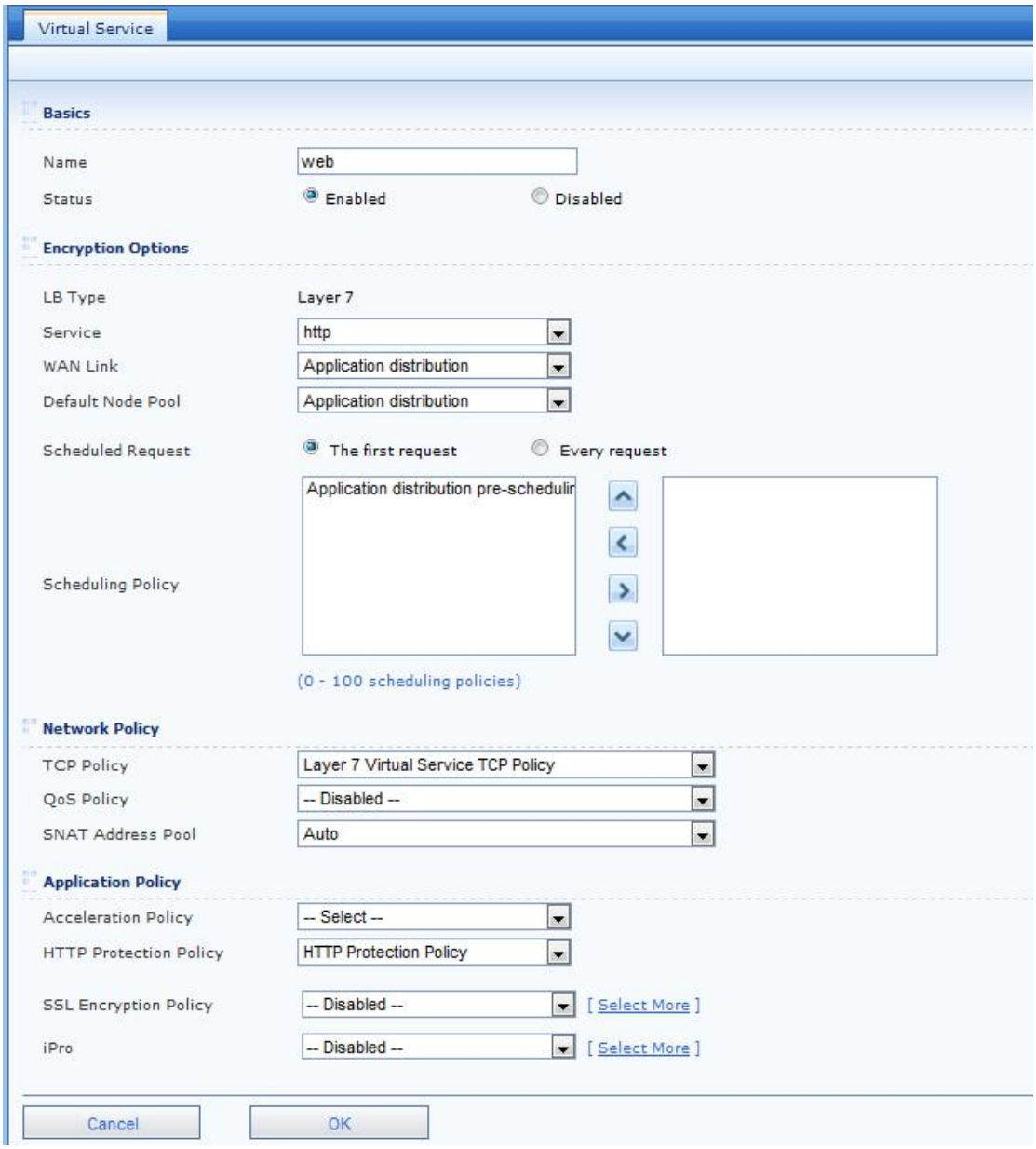
5. Refer to Chapter 6, **Configuring Scheduling Policy** to create a scheduling policy, select a service and source IP range. **Advanced** fieldis not required. For **Node Pool** field, you can select the one configured in the fouth step; In **Action for Match Failure** filed, select **Try next One**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



6. See Chapter 6, **Configuring Virtual Service** to create a layer 7 virtual service, and associate the configured options as well, as shown below:

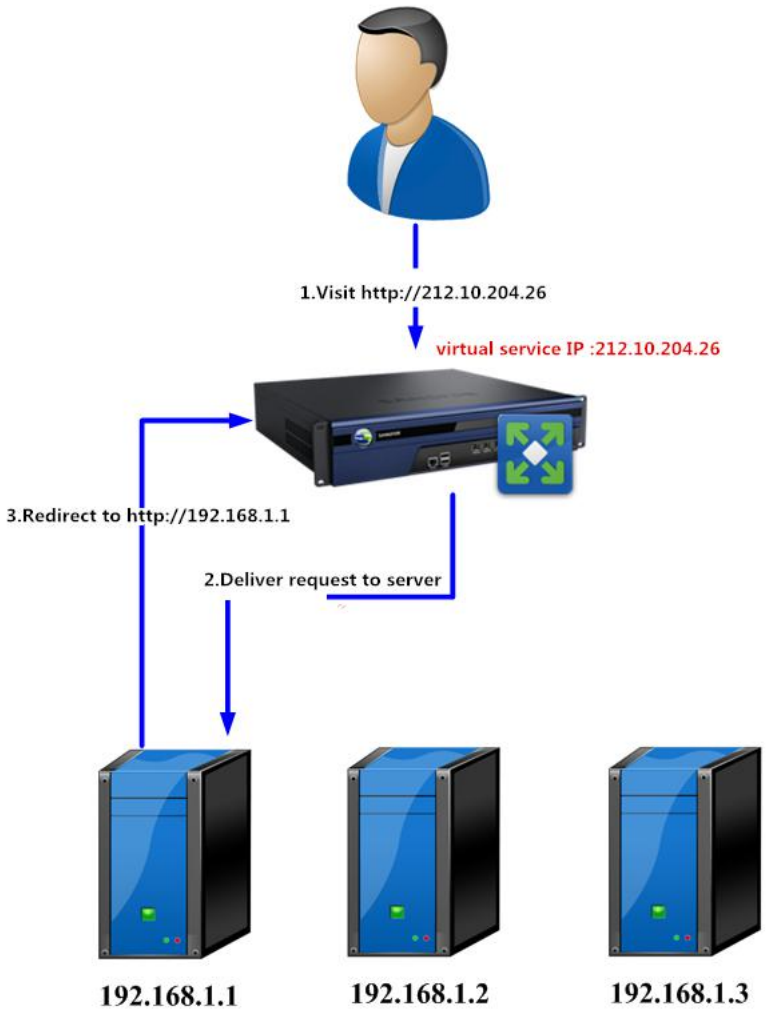
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



14.7 HTTP Rewriting Case

There are a number of HTTP servers providing Web service in customer network. The ADC can implement balancing the load on the servers. When clients access root directory of a website http: //212. 10. 204. 26, the back-end server will redirect the access to local directory http: //192. 168. 1. 1/login of the node's IP, leading to the client unable to access. It's necessary to rewrite the HTTP response header of back-end server, that's to rewrite http: //192. 168. 1. 1/login to http: //212. 10. 204. 26/login. To make subsequent requests from user scheduled to 192. 168. 1. 1, you need to configure HTTP rewriting policy.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Configuration steps are as follows:

1. Go to the **Load Balancing > Service** page, and create a HTTP-based service. This step can be ignored.

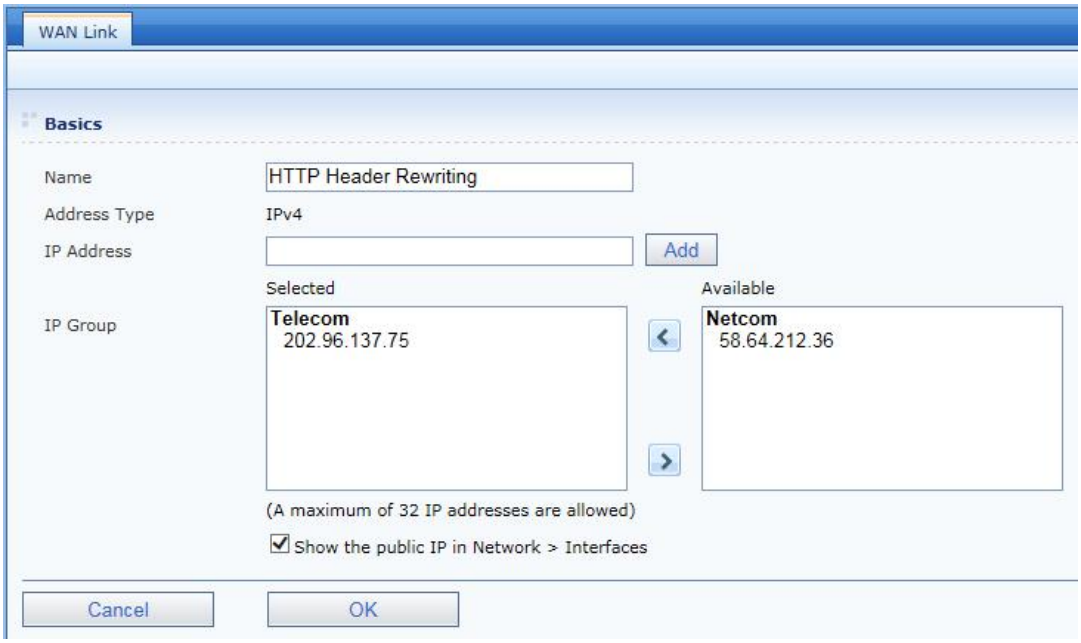
Service

Add Delete

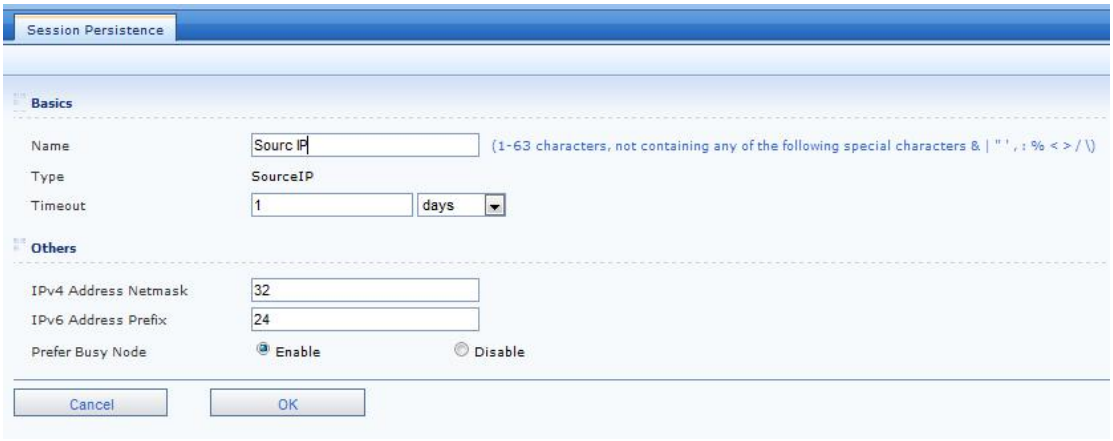
Name	Type	Port
http	HTTP	80
smtp	TCP	25
pop3	TCP	110
dns	DNS	53
https	HTTPS	443
ssl	SSL	443
imap_ssl	SSL	993
smtp_ssl	SSL	465
pop3_ssl	SSL	995
radius_auth	RADIUS	1812
radius_acct	RADIUS	1813
ftp	FTP	21

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

2. Go to the **Load Balancing > WAN Link** page, create a WAN link, and move the selected the WAN link IP address from **Available** box to **Selected** box, as shown in the following figure:

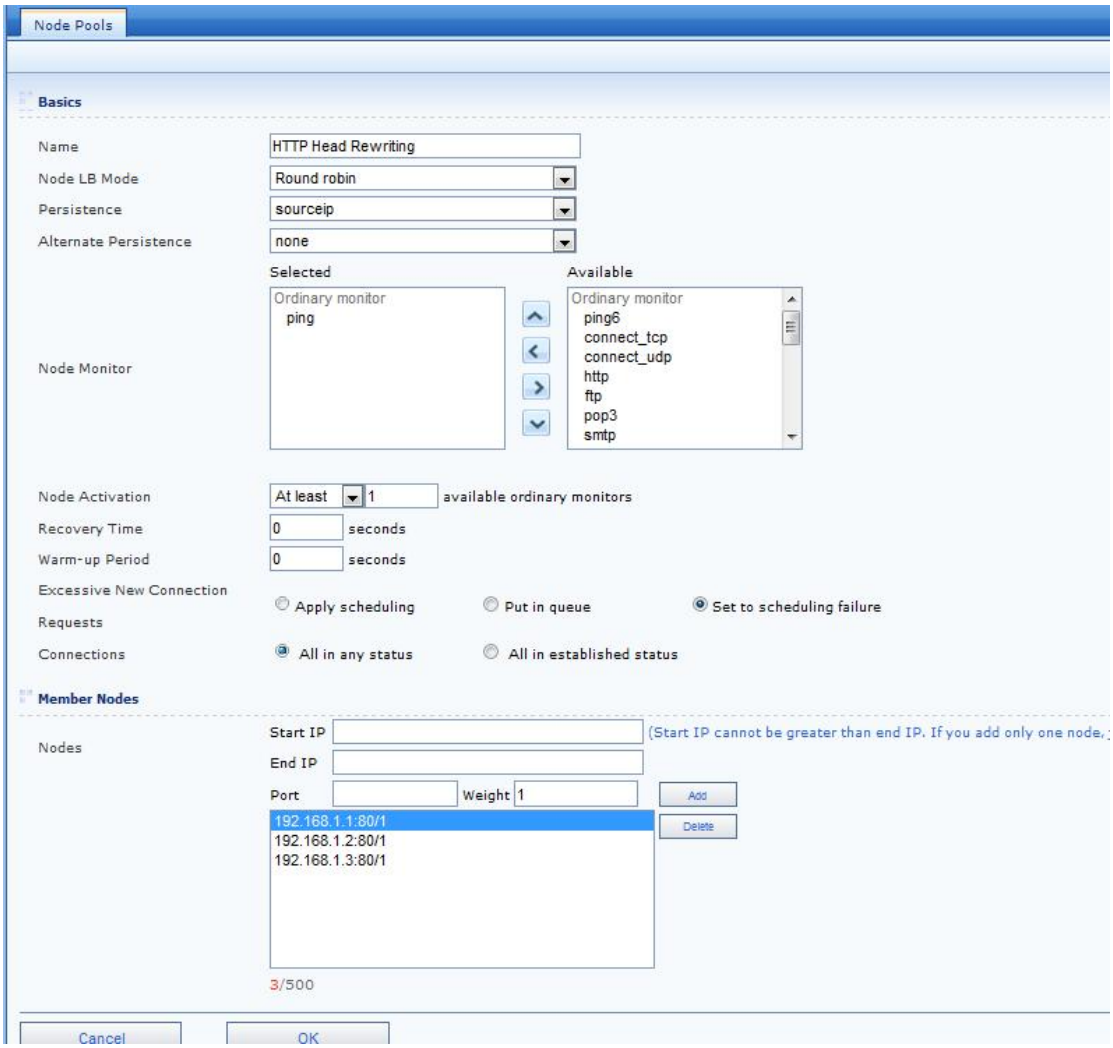


3. Create a session persistence on the **Load Balancing > Persistence > Session Persistence** page, and configure the following fields,



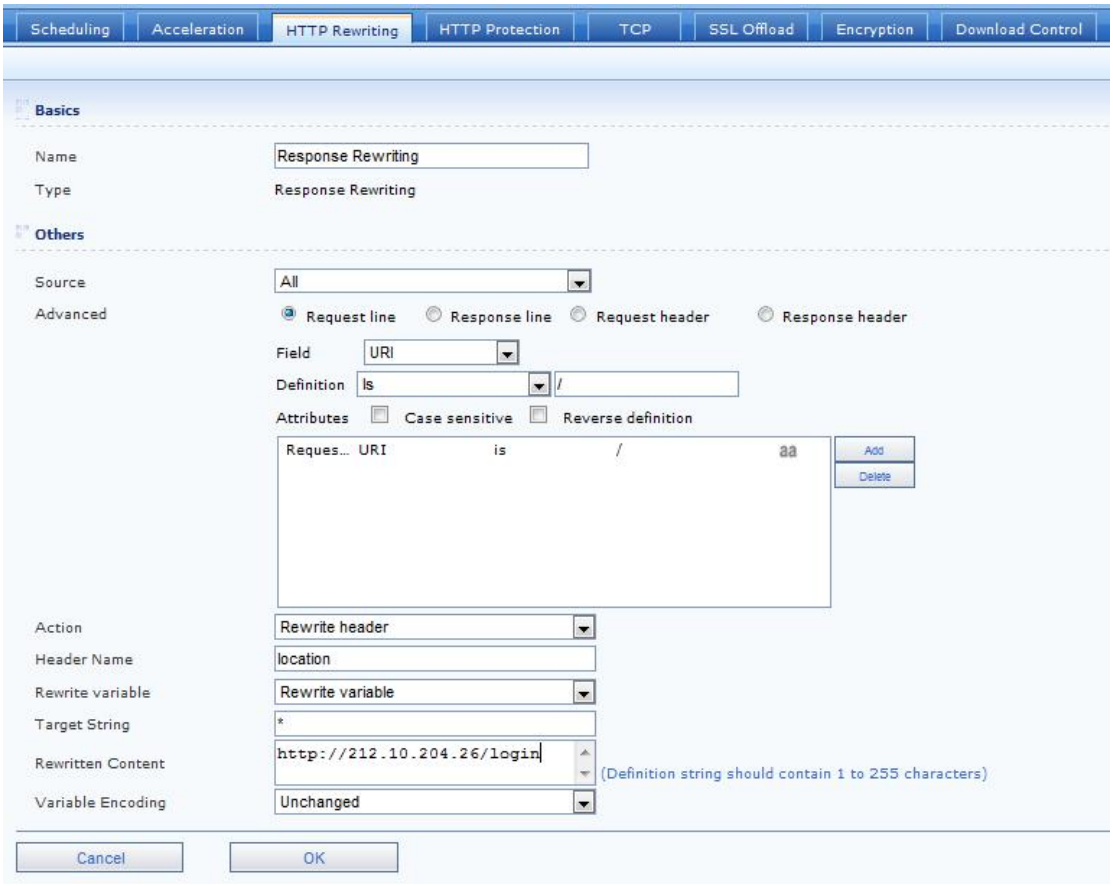
4. Go to the **Load Balancing > Node Pools** page, and create a node pool. Then add the IP addresses of the servers into the node pool, and specify a node monitor and persistence method. In **Node LB Mode** field, you can select **Round robin**, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



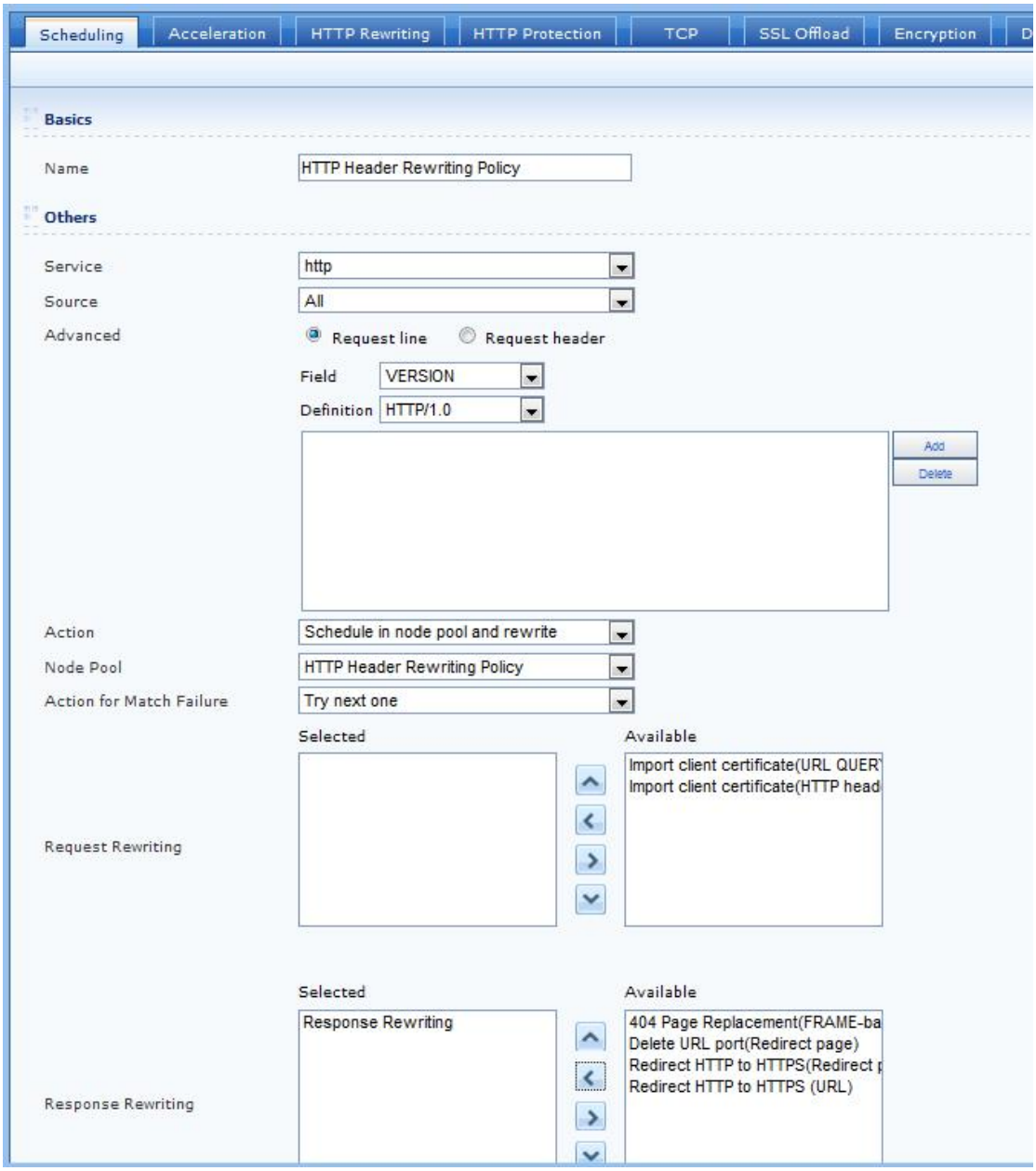
5. Go to the **Load Balancing > Policy > HTTP Rewriting** page, create a response rewriting, and associate the already-configured options, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



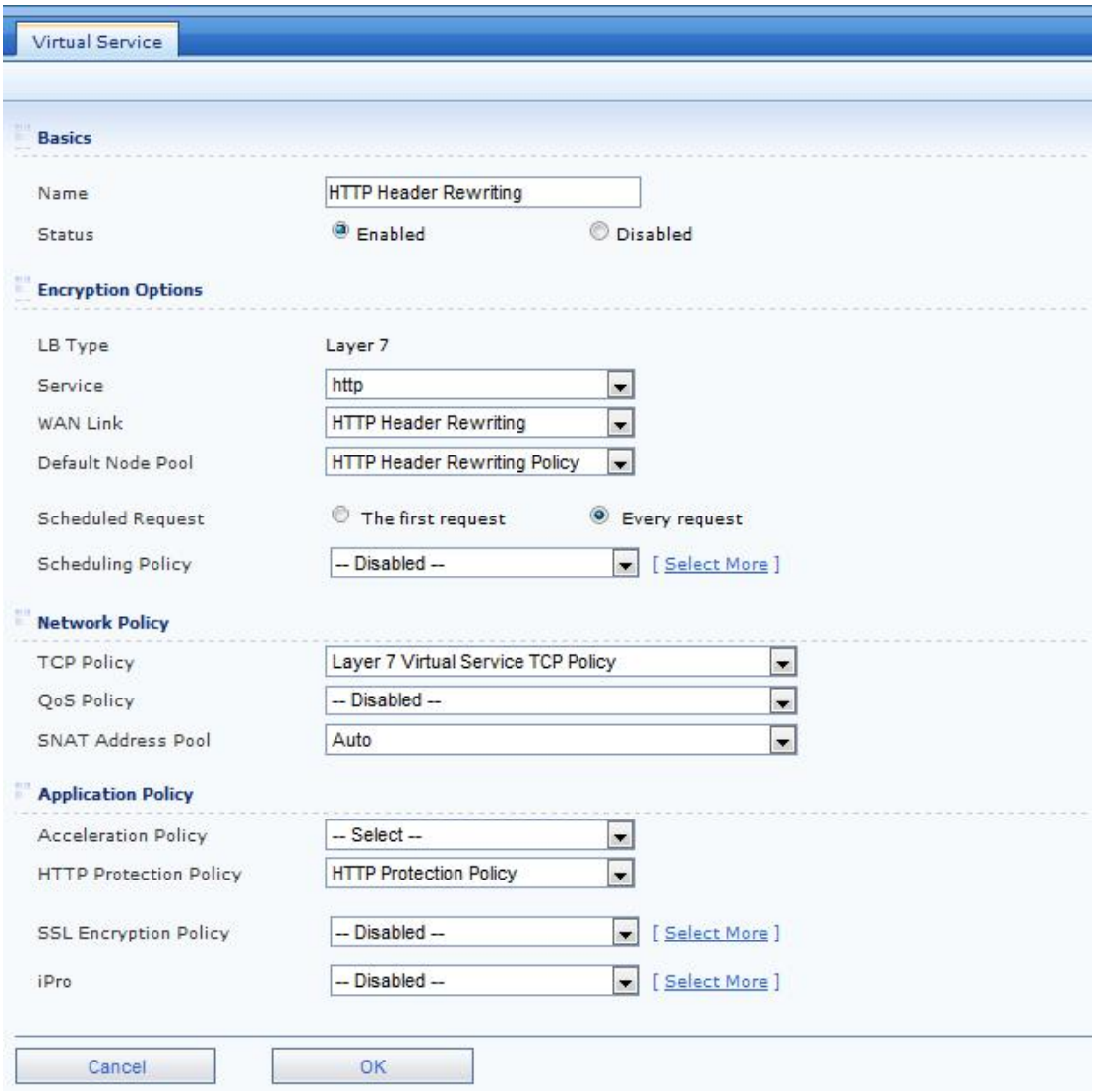
6. Go to the **Load Balancing > Policy > Scheduling** page, create a scheduling policy and associate the already-configured options, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



7. Go to the **Load Balancing > Virtual Service** page, create a layer 7 virtual service, and associate the configured options as well, as shown below:

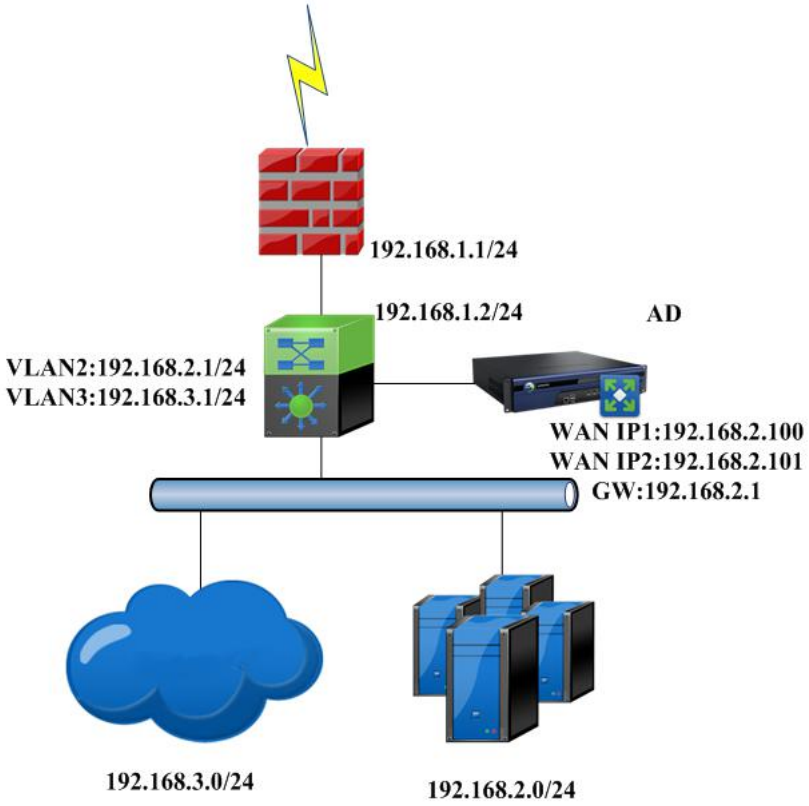
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



14.8 Direct Route mode（DR mode）

One customer wants to balance the load on the Web servers without using AD unit to achieve SNAT. The data packets from servers are sent to client directly through layer 3 switch without flowing through the ADC, in order to reduce the load burden on the ADC.

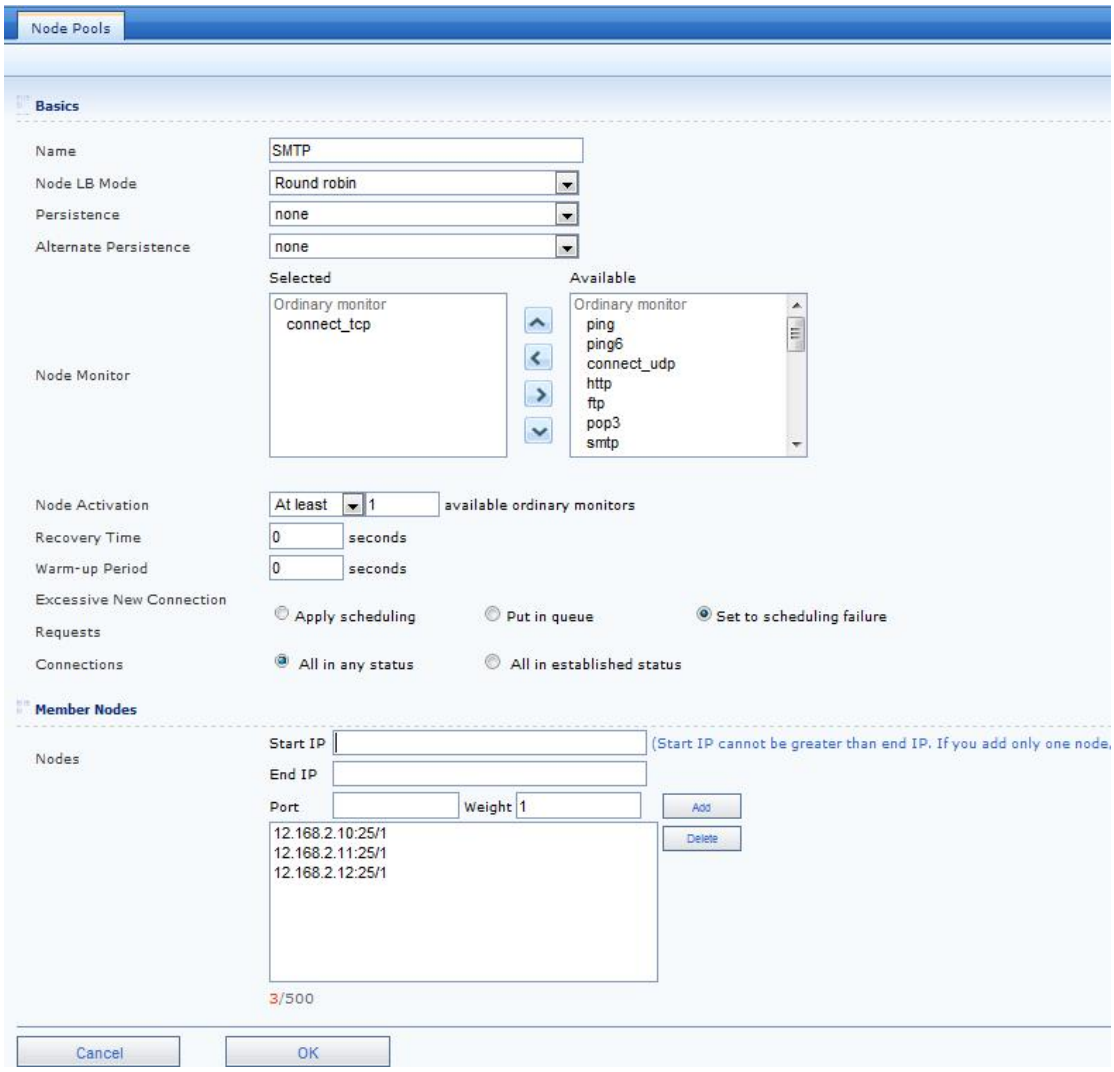
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Configuration steps are as follows:

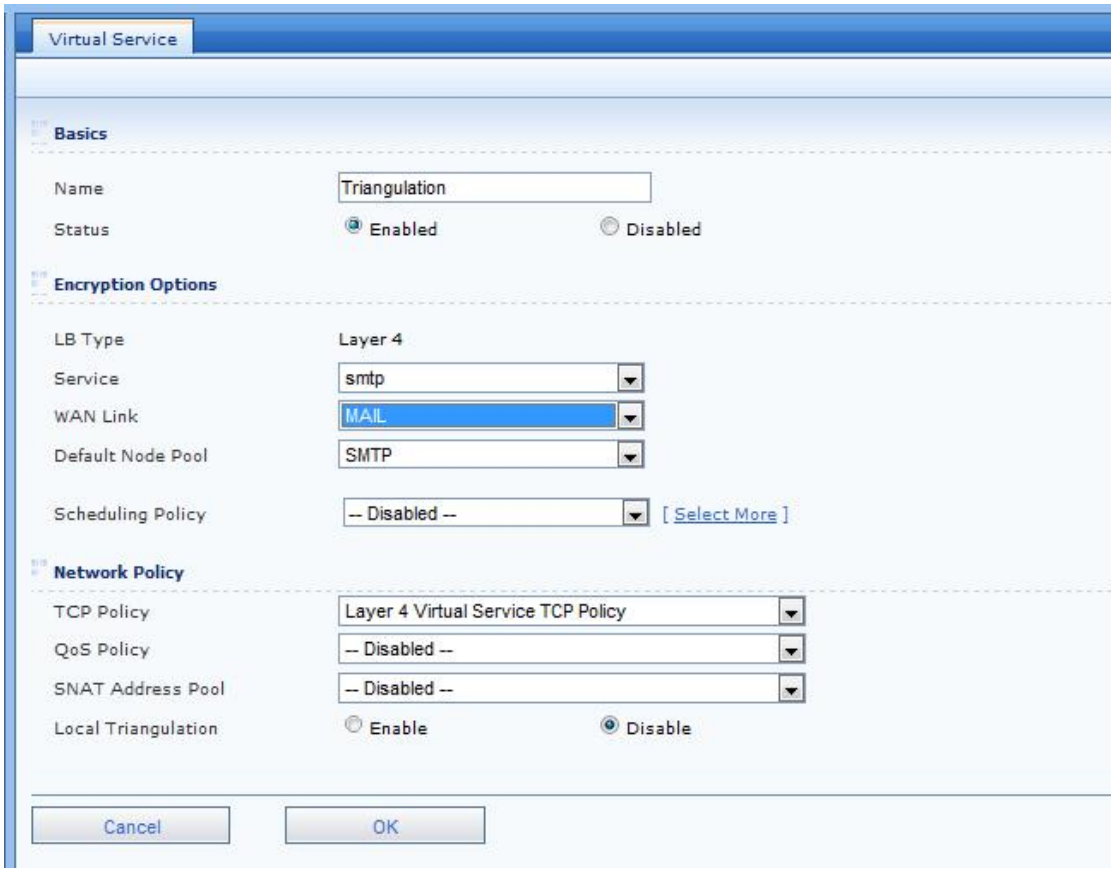
1. Refer to Chapter 6, **Configuring Service** to create a service. This step can be ignored for there is HTTP service on the ADC by default.
2. Create a WAN link and add the WAN links to **IP Group** list. For how to configure the WAN link, please see Chapter 6, **Configuring WAN Link**.
3. Refer to Chapter 6, **Configuring Node Pool** for creating a node pool. Then add the IP address of the server into the **Nodes** list, and specify a node monitor. In **Node LB Mode** field, you can select **Round robin**, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



4. Create a layer 4 virtual service and enable **Local Triangulation**, as shown below:

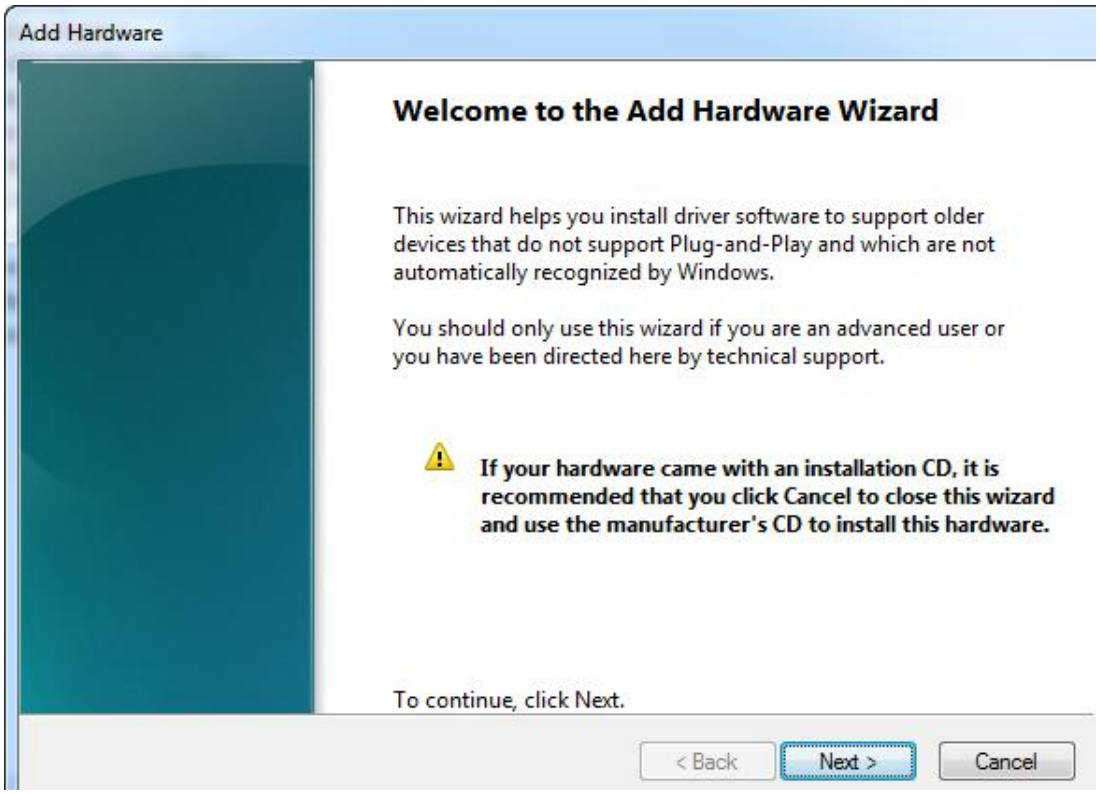
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

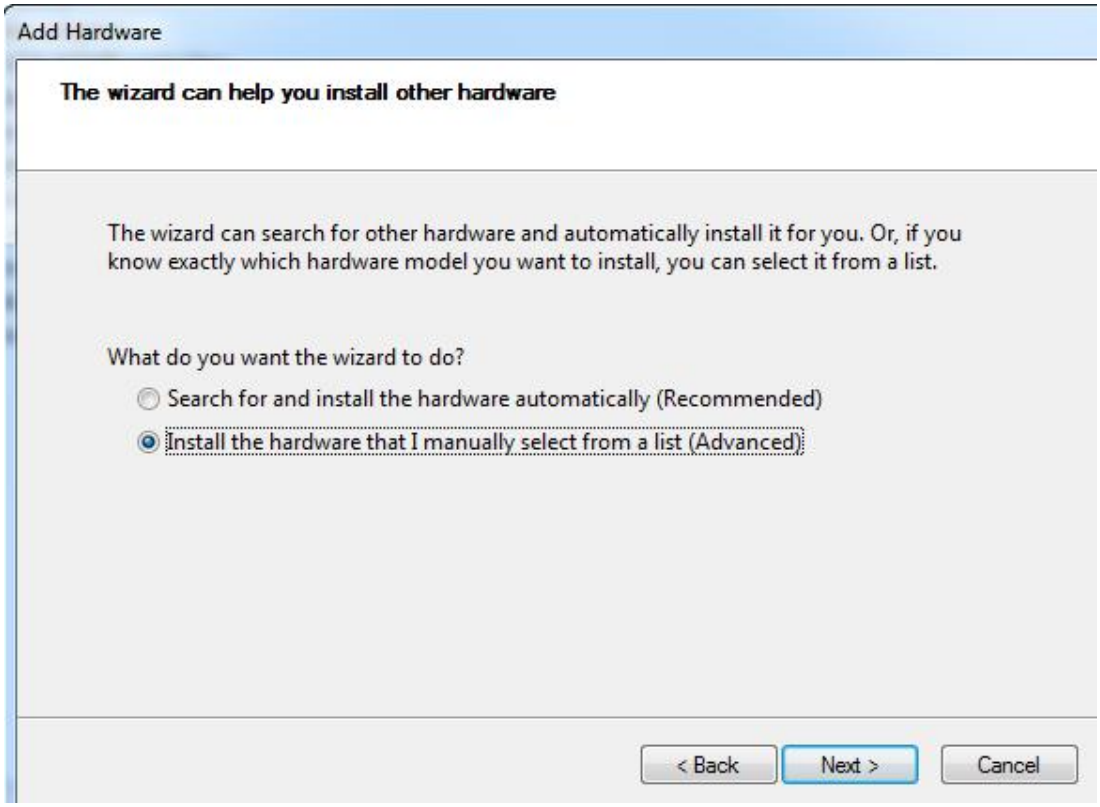


5. Add a virtual network card Loopback Adapter on the two servers and set IP address of virtual service IP group as that of the network card, which is set to 192. 168. 2. 100 in this sample, as shown in the following figure:

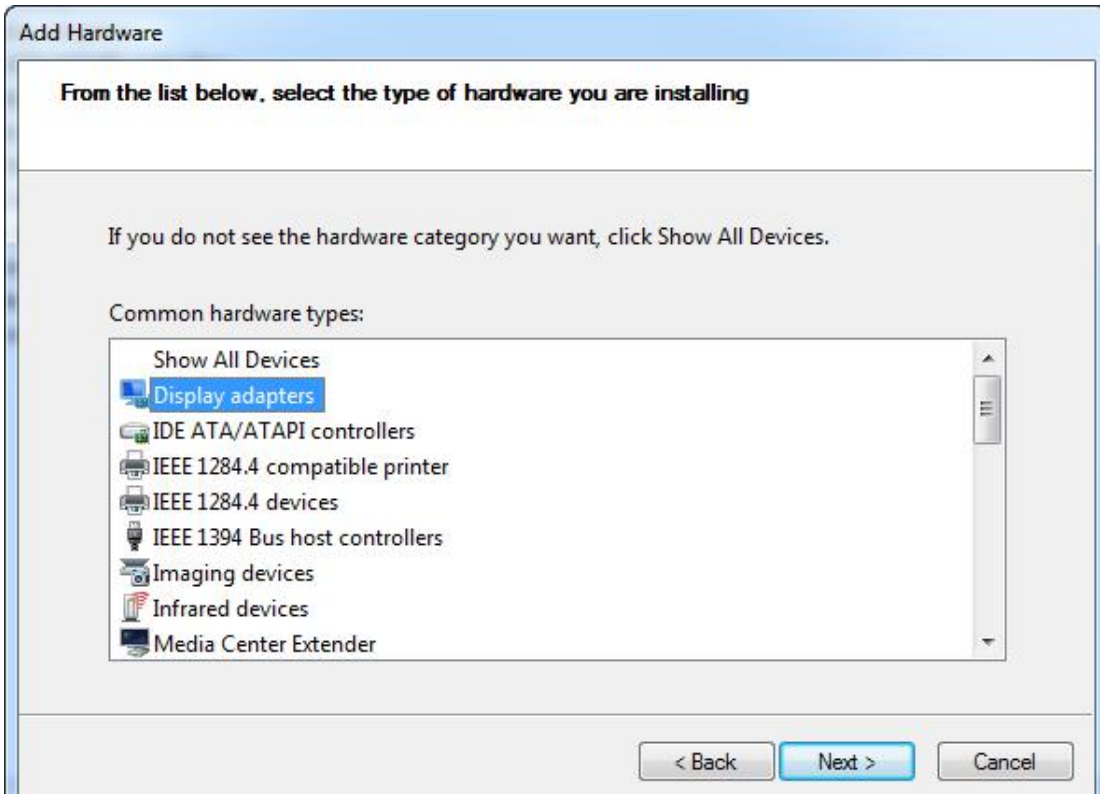
Firstly, open the control panel on the server, and then left-click on **Device Manager**, and click **Action** on its menu bar to select **Add legacy hardware** to enter the following page:

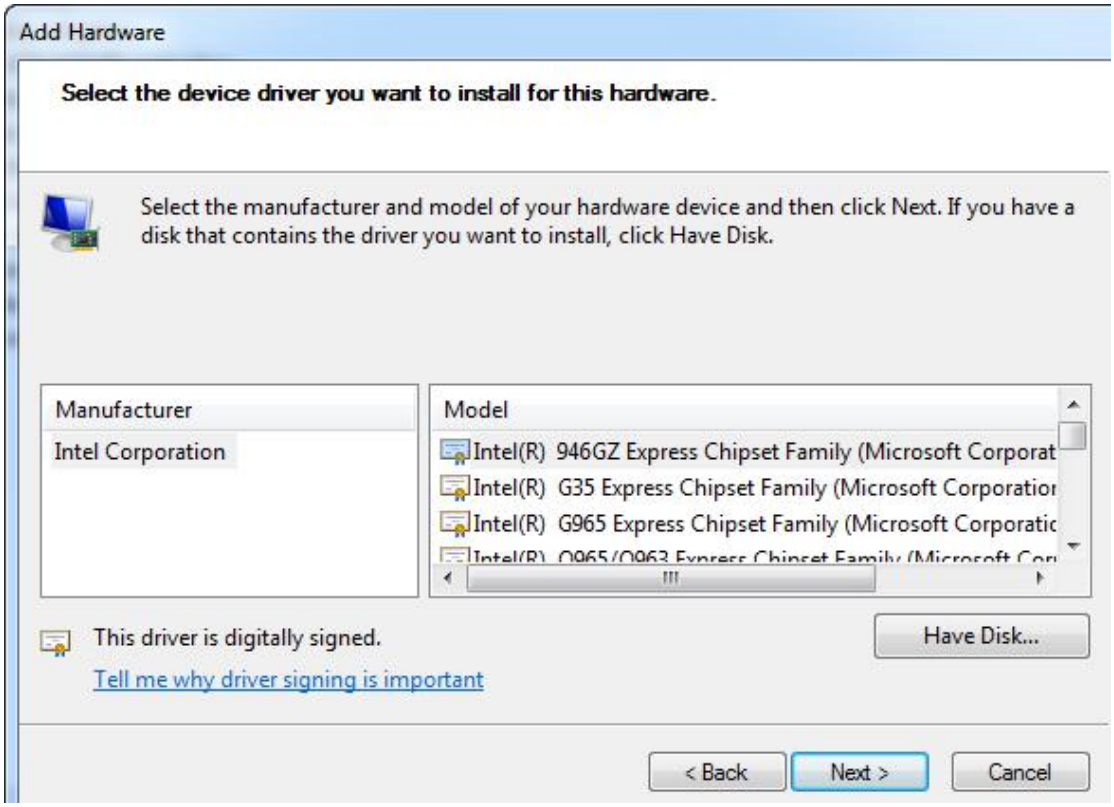
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





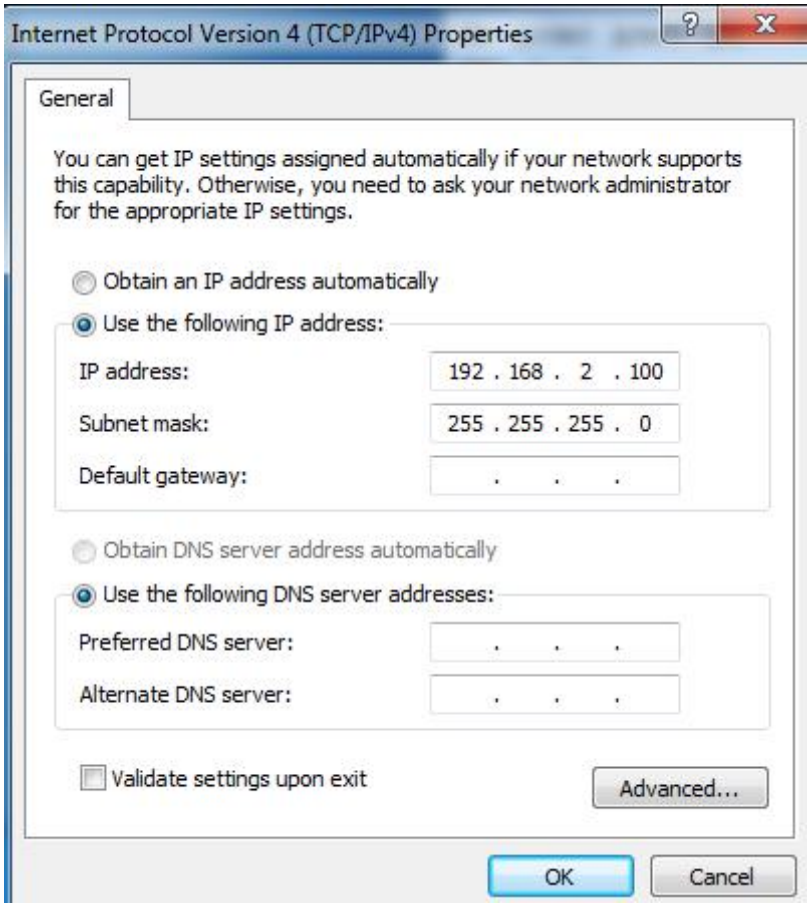
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





After adding the hardware completed, look for the network card and modify its IP address, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



6. You have finished the configuration.



1. In this case, if the **Local Triangulation** is enabled and SNAT is applied to all the source IP, the local triangulation can not be implemented, and the data packets from the servers will still flow through the AD unit.
2. In bypass mode, there needs to configure several IP addresses on the WAN interface. The first IP can not be used to distribute virtual service; otherwise, the node monitor will be unable to monitor the node. As the IP of virtual service distributed by local triangulation is the loopback IP on the server, if the AD unit sends packets with this loopback IP to the server, the server can not respond to AD unit.

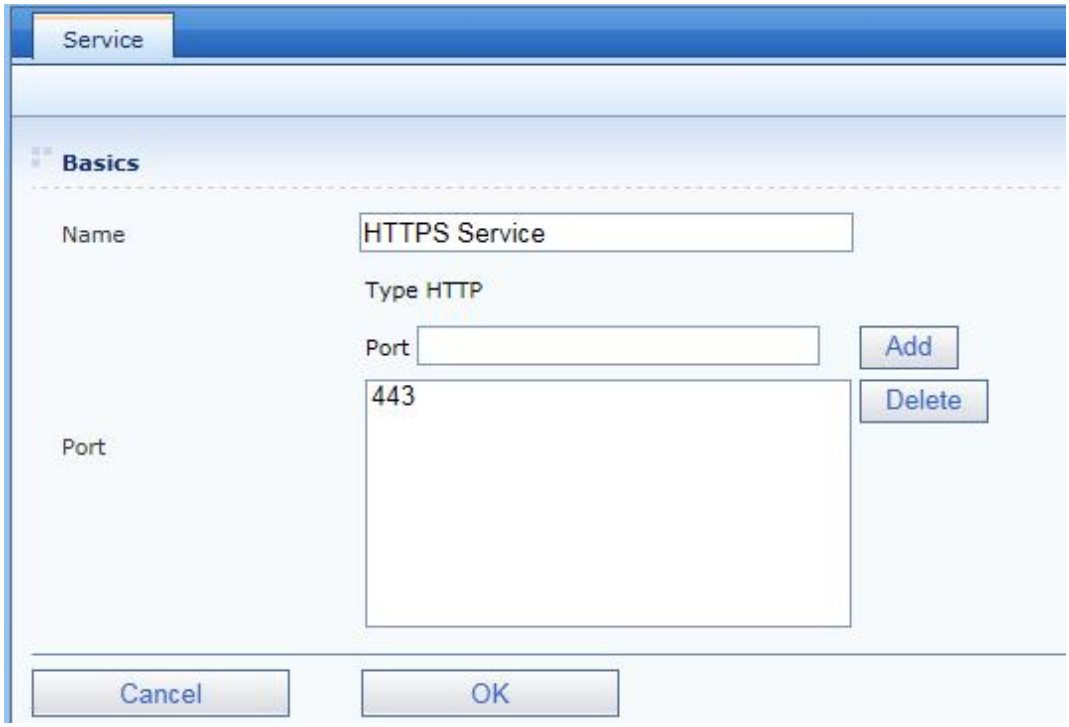
14.9 SSL Policy

Requirements: Deploy the AD unit in route mode. The servers provide HTTP service. When the clients access the servers, back-end AD can establish HTTPS tunnel to encrypt the data transmitting on public network and achieve session persistence for client authentication.

Configuration steps are as follows:

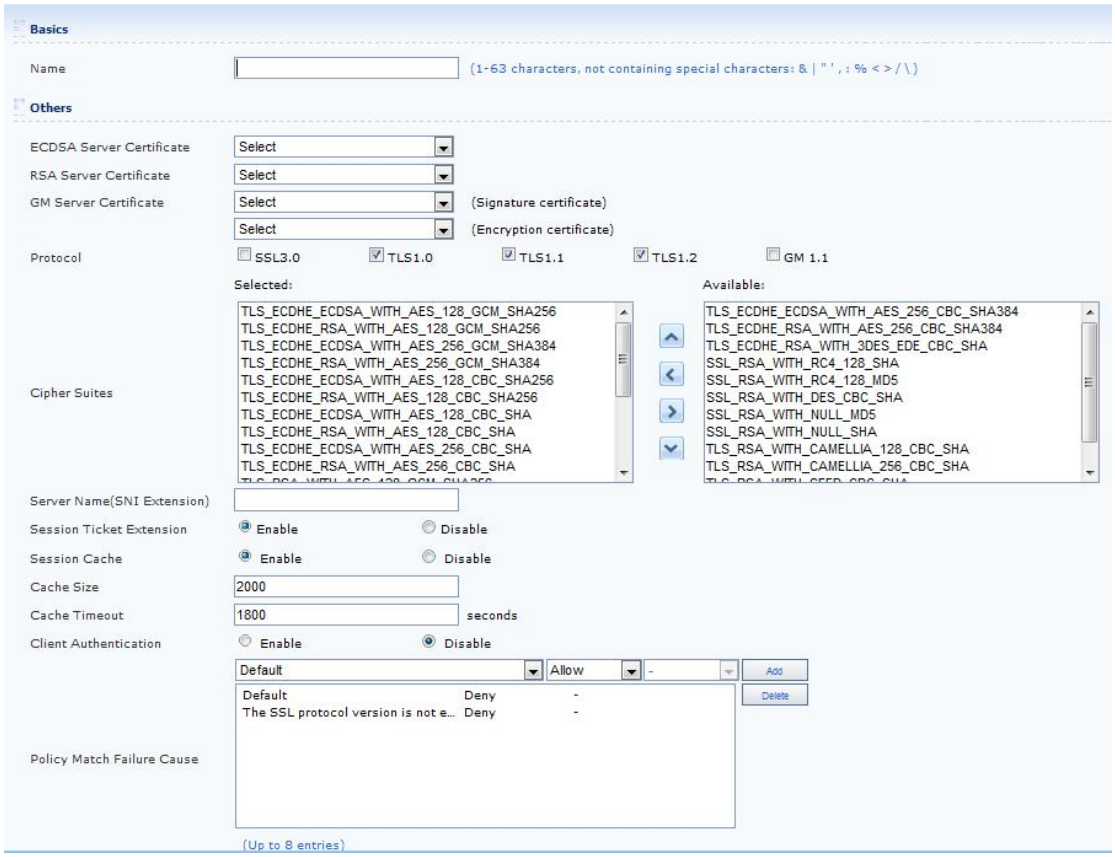
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

1. Create a HTTPS service. For how to configure it, see Chapter 6, **Configuring Service**.



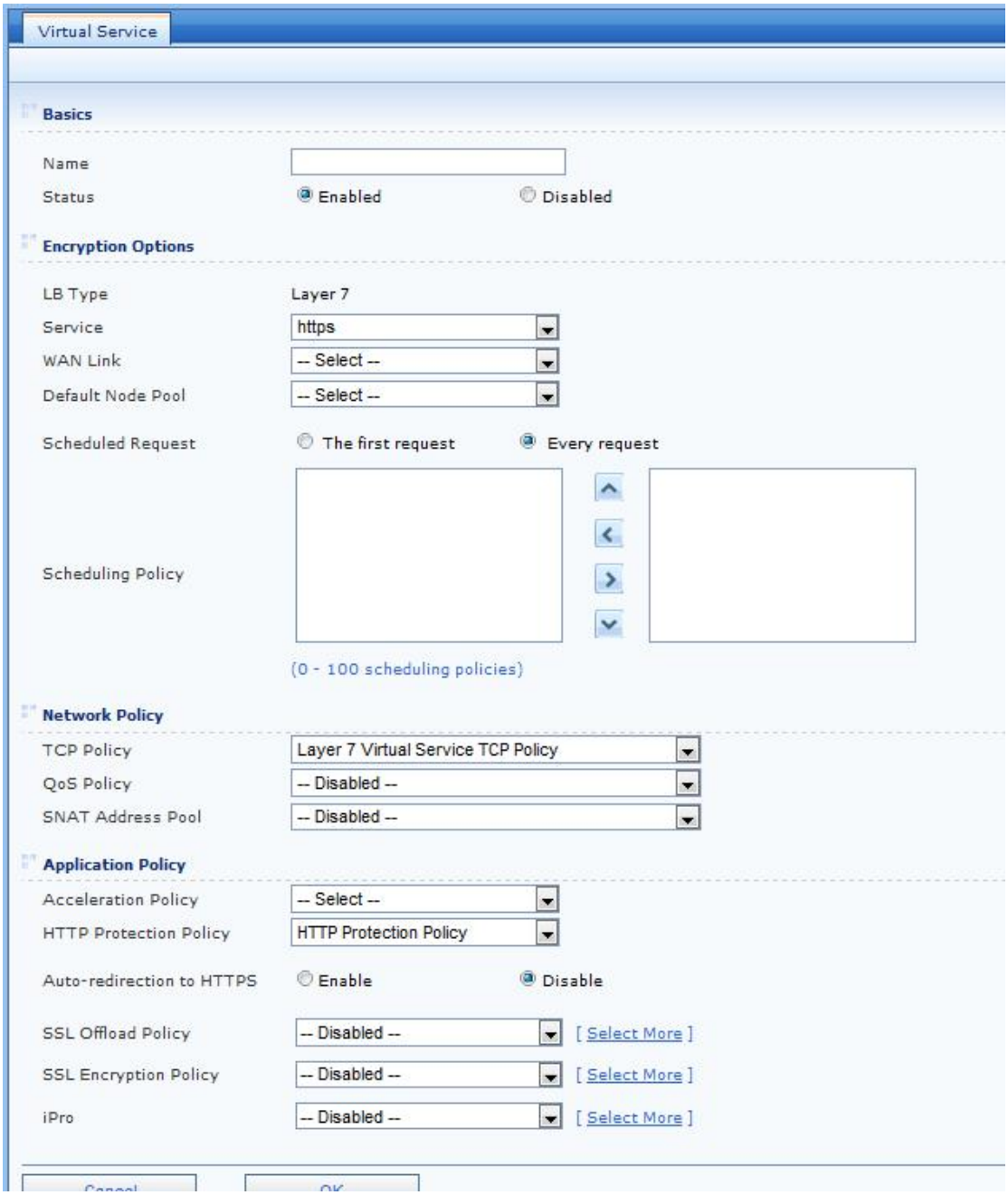
2. Create a **WAN Link** and add the WAN link to **IP Group** field. For configuration details, please refer to Chapter 6, **Configuring WAN Link**.
3. Create a server certificate. For configuration details, please see Chapter 6, **Generating Server Certificate**.
4. Refer to Chapter 6, **Configuring Node Pool** for creating a node pool. And then add the IP address of the server into the node pool, and specify a node monitor. In **Node LB Mode** field, select **Round robin**, as shown below:
5. Create a SSL policy. For configuration details, please refer to Chapter 6, **Configuring SSL Policy**, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



6. Create a layer 7 virtual service and associate the configured options. For more, please see Chapter 6, **Configuring Virtual Service**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



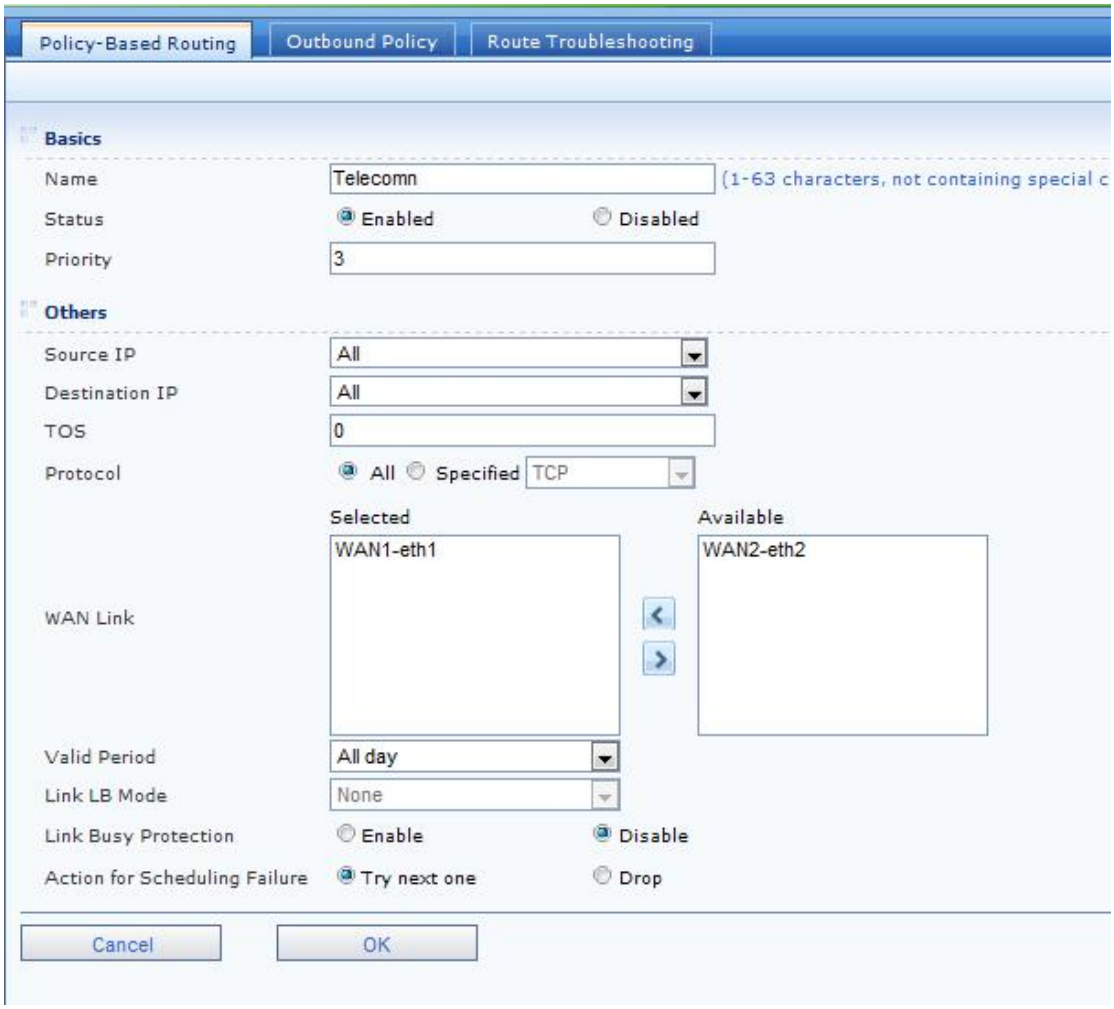
14.10 Policy-Based Routing

The SANGFOR AD unit is deployed in route mode at the network egress in customer network. There are two WAN links: Telecom and Unicom. When the internal users access to the Internet, if the destination IP address belongs to Telecom network segment, the data will flow on Telecom link; if it belongs to Unicom network segment, the data will flow on Unicom link; if the target IP address does not belong to any one of them, the AD unit will select a more effective link by detecting the destination IP address dynamically.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

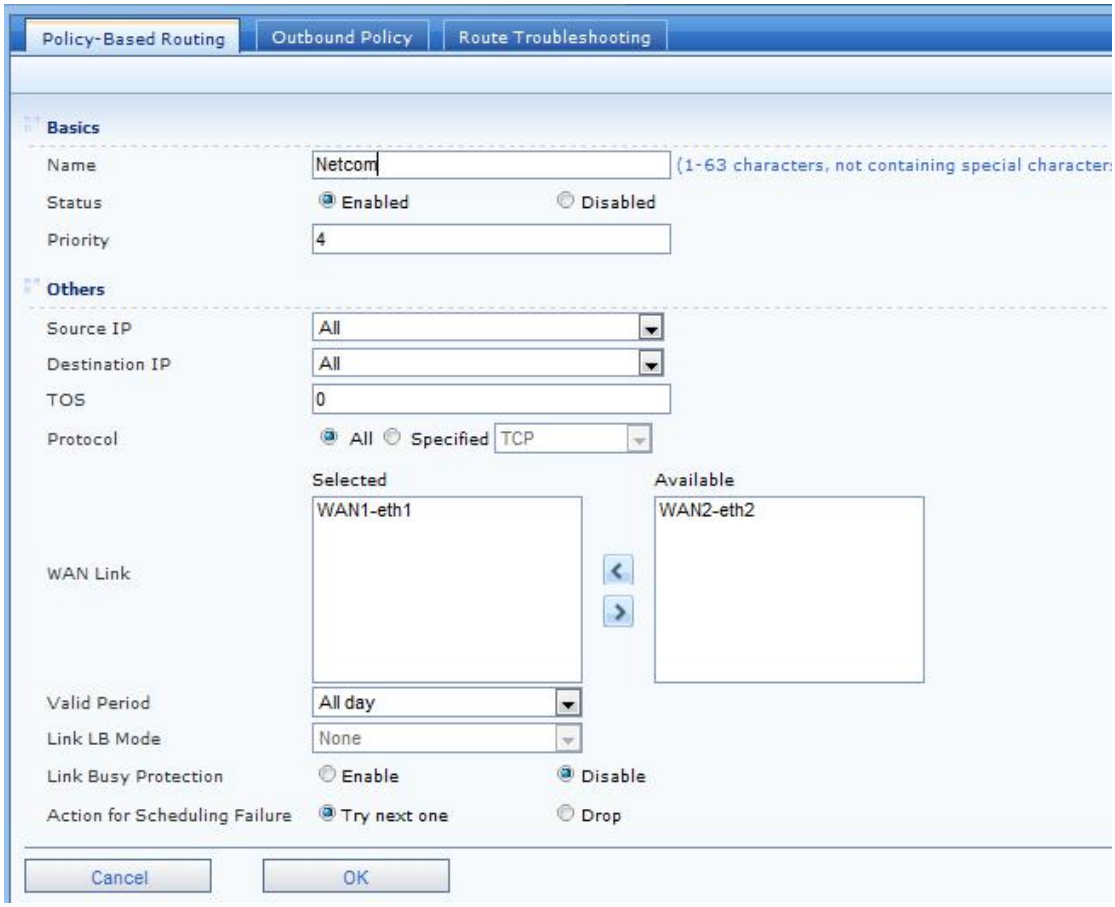
The configuration steps are as follows:

1. Create a policy-based routing to make the data packets in which target IP belongs to Telecom network segment flow over Telecom link. Specify a destination IP address and WAN link, as shown in the following figure:



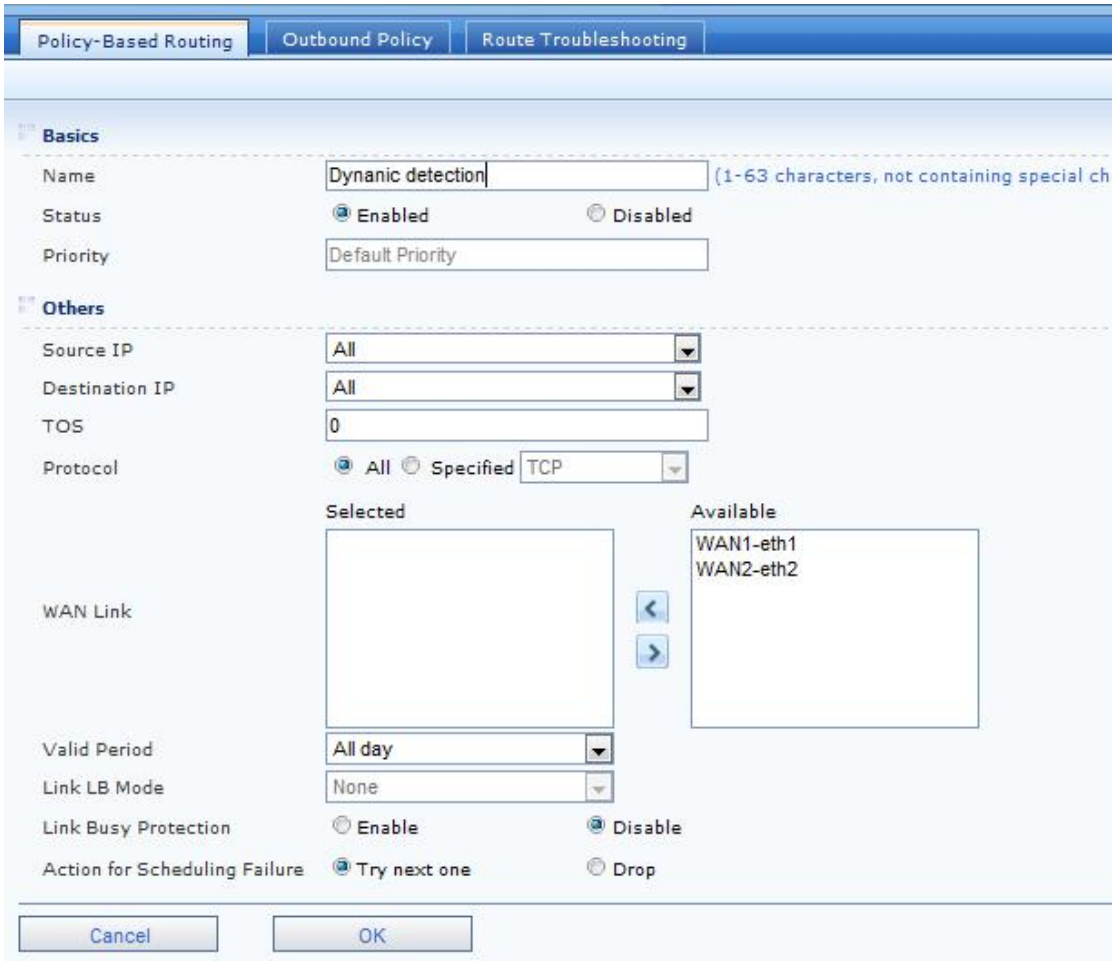
2. Create a policy-based routing to make the data packets in which target IP address belongs to Unicom network segment flow over Unicom Link. Specify a destination IP address and WAN link, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



3. Create a policy-based routing for the data packets in which target IP does not belong to Telecom, nor Unicom. Specify a destination IP address and WAN link, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



After configuring completed, you can view the configuration page of policy-based routing, as shown in the following figure:



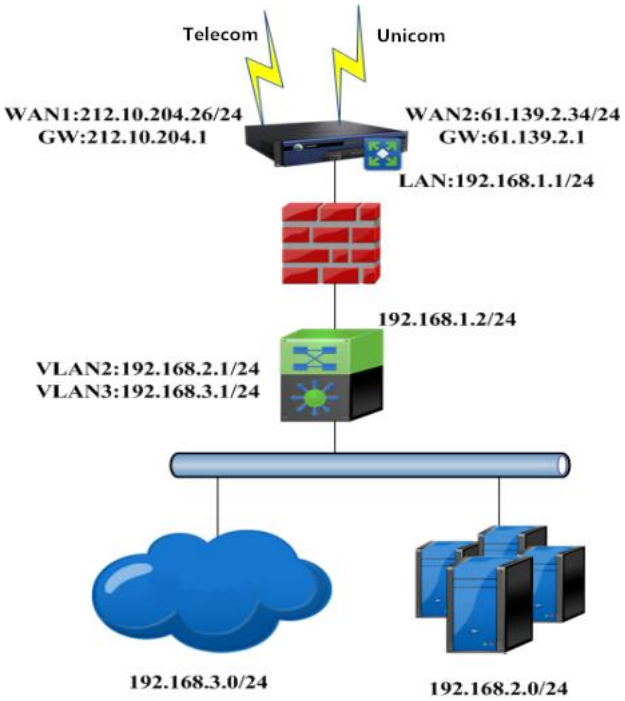
14.11 Intelligent DNS

14.11.1 Scenario 3: Single Site Intelligent DNS

In customer network, the SANGFOR ADC is deployed at the network egress in route mode. There are two WAN links: Telecom (212. 10. 204. 26) and Unicom (61. 139. 2. 34). The LAN servers (192. 168. 2. 0) connect to the layer 3 switch. The external users access the server by typing www. sangfor. com into address bar, when the IP address of client-side belongs to Telecom network segment, the access data will flow over Telecom link; when it belongs to Unicom network segment, the access data will flow over Unicom link; if it does not belong to any one of them, the AD unit will select a more effective link by detecting the destination IP

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

address dynamically. The network topology is as shown below:



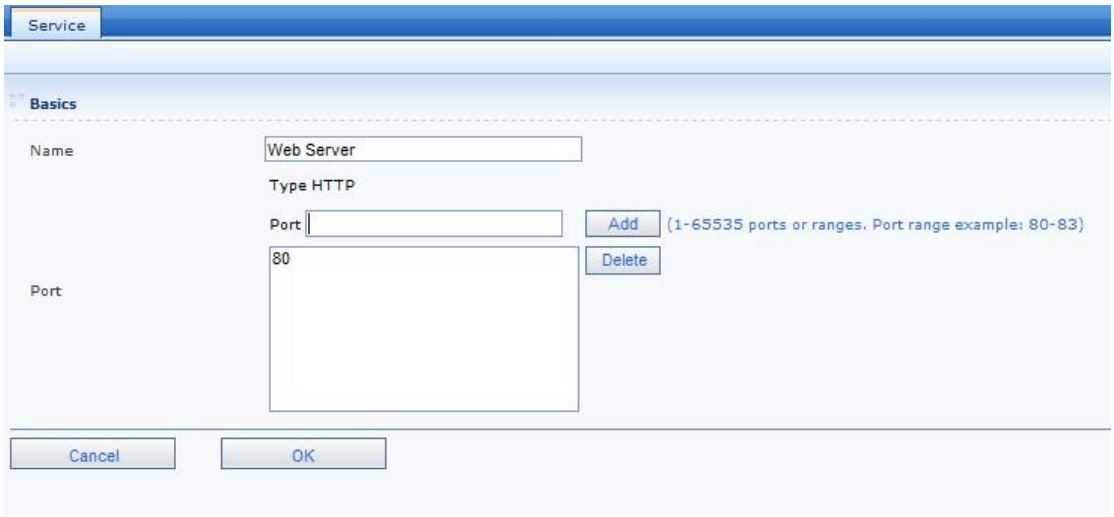
Preparations: Apply for two DNS records on the domain name provider:

NS record: www sangfor. com--- > ns1. sangfor. com

A record: ns1. sangfor. com--- > 212. 10. 204. 26 (or 61. 139. 2. 34).

The configuration steps are as follows:

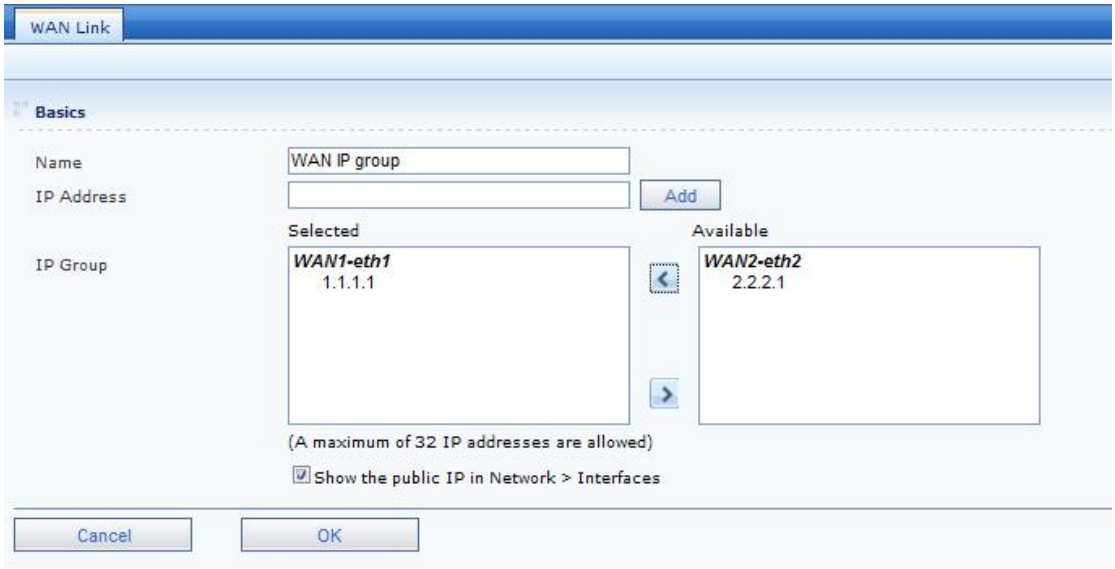
1. Configure basic network, such as physical interface. For configuration details, please see Chapter 9, **Configuring Interface**.
2. Go to the **Load Balancing > Service** page, and create a service, specify service type and port, as shown below:



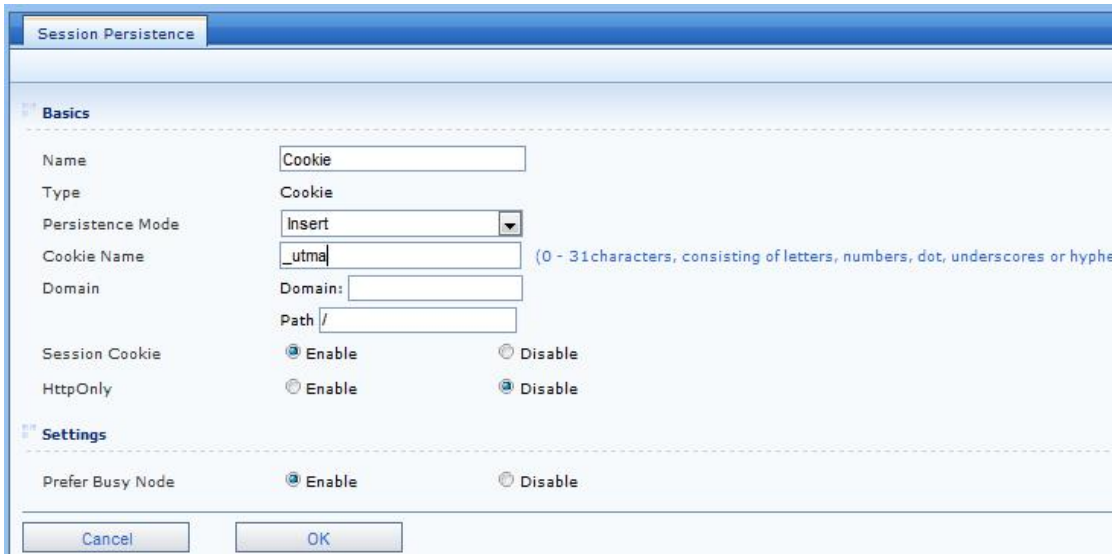
3. Go to the **Load Balancing > WAN Link** page, and create a WAN link, then move the two

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

WAN links from **Available** box to the **Selected** box, as shown below:

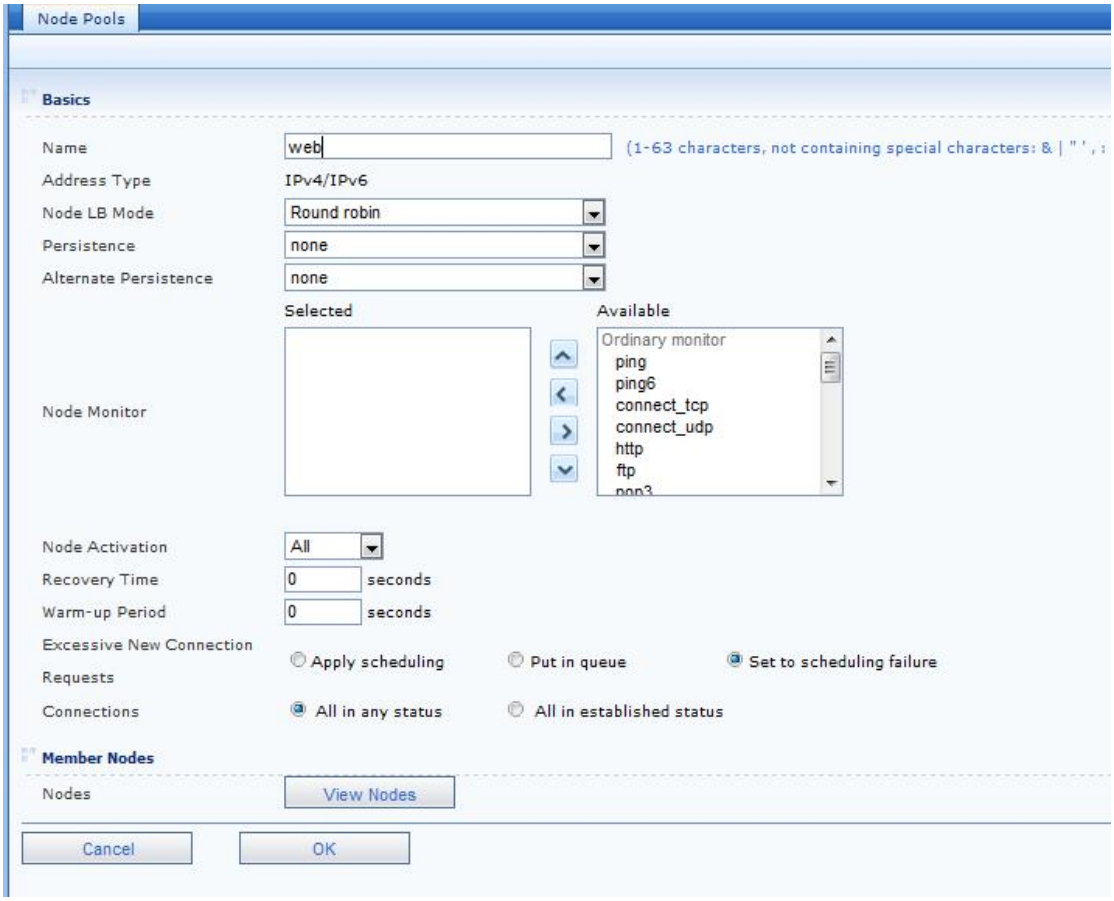


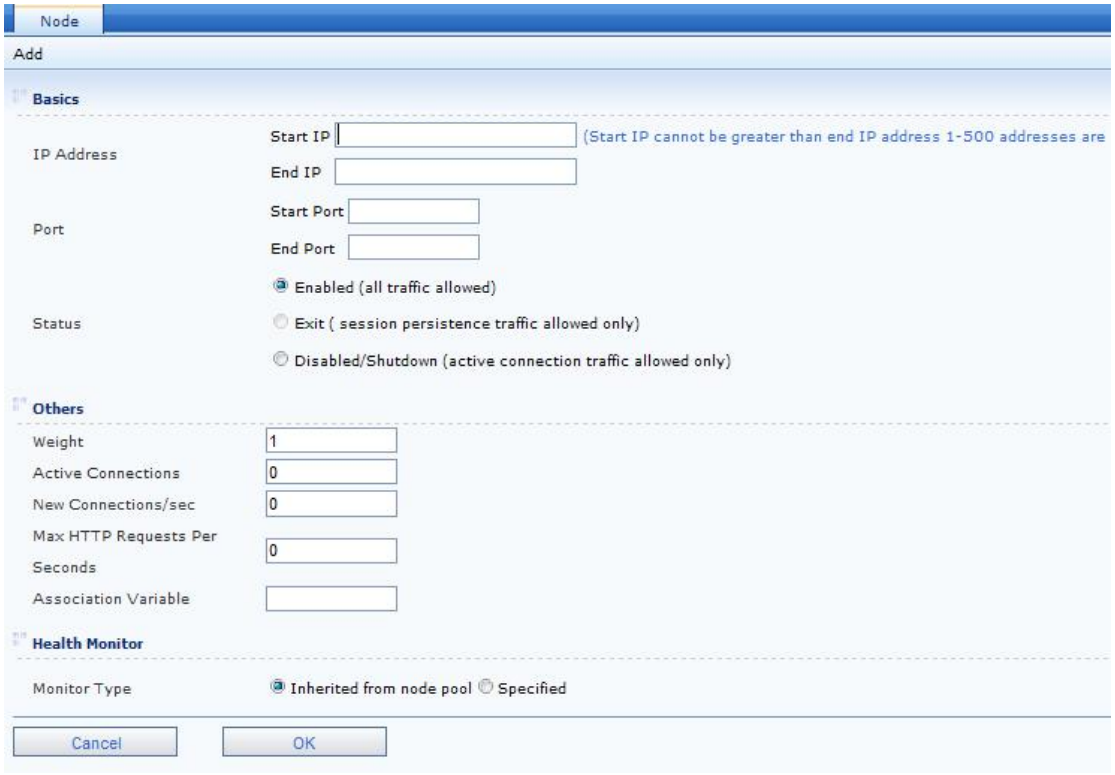
4. Create a session persistence on the **Load Balancing > Persistence > Session Persistence** page. Assume the customer wants to create a session persistence based on cookie.



5. On the **Load Balancing > Node Pool** page, you can create a node pool, and add the IP addresses of the servers into the node pool field.

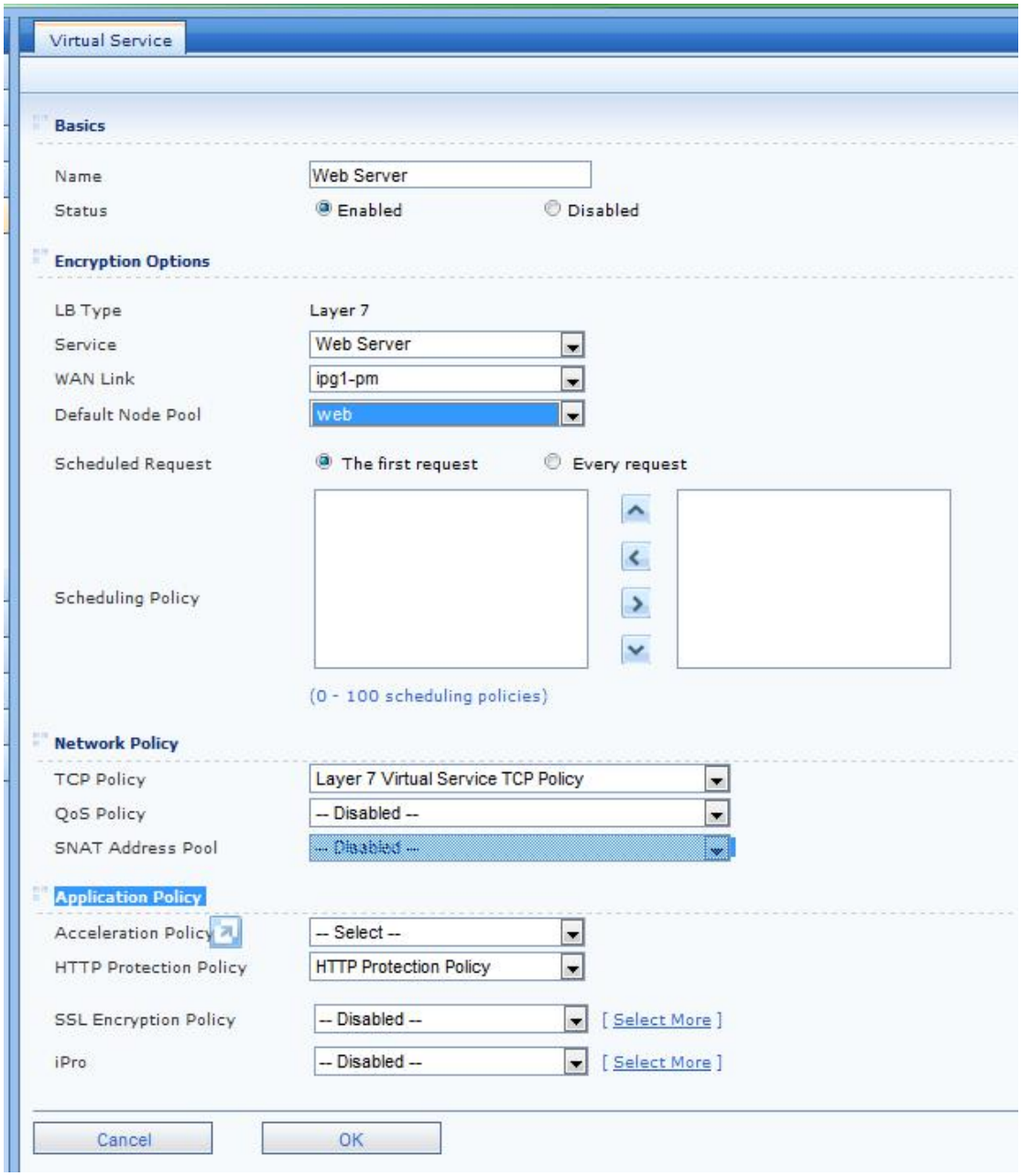
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





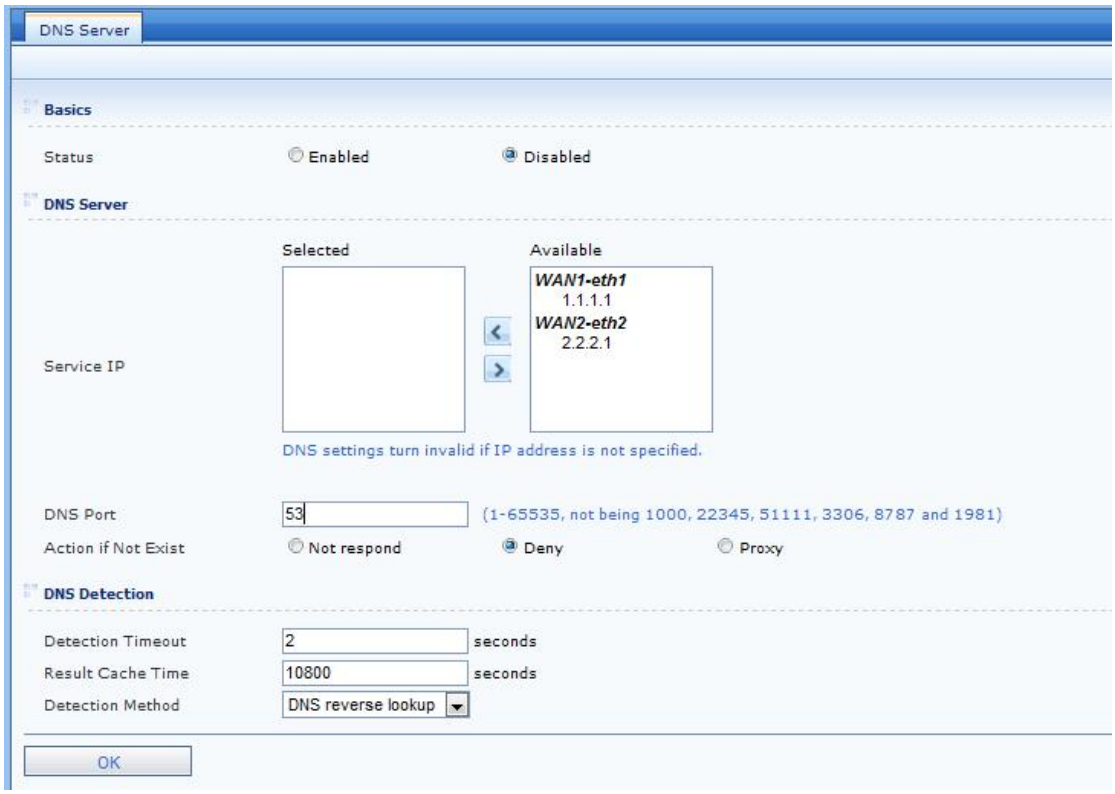
6. Go to the **Load Balancing > Virtual Service** page, create a layer 7 virtual service and specify a service and node pool, WAN Link as well.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



7. Go to the the **Intelligent DNS > DNS Server** page, add the service IP of the DNS server.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



8. Create a local virtual IP pool on the **Intelligent DNS > Virtual IP Pool > Local Virtual IP Pool** page, add the public IP which needs to be distributed. In **Preferred Policy** field, select **Static Proximity**; in **Alternate Policy** filed, select **Dynamic Proximity**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



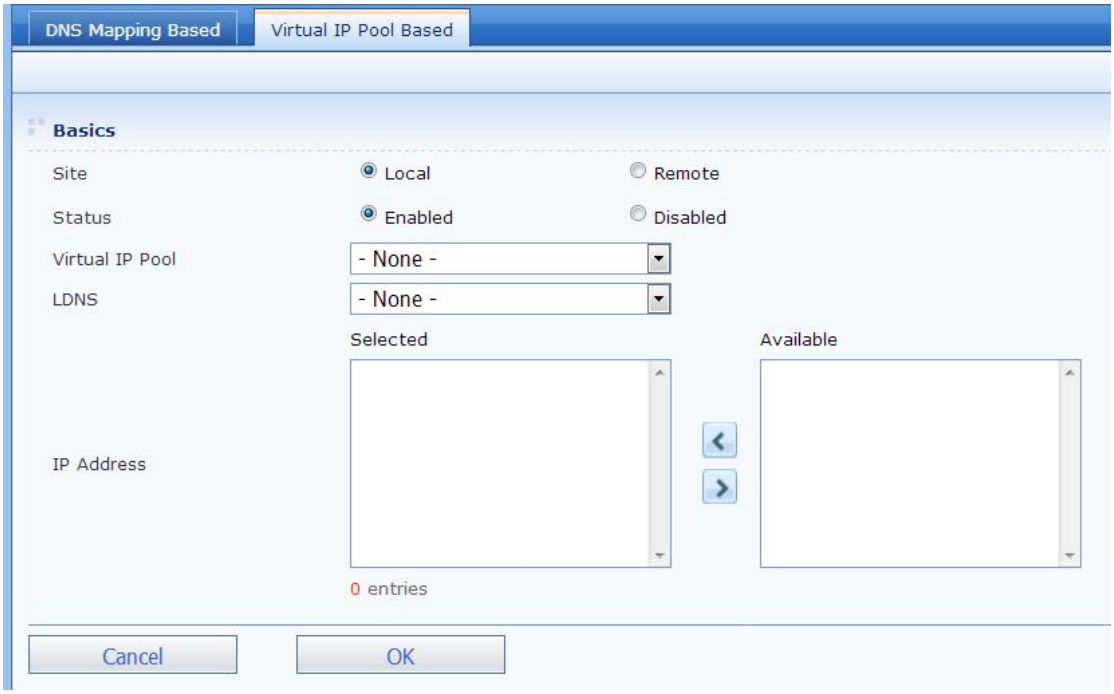
9. Go to the **Intelligent DNS > DNS Mapping > Local DNS Mapping** page, create a local DNS mapping and add the domain name which needs to be resolved, specify the virtual IP pool which needs to be distributed as well.

10. Go to the **Intelligent DNS > LDNS > Local LDNS** page, and create two LDNS, one for adding Telecom network segment, the other one for adding Unicom network segment.

11. Go to **Intelligent DNS > Static Proximity > Virtual IP Pool Based** page, create two static proximity policies. When clients access www. sangfor. com, if the LDNS request is from Telecom link, return 212. 10. 204. 26 as resolved IP; if it's from Unicom link, return 61.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

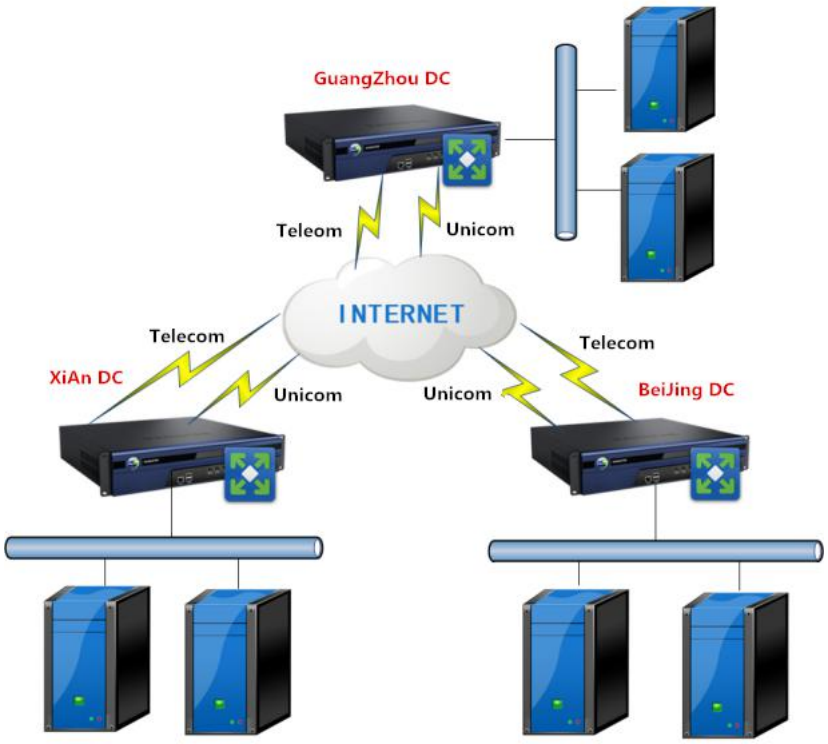
13. 2. 34 as resolved IP.



14.11.2 Scenario 4: Distributed Intelligent DNS

One customer has three Web servers as portal website located respectively in Guangzhou, Beijing and Xi'an. External users access the website via www. sangfor. com. The WAN links are Telecom and Unicom, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Requirements:

1. The requests of the users from the north and northeast of China should be scheduled to the ADC deployed in Beijing. The requests of the users should flow via the link determined by which ISP the user belongs to, Telecom or Unicom. The requests of the users whose IP does not belong to Telecom, nor Unicom, will go through the link selected by detecting destination IP address dynamically.
2. The requests of the users from the northwest and southwest of China should be scheduled to the ADC deployed in Xi'an. The access requests of the users should flow via the link determined by which ISP the user belongs to. The requests of users belonging to other ISP will go through the link selected by detecting destination IP address dynamically.
3. The requests of the users from the central China and south of China should be scheduled to the ADC deployed in Guangzhou. The access requests of the users should flow via the link determined by which ISP the user belongs to. The requests of users belonging to other ISP will go through the link selected by detecting destination IP address dynamically.
4. The requests of the users from the other areas should be scheduled to the ADC deployed in Beijing.

Take the AD unit deployed in Guangzhou for example. Link 1 is Telecom link (212. 10. 204. 26), link 2 is Unicom link (61. 139. 2. 34). The LAN server (192. 168. 1. 2) connects to the LAN switch.

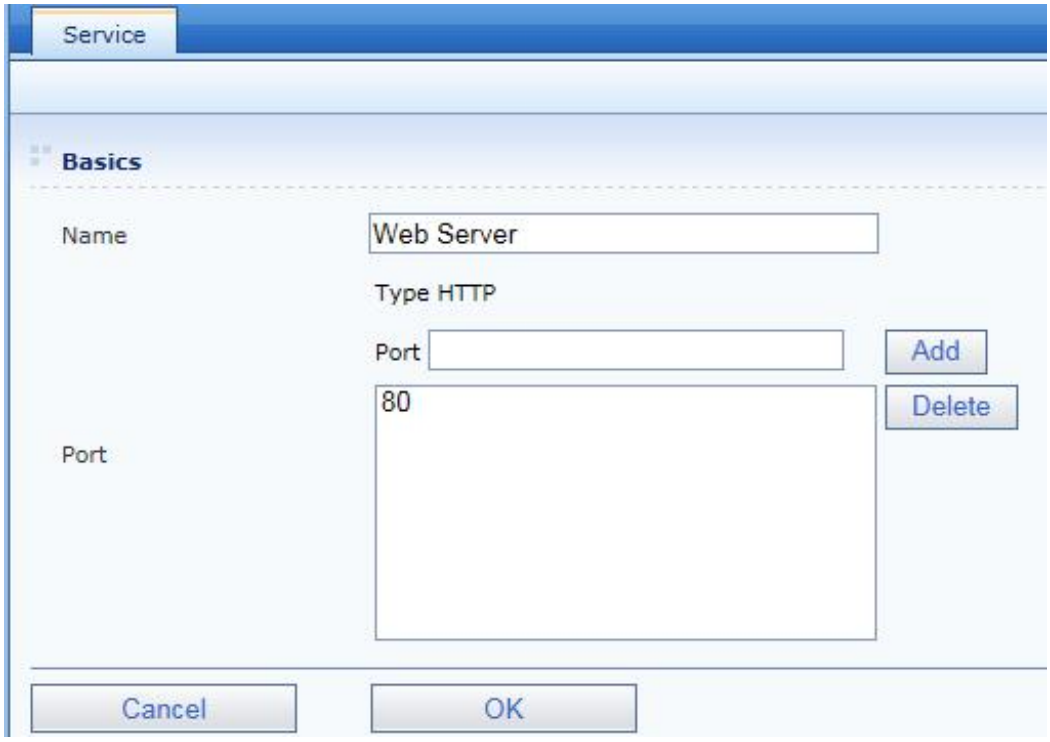
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Preparations: Apply for two DNS records on the domain name provider:

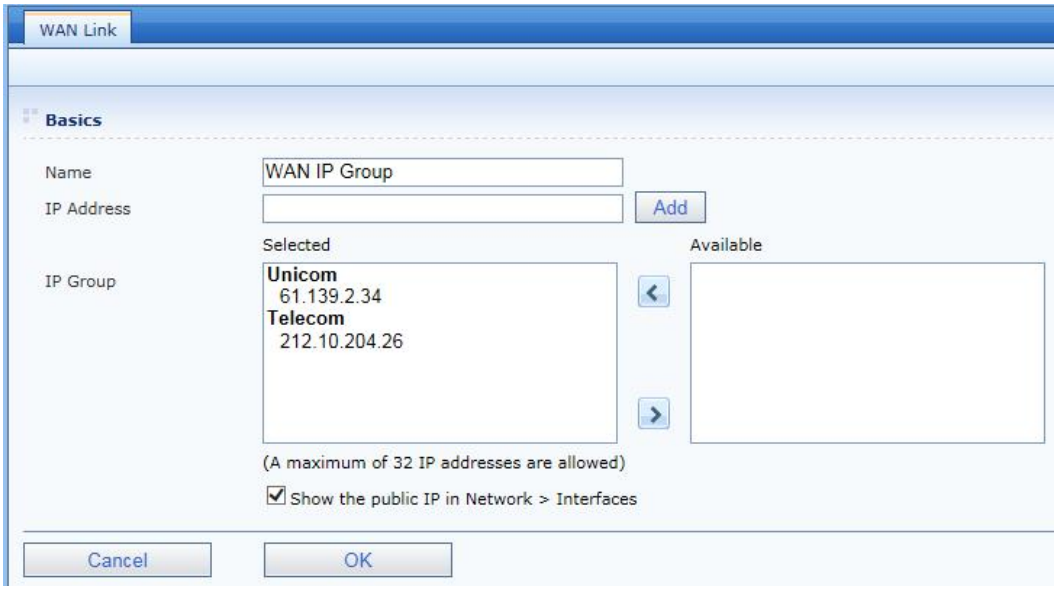
NS record: www. Sangfor. com--- > ns1. sangfor. com, A record: ns1. sangfor. com--- > 212. 10. 204. 26 (or 61. 139. 2. 34).

The configuration steps are as follows:

1. Go to the **Load Balancing > Service** page, create a service, and specify service type and port.

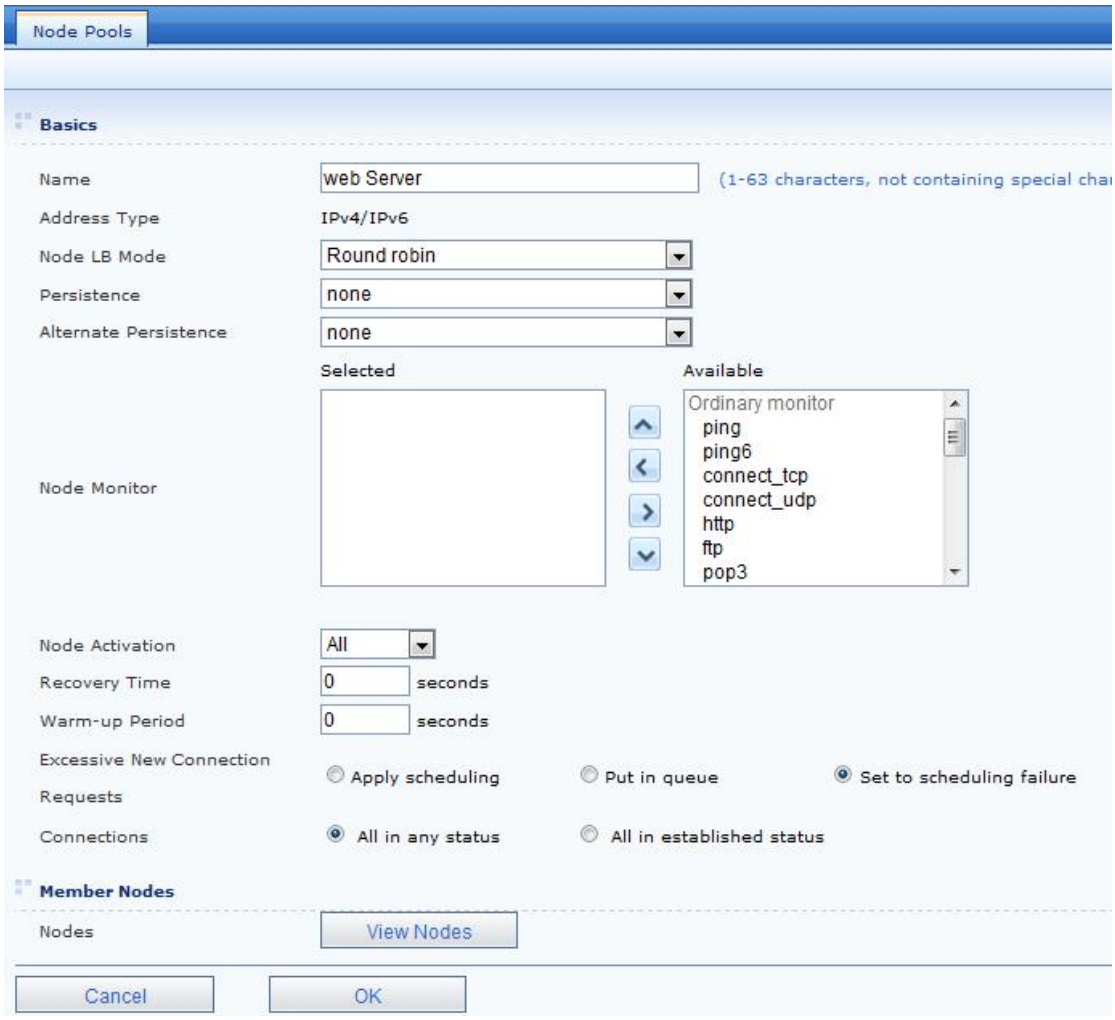


2. Go to the **Load Balancing > WAN Link** page, create a WAN link and move the two WAN link IP addresses which need to be distributed from **Available** box to **Selected** box.



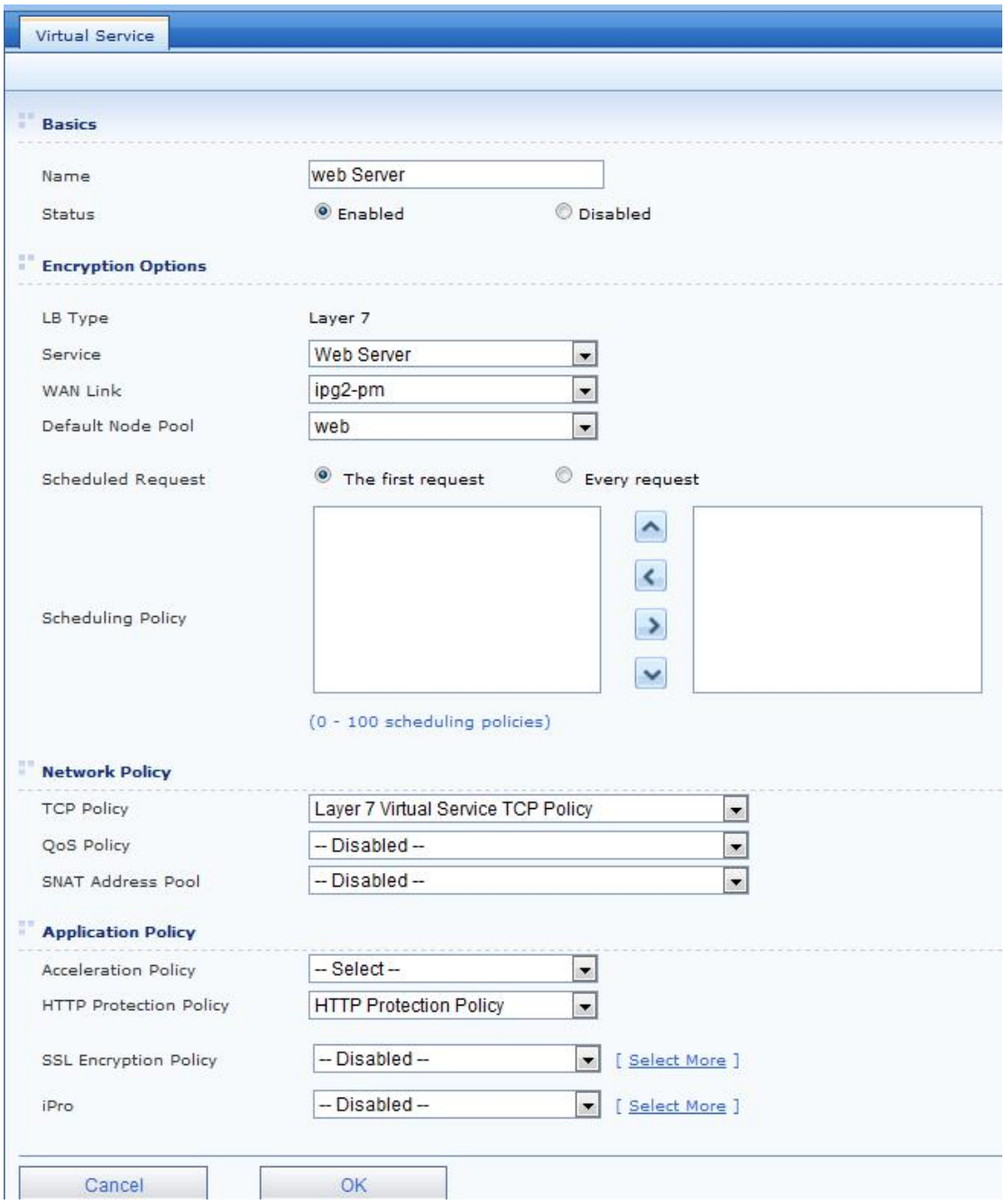
3. Go to the **Load Balancing > Node Pools** page, create a node pool and add the IP address of the server into the node pool filed.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



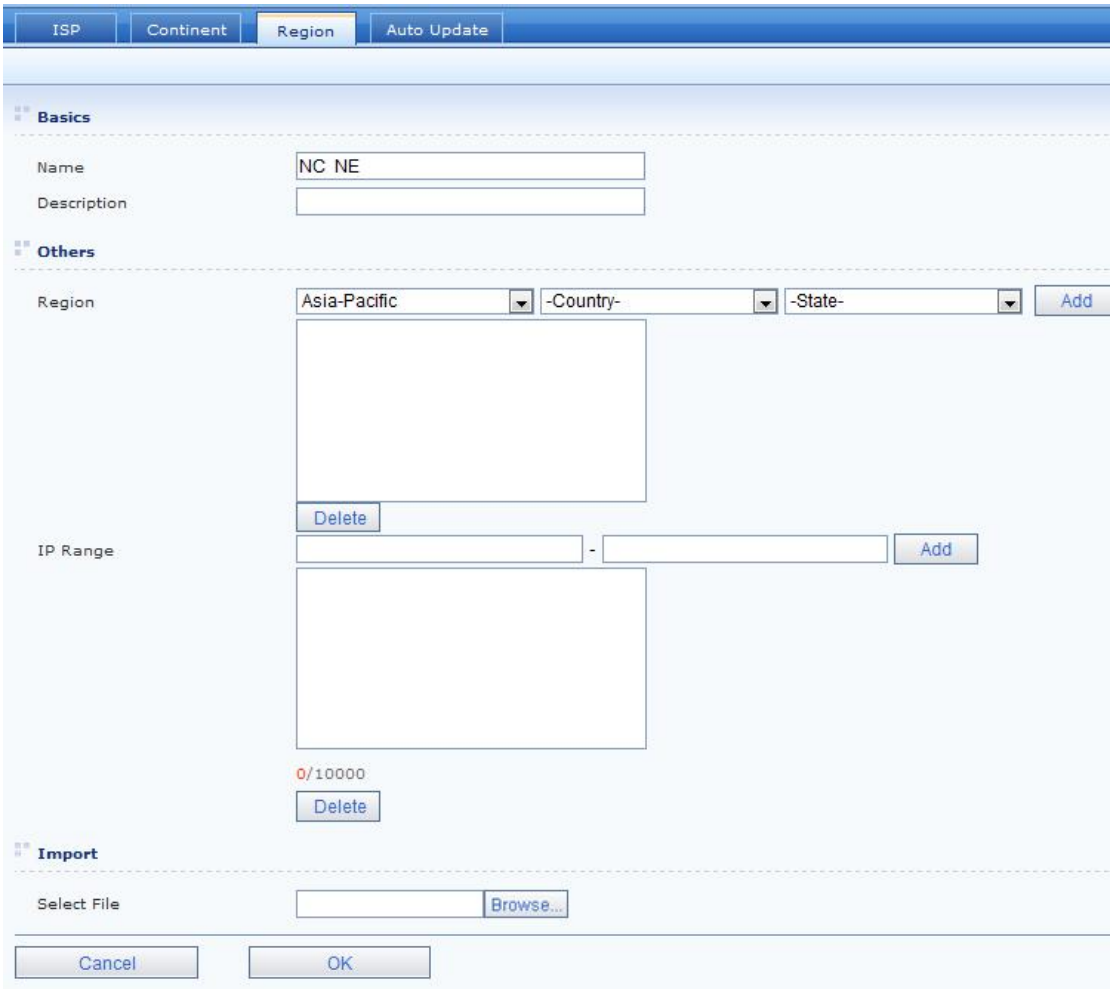
4. Go to the **Load Balancing > Virtual Service** page, create a layer 7virtual service, specify a service, node pool and WAN link.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

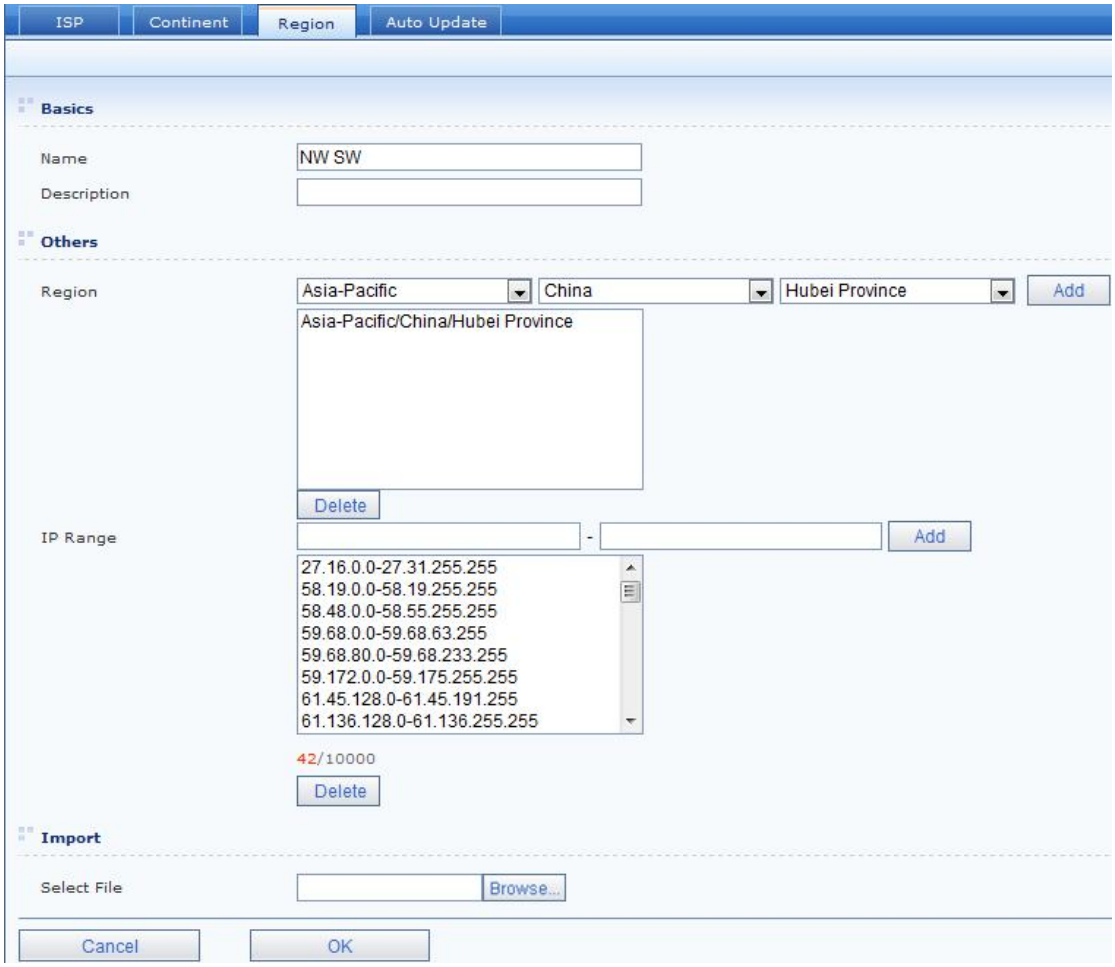


5. Go to the **Objects > IP Group > Region** page, create a region and add the IP address segment of the north /northeast, northwest /southwest, and the central /south, and the other regions as well, as shown below:

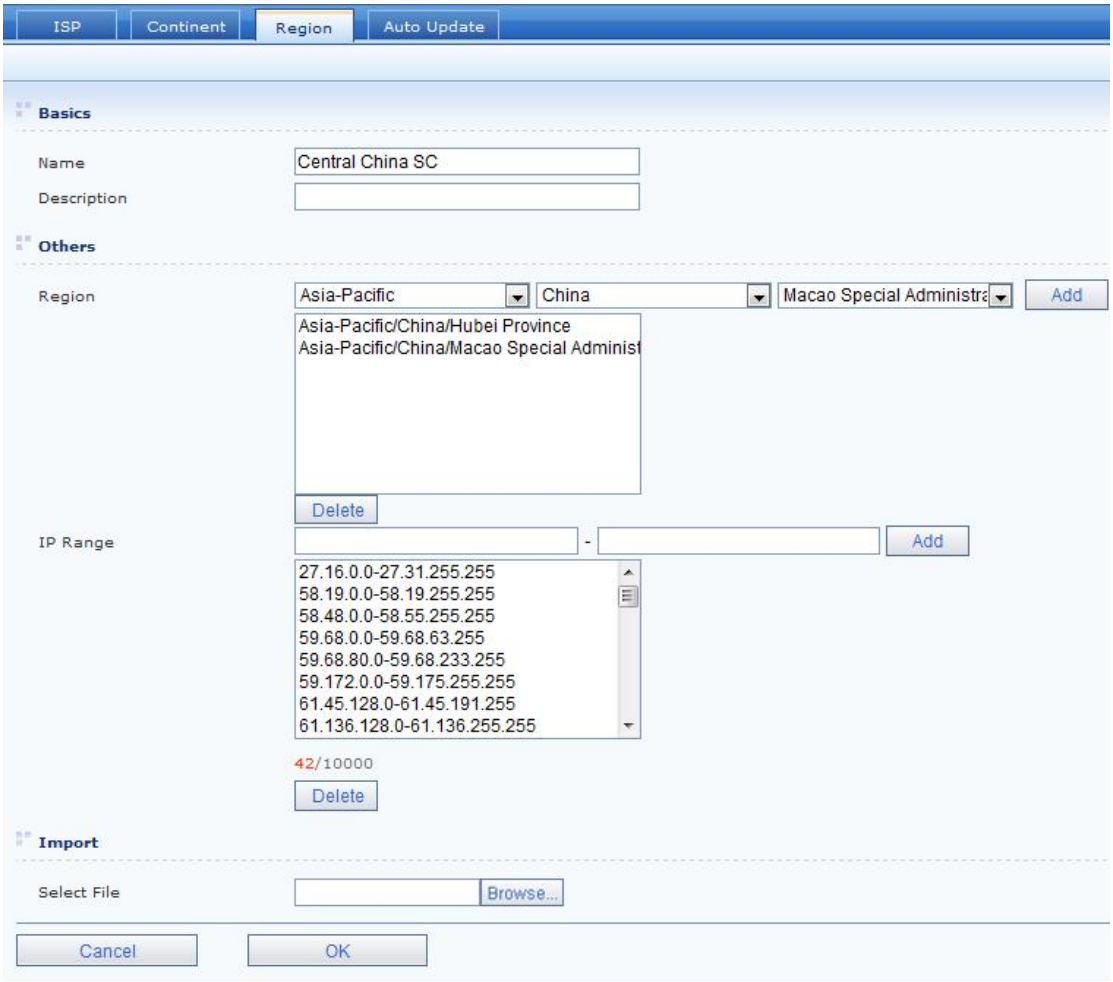
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



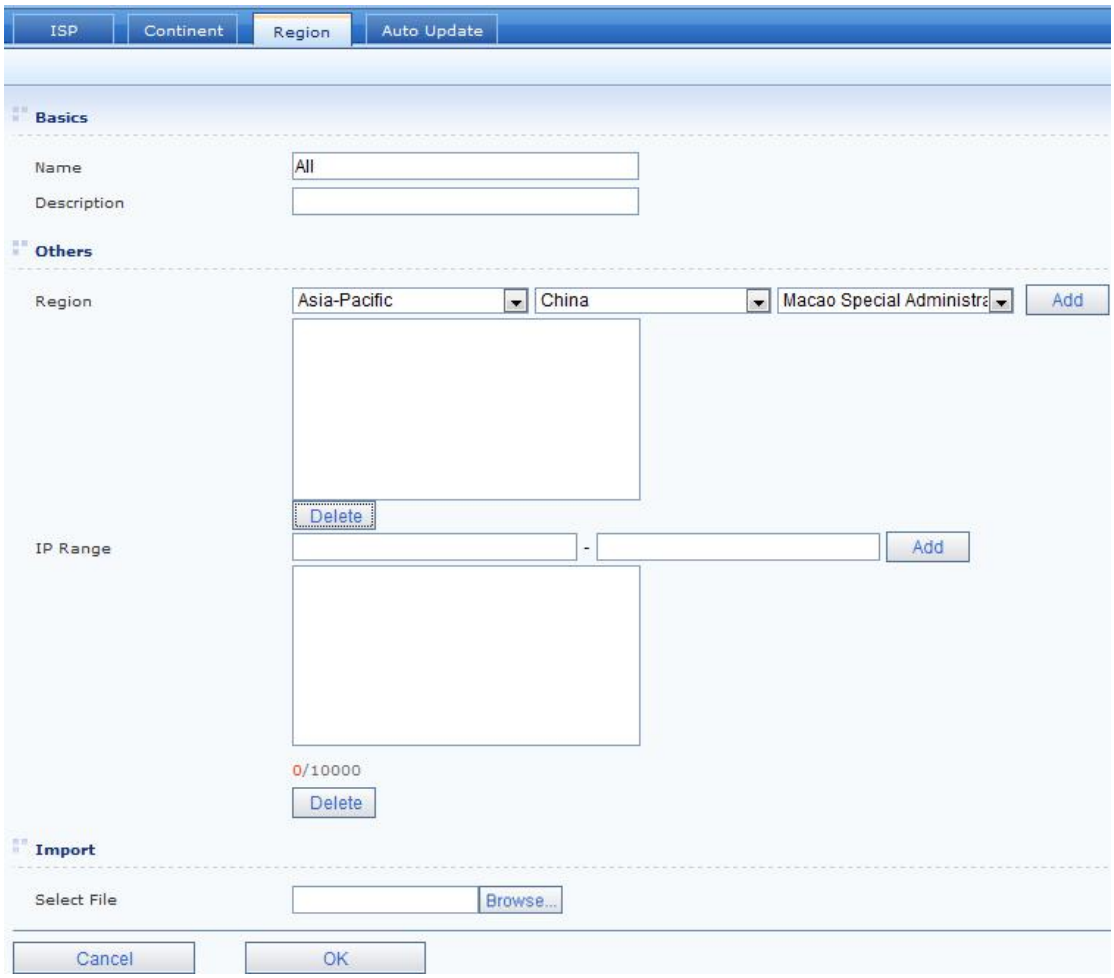
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

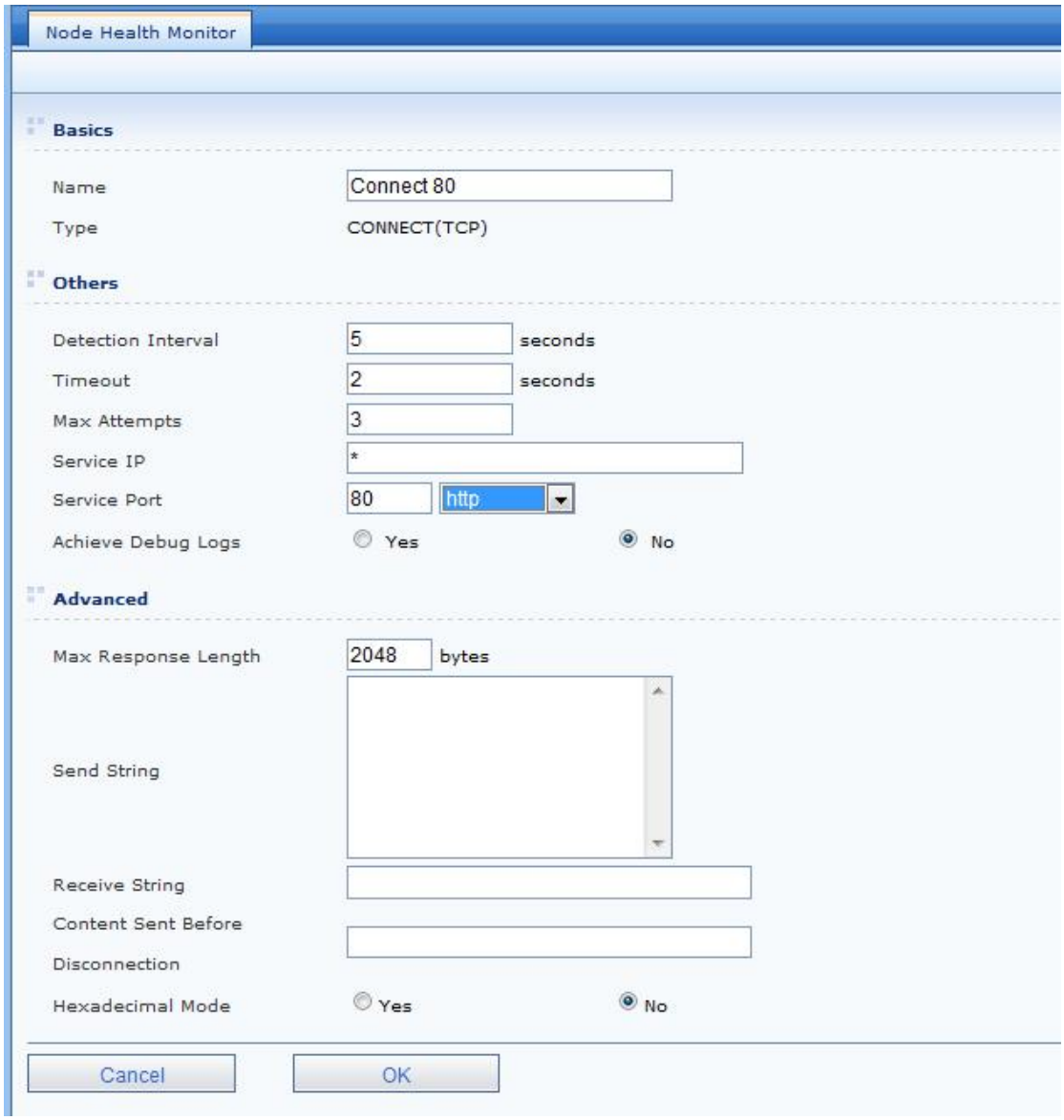


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



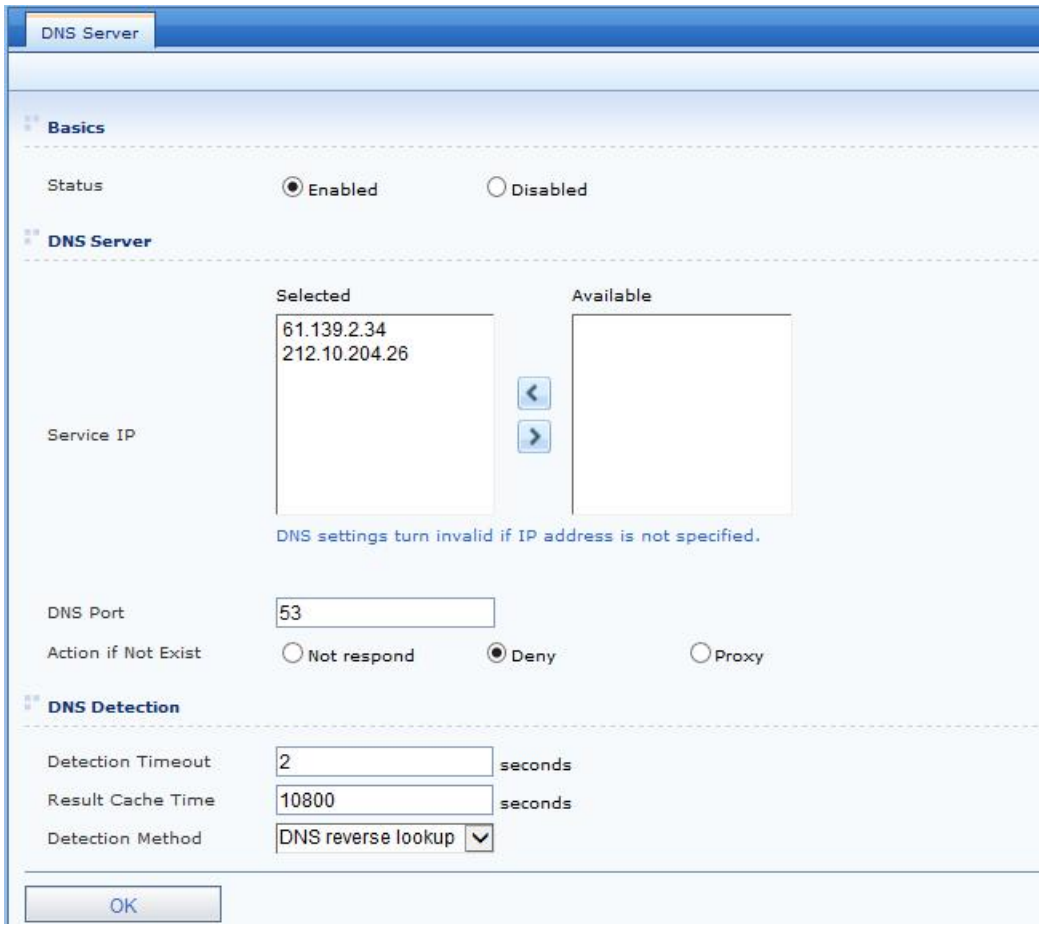
6. Go to the **Load Balancing > Node Monitor > Node Health Monitor** page, create a CONNECT(TCP)-based monitor and specify CONNECT 80 as its name, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



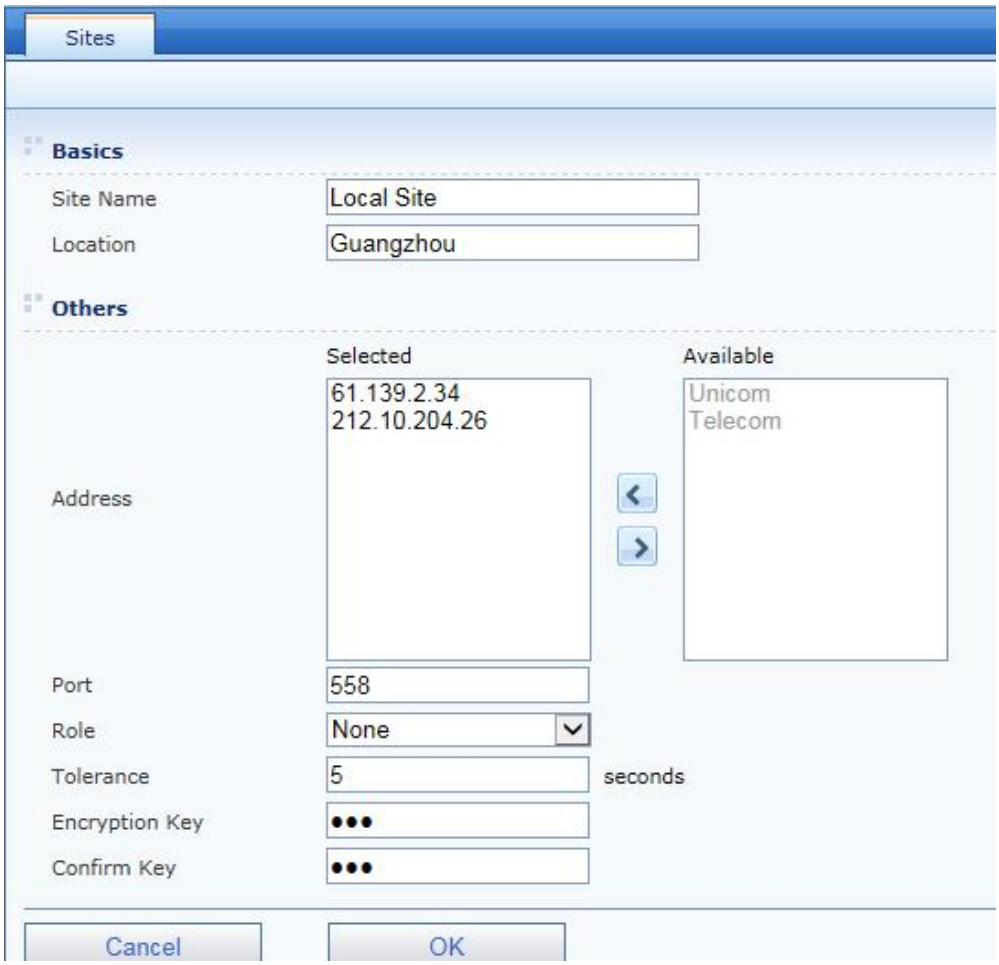
7. Go to the **Intelligent DNS > DNS Server** page, and add a service IP of the DNS server, as shown below:

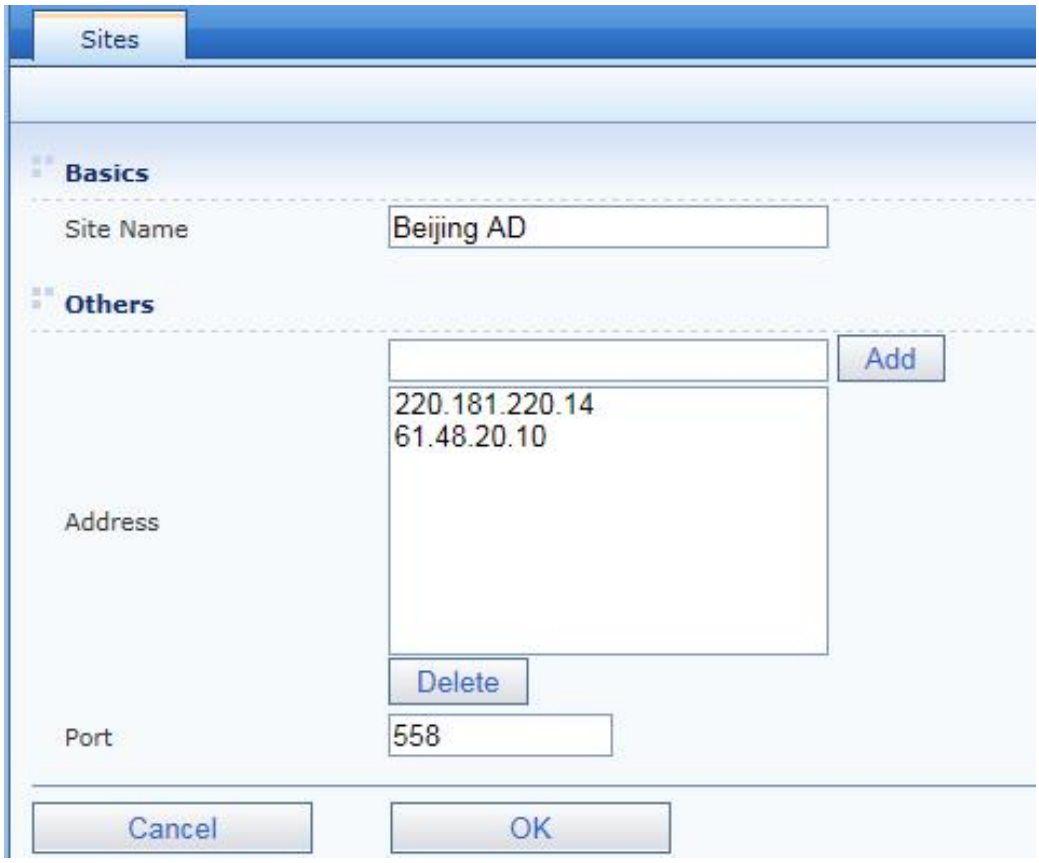
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



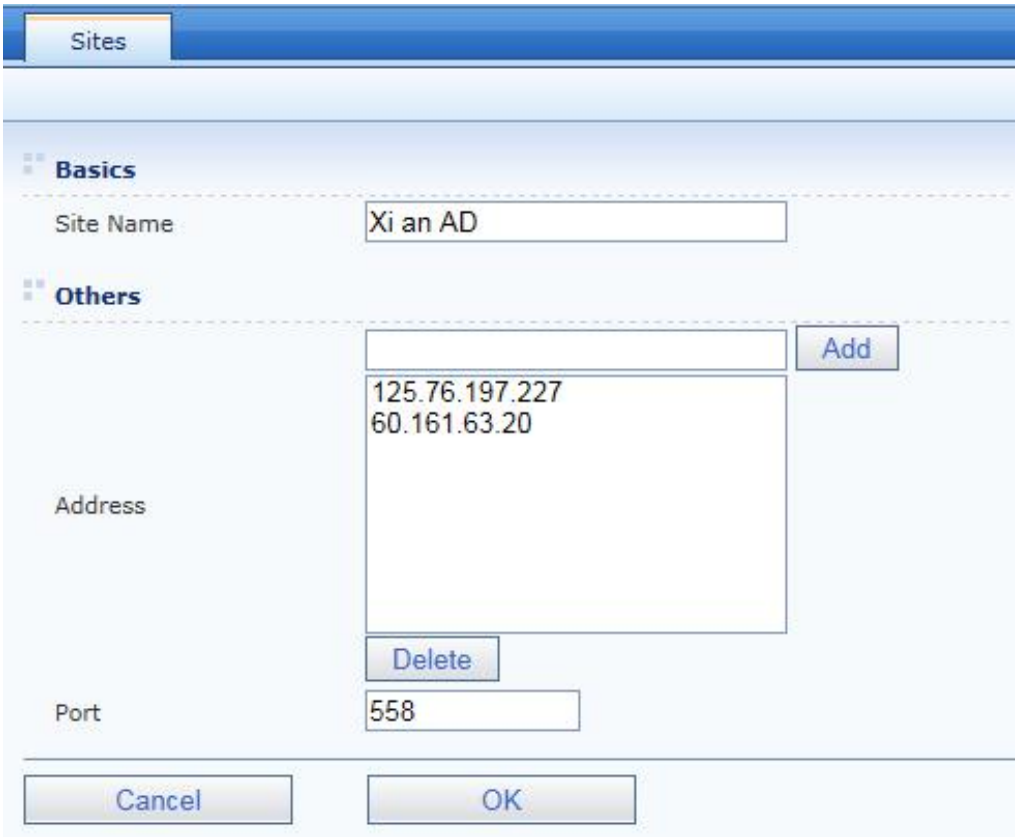
8. Go to the **Intelligent DNS > DNS Server** page, create three sites and define them as **Local Site**, **Beijing AD** and **Xi an AD** respectively, as shown in the following figures:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



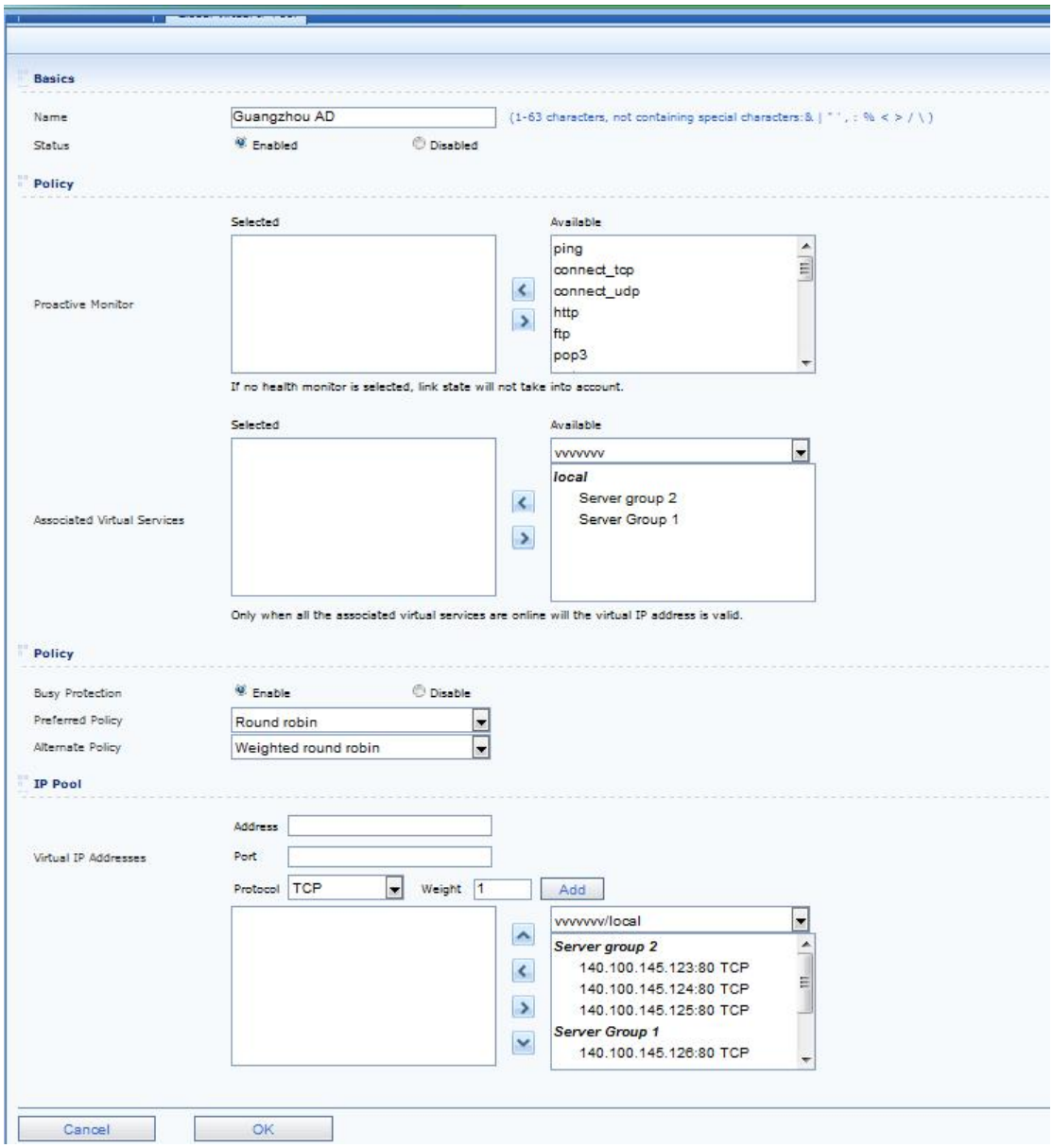


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



9. Go to the **Intelligent DNS > Virtual IP Pool > Global Virtual IP Pool** page, create three virtual IP pools and define them as **Guangzhou AD**, **Beijing AD** and **Xi an AD** respectively, and specify a port and the IP address which needs to be distributed, as shown in the following figure:

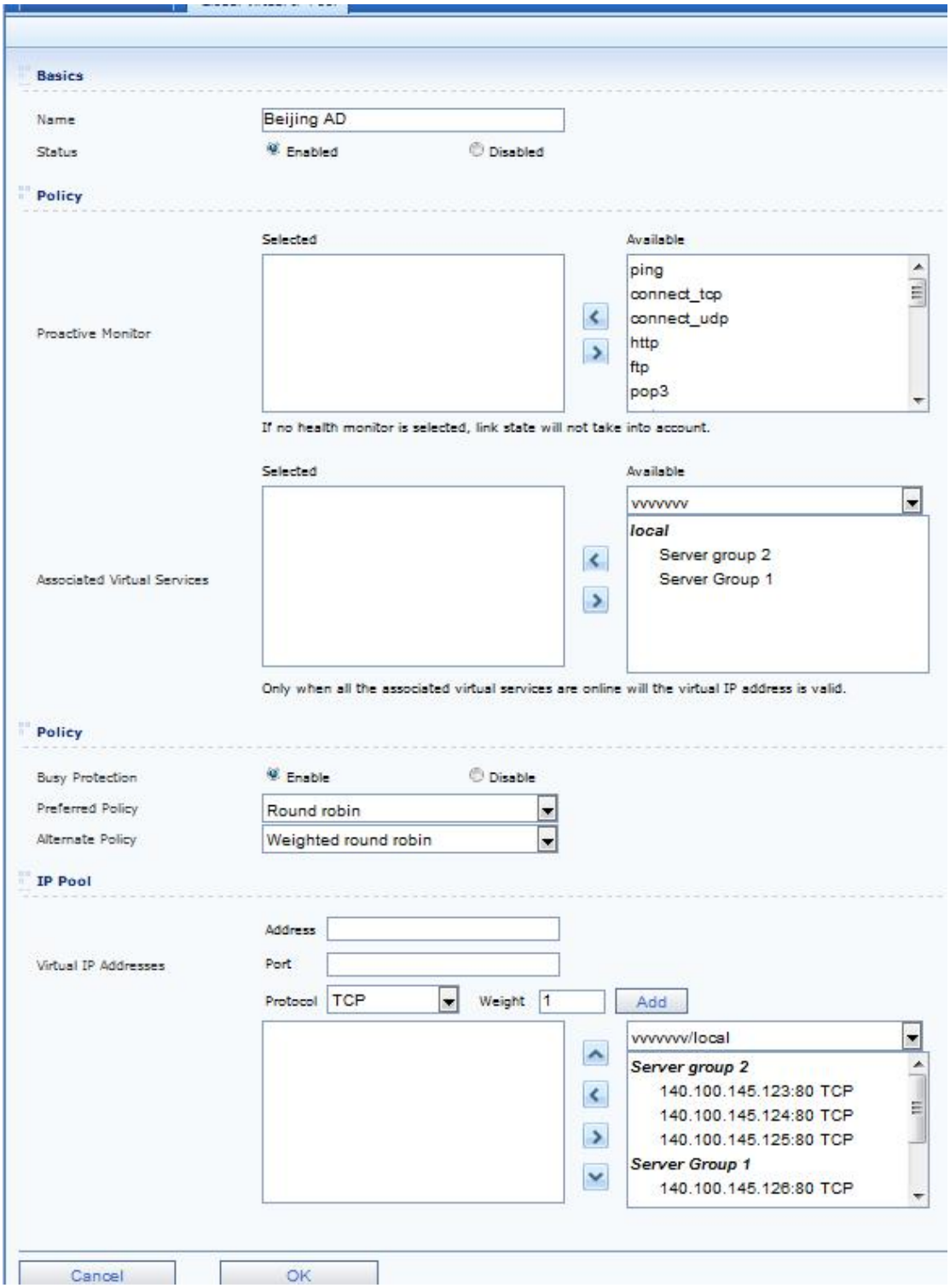
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



In **Virtual IP Addresses** filed, select the IP address and port distributed by the AD unit located in Guangzhou. The IP address and port of Web virtual service (Beijing) and Web virtual service (Xi'an) are synchronized from the AD units deployed in Beijing and Xi'an respectively.

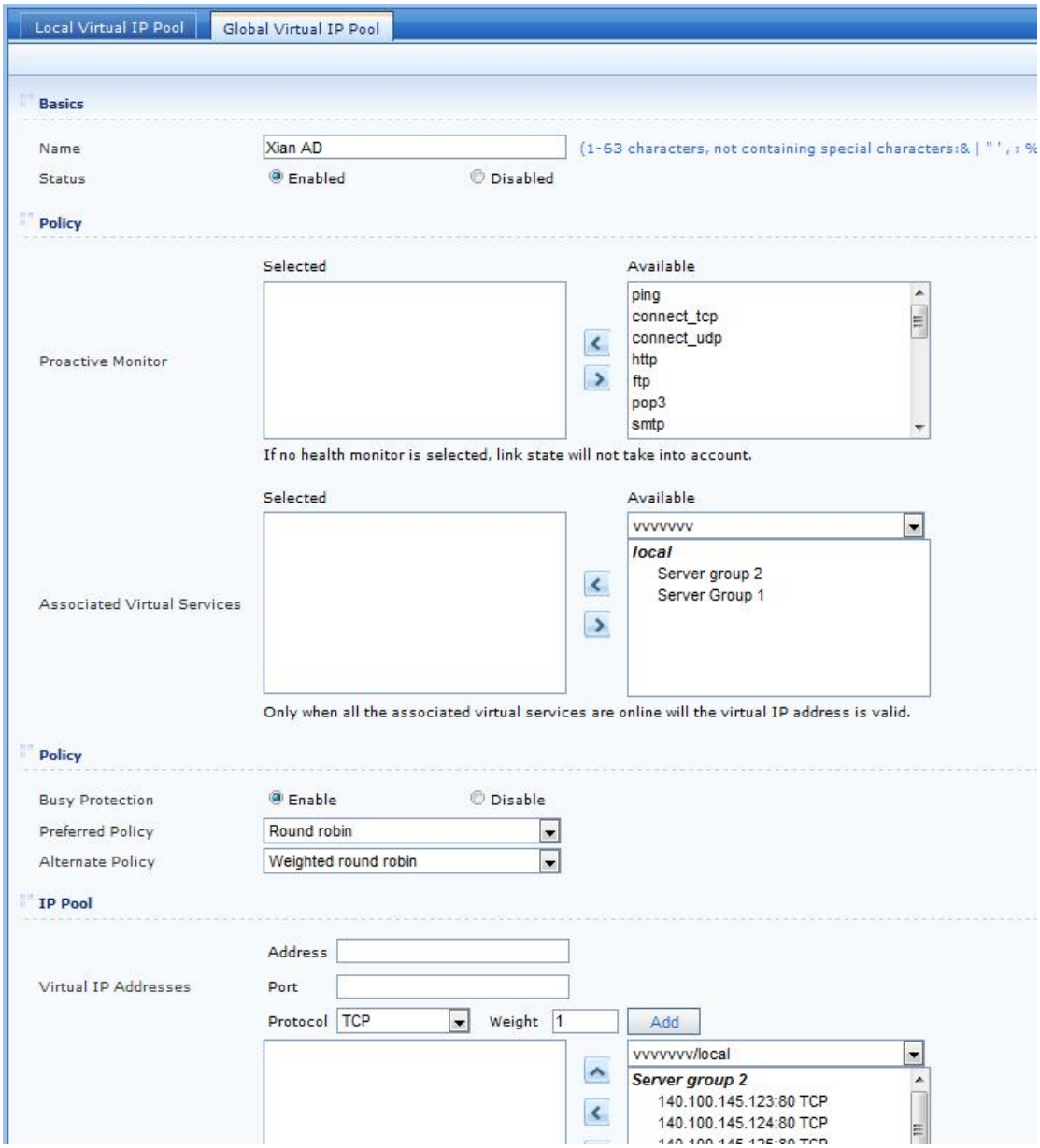
Select the IP address and port distributed by Web virtual service (Beijing), and specify a node monitor.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



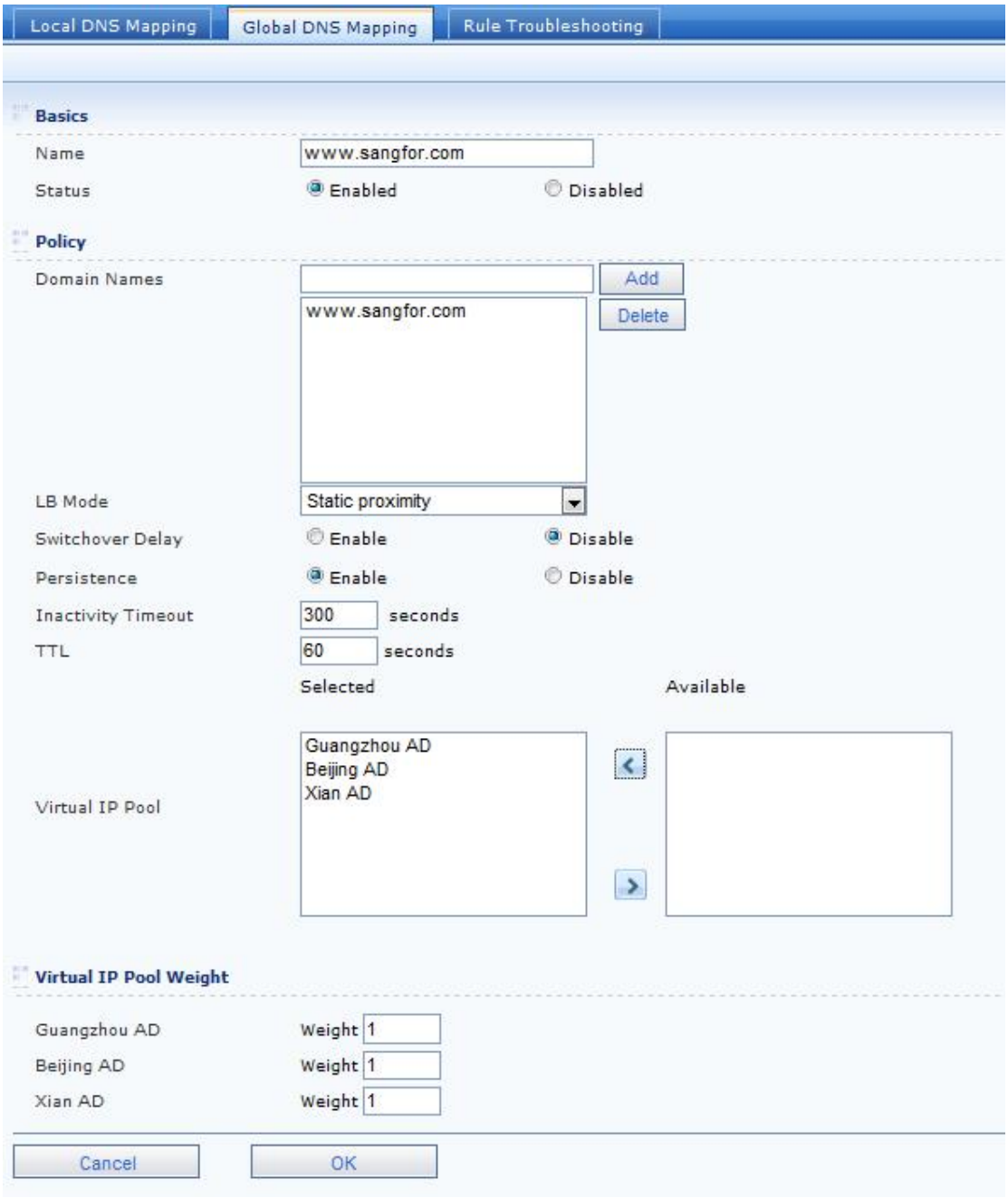
Select the IP address and port distributed by Web virtual service (Xi'an), and specify a node monitor.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



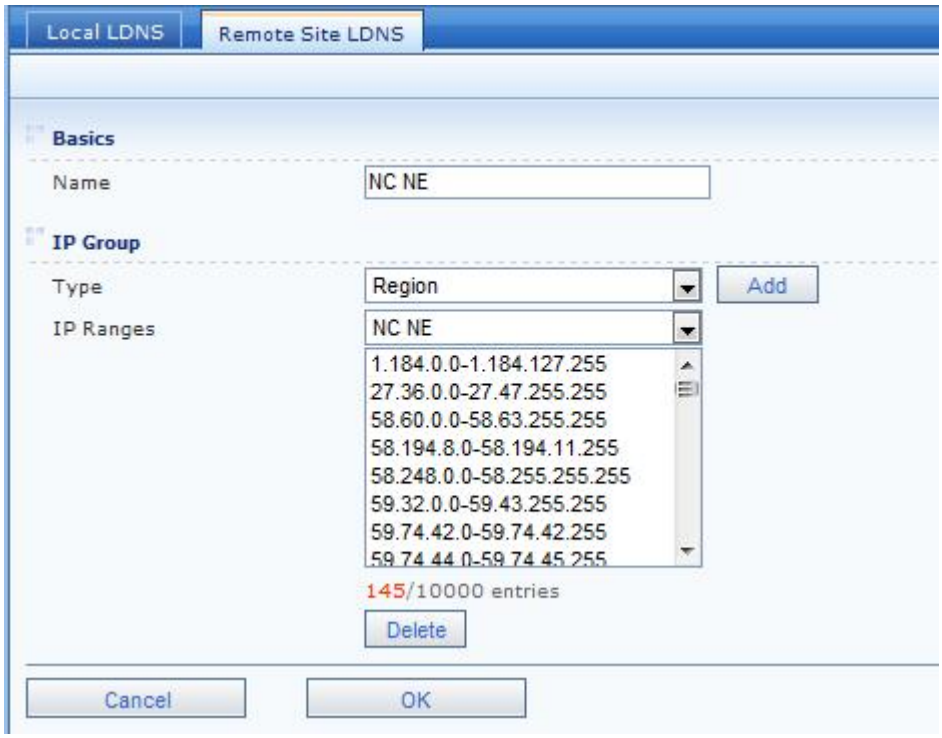
10. Go to the **Intelligent DNS > DNS Mapping > Global DNS Mapping** page, and create a DNS mapping, as shown below:

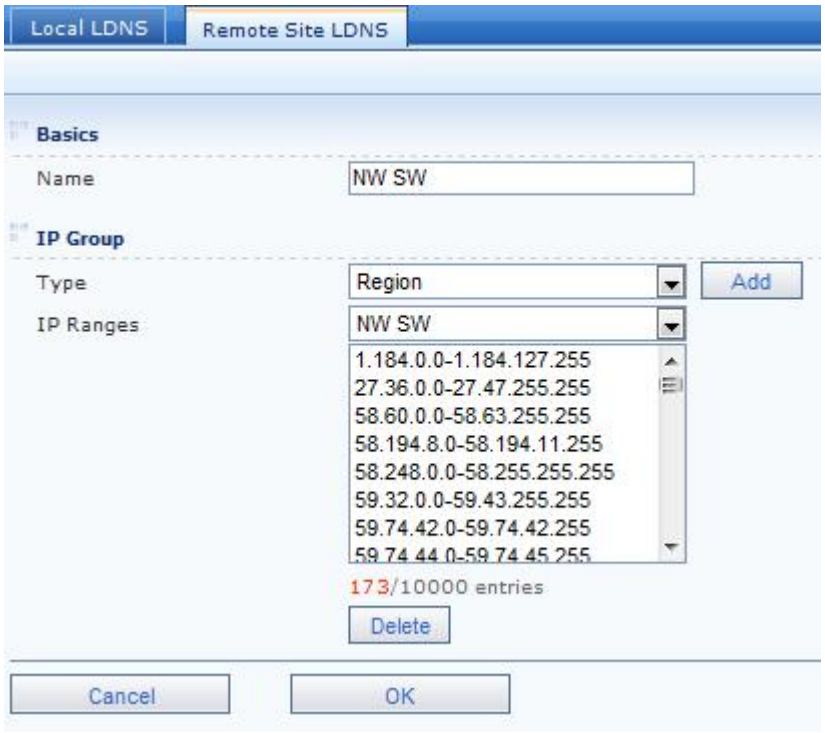
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



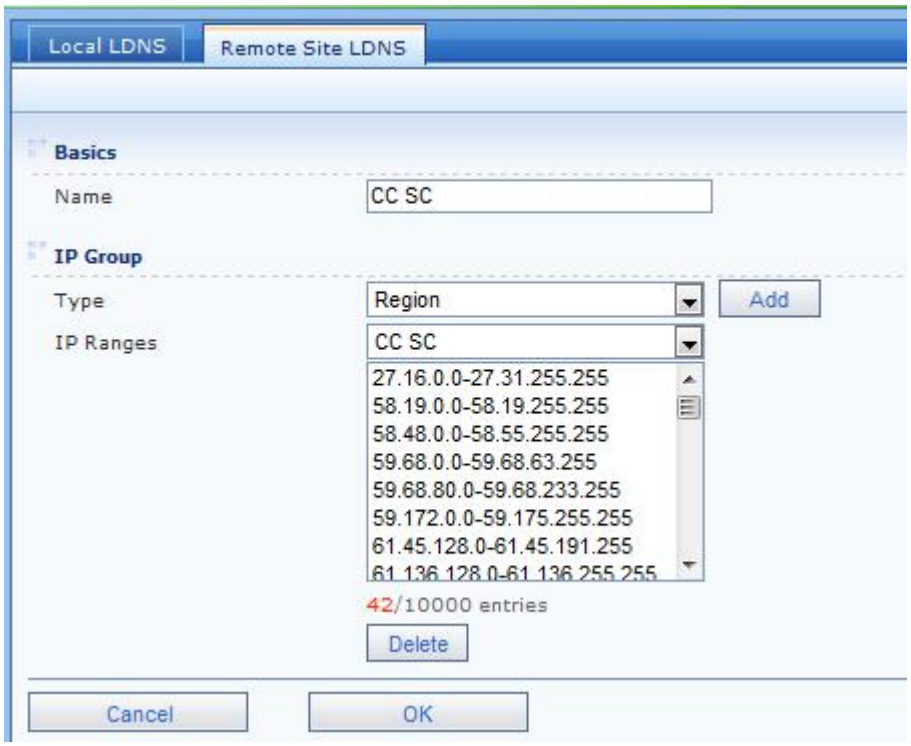
11. Go to the **Intelligent DNS > LDNS > Global LDNS** page, and create five LDNS and define them as **North /Northeast China**, **Northwest /Southwest China**, **Central /South China**, **All Regions**, and **Telecom**, **Unicom** as well.

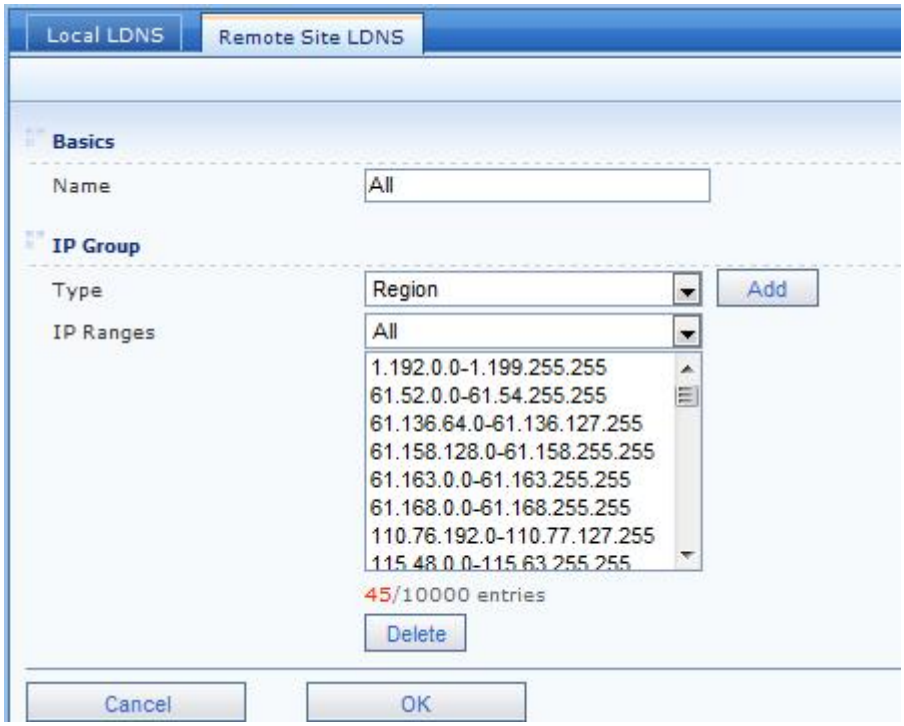
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



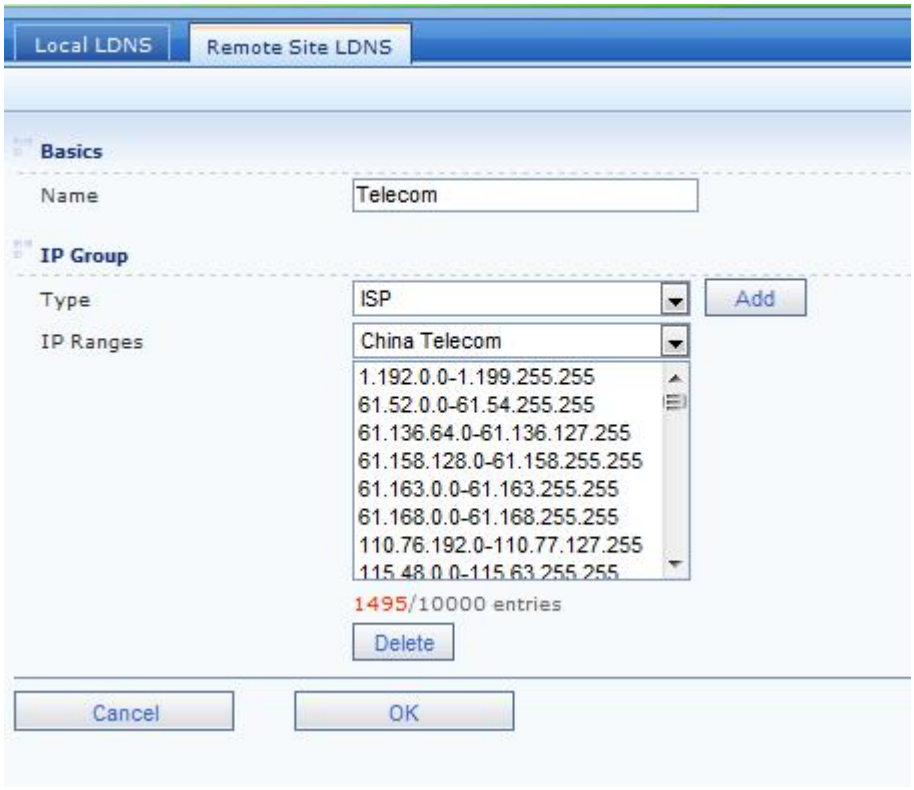


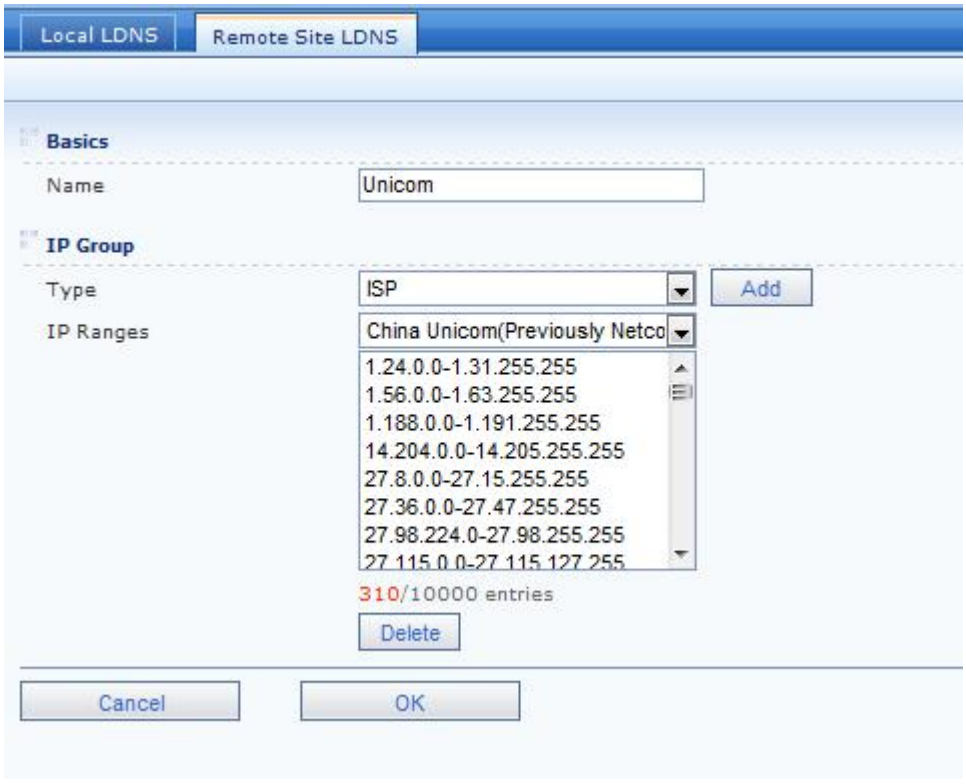
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



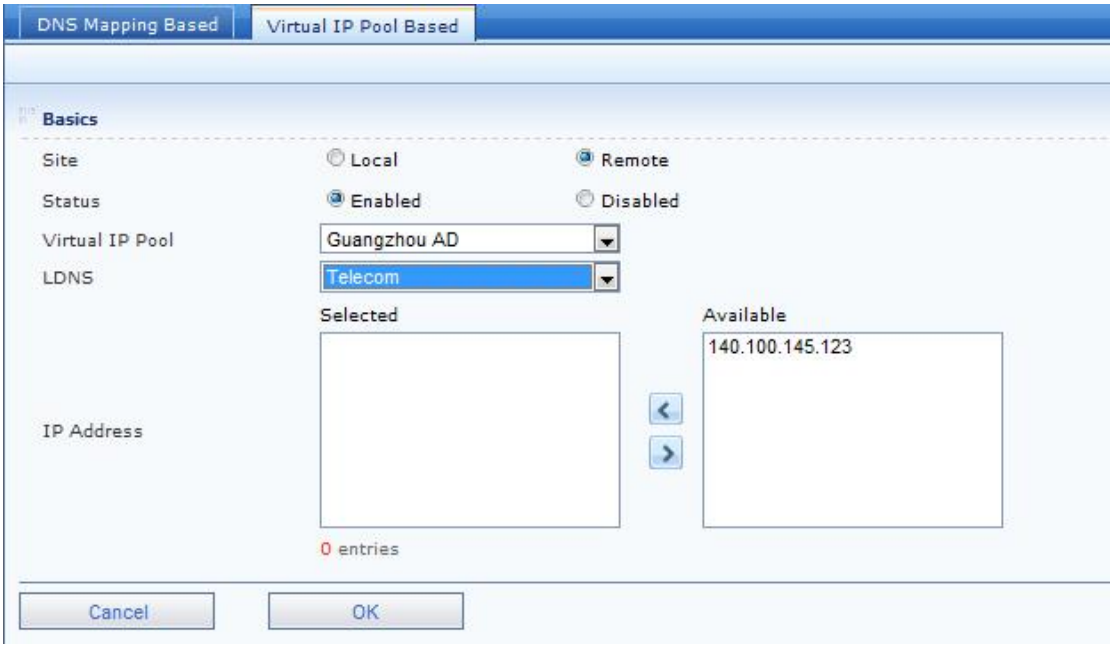


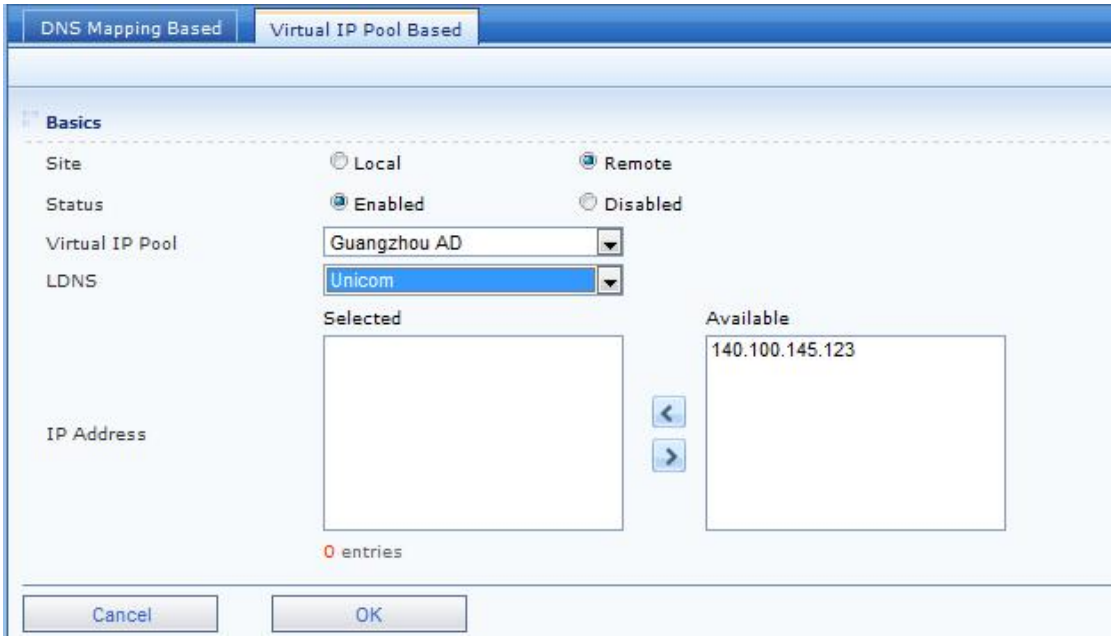
12. Go to the **Intelligent DNS > Static Proximity > DNS Mapping Based** page, and create three polices, as shown in the following figure:

13. Go to the **Intelligent DNS > Static Proximity > Virtual IP Pool Based** page, and create six policies, return corresponding IP address to users according to the ISP when DNS

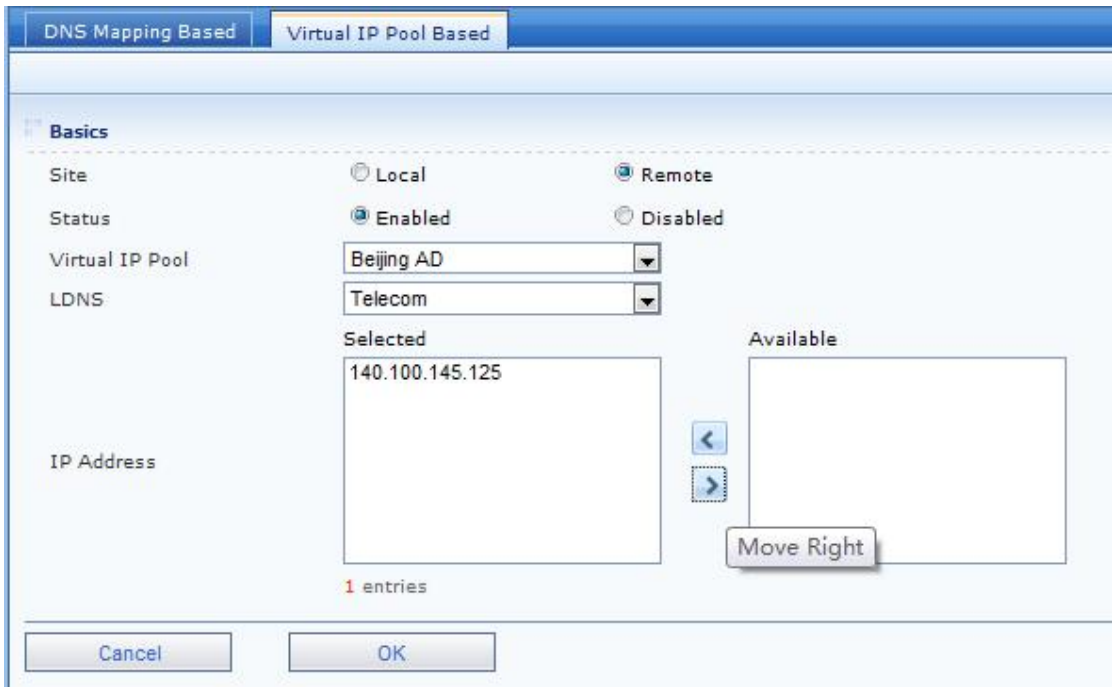
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

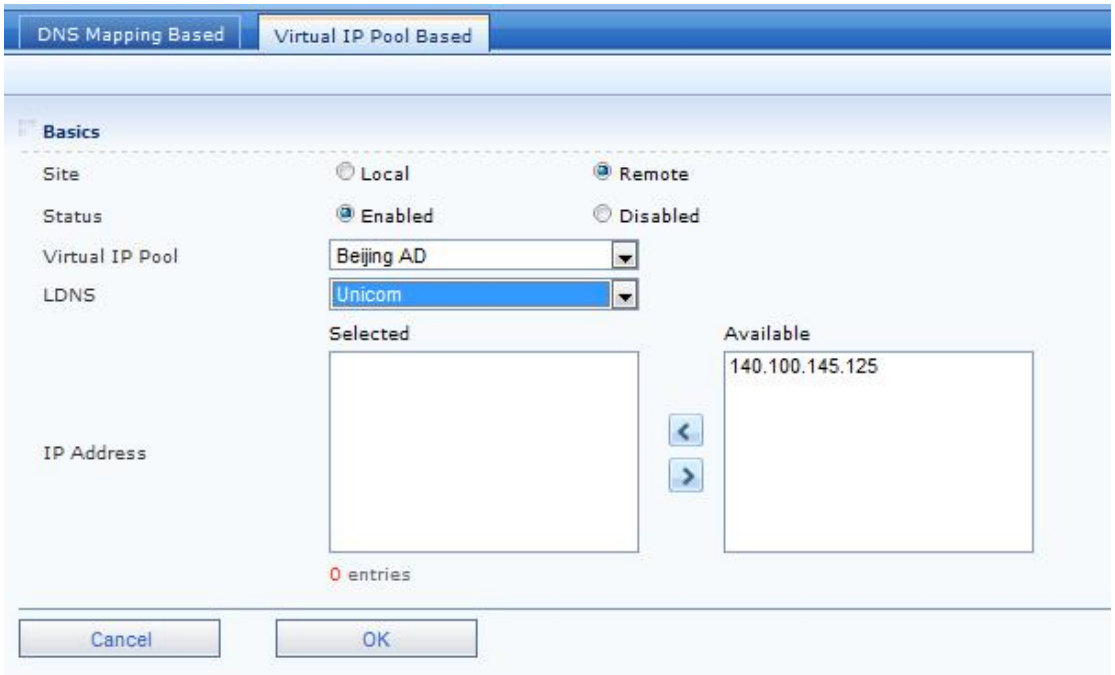
request is scheduled to a virtual IP pool.



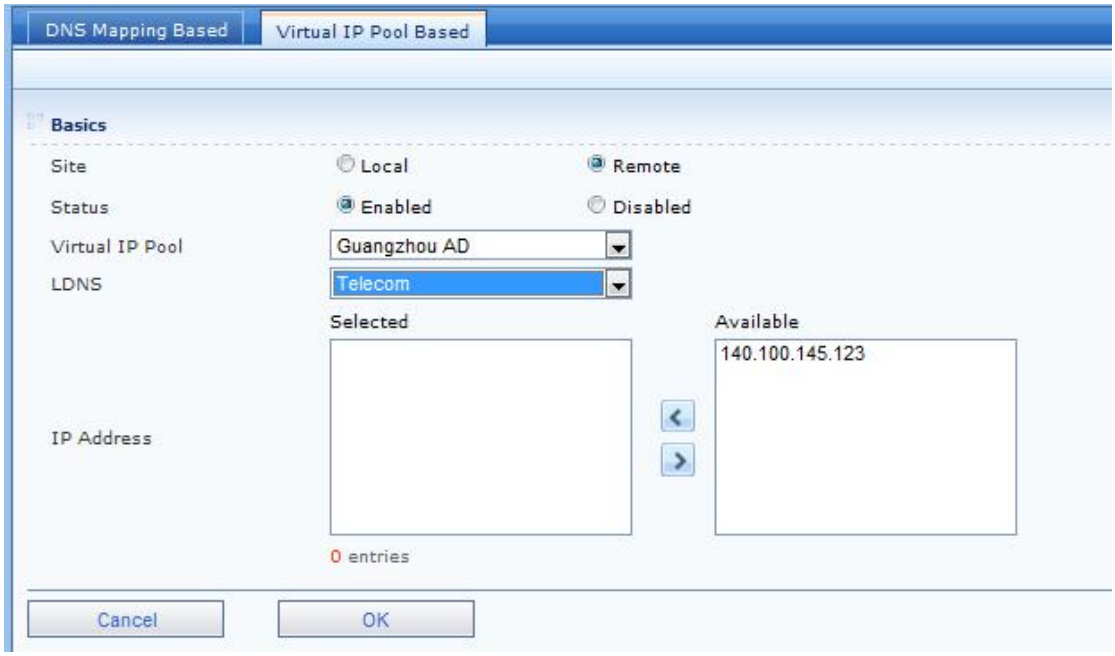


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





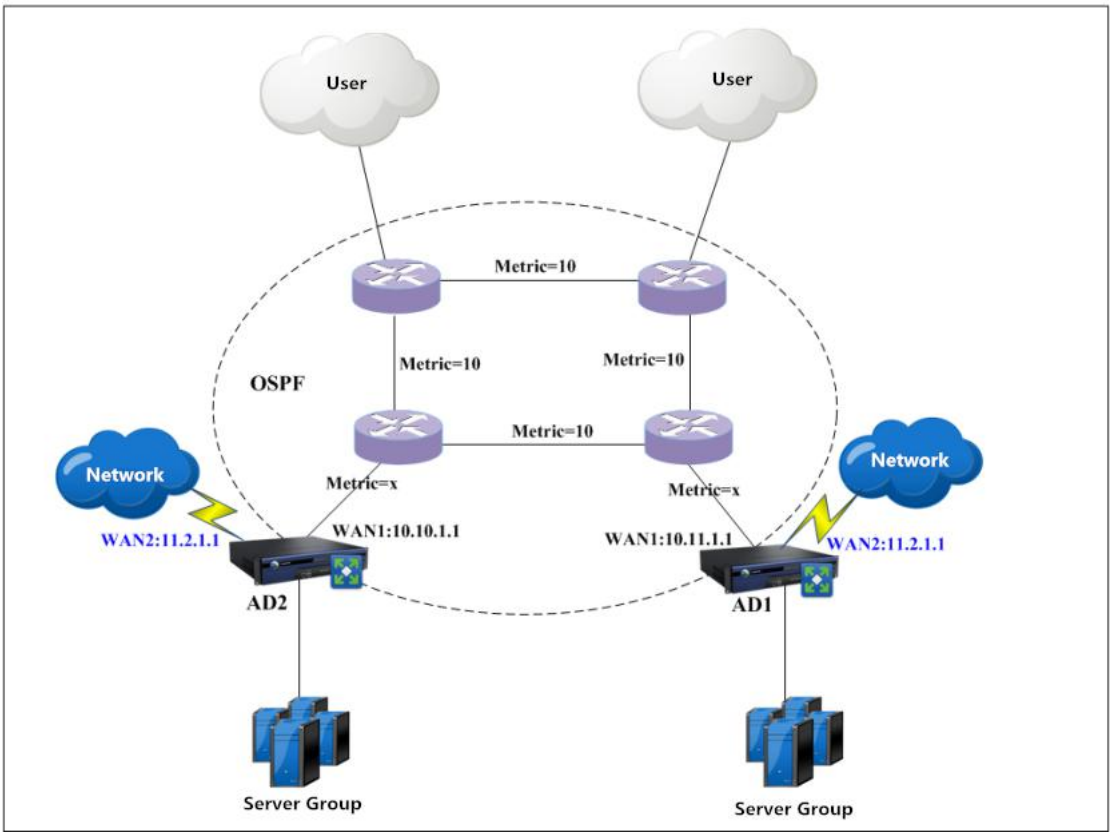
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



14.12 IP-Anycast

There are two server clusters: server cluster1 and server cluster2, which provide the same services, in customer network. OSPF protocol is enabled on the two AD units, and virtual services are configured. The IP address of virtual service IP group distributed by AD1 unit is 11. 2. 1. 1, while that of virtual service IP group distributed by AD2 unit is 11. 2. 1. 1. When user accesses the virtual service, the best link should be selected automatically for the user accessing server cluster1 or server cluster2. And there needs to implement redundancy backup, that means when the virtual service of one AD unit is unavailable, the users' request will be scheduled to other AD unit automatically.

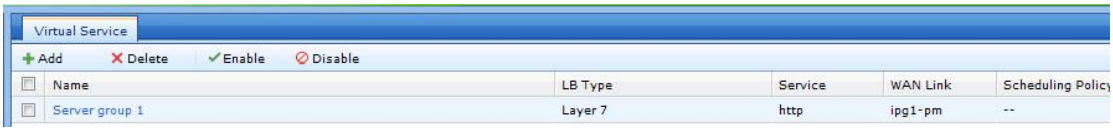
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



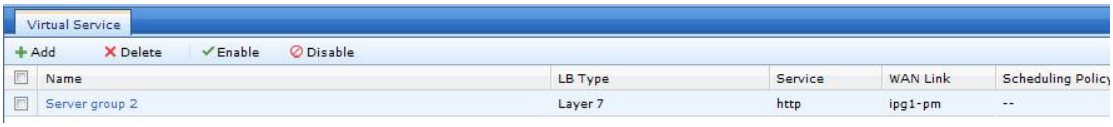
The configuration steps are as follows:

1. Configure virtual service, please refer to this chapter, **Configuring Server Load Balancing**. The virtual service configuration on the two AD units in this case, is shown as below:

The virtual service configured on AD1 unit:



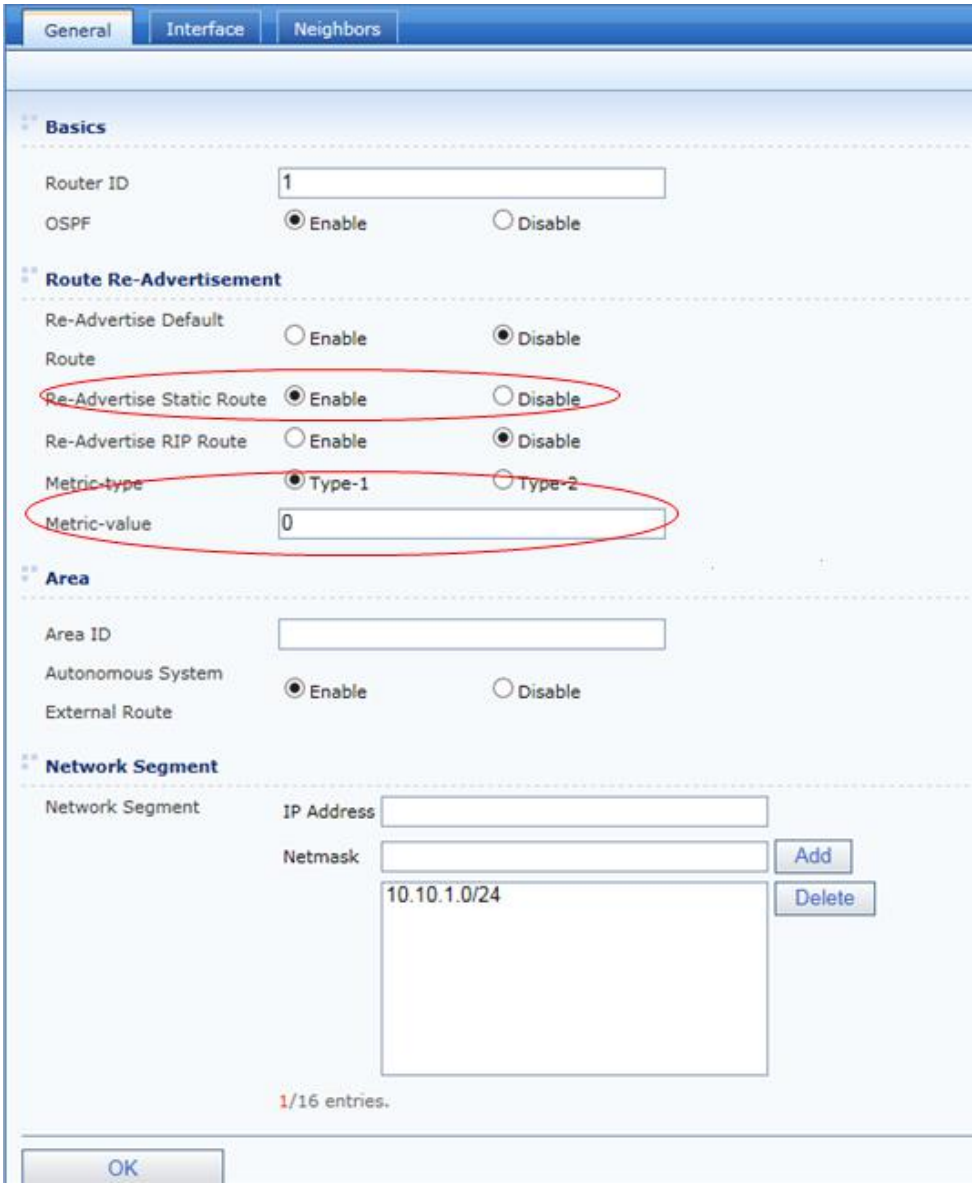
The virtual service configured on AD2 unit:



2. Enable **OSPF**. For configuration details, see Chapter 8, **OSPF**. If you want to use IP-Anycast feature, you must enable **Re-Advertise Static Route**, and select **Type-1** as Metric-type, and specify a value for Metric-Value (it's usually set as zero); you can also select **Type-2** by default. Recommend to use **Type-1** when the users access with accurate proximity principle.

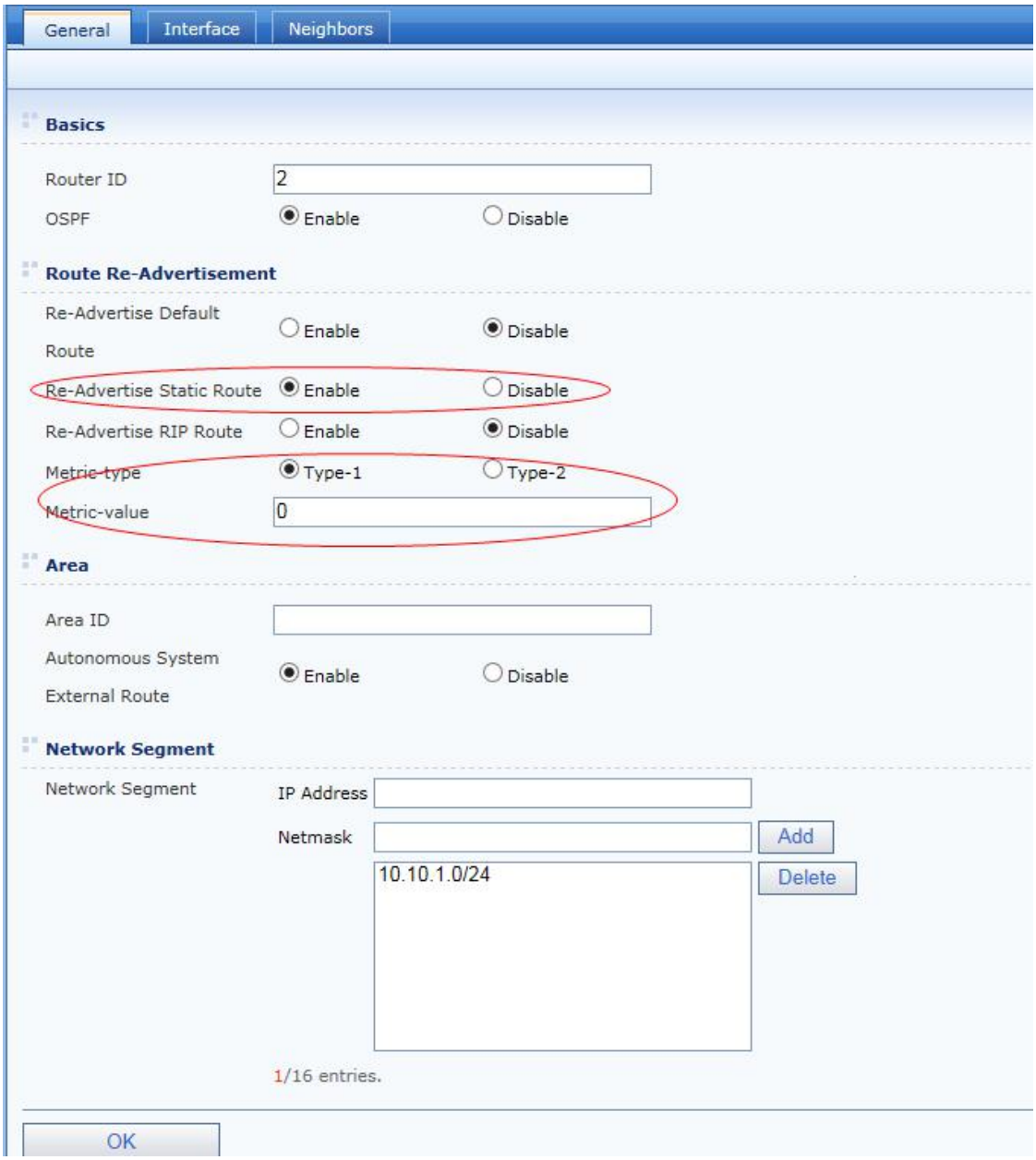
Configure OSPF on AD1 unit:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



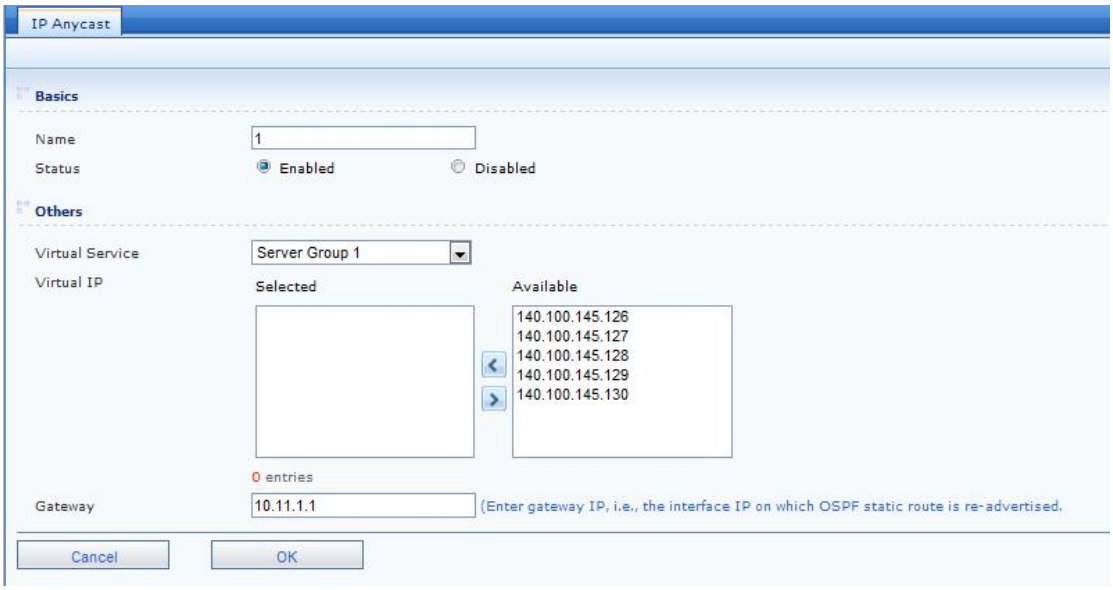
Configure OSPF on AD2 unit:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

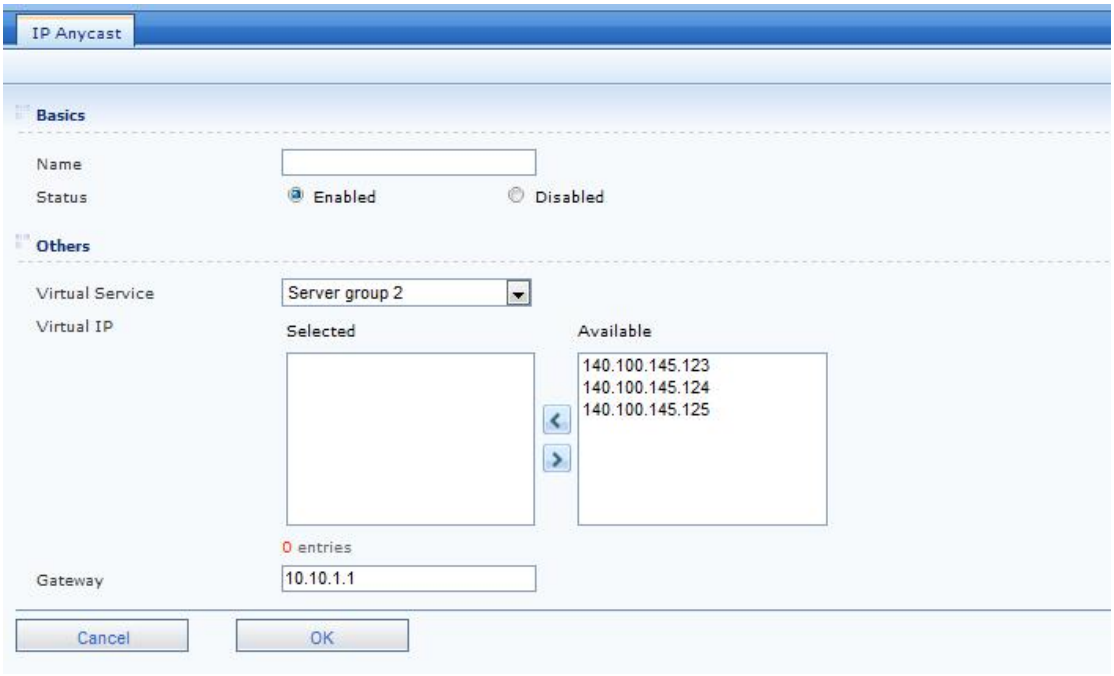


3. Configure IP-Anycast on the two AD unit. On AD1unit, configure IP-Anycast, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



On AD2 unit, configure IP-Anycast, as shown below:



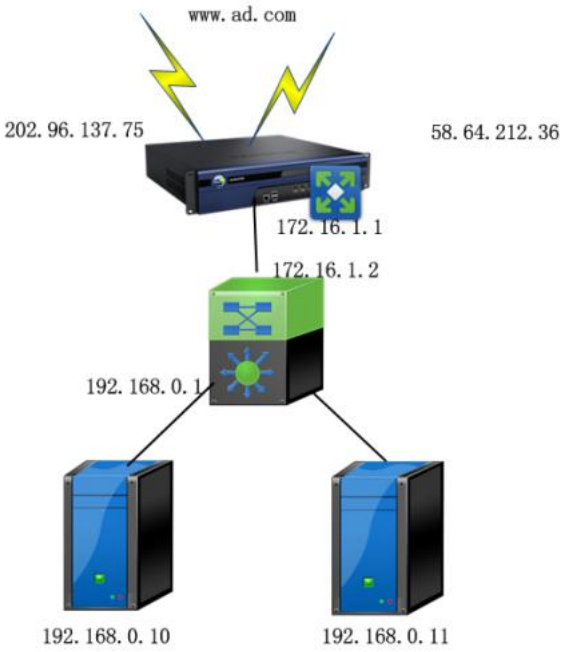
4. Configuration is finished. Then, the router will select the best path to reach the AD unit by calculating metric value. When user accesses server, the router will forward request to corresponding AD unit via the best path. The virtual service on AD1 unit is unavailable, the unit will advertise to the OSPF region to remove the corresponding route, and then the user will access to the virtual IP on AD2 unit.

14.13 DNS Proxy

In customer network, the network topology is shown in the following figure. AD unit is deployed in route mode, and it acts as gateway to proxy internal users to access the Internet.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

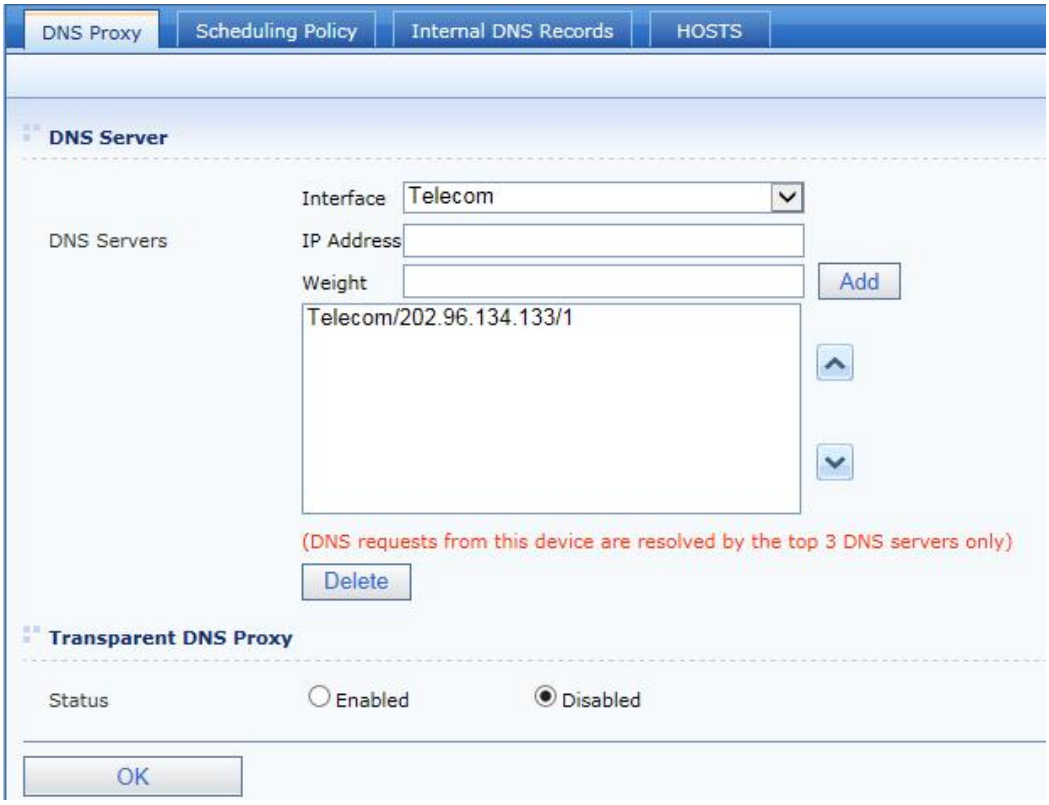
There are two WAN links Telecom and Unicom. The IP of Telecom link is 202. 96. 137. 75, and that of Unicom link is 58. 64. 212. 36. The two IP map to the same domain name: www. ad. com. The IP address of the LAN interface on AD unit is 172. 16. 1. 1. A layer 3 switch is placed behind AD unit. IP address of its interface used to connect to AD unit is 172. 16. 1. 2, and that of the interface used to connect to the intranet is 192. 168. 0. 1. The network segment used by internal hosts is 192. 168. 0. 0/24. There are two servers which provide same Web service, and their IP addresses are 192. 168. 0. 10 and 192. 168. 0. 11. The requirement of the customer is that the AD unit can implement domain name resolution and forward DNS requests.



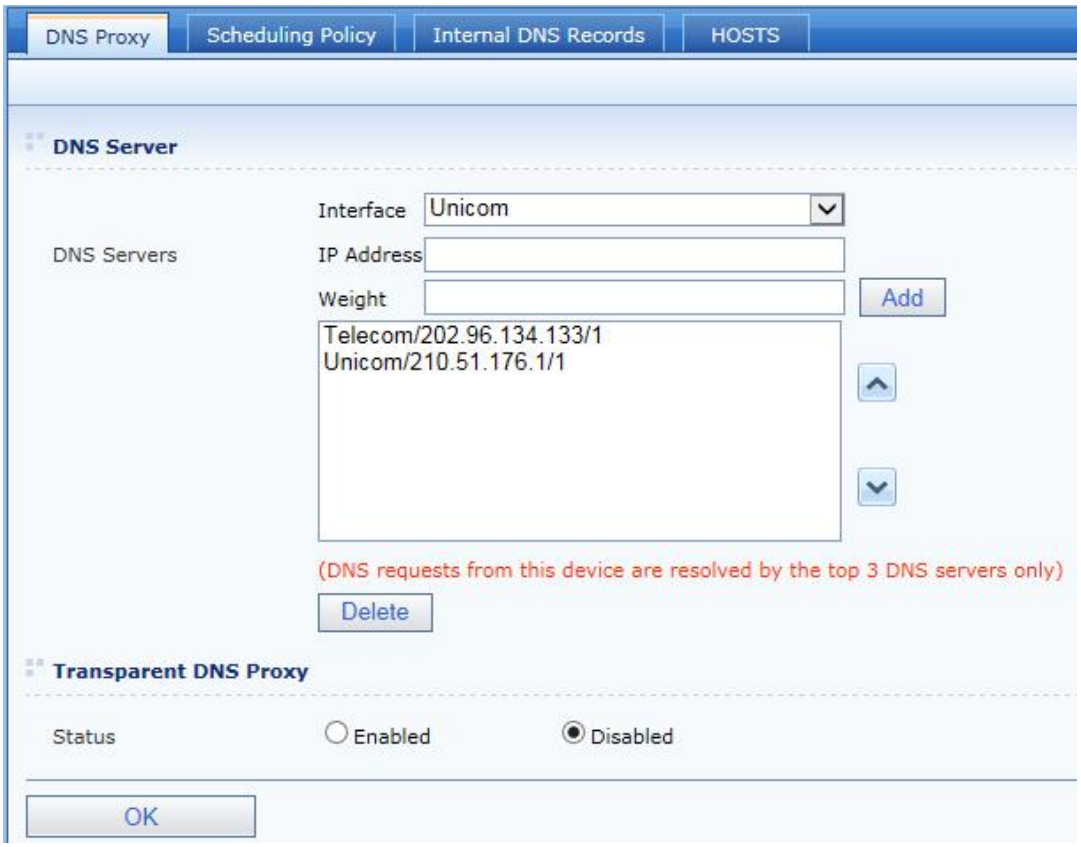
To create DNS proxy, you should do:

1. Go to the **Network > DNS Proxy** page, create a DNS server for Telecom link, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

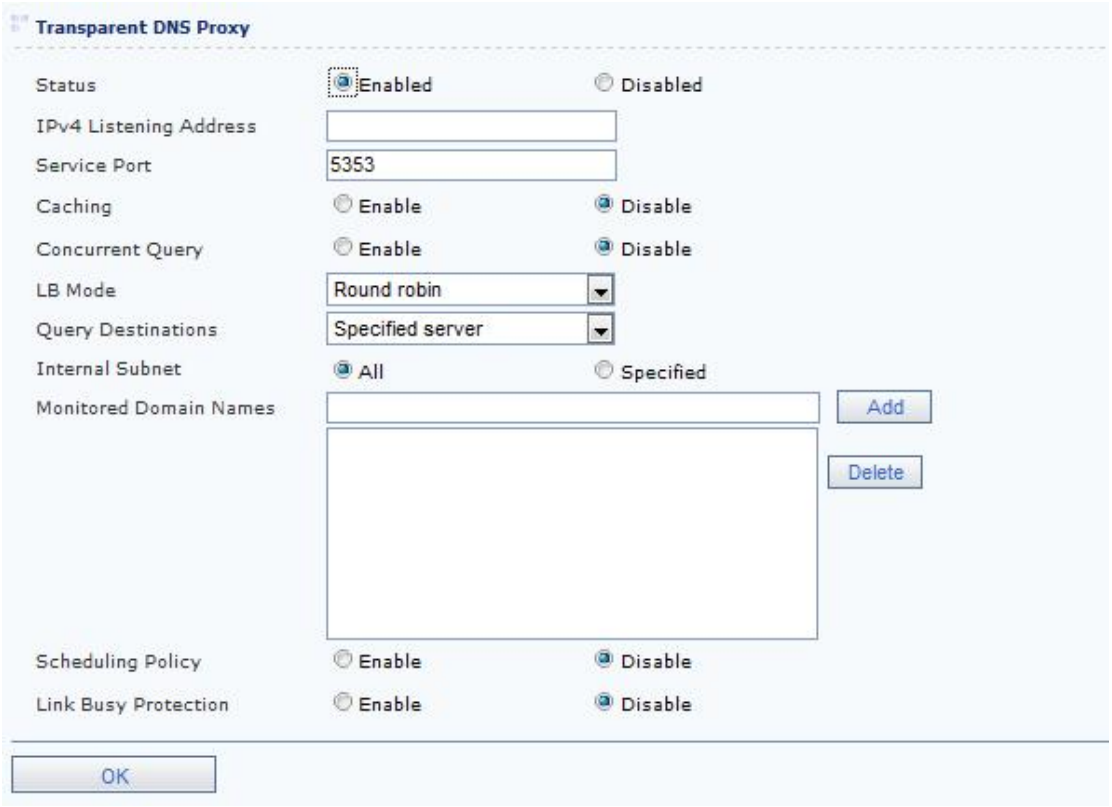


2. Go to the **Network > DNS Proxy** page, create a DNS server for Unicom link, as shown in the following figure:



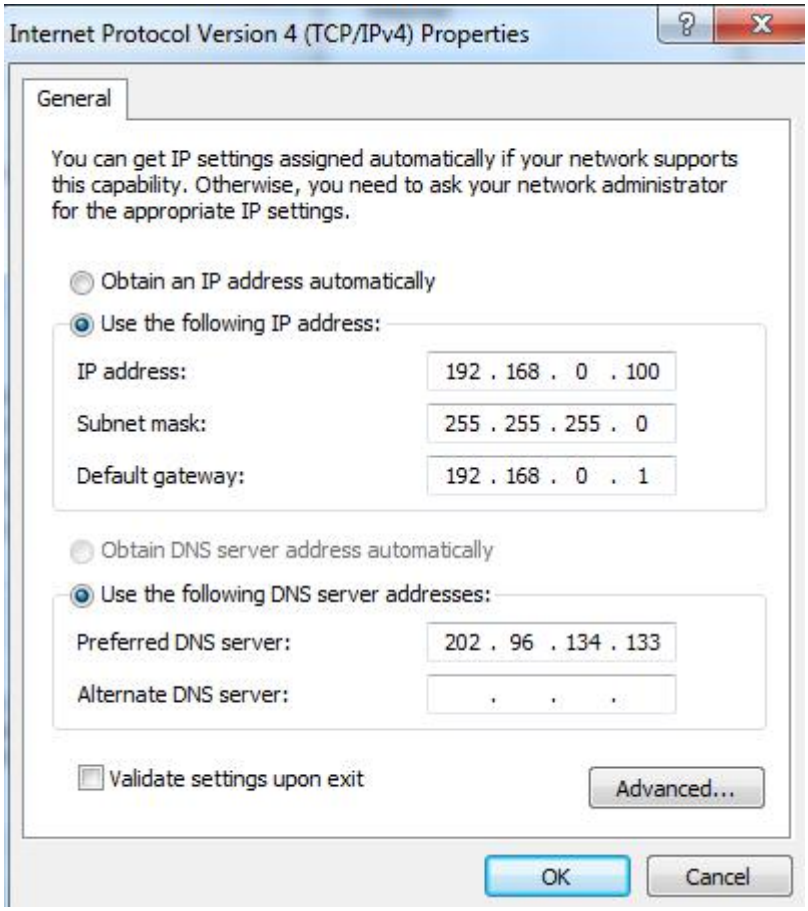
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

3. Enable **Transparent DNS Proxy** on the **Network > DNS Proxy** page, as shown below:



4. Set an IP address for the DNS server on internal computer, as shown below:

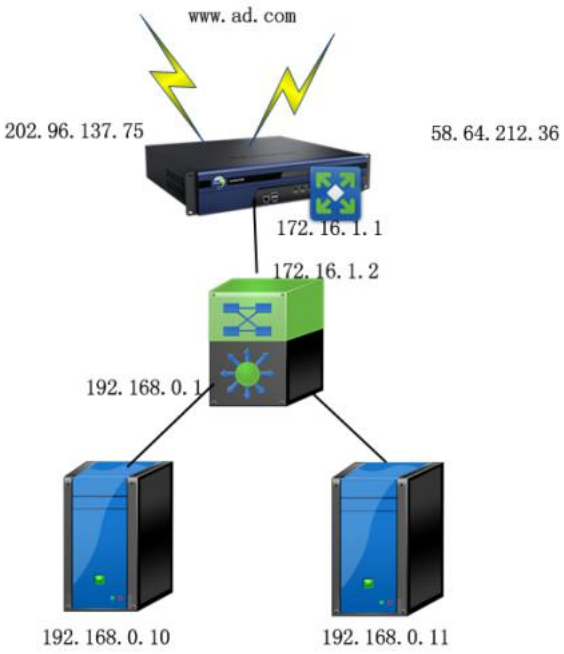
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



14.14 Outbound Scheduling Policy

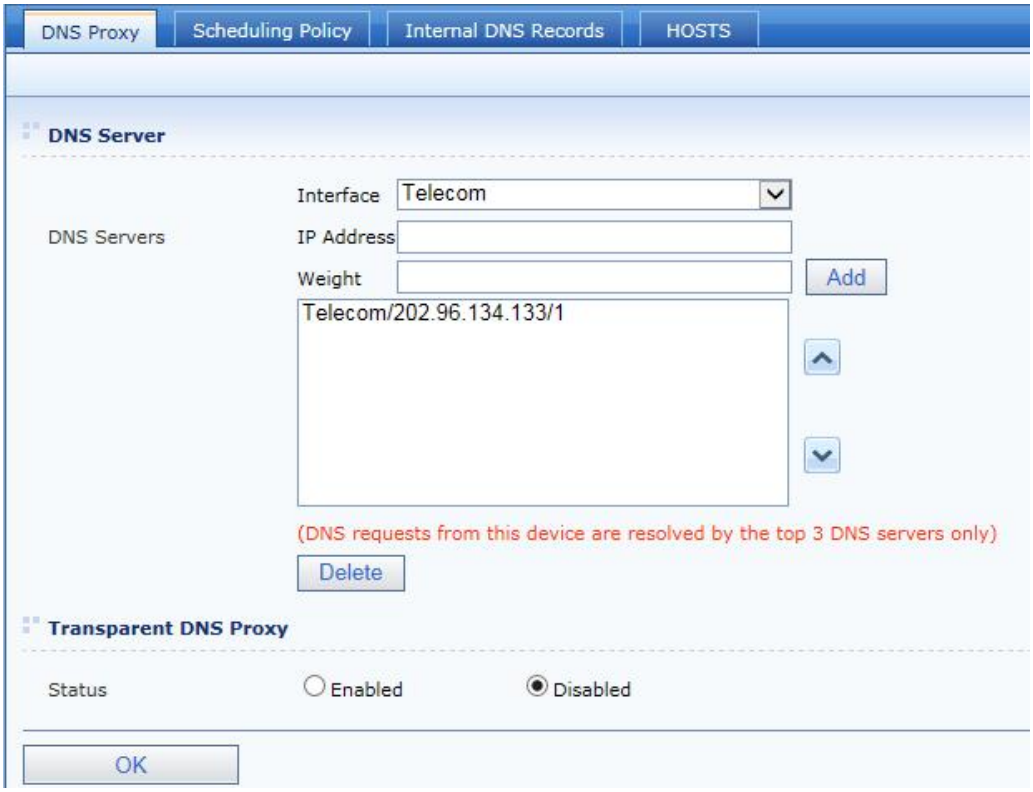
In one customer network, the network topology is shown in the following figure. AD unit is deployed in route mode, and it acts as gateway to proxy internal users to access to Internet. There are two WAN links Telecom and Unicom. The IP address of Telecom link is 202. 96. 137. 75, and that of Unicom link is 58. 64. 212. 36. The two IP map to the same domain name: www. ad. com. The IP address of the LAN interface on AD unit is 172. 16. 1. 1. The layer 3 switch is placed behind AD unit. IP address of its interface connected to AD unit is 172. 16. 1. 2, and that of the interface connected to the intranet is 192. 168. 0. 1. The network segment used by internal hosts is 192. 168. 0. 0/24. There are two servers which provide same Web service, and their IP addresses are 192. 168. 0. 10 and 192. 168. 0. 11. The customer wants that the AD unit can implement domain name resolution and forward DNS requests. When www. sina. com. cn is accessed on the host with IP address 192. 168. 0. 100, the corresponding DNS request only flows over Telecom link.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



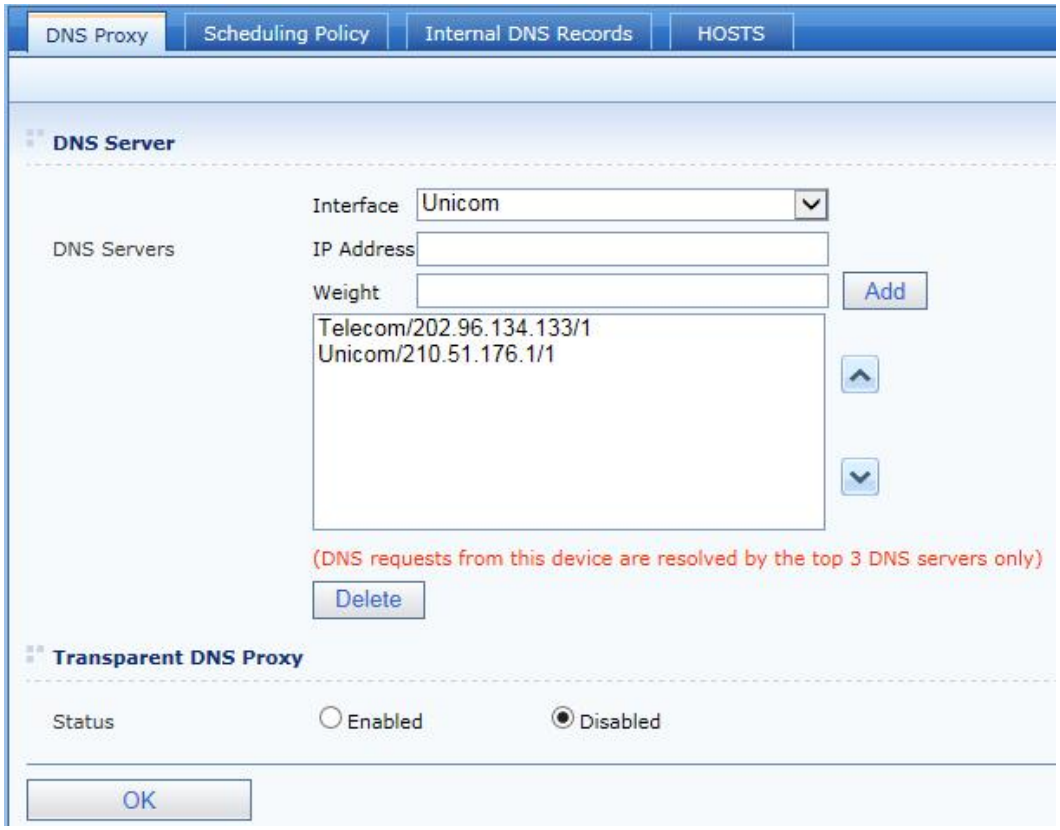
The configuration steps are as follows:

1. Go to the **Network > DNS Proxy** page, create a DNS server for Telecom link, as shown in the following figure:

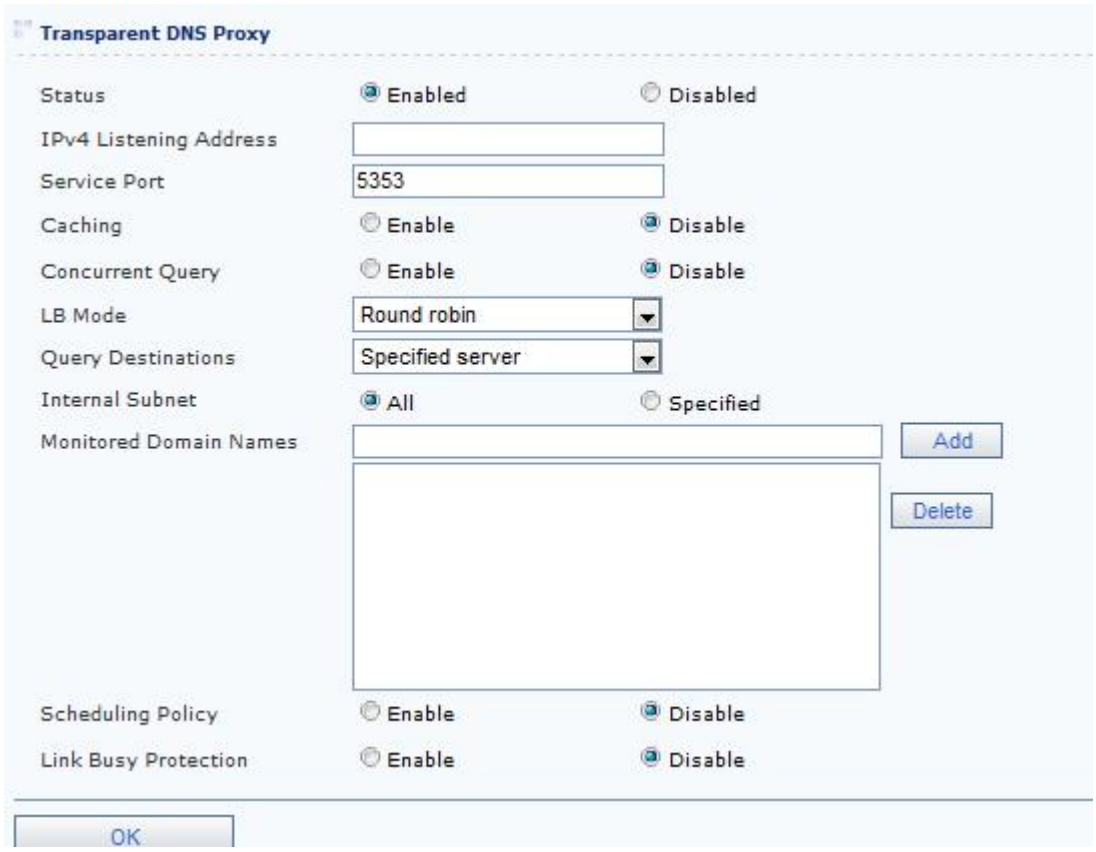


2. Go to the **Network > DNS Proxy** page, create a DNS server for Unicom link, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

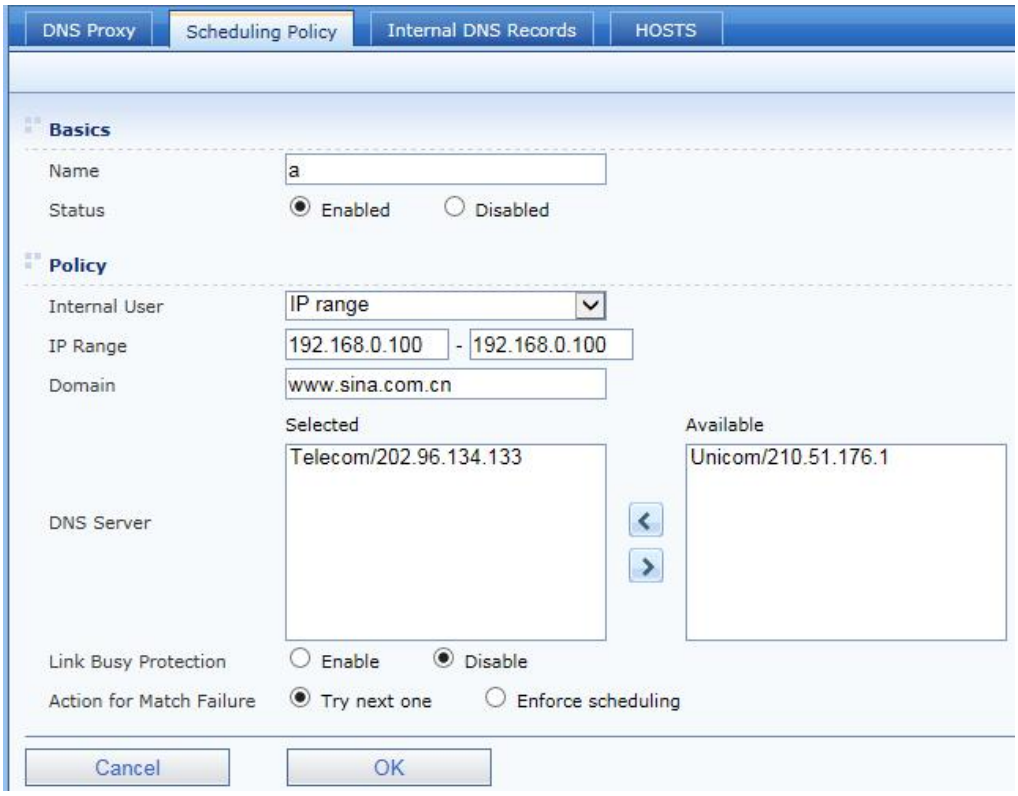


3. Enable **Transparent DNS Proxy** on the **Network > DNS Proxy** page, as shown below:



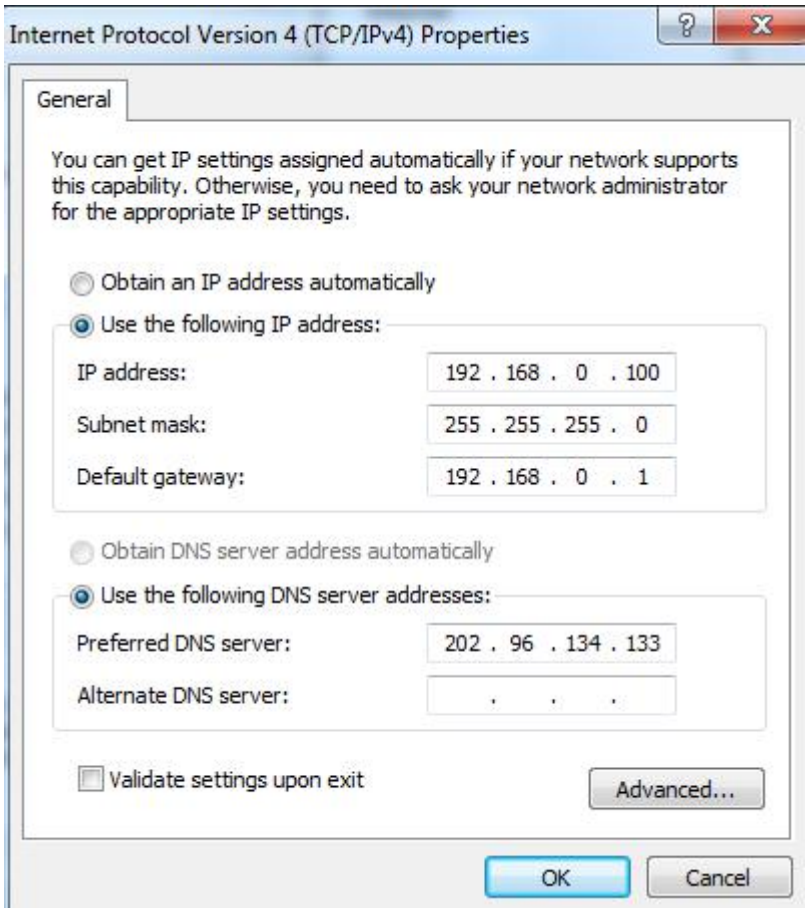
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

4. Go to the **Network > DNS Proxy > Scheduling Policy** page, create a scheduling policy to make the DNS request from the host with IP address 192. 168. 0. 100 only flow over Telecom link to resolve the domain name: www. sina. com. cn, as shown below:



5. Set an IP address for the DNS server on internal computer, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

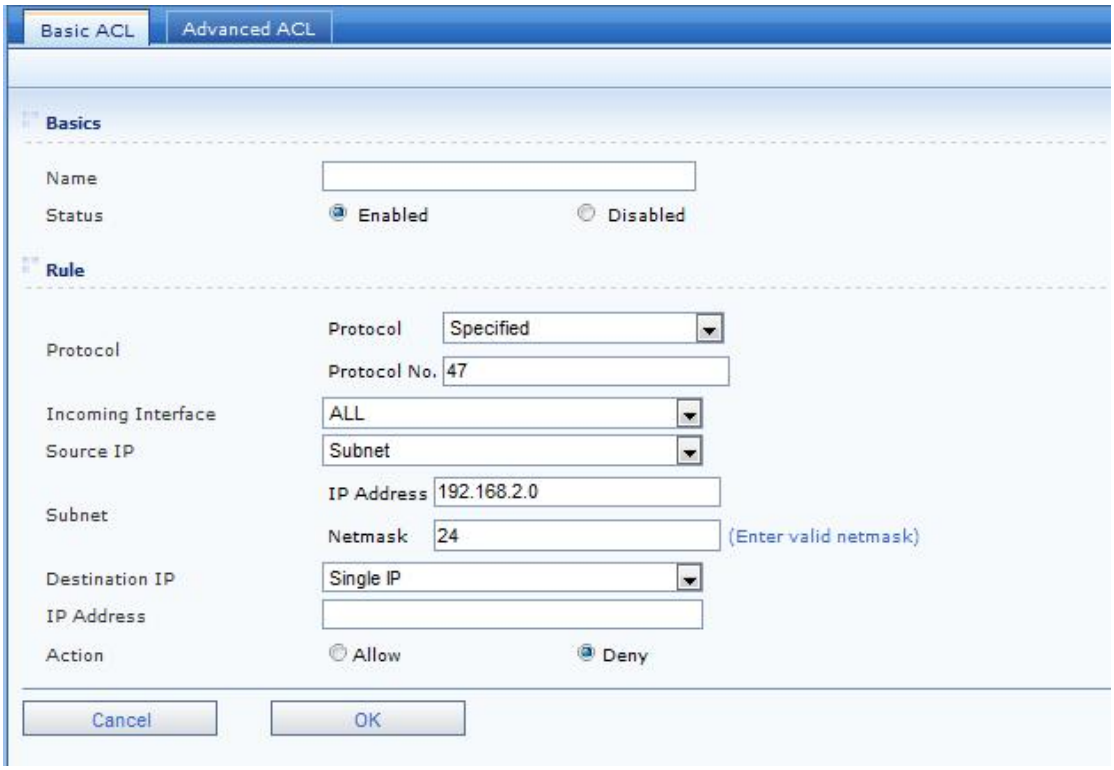


14.15 ACL

In one customer network, The AD unit is deployed at network egress in route mode. The customer wants to forbid the data packets encapsulated with GRE (protocol number is 47) to access the LAN servers on the network segment 192. 168. 2. 0.

Go to the **Network > ACL > Basic ACL** page, set the five elements of data packets to forbid the data packets which carry the following information: protocol number is 47 and destination IP address is the one on the network segment 192. 168. 2. 0, as shown in the following figure:

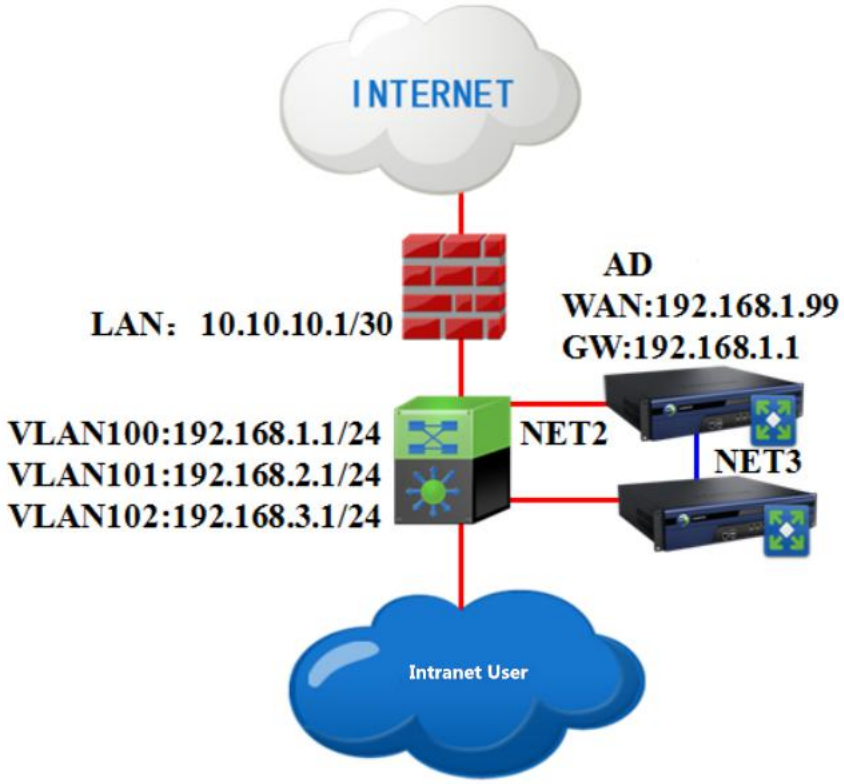
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



14.16 High Availability

In one customer network, there needs to balance the load on servers with AD unit deployed in bypass mode, and implement HA feature. When one AD unit gets down, the other one can take over to work as active unit. The following figure shows the network topology.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



HA Configuration Specification:

Step 1: Configure host A, including configuring basic network, virtual service and HA, and ensure the

host deployed in real network can operate normally

Step 2: Only configure HA feature on host B, and then turn it off. Connect the HA interface (selected by

heartbeat line) on host B to the corresponding interface on host A.

Step 3: Turn host B on.

Step 4: After host B turned on, it becomes standby unit. Host A will synchronize its configuration to host

B. If ALARM light on host B is blinking all the time, indicate that host B operates normally.

Step 5: Turn off host A or disconnect the interface configured link failure detection to check whether HA

Failover will happen and the application is normal. If it's normal, indicate that HA feature Is normal.

Configuration is completed.

Introducing methods of configuring HA on AD unit:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Step 1: Select any one of the AD units as host A, and configure basic network, virtual service, etc.

And ensure the internal users can access the virtual service successfully through AD unit. For configuration details, see Chapter 6, **Load Balancing** and Chapter 9, **Network**.

Step 2: Go to the **System > High Availability > HA mode** page on host A, select **Active-Standby**, as shown in the following figure:



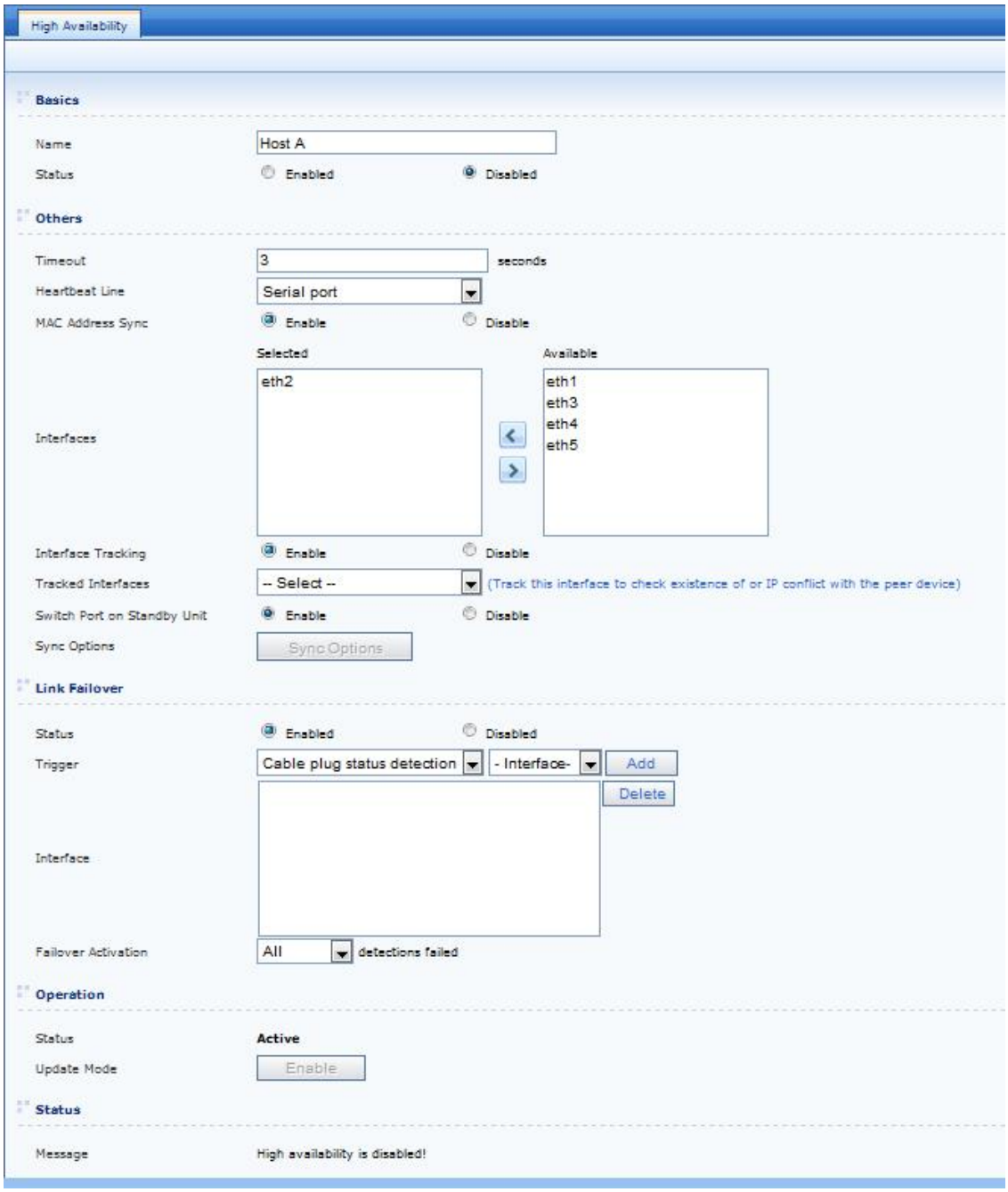
Step 3: Go to the **System > High Availability** page on host A, and enter Host A in **Name** filed. Select

NET3 as heartbeat line and specify 1. 1. 1. 1 as its IP address. Enable **Sessions** and disable **All**

(It needs to be enabled in local triangulation). Enable **MAC Address Table** and move NET2 from

Available box to **Selected** box in **Interfaces** field, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

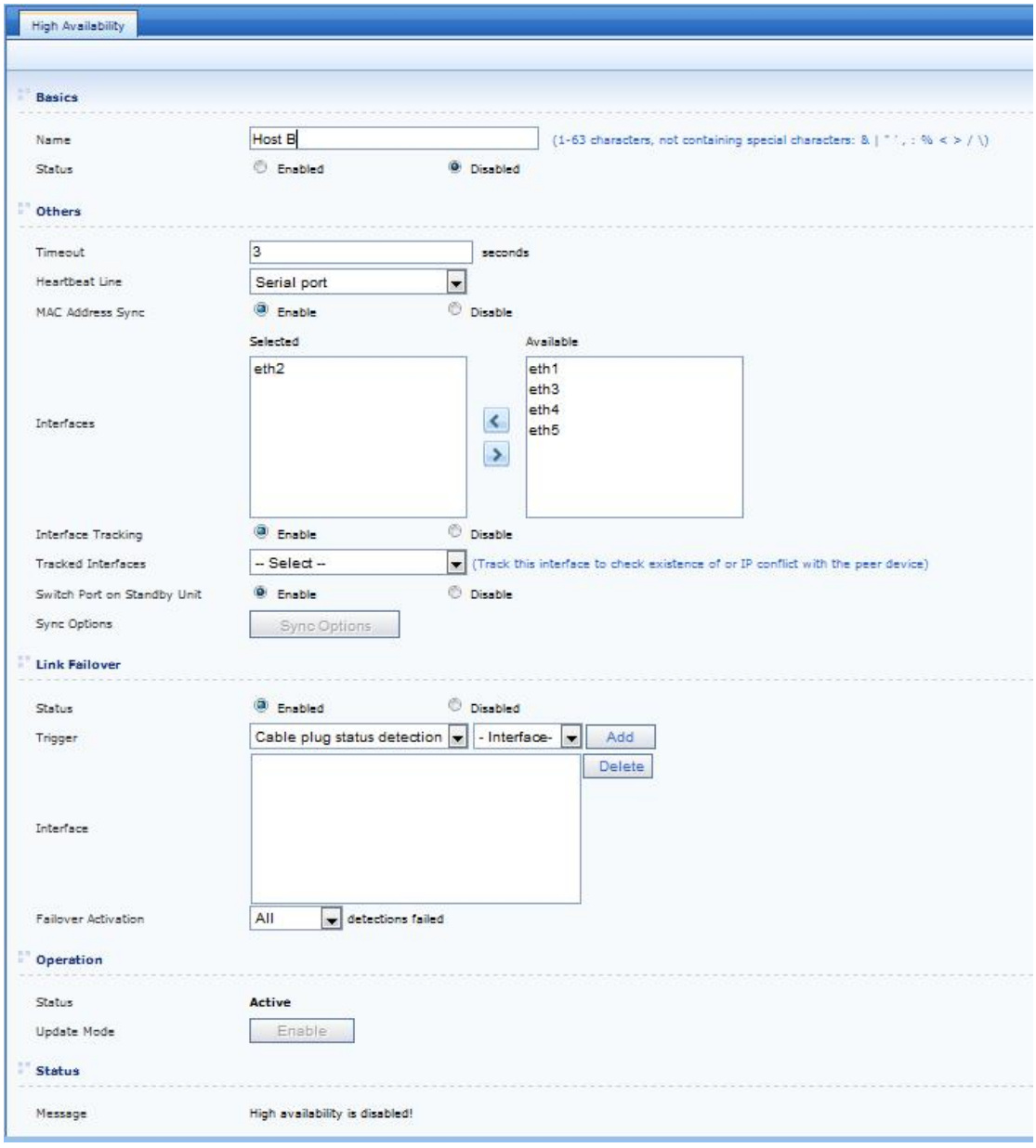


Step 4: Go to the **System > High Availability > HA mode** page on host B, select **Active-Standby**, as shown in the following figure:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Step 5: Go to the **System > High Availability** page on host B, and enter Host B in **Name** field. Select
NET3 as heartbeat line and specify 1. 1. 1. 2 as its IP address. Enable **Sessions** and disable **All** (It
needs to be enabled in local triangulation mode). Enable **MAC Address Table** and move NET2 from **Available** box to **Selected** box in **Interfaces** field as shown in the following figure:



Step 6: Turn off host B and connect its NET3 interface to that on host A.

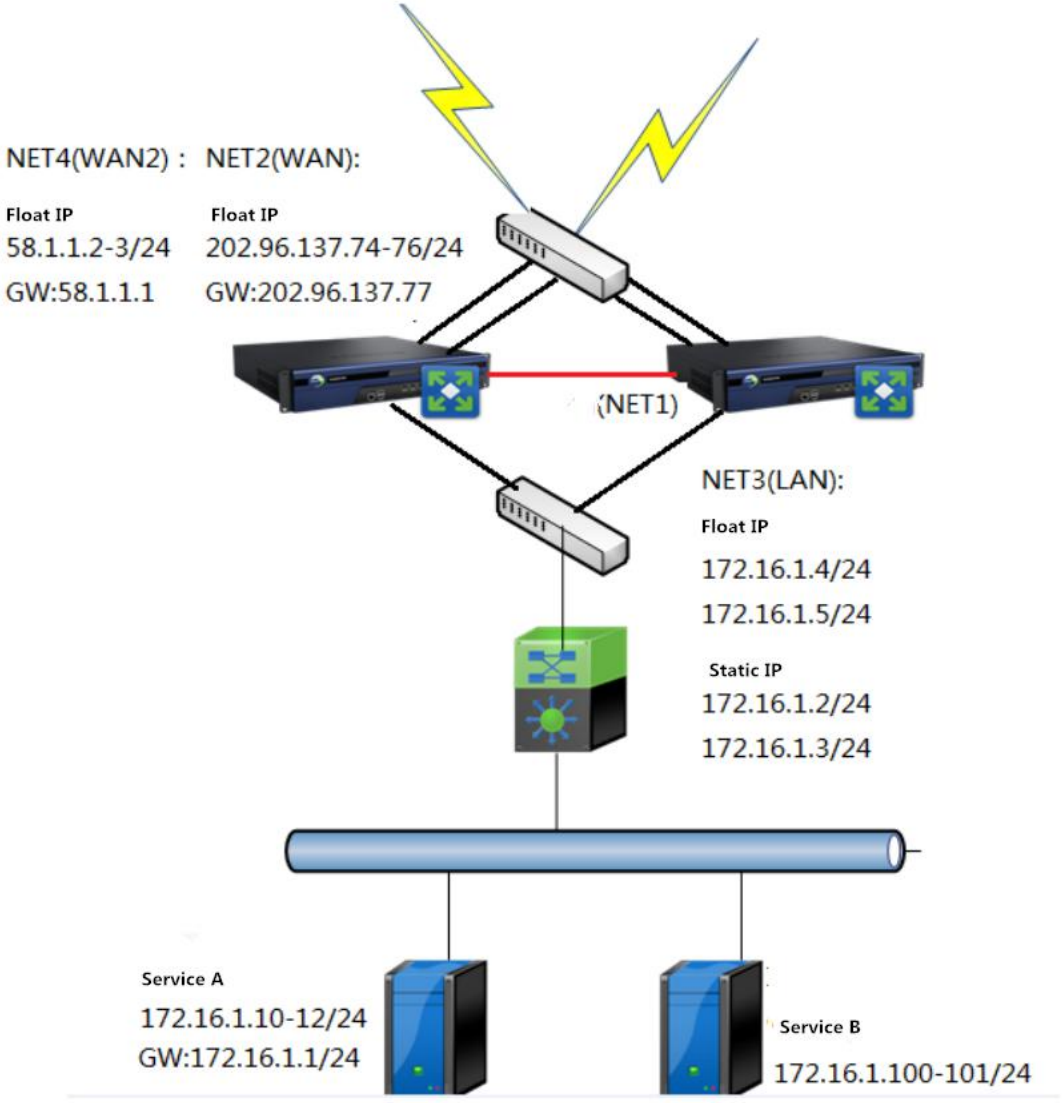
Step 7: Turn on host Band. Then it becomes standby host. Host A will synchronize its configuration to it. If ALARM light on host B is blinking all the time, indicate that host B operates normally.

Step 8: Turn off host A or disconnect the interface configured link failure detection to check whether HA failover will happen and the application is normal. If it's normal, indicate that HA feature Is normal. Configuration is completed.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

14.17 Cluster Deployment

The topology of one customer is as follows: There are two ADCs which are deployed in Router mode, together with two WEB servers, WEB server A and WEB server B. When users in the public network access WEB server A in the local area network, WEB server A functions as an active node, when users access WEB server B, WEB server B will function as an active node and when one of the two WEB servers fails, the other server will automatically take over the service.



Cluster configuration:

1. Configure node A to create a cluster.
2. After the cluster is created successfully, configure network, SNAT, DNAT, virtual service and traffic groups.
3. Connect two units' HA interfaces with crossover cable or connect the two units to the same switch. Note that the two unis should use the same interface as HA interface.
4. Configure node B to create a cluster.

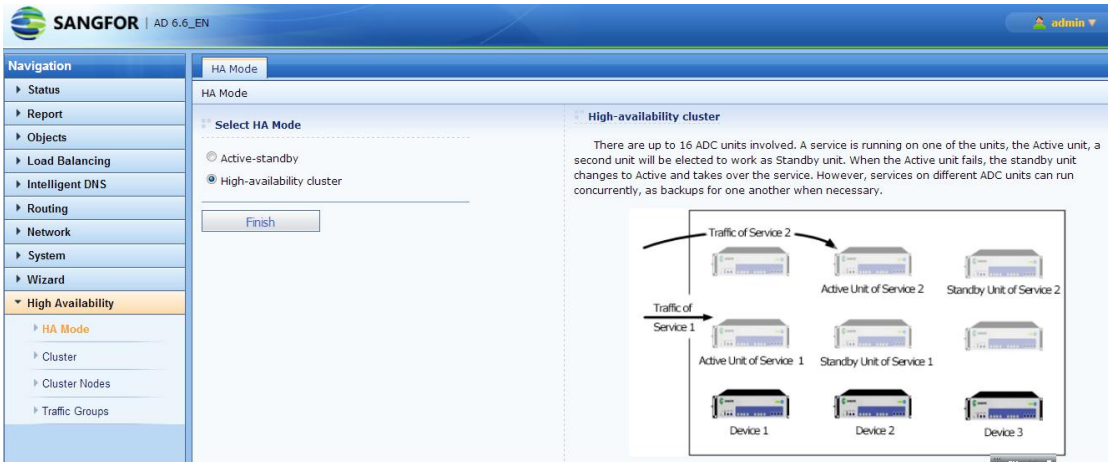
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

5. Add node B to the cluster and check whether both node A and node B are online. When node B gets online, configurations will be automatically synchronized.

6. Shut down node A or plug out the cable to test whether cluster is configured successfully.

Configure cluster as shown below:

1. Select an ADC unit randomly as node A and create a cluster.

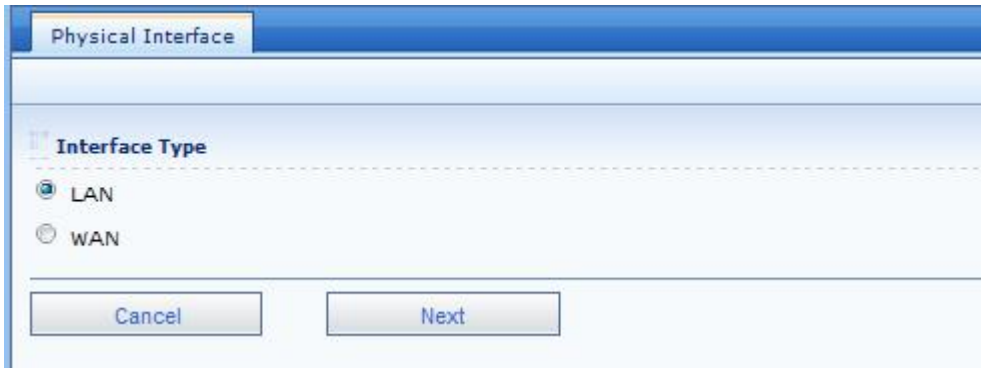




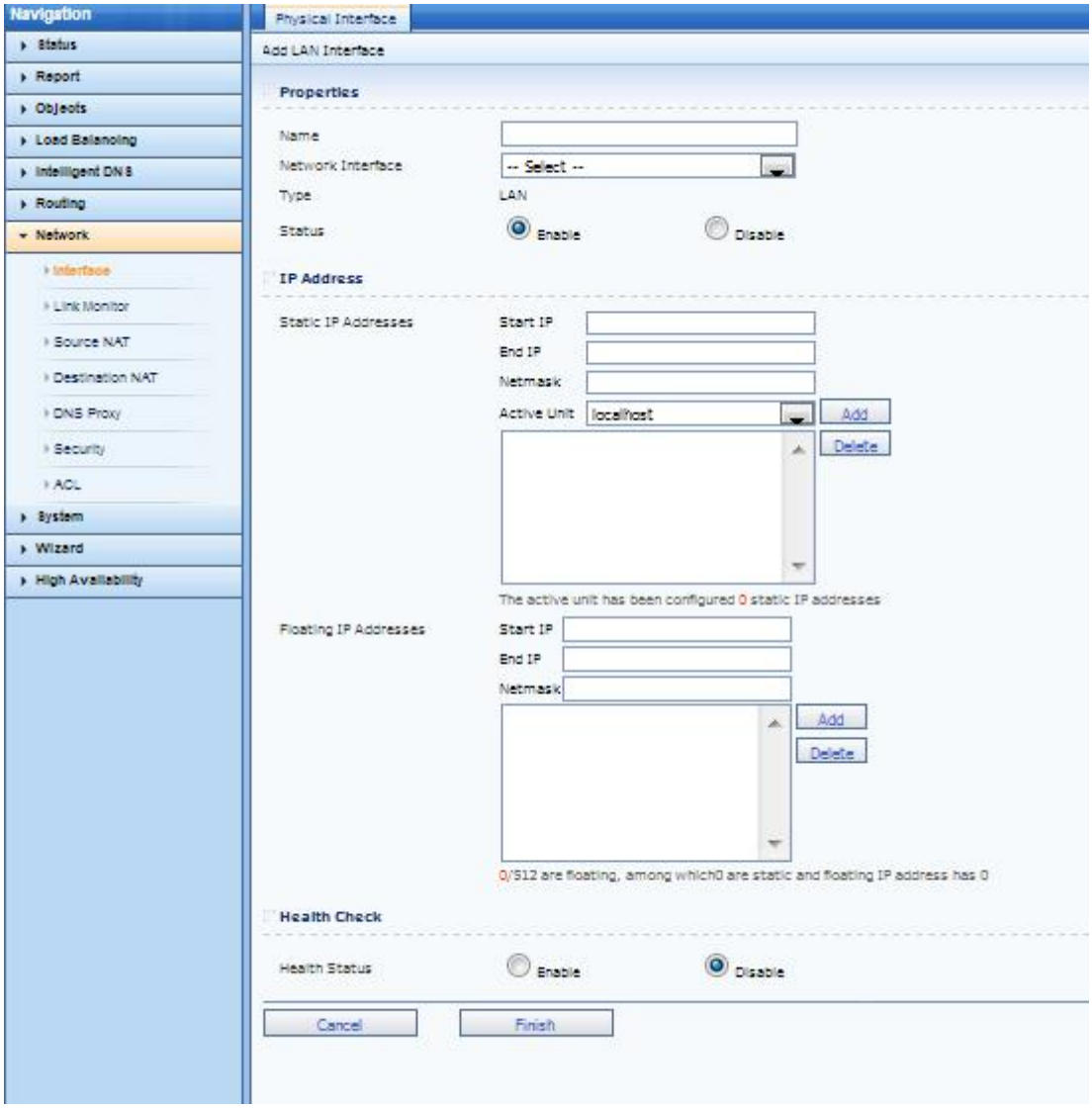
2. Log in to the cluster control, the default username and password are both cluster.

3. Go to **Network > Interface > Add**, select **LAN** for **Interface Type**, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Click **Next** to configure static IP address and floating IP address, and enable **Health Check**:



Static IP Addresses: Static IP address is used to communicate with node pool so as to obtain health status of node pool. Static IP address is not mandatory, as long as every ADC unit can obtain health status of node pool. If the node pool is on LAN, static IP address should be configured on LAN not on WAN.

The static IP address of node B cannot be configured until node B is joined to cluster.

Floating IP addresses: Floating IP address is configured for different virtual services. Each

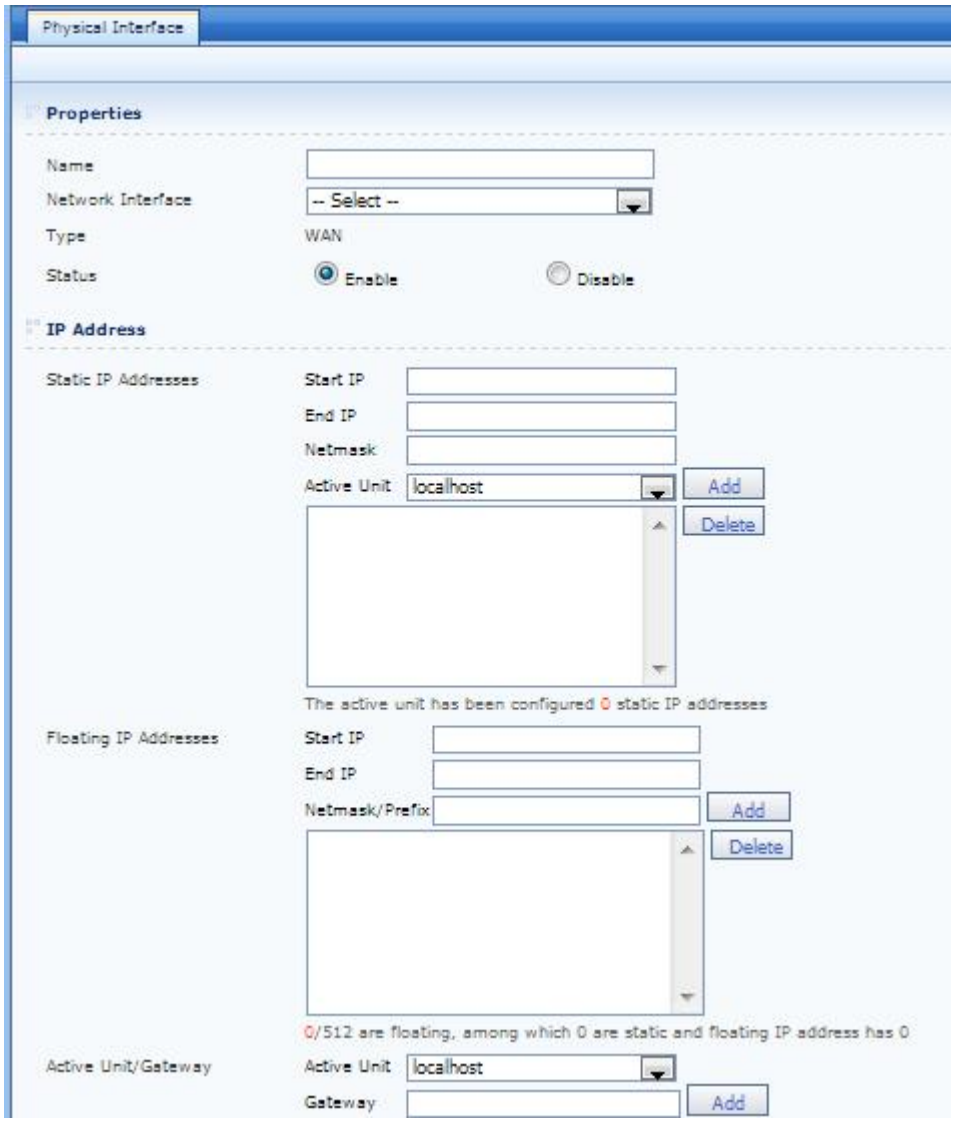
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

virtual service requires at least one floating IP address.

4. Go to **Network > Interface > Add,** select **WAN** for **Interface Type**, as shown in the following figure:



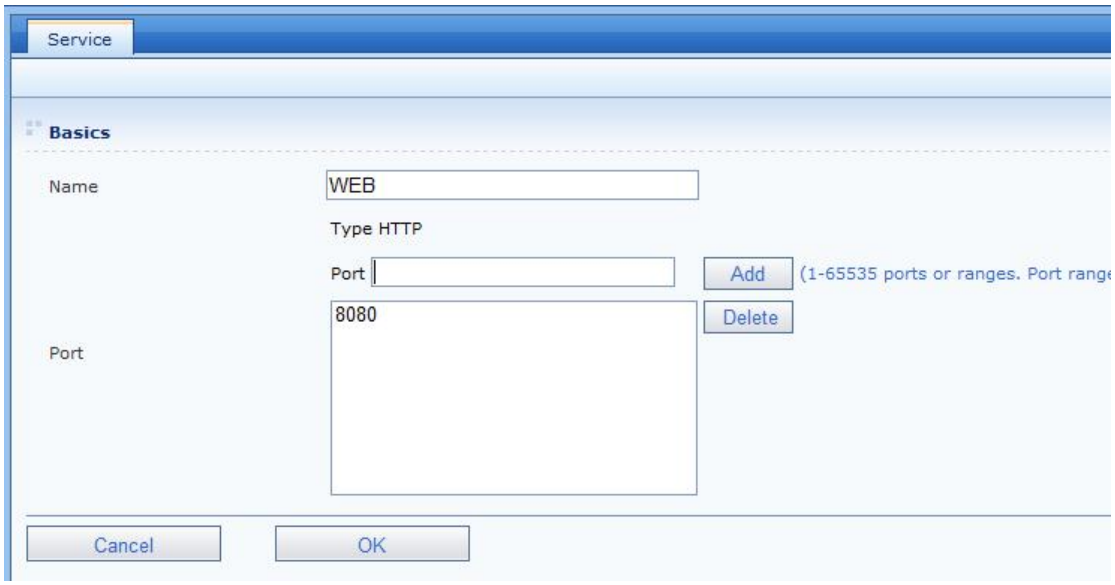
Click **Next** to configure floating IP address for WAN port, as shown in the following figure:



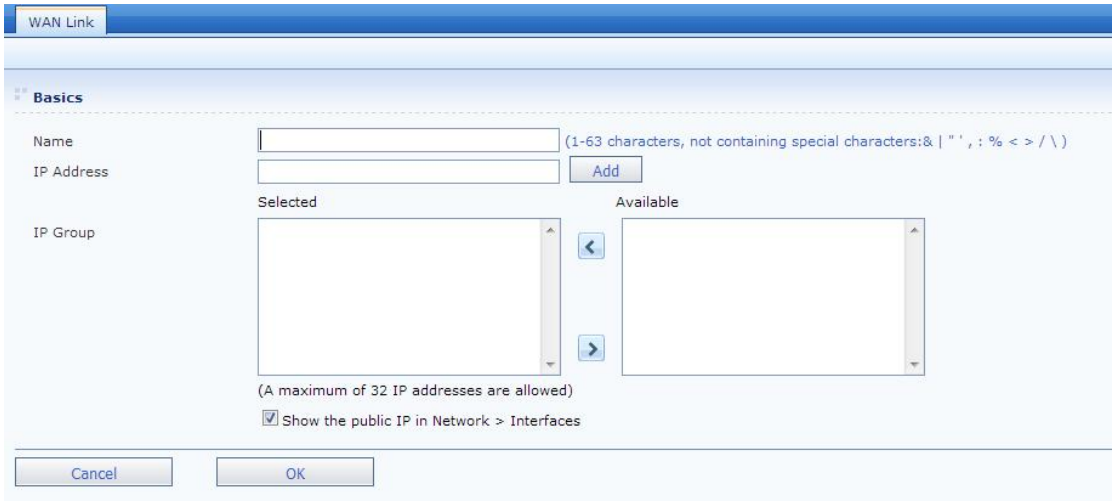
5. Go to **Load Balancing > Service > Add, select HTTP** and click **Next** to configure HTTP port,

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

as shown in the following figure:

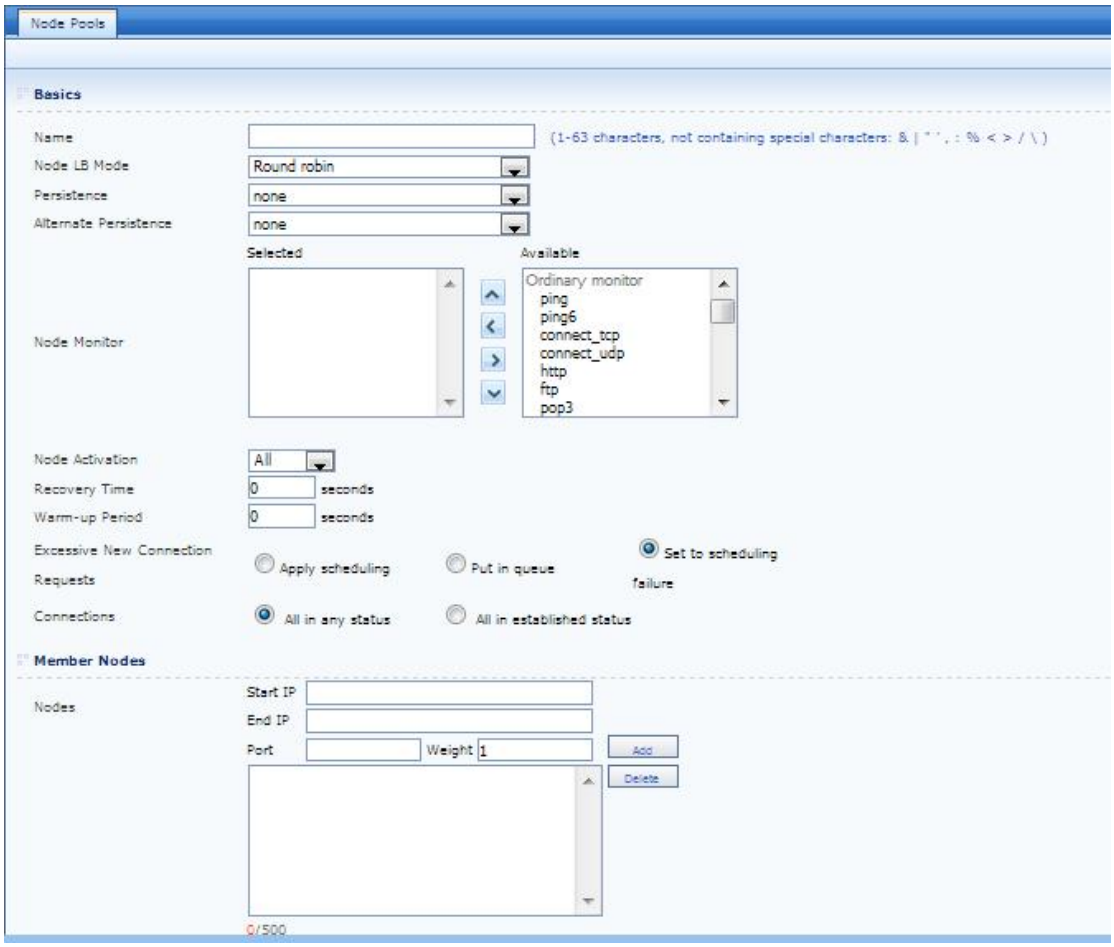


Go to **Load Balancing > WAN Link > Add** to configure IP group, as shown in the following figure:



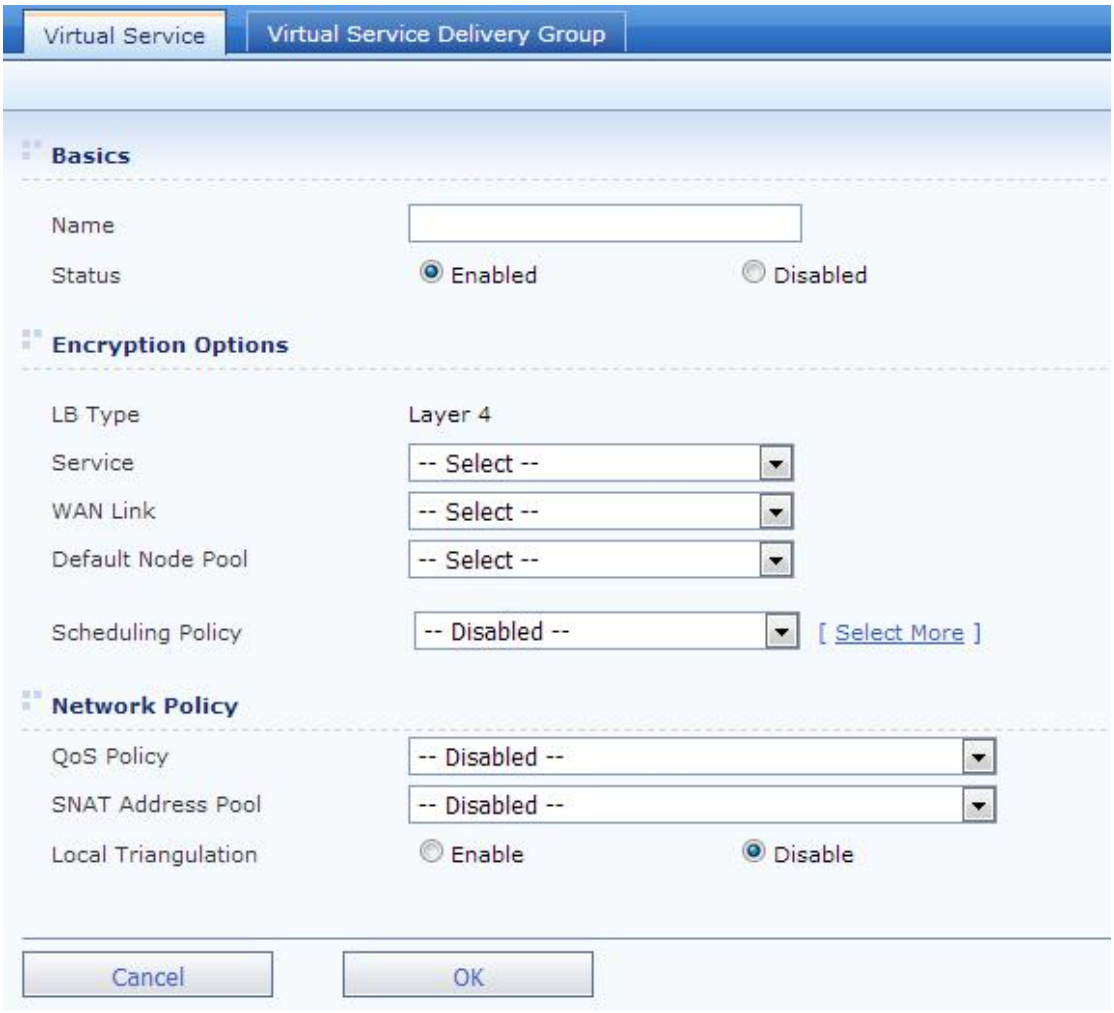
Go to **Load Balancing > Node Pools** to configure node pools:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

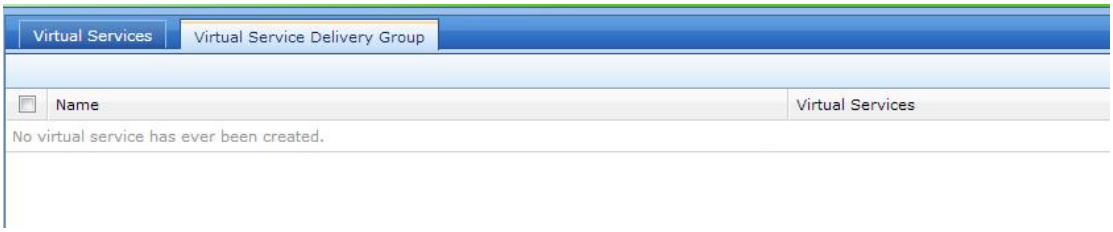


Go to **Load Balancing > Virtual Service** to configure virtual service:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



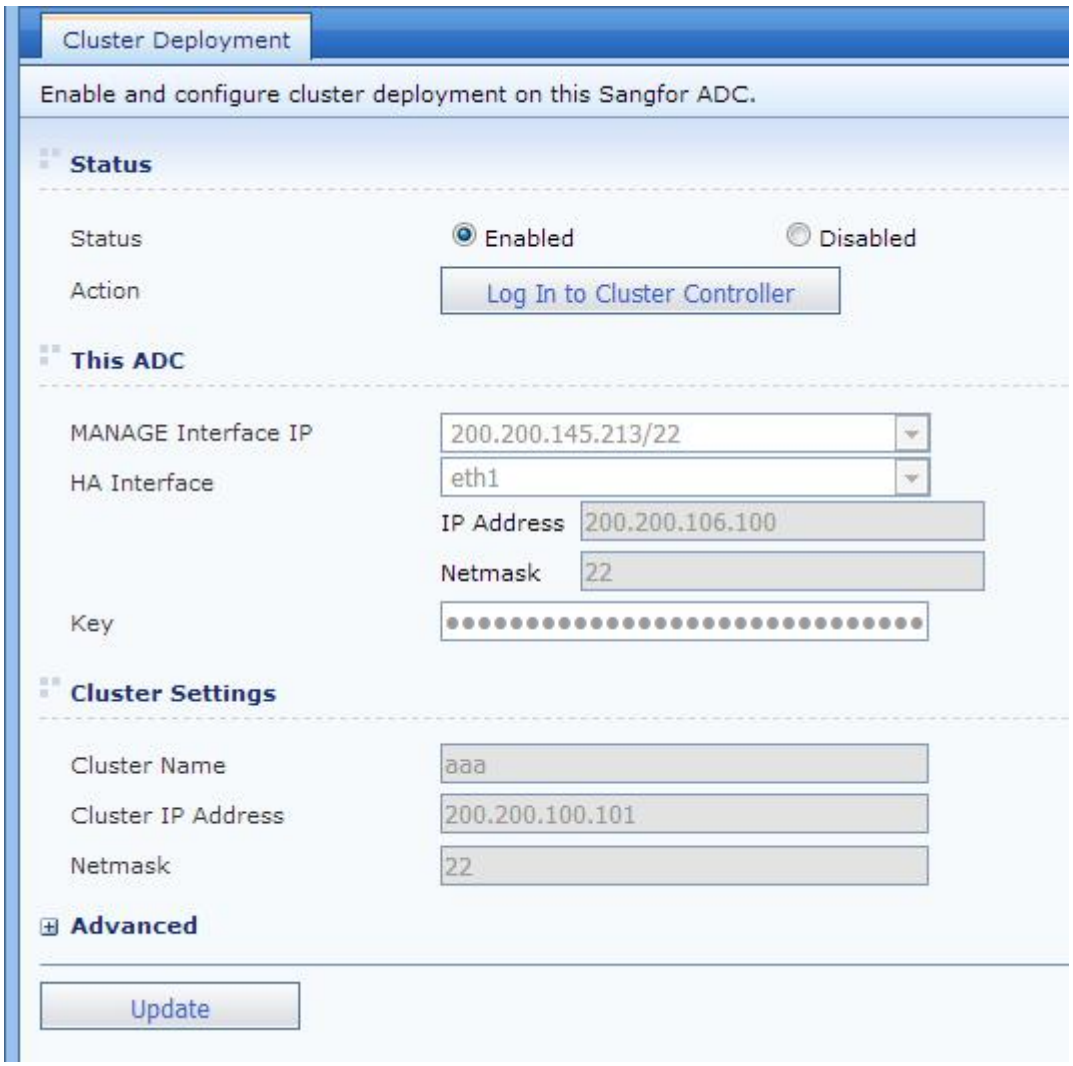
After configuring virtual service, virtual service delivery group will be automatically created, as shown in the following figure:



6. Connect two units' HA interfaces(NET1) with crossover cable or connect them to the same switch. Note that the two units should use the same interface as HA interface.

7. Configure node B and join it to the cluster. Log in to the Web admin console of node B and go to High Availability > Cluster to configure as follows:

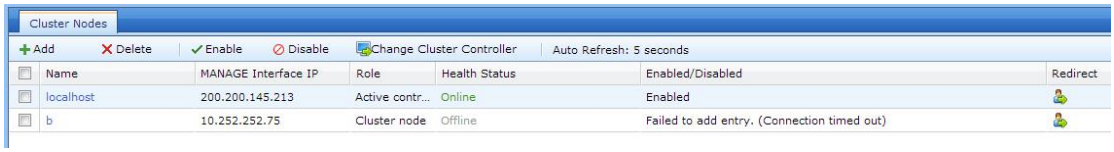
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



7. Go to High Availability > Cluster Nodes to add new node to cluster:

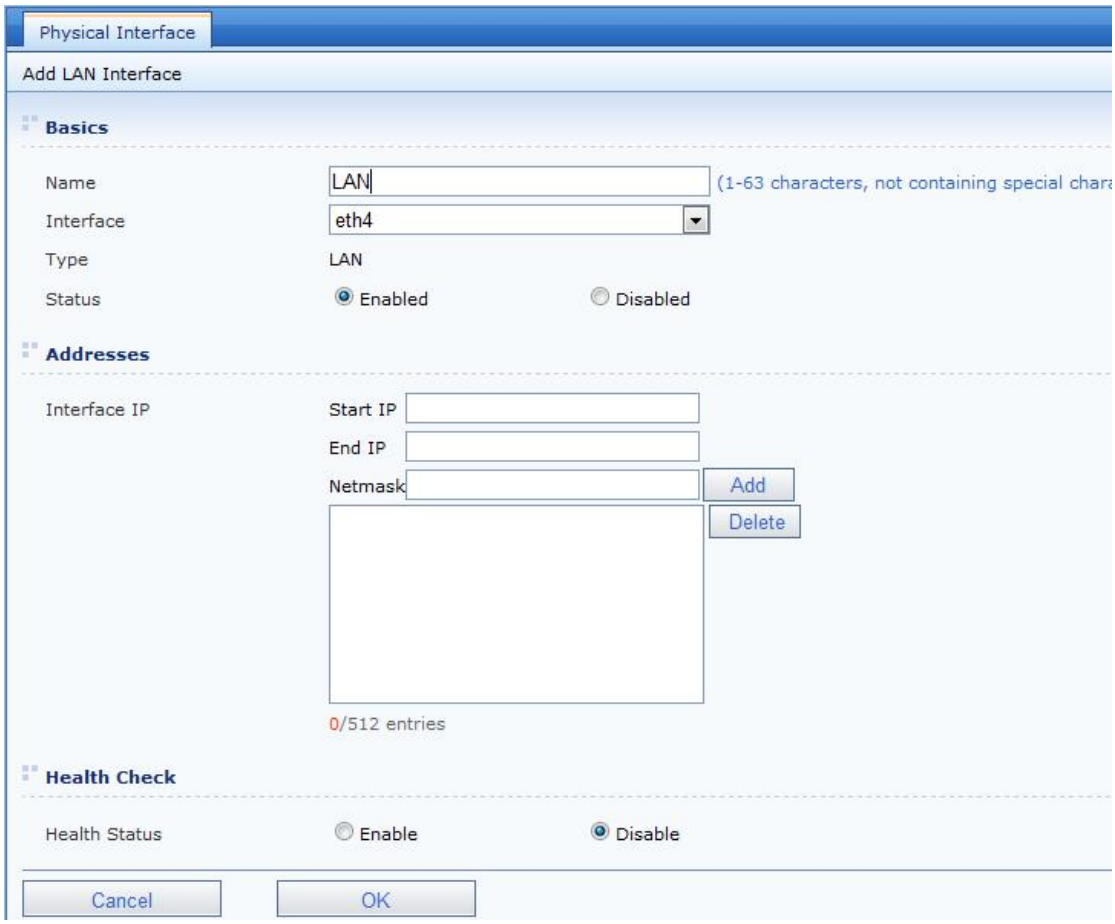


After node B is joined to cluster, the status of node B is Failure, indicating that the configurations are being synchronized. After the configurations have been synchronized, status of both of the two nodes are Online, indicating that the cluster has been created successfully.

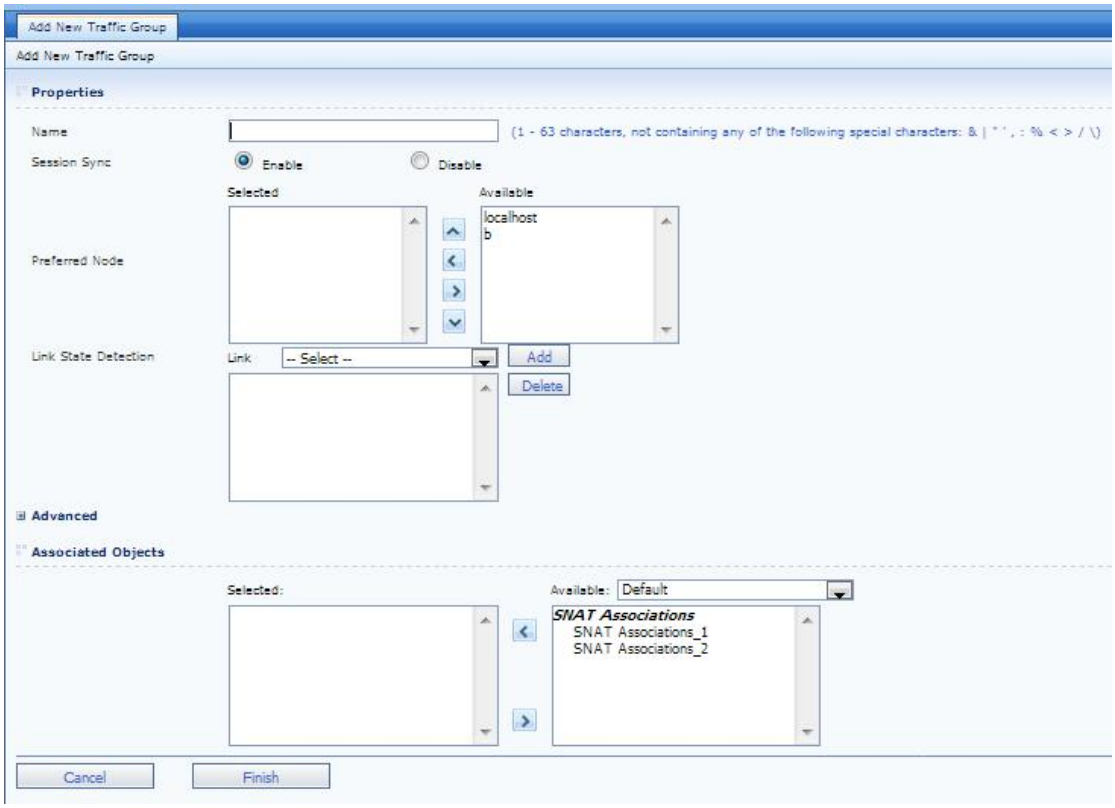


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

8. Go to **Network > Interface** to configure static IP address for node B:



9. Go to **High Availability > Traffic Groups** to configure traffic groups, as shown below:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

Session Sync: Once enabled, sessions will not be interrupted when active node switches to standby node.

Preferred Node: Displays available nodes for you to choose from.

Link State Detection: Specifies links which will be detected, and node will be switched once links are detected to be in fault.

Priority: Specifies weight of the traffic groups. Active node and standby node are selected based on the sum of weight of the traffic groups.

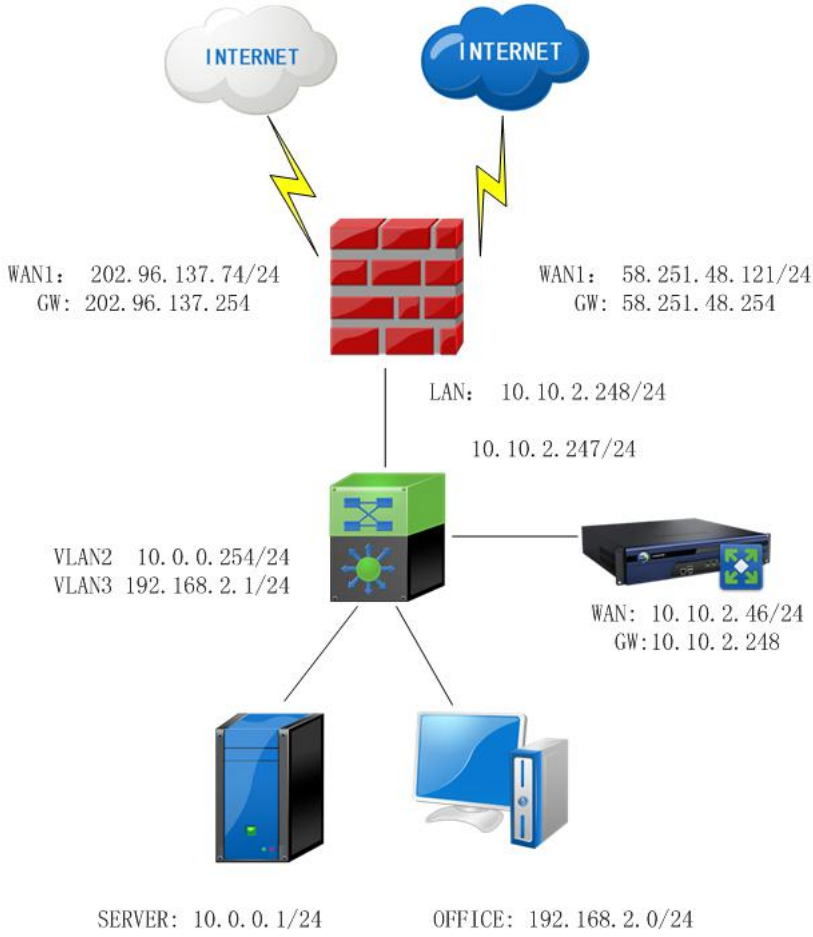
Virtual MAC Address: Specifies virtual MAC address of certain link. There is no need to flush MAC address for switch and router when node switches, so as to enhance switching efficiency.

Associated Objects: Specifies associated virtual service groups, floating IP address, SNAT, DNAT, etc. Traffic group is the smallest unit upon which node switches.

14.18 Virtual Link Health Detection

In one customer network, there are two WAN links: Telecom and Unicom. There is a LAN server providing HTTP service (port 80). The external users access the server with the IP address of WAN links. AD unit is deployed in single-arm mode. The requirements of the customer is that there needs to balance the load on inbound links and check whether the ISP gateway of WAN link is normal. If Telecom link or Unicom link is down, the IP of that unavailable link will not return to users, and make sure users can still access to the server successfully in this case.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



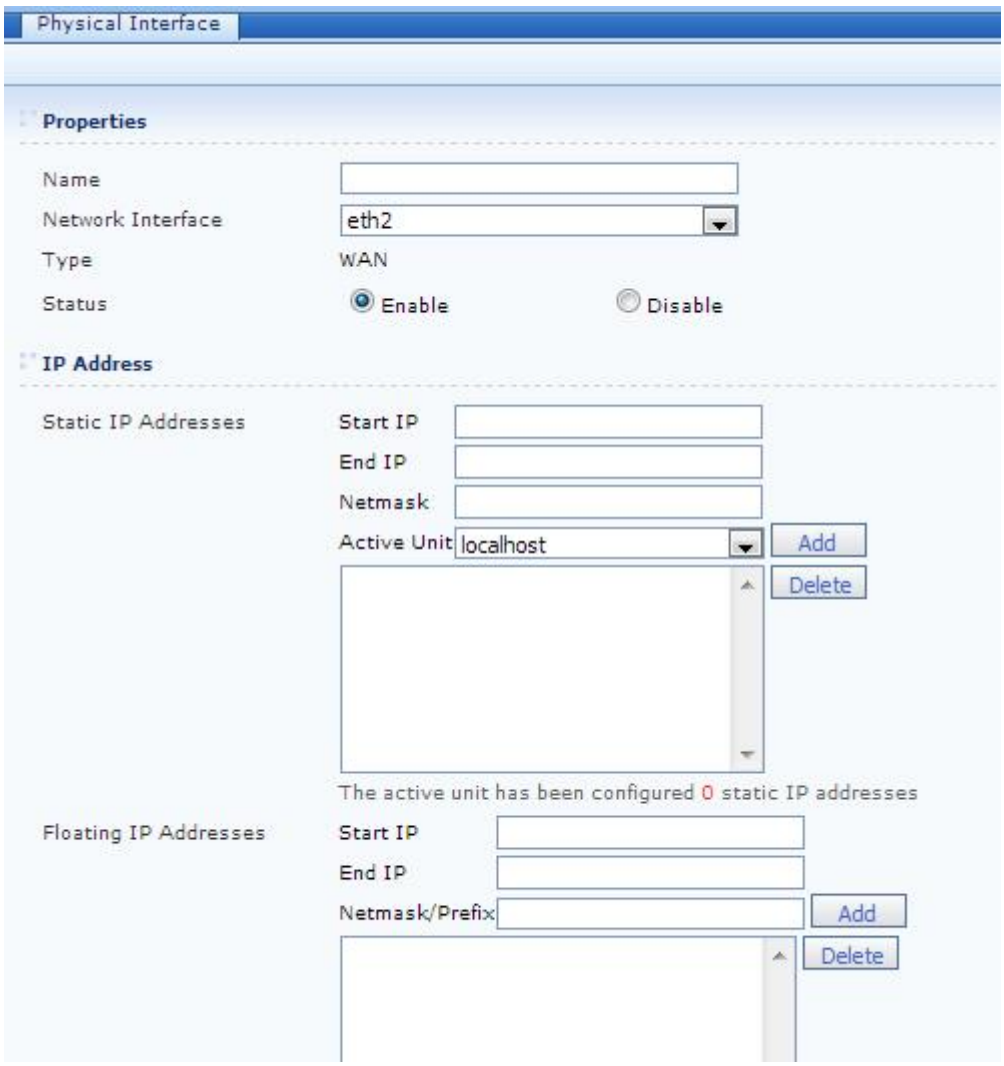
Preparations: Apply for two DNS records on the domain name provider:

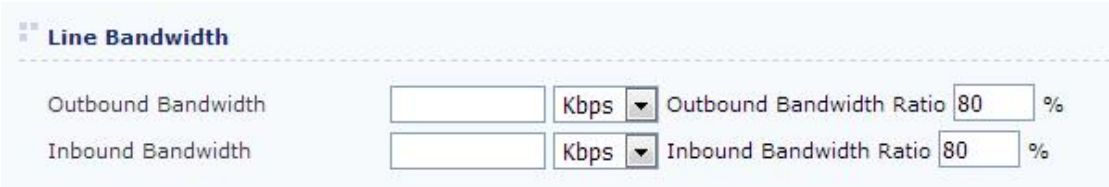
NS record: www. sangfor. com- > ns1. sangfor. com; A record: ns1. sangfor. com- > 202. 96. 137. 74 (or 58. 251. 48. 121).

Configuration steps are as follows:

1. Go to the **Network > Interface > Physical Interface** page, create a WAN interface, and bind the IP address of Telecom link to it, as shown below:

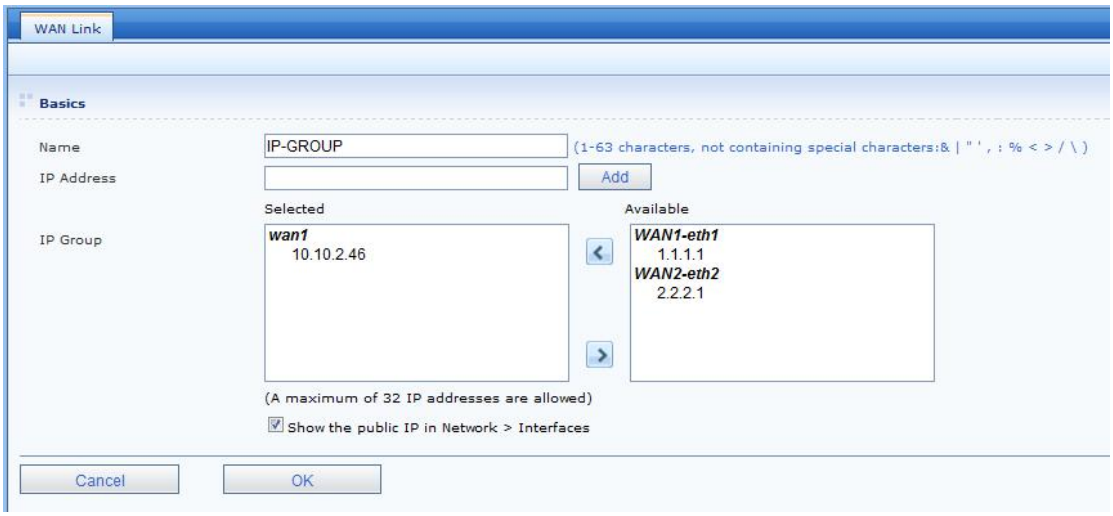
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





2. Go to **Load Balancing > WAN Link** page, create a WAN link. Select the IP of WAN link and click < arrow to move it from **Available** box into **Selected** box in **IP Group** field.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

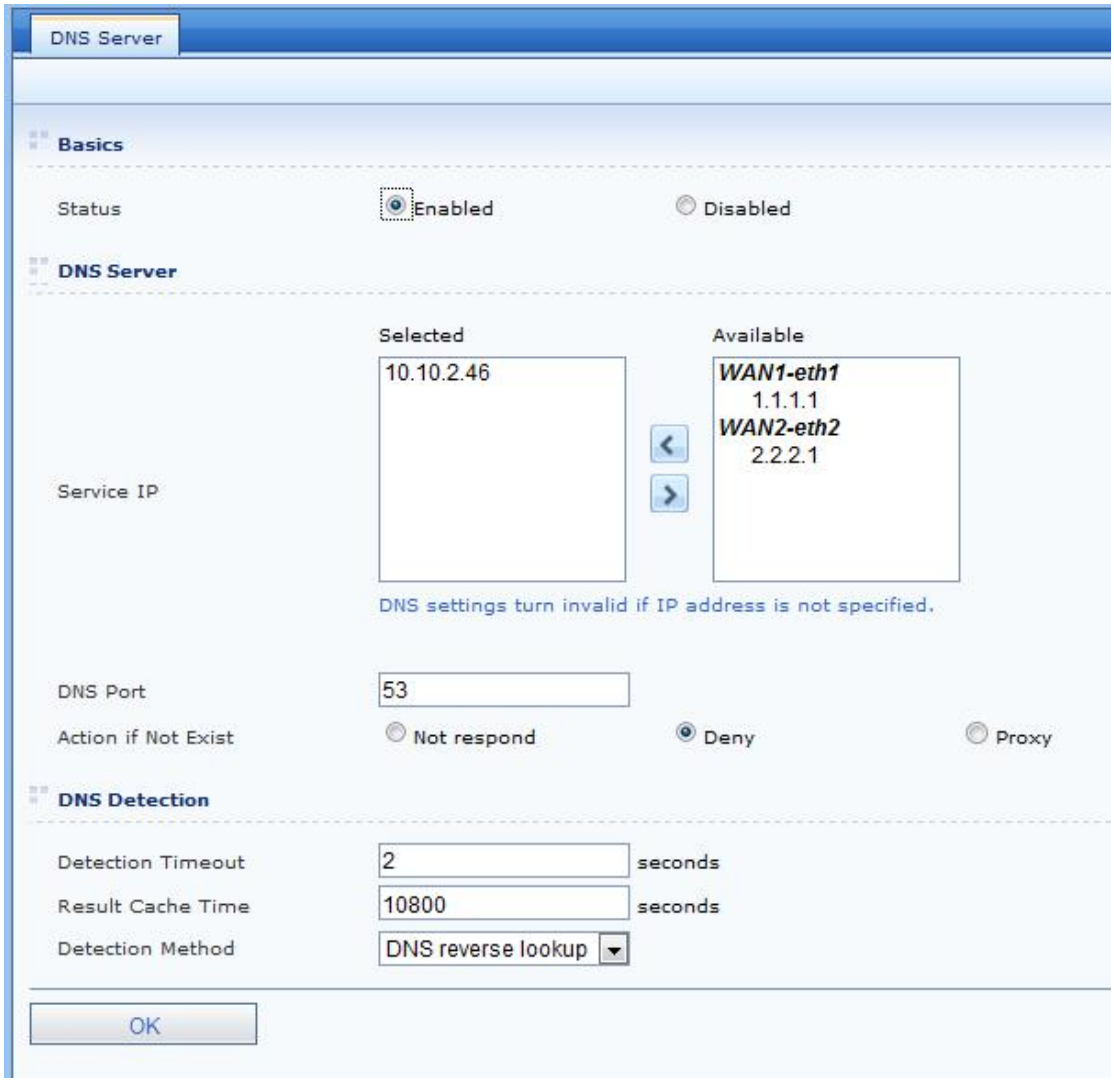


3. Create a node monitor on the **Load Balancing > Node Monitor** page, in order to monitor whether the gateway operates normally. Now take Ping for example, the configuration for Unicom link is the same.



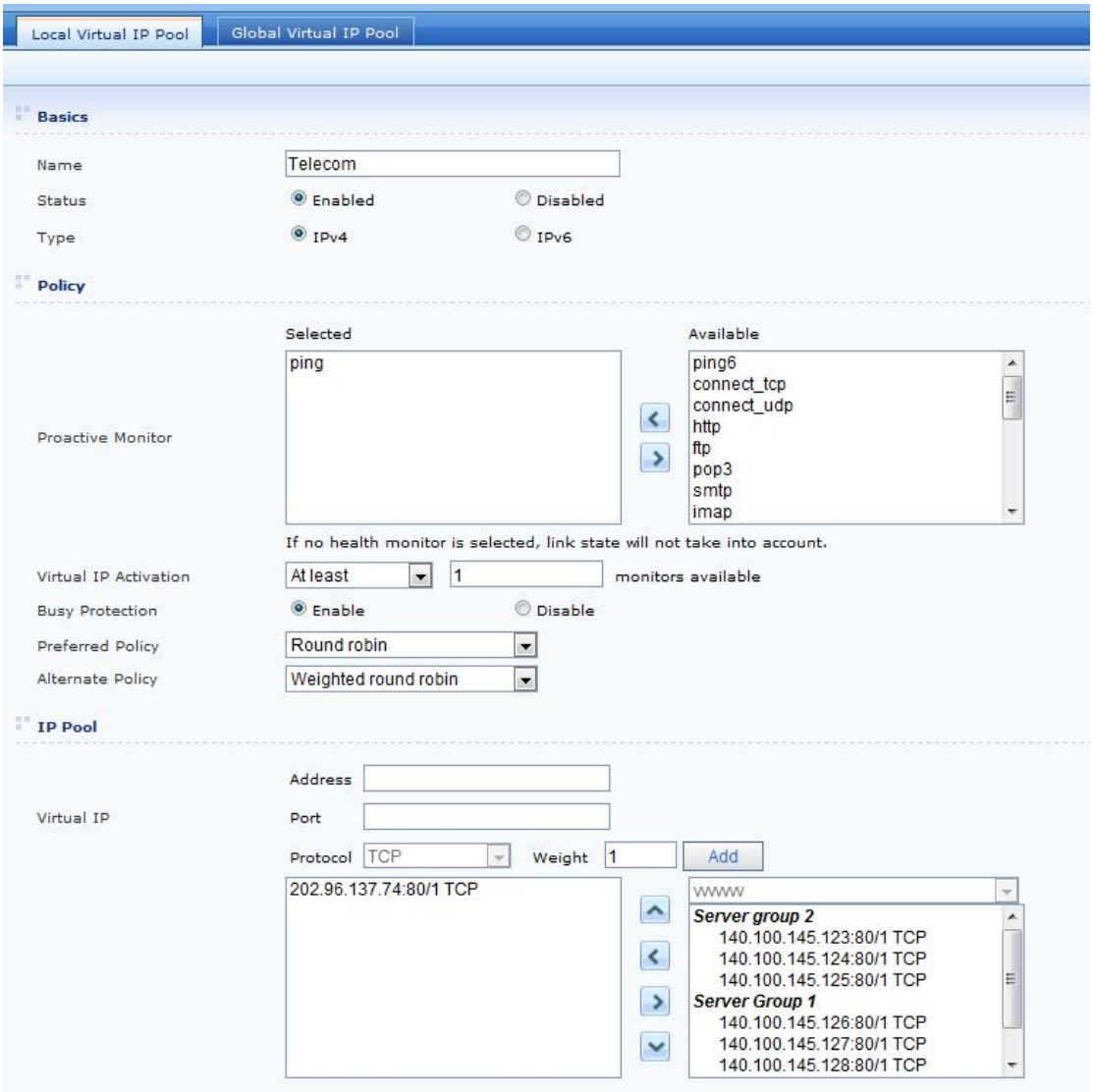
4. Configure a DNS server on the **Intelligent DNS > DNS Server** page, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



5. Go to the **Intelligent DNS > Virtual IP Pool > Local Virtual IP Pool** page, and create a virtual IP pool. Now take Telecom for example, the configuration for Unicom link is the same.

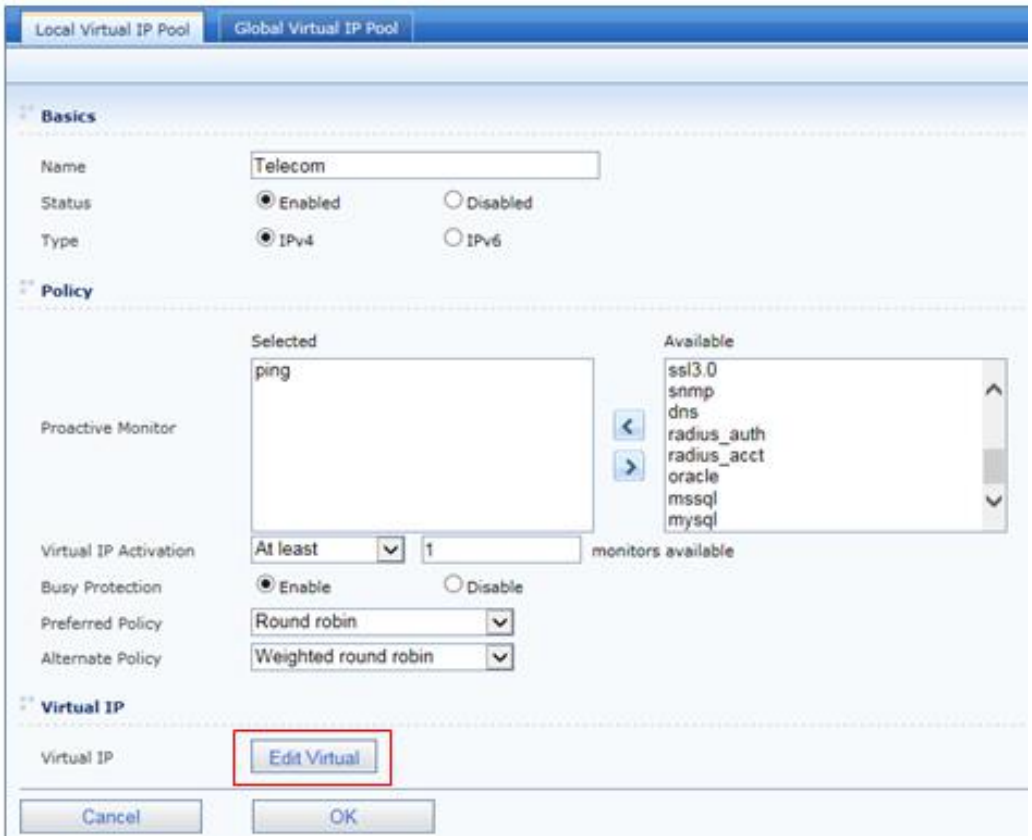
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



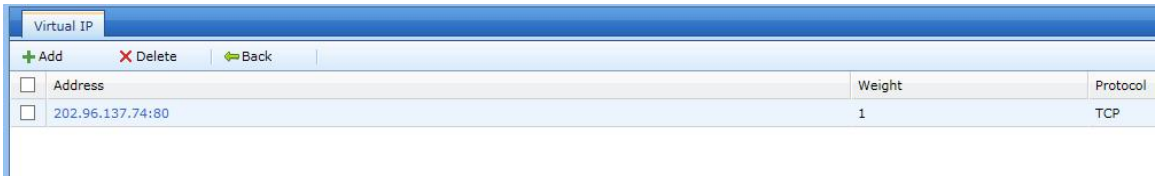
After configuring completed, edit the newly-created local virtual IP pool and click 

, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

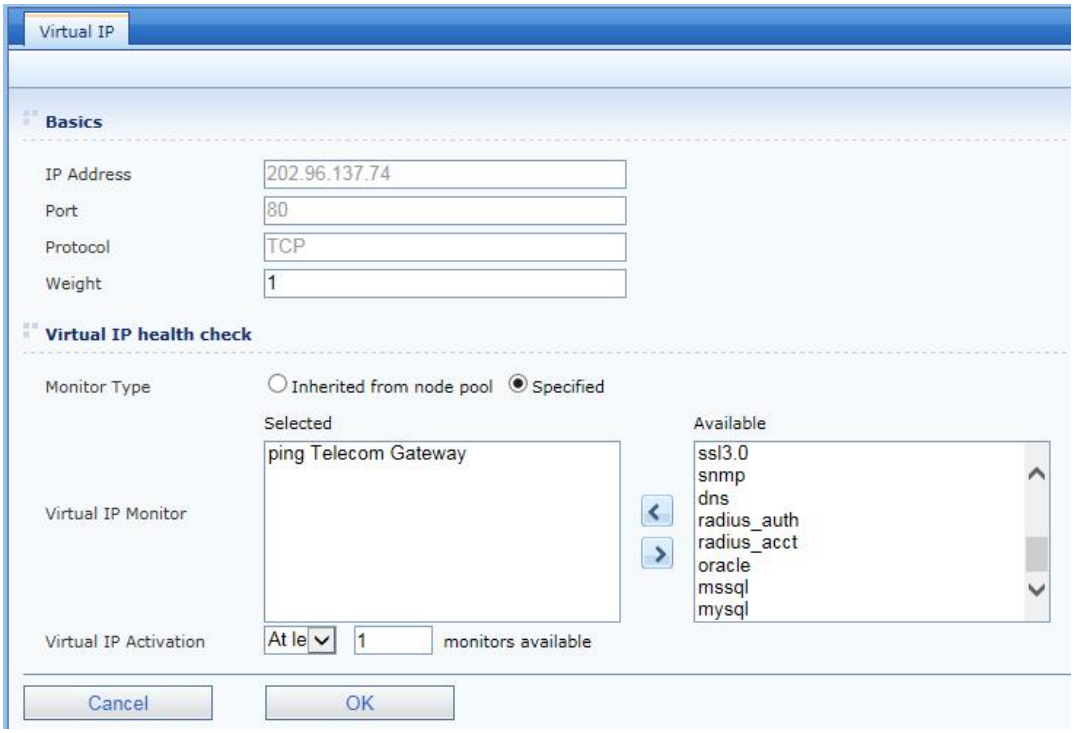


Then, you will be redirected to the following page:



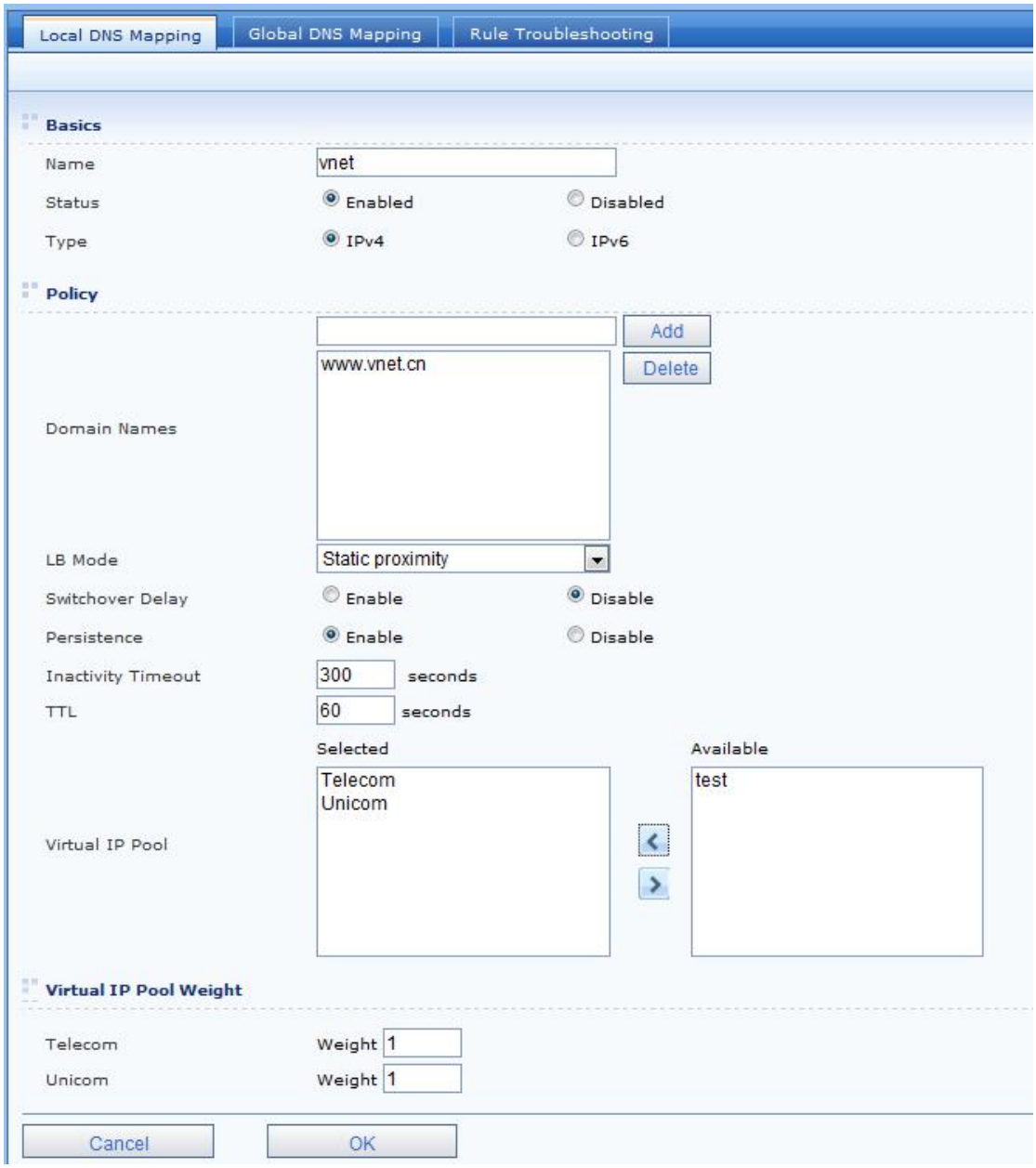
Click on address 202. 96. 137. 74: 80, Select **Specified** in **Monitor Type** field. In Virtual IP Monitor list, select **ping Telecom Gateway**, and move it from **Available** box into **Selected** box, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



6. Create a local DNS mapping on the I**ntelligent DNS > DNS Mapping > Local DNS Mapping** page, as shown in the following figure:

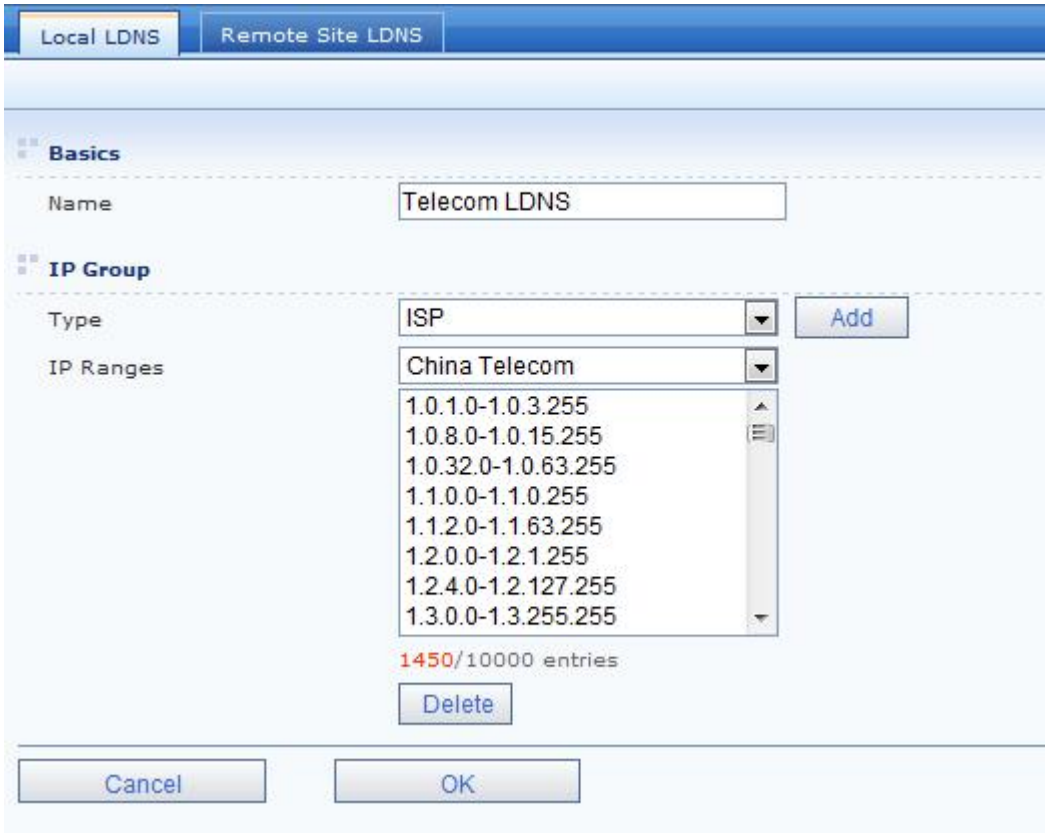
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



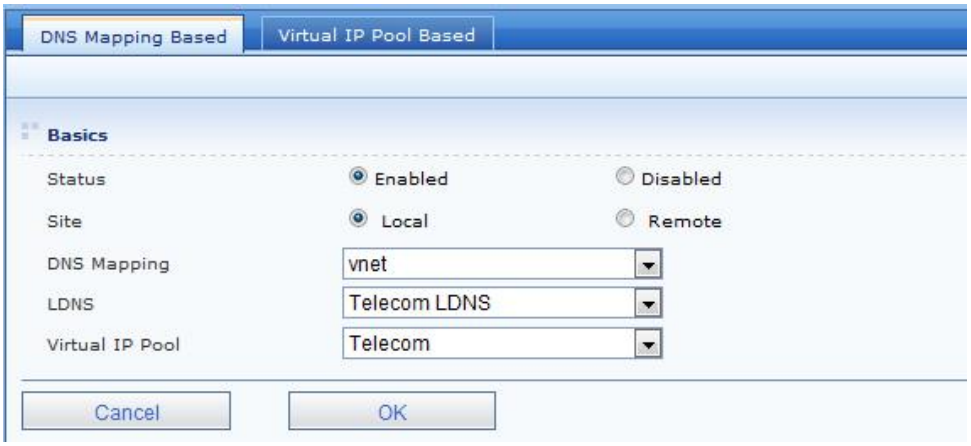


7. Create a local LDNS on the I**ntelligent DNS > LDNS > Local LDNS** page, and select **ISP** in

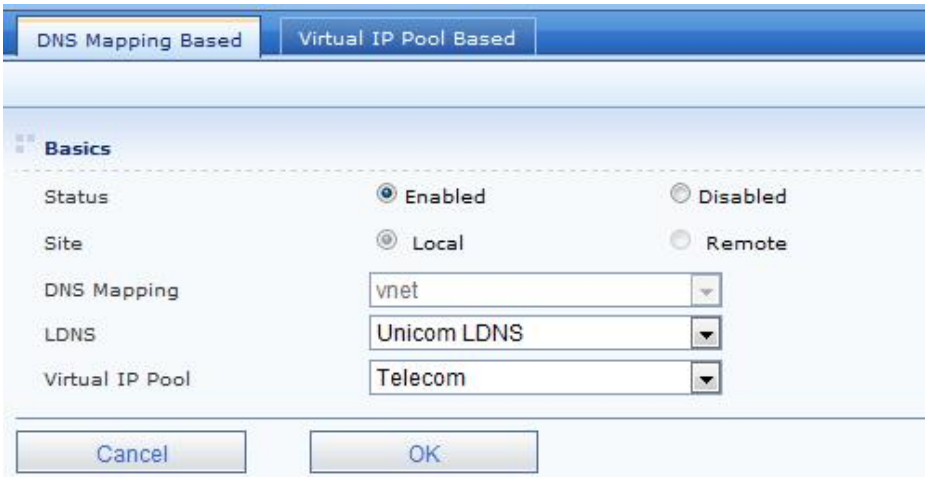
Type field, and specify **Telecom** in **IP Range** field, as shown in the following figure: (Configuration for Unicom link is the same.)



8. Create a DNS mapping based on the **Intelligent DNS > Static Proximity > DNS Mapping Based** page, as shown below:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



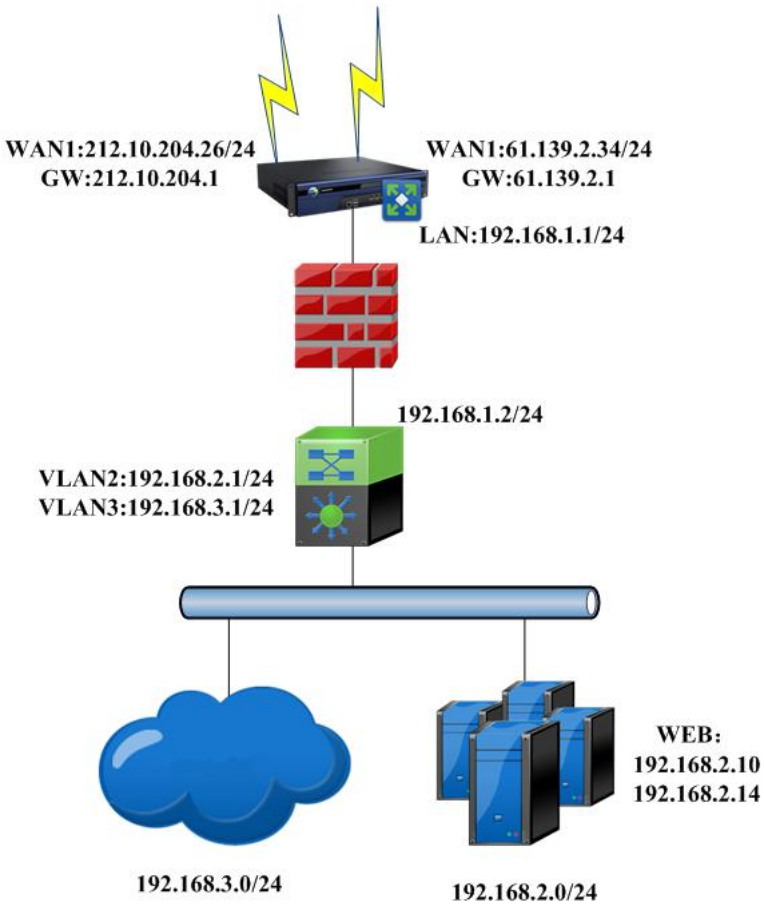
9. Create a node poll and virtual service. The configuration steps will not be illustrated here.

14.19 Comprehensive Case

In one customer network, there are two WAN links: Telecom and Unicom, each with 100M bandwidth. AD unit is deployed in single-arm mode. And there are two LAN servers providing Web service on port 80. The external users access the servers via the same domain name: www. sangfor. com, which directs to 212. 10. 204. 26 with A record. Requirements of the customer:

1. When external user accesses the domain name, if he/she belongs to Unicom, the access request will flow via Unicom link; if he/she belongs to Telecom, the access request will flow via Telecom link; if he/she belongs to other ISP, the access request will flow over the best link selected automatically.
2. Users on network segment 200. 100. 100. 0/24 access to the server whose IP is 192. 168. 2. 10. Load balances the servers when other users access them.
3. When internal users access to Internet, the data from intranet will go through the link selected automatically by AD unit.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Preparations: Apply for two DNS records on the server of the domain name provider:

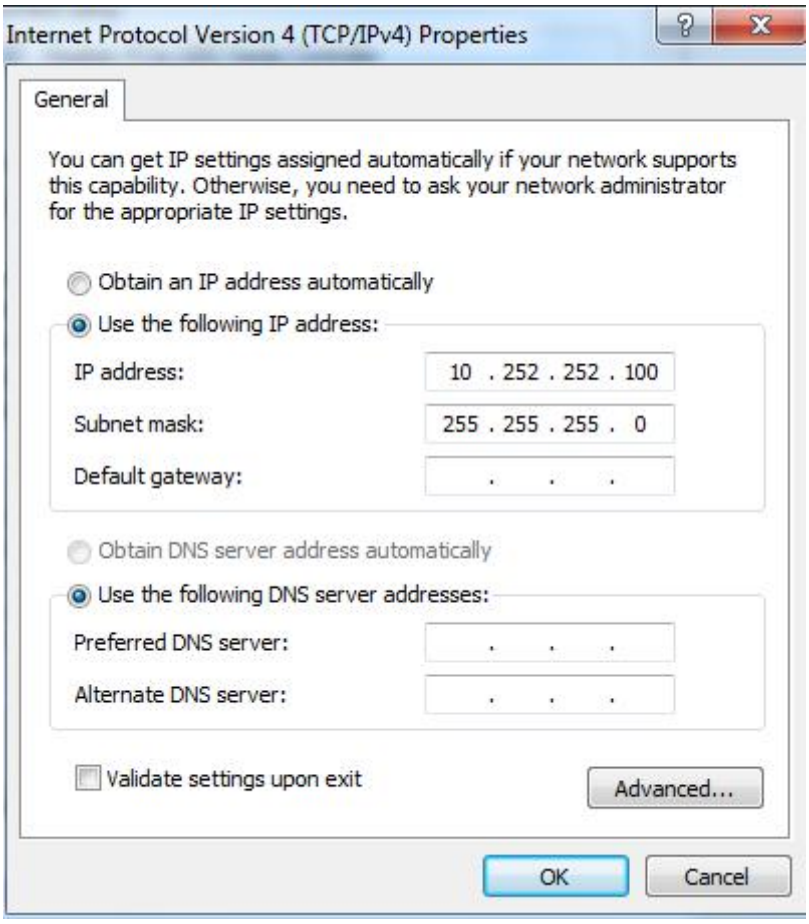
NS record: www. sangfor. com- > ns1. sangfor. com; A record: ns1. sangfor. com- > 212. 10. 204. 26(or 61. 139. 2. 34).

Configuring before deploying device:

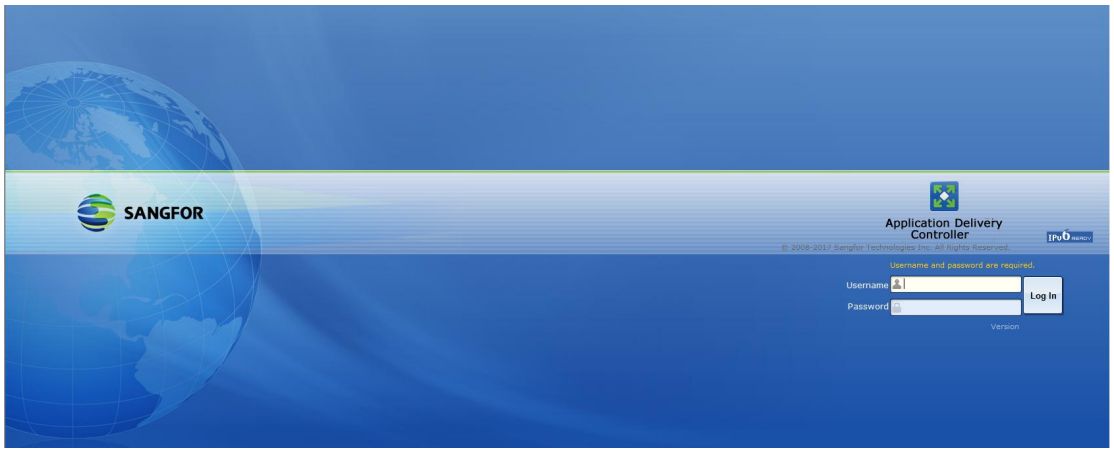
1. Turn on AD unit, connect the MANAGE interface on the AD unit with a network cable, and set the

IP address of the network card to10. 252. 252. 100, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



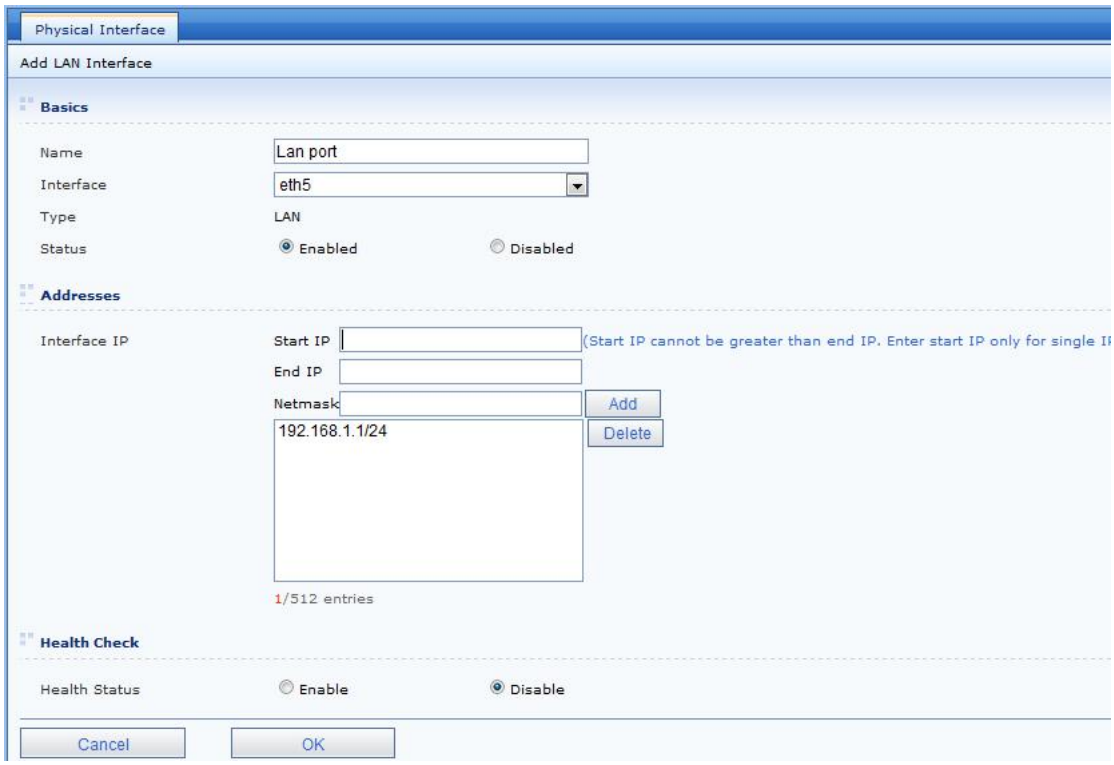
2. Open IE browser, type the URL address https: //10. 252. 252. 252 into address bar, you will be redirected to the login page and enter the default username and password: admin /admin, as shown below:



3. Create a LAN interface on the **Network > Interface > Physical Interface** page, as shown in the following figure:

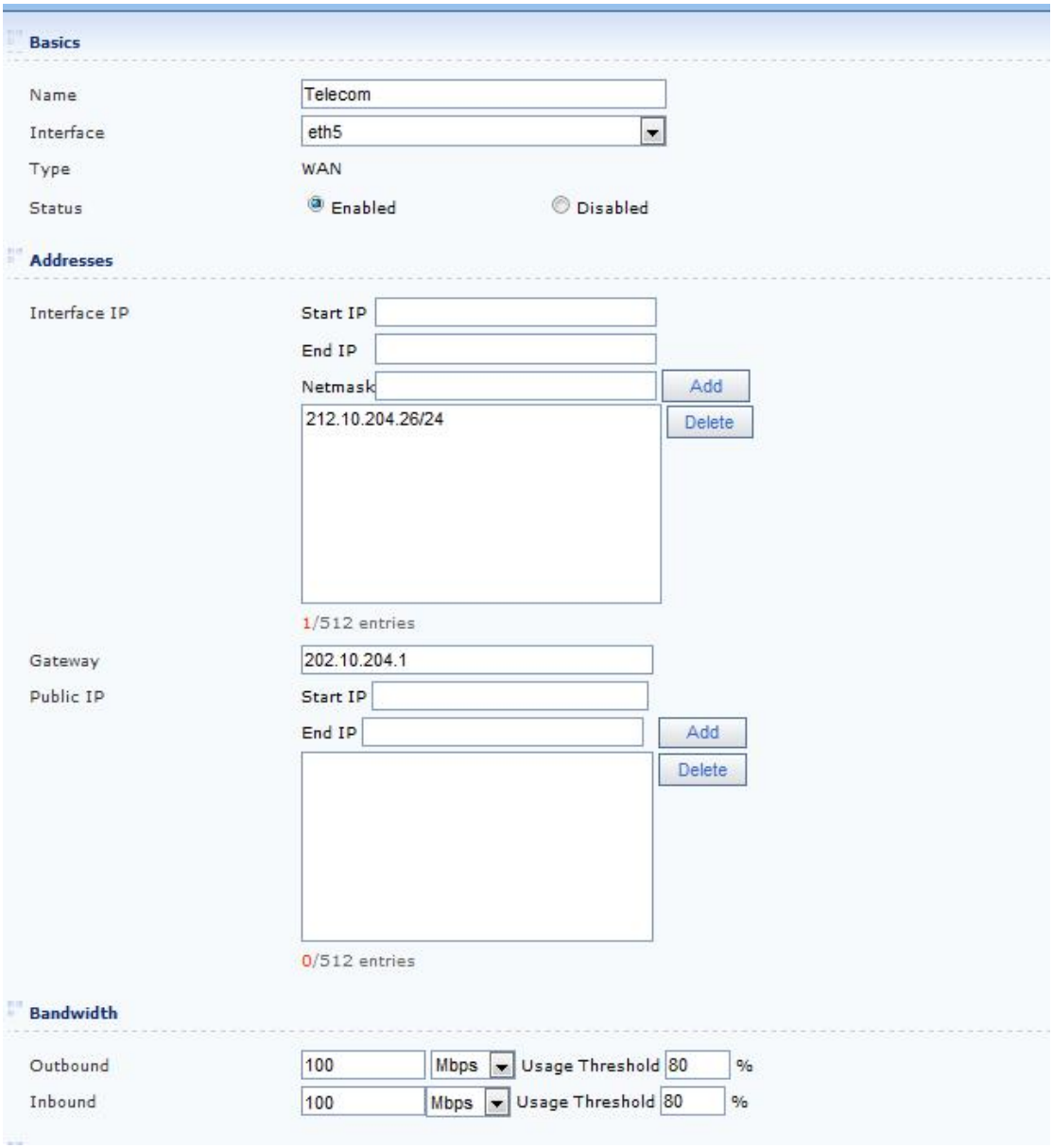
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



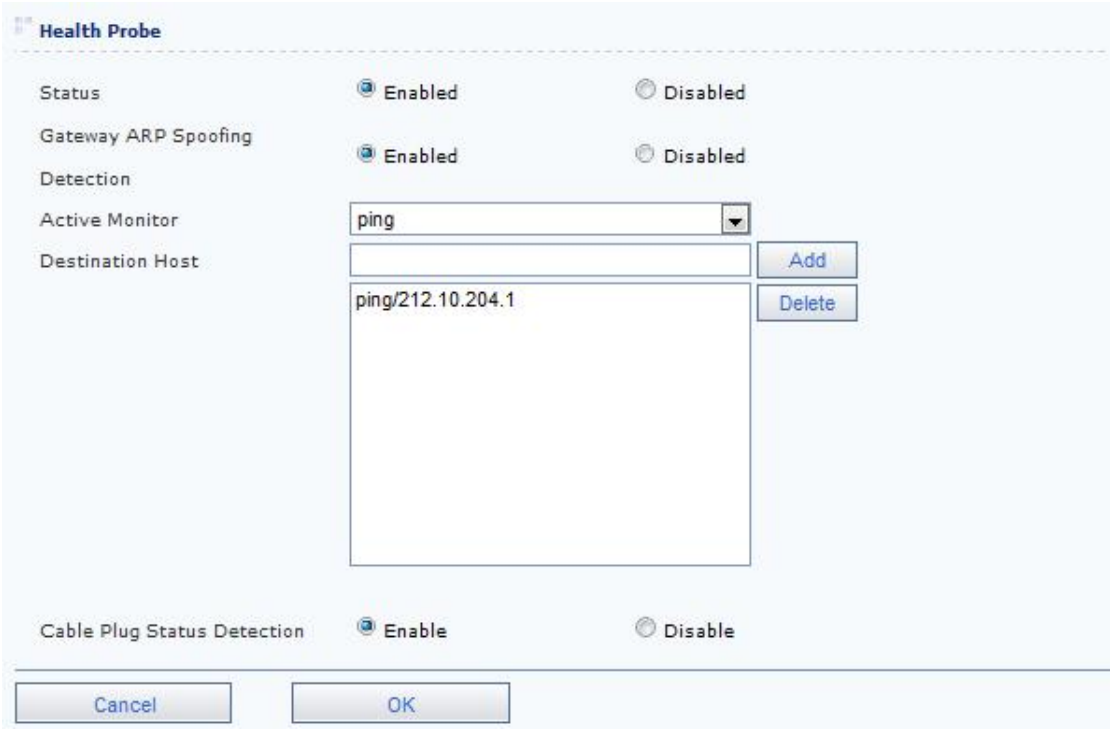


4. Create a WAN interface for Telecom on the **Network > Interface > Physical Interface** page, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



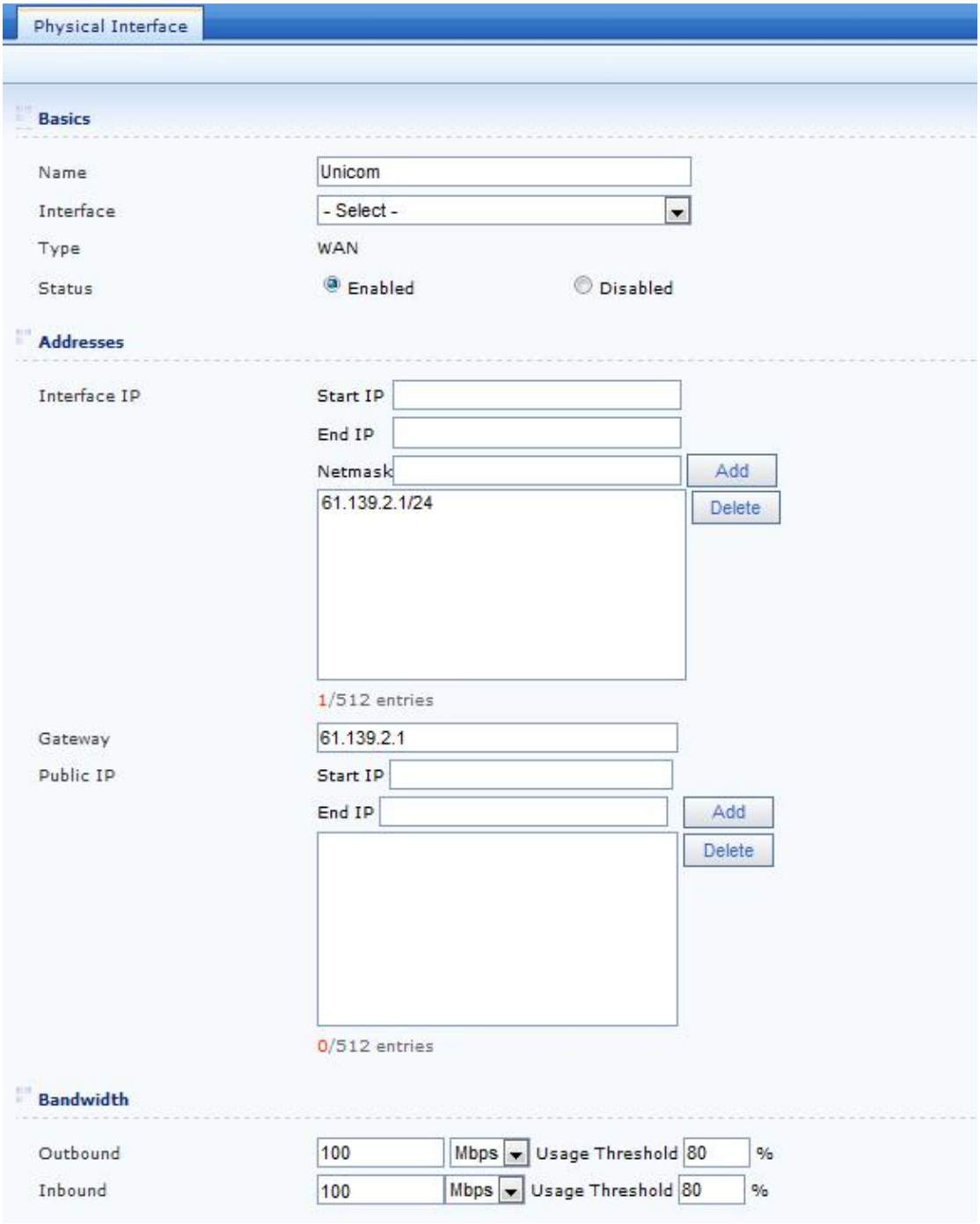
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



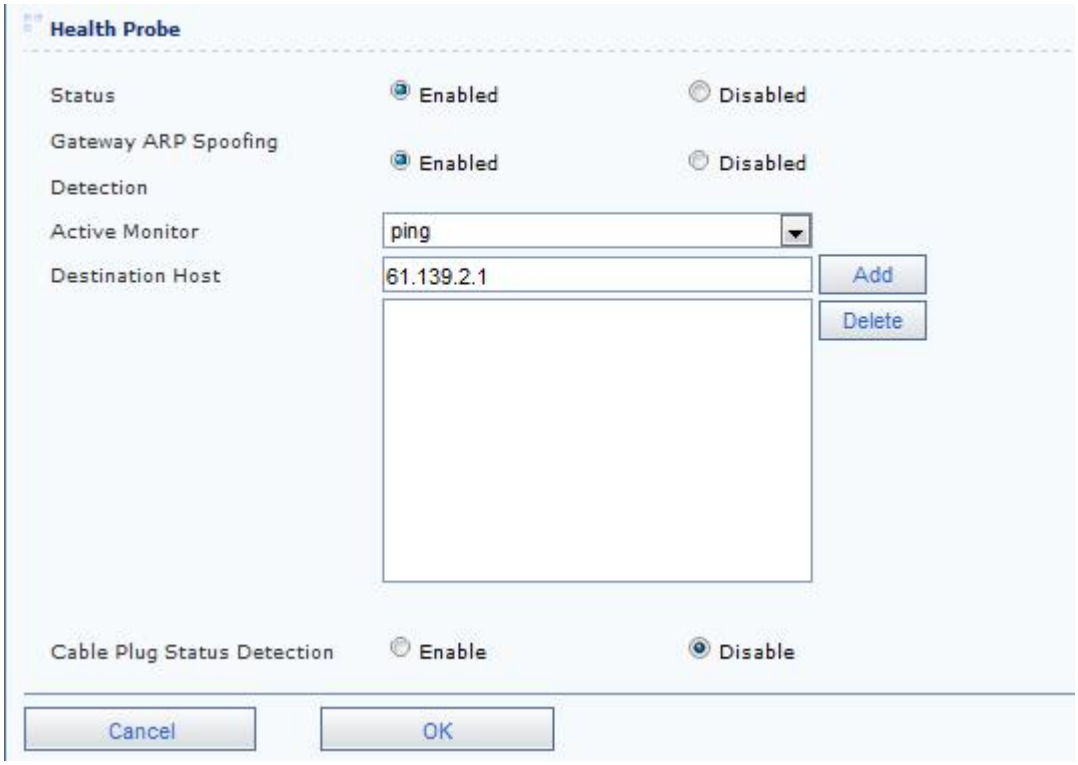
5. Create a WAN interface for Unicom on the **Network > Interface > Physical Interface** page, as shown below:



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

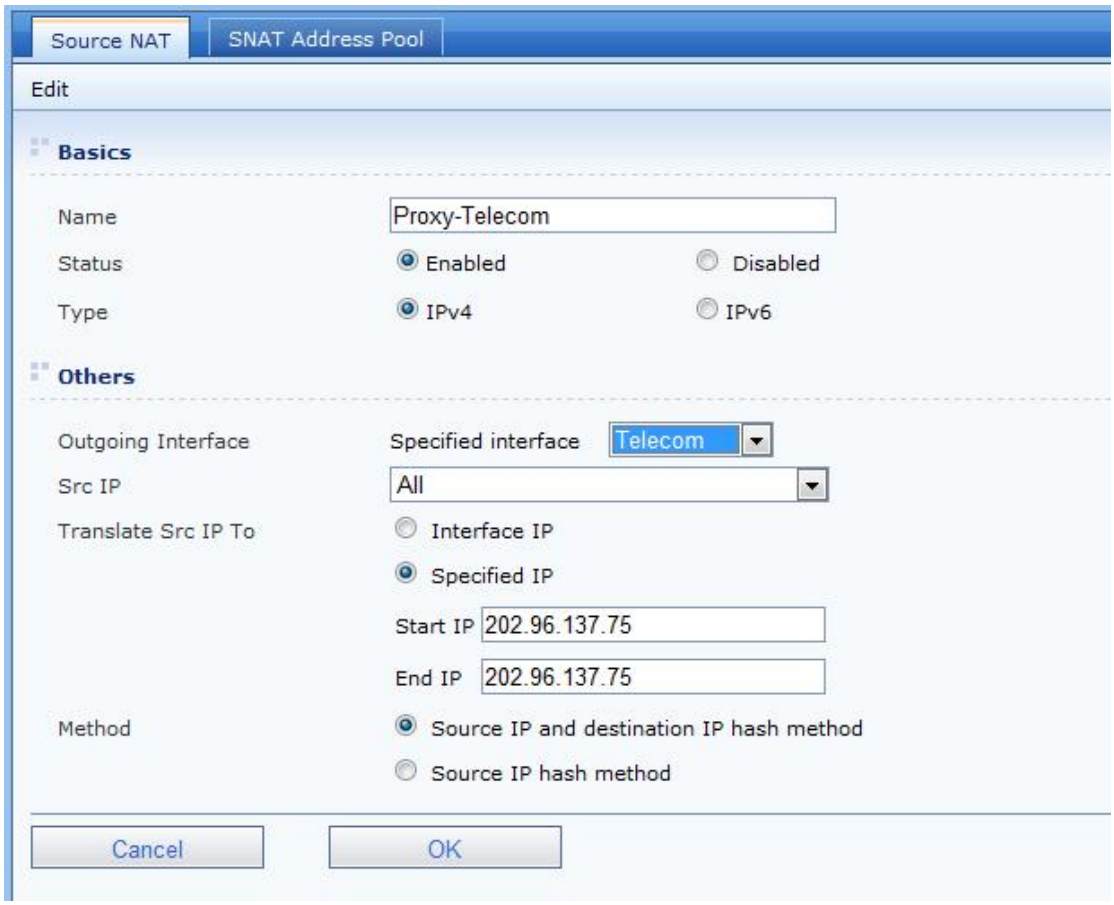


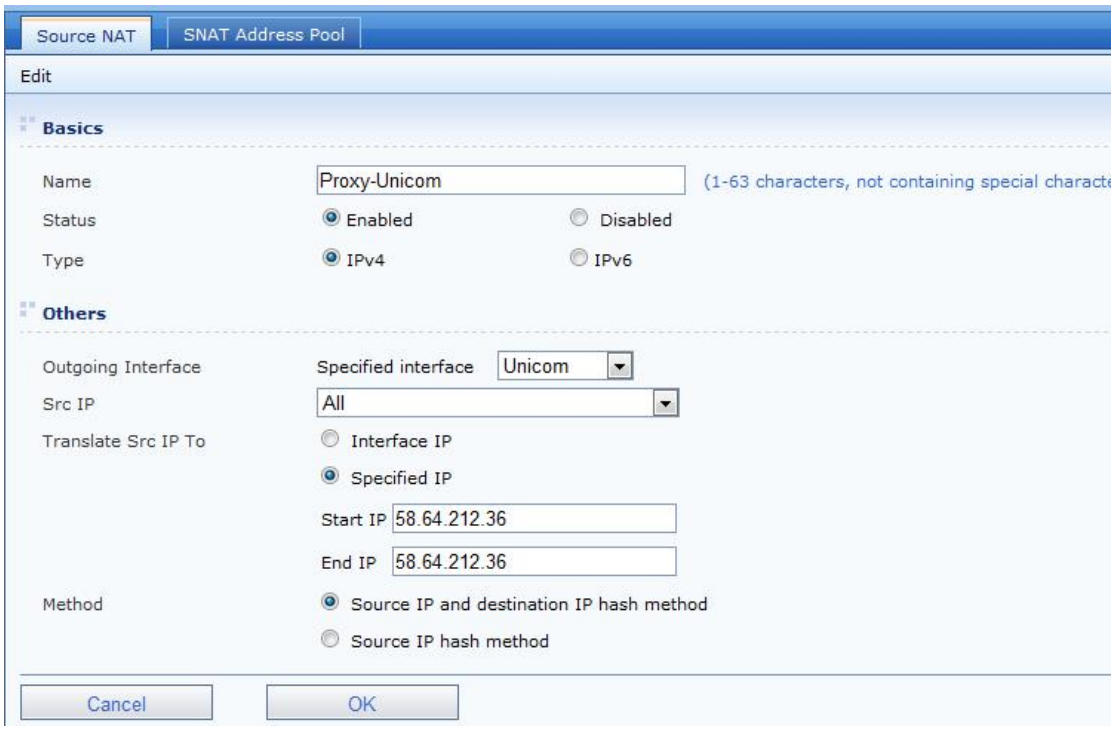
6. Go to the **Routing > Static Route** page, and create a static route which can reach the intranet, as shown in the following figure:



7. As the AD unit needs to proxy internal users and servers to access to Internet in this case, there needs to configure corresponding proxy policy. Create source NAT rule on the **Network > Source NAT** page, as shown in the following figure:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

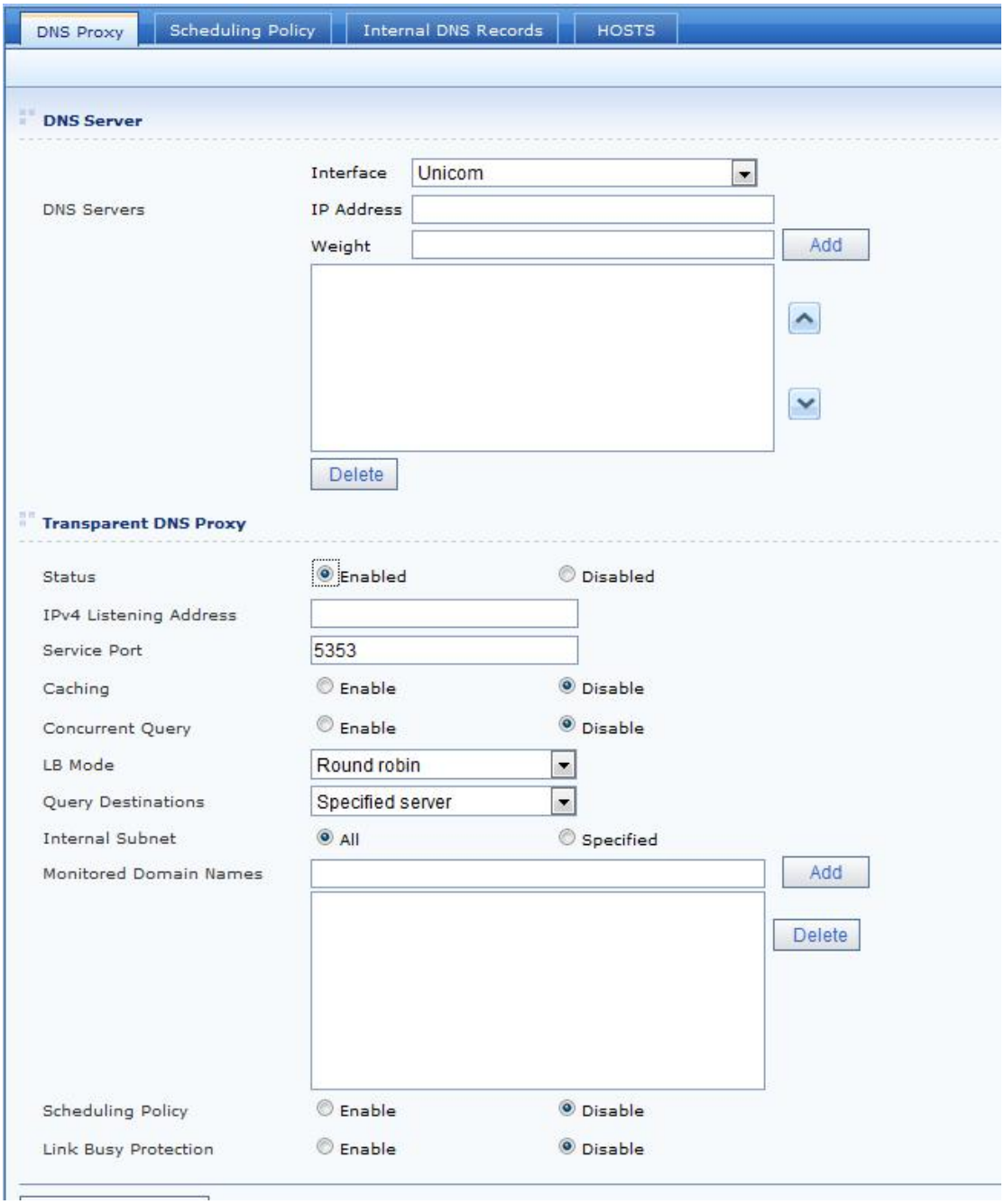




Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

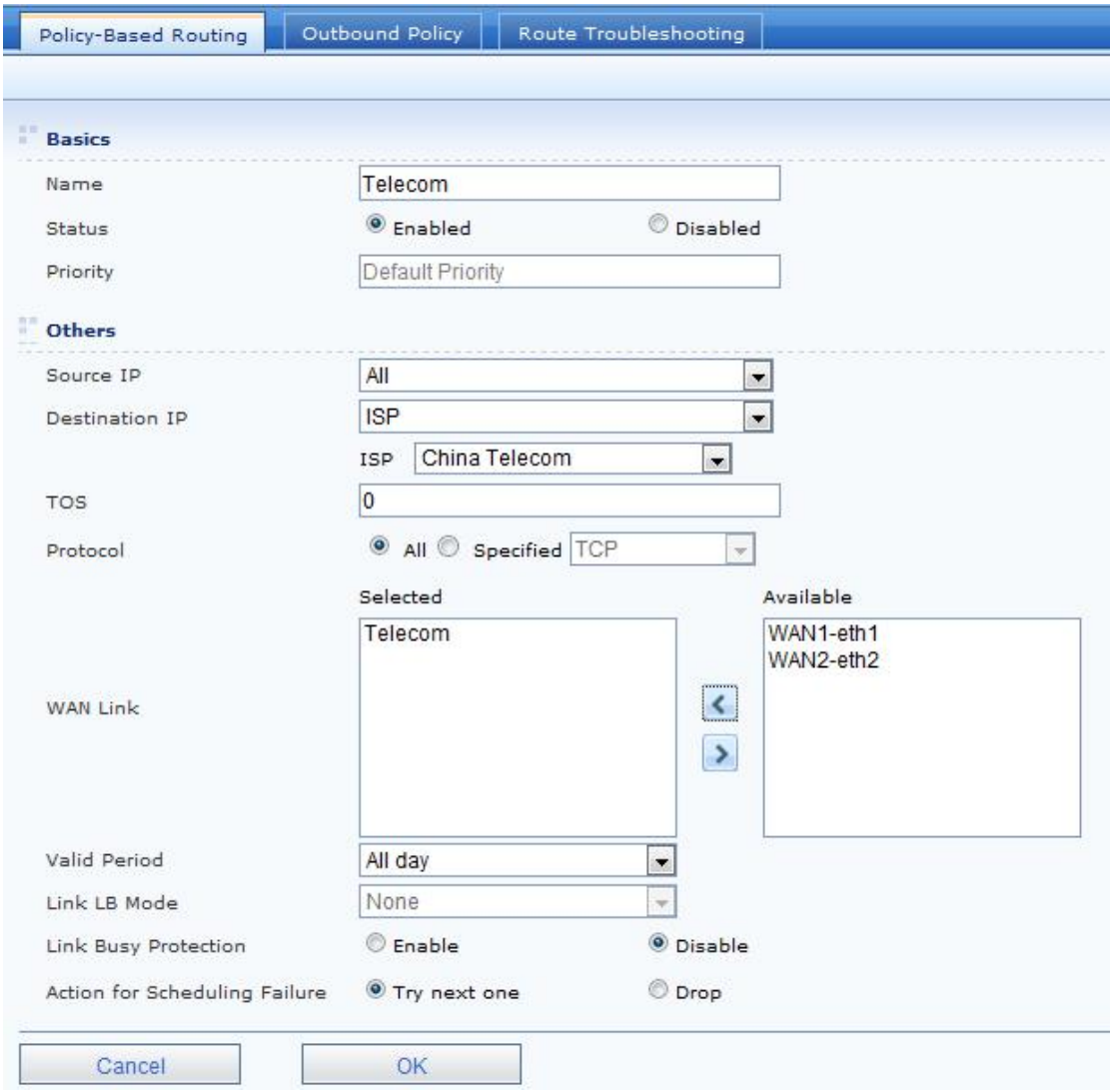


8. Go to the **Network > DNS Proxy** page, configure a DNS proxy, and add the IP addresses of DNS servers of WAN links: Telecom and Unicom in **DNS Servers** field.

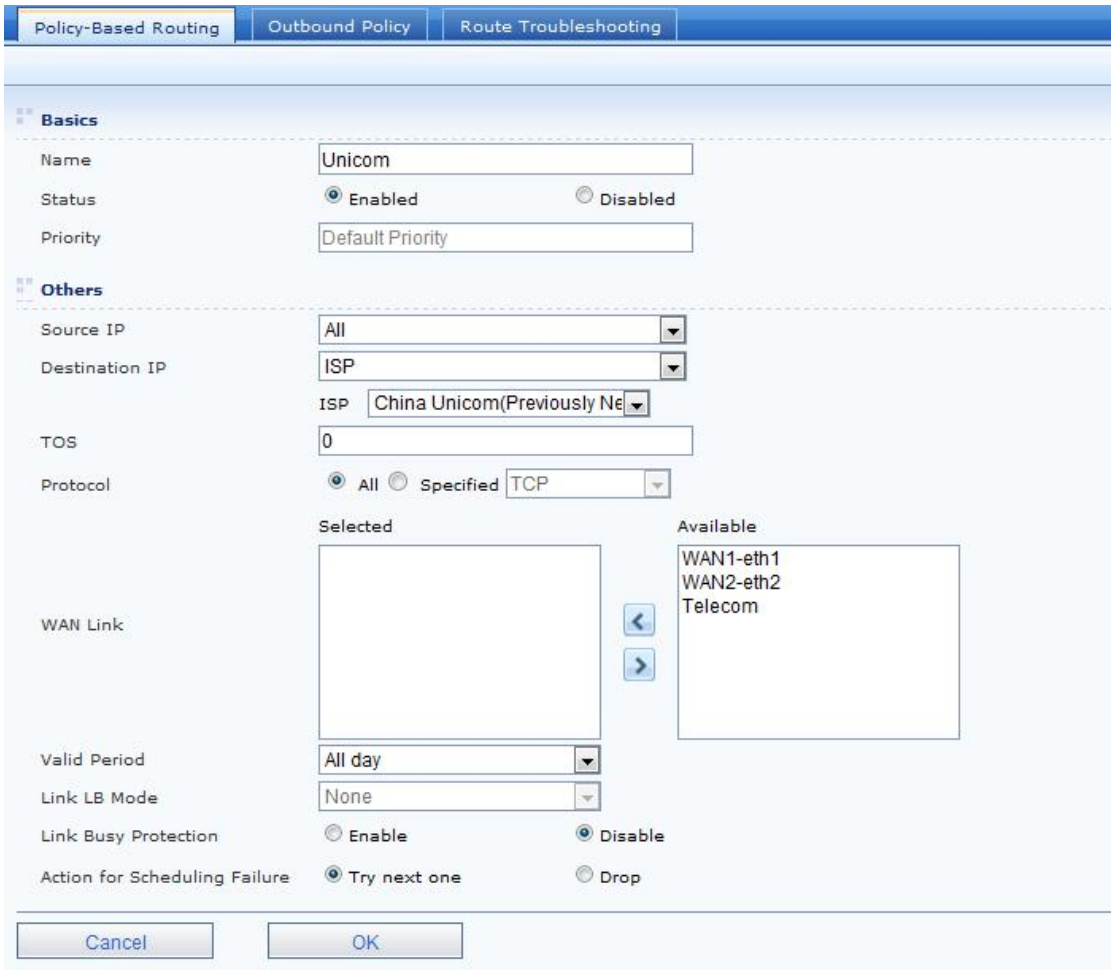


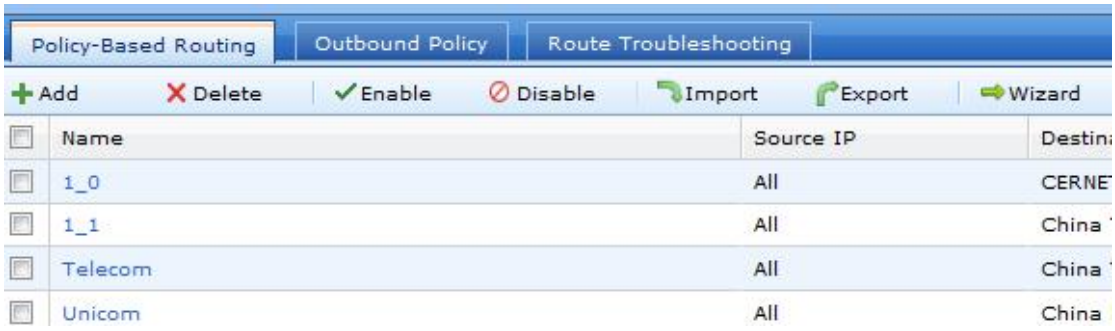
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

9. Go to the **Routing > Policy-Based Routing** page, and create two corresponding policy-based routing policies, so that when internal users access to Unicom server, the data only flow via Unicom link; while internal users access to Telecom server, the data only flow via Telecom link. There is a default routing policy selected by weighted least traffic on AD unit.



Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



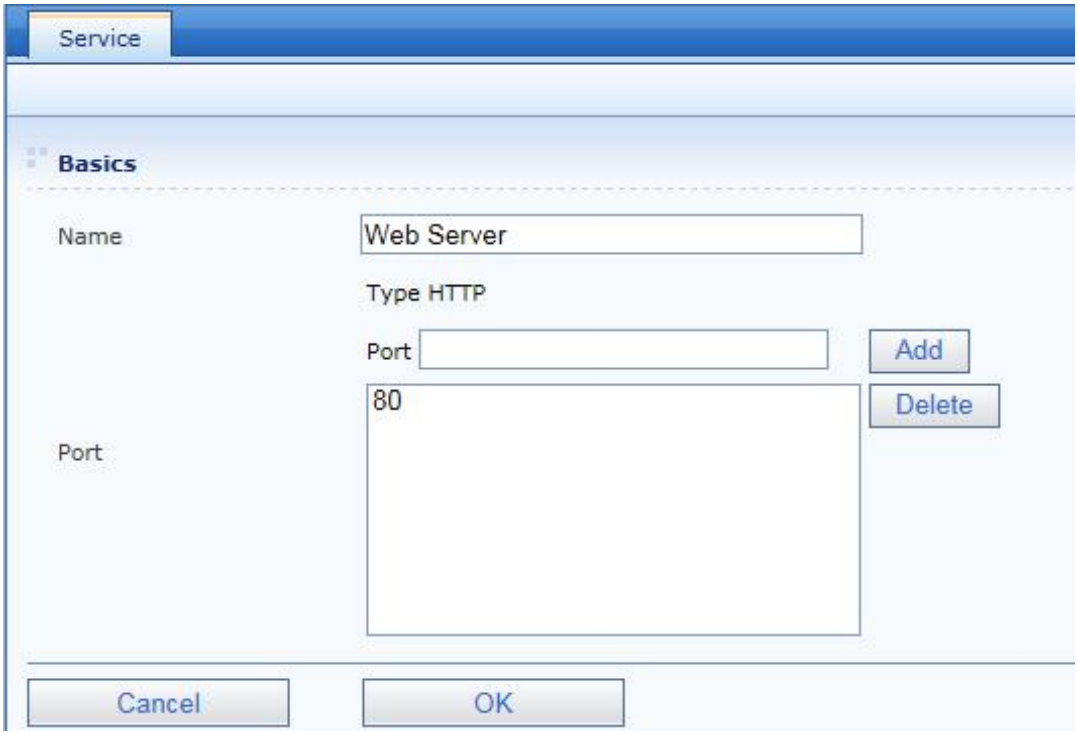


After completing the above configuration steps, deploy the AD unit in the network as displayed in above network topology. If it can operate normally, you can configure load balancing for servers and links.

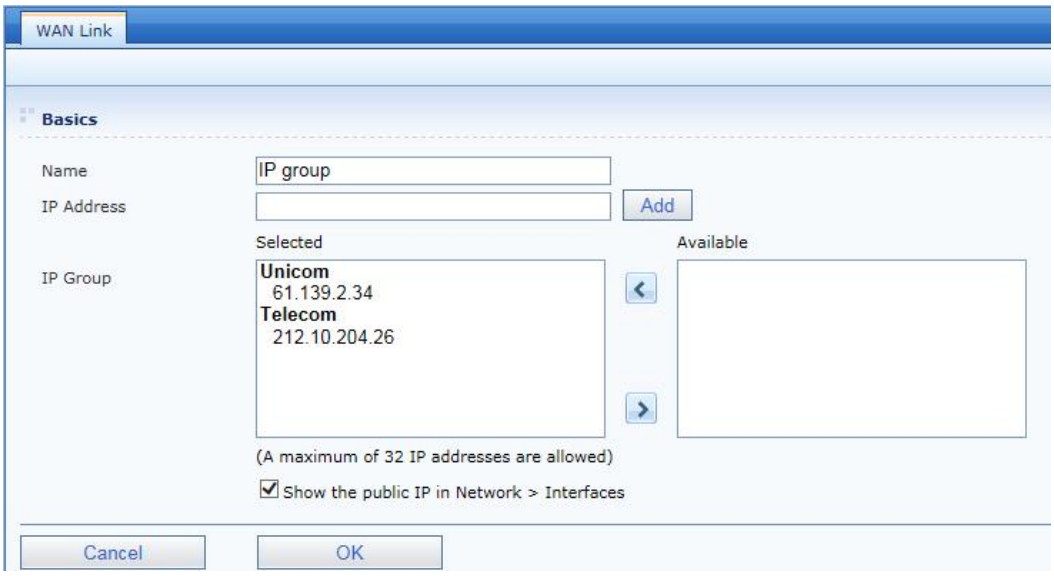
Configuration steps of balancing load on servers and links:

1. Go to the **Load Balancing > Service** page, create a Web service, and specify a service type and port number, as shown below:

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

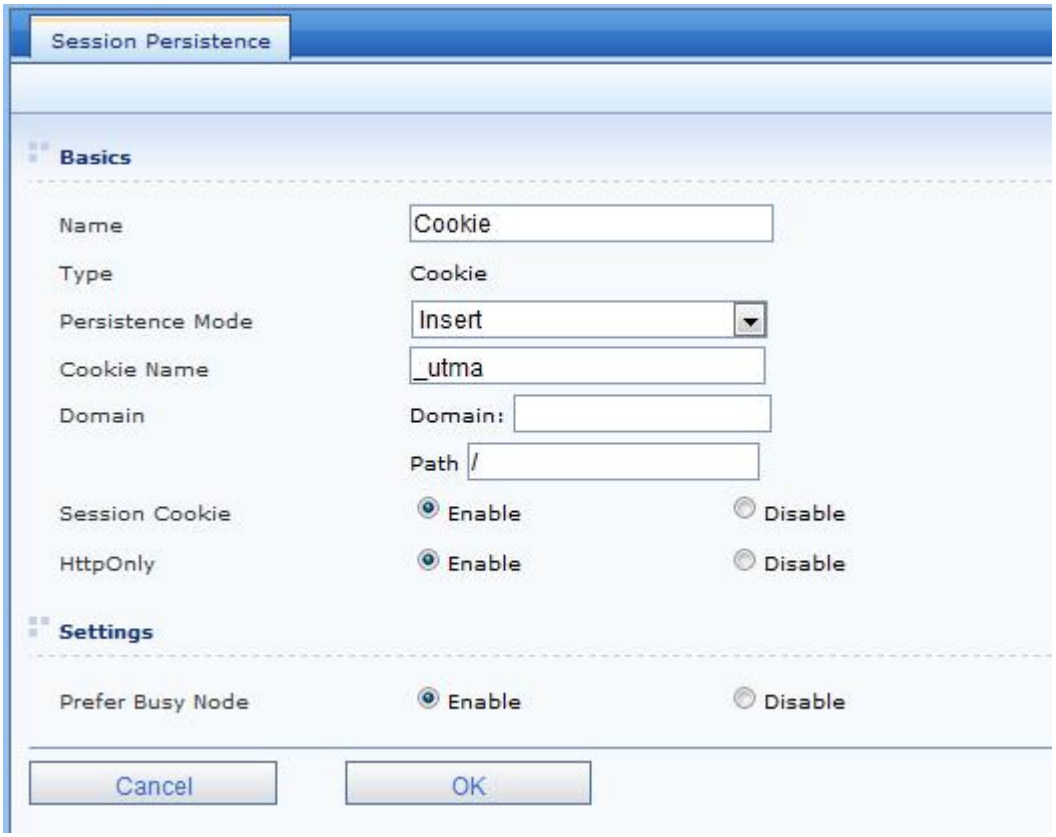


2. Go to the **Load Balancing > WAN Link** page, create a WAN link and move the two WAN link IP addresses from **Available** box into **Selected** box.



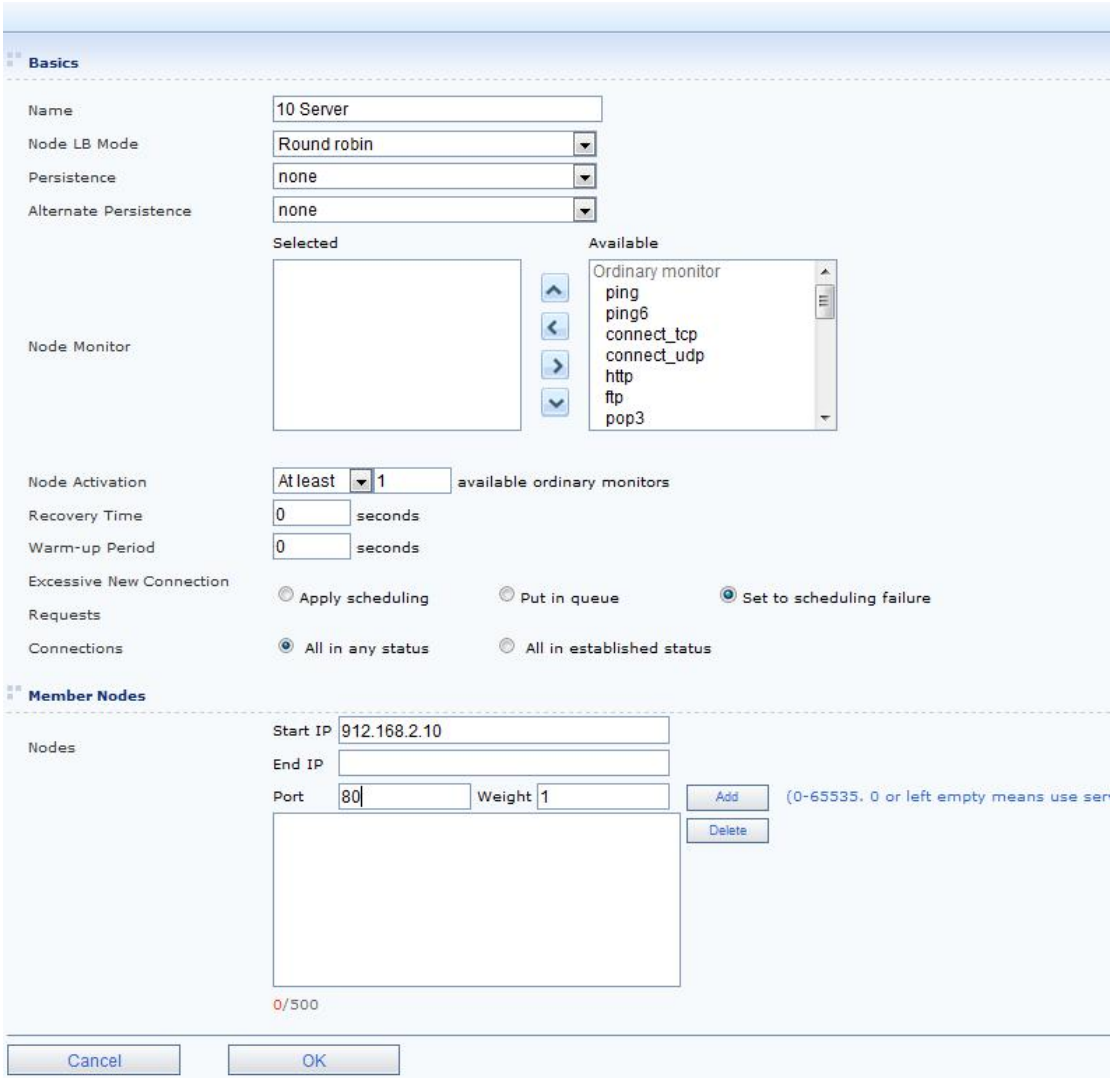
3. Go to the **Load Balancing > Persistence > Session Persistence** page, create a session persistence. Assume that the customer wants to implement a session persistence based on cookie name.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

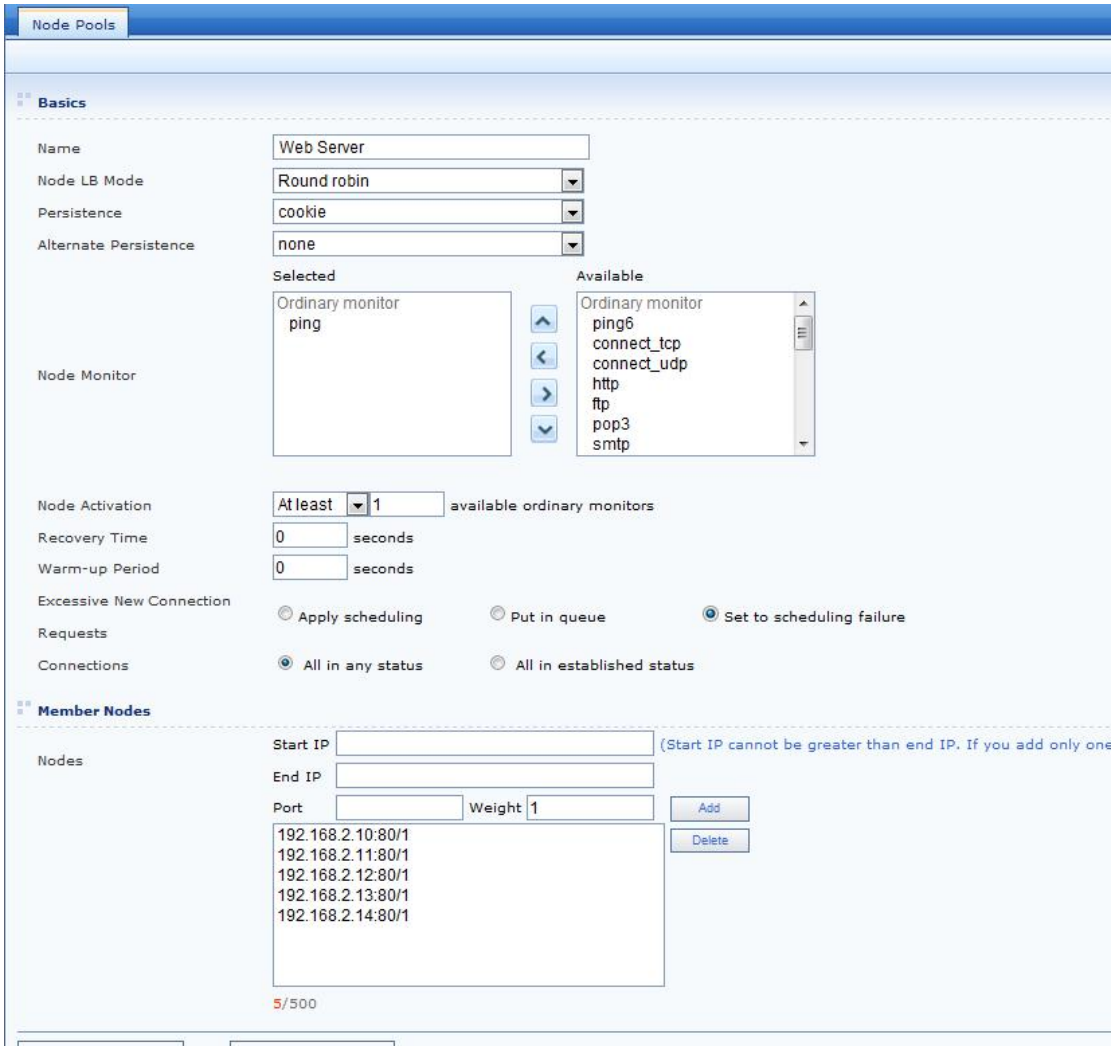


4. Go to **Load Balancing > Node Pools** page, and create two node pools. One node pool only contains the server with IP address 192. 168. 2. 10, used for scheduling policy, the other one contains the IP addresses of all the servers, used for server load balancing scheduling.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

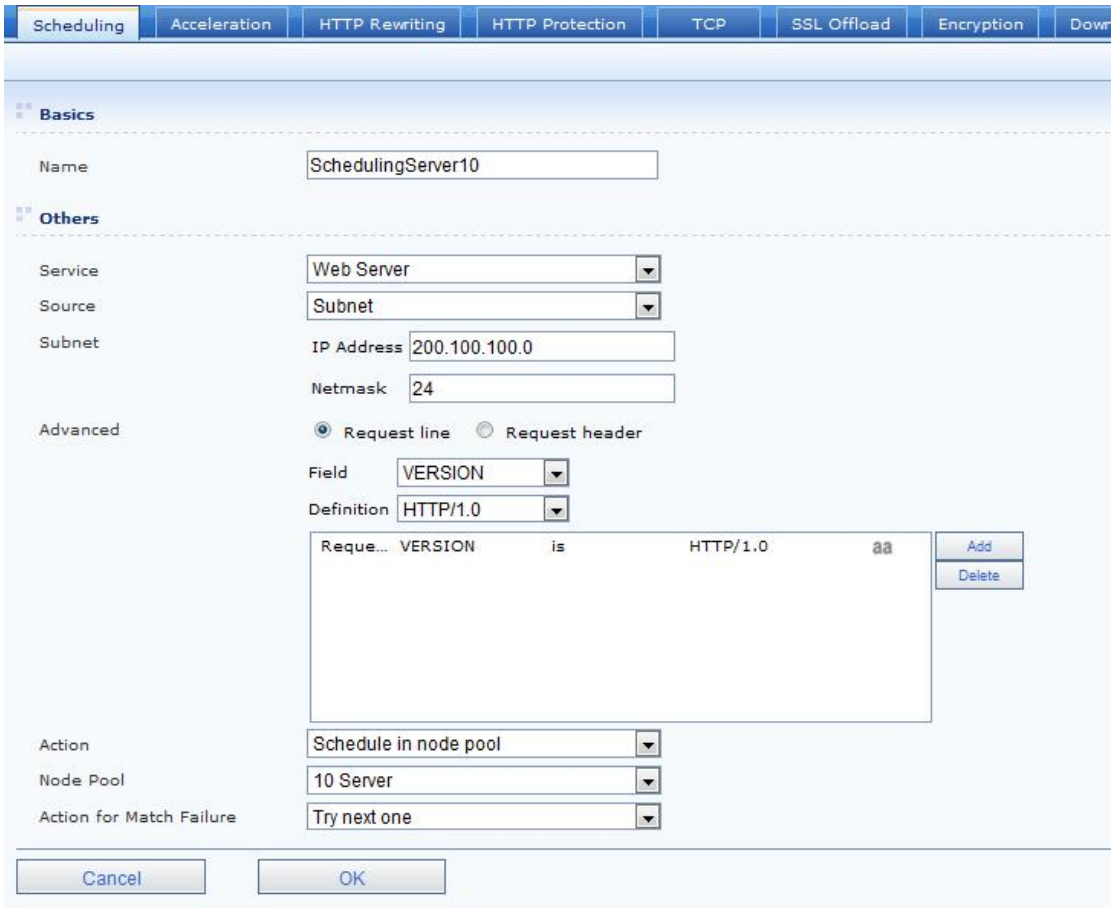


Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



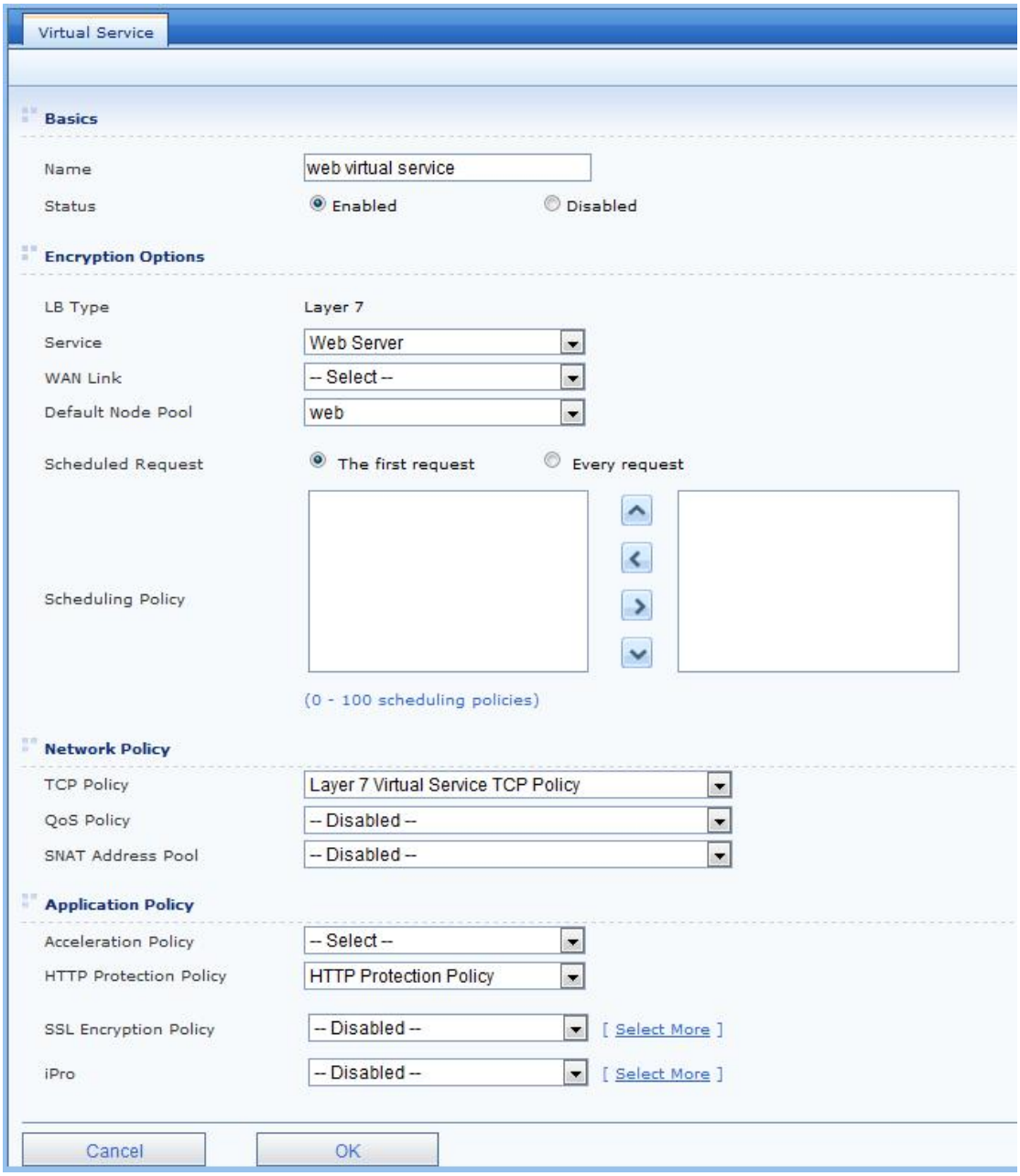
5. Go to **Load Balancing > Policy > Scheduling** page, and create a scheduling policy to have the request from the users on network segment 200. 100. 100. 0/24 scheduled to the server whose IP address is 192. 168. 2. 10 all the time.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



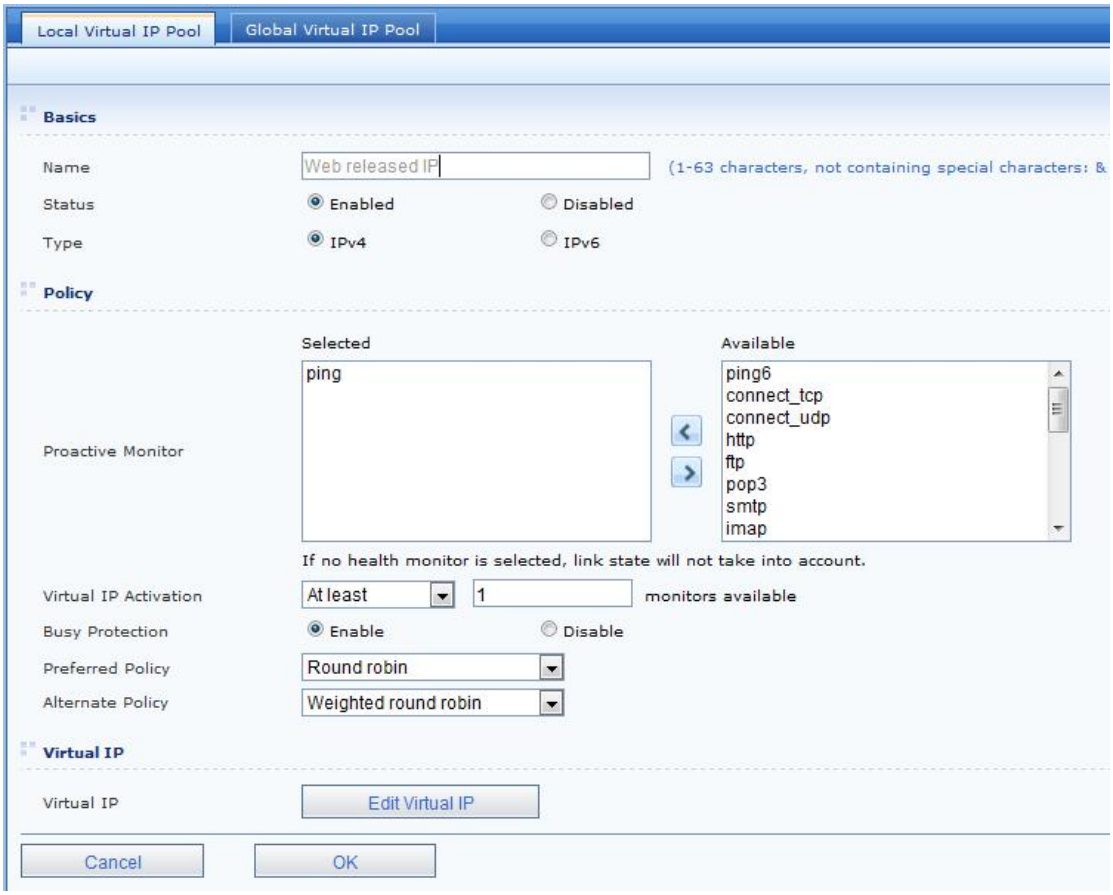
6. On the **Load Balancing > Virtual Service** page, create a layer 7 virtual service, and associate the already-configured service, node pool, WAN link and scheduling policy.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



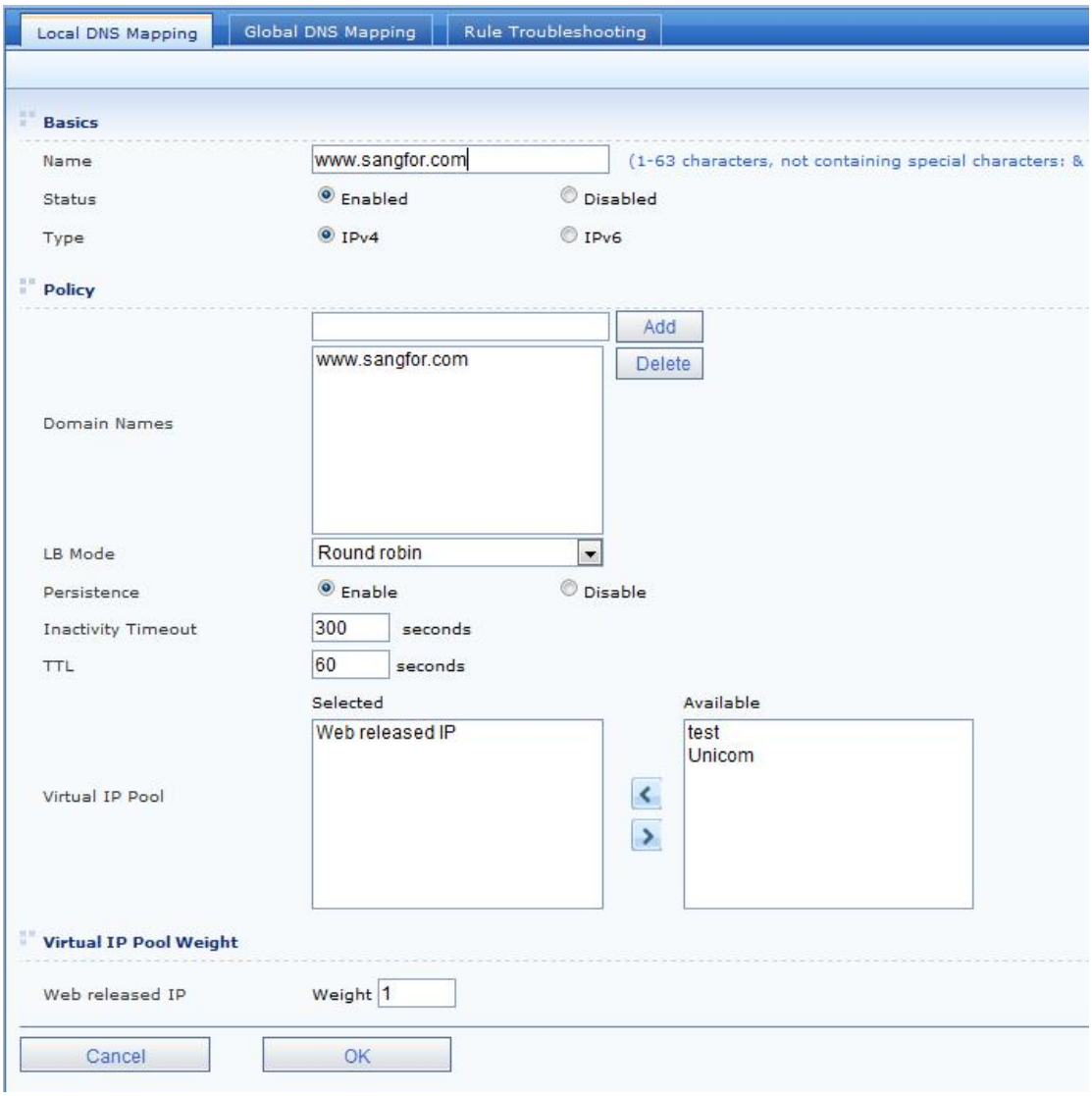
7. Go to **Intelligent DNS > Virtual IP Pool > Local Virtual IP Pool** page, create a local virtual pool and add the public IP addresses which need to be distributed. In **Preferred Policy** field, select **Static proximity**; in **Alternate Policy** field, select **Round trip time**.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



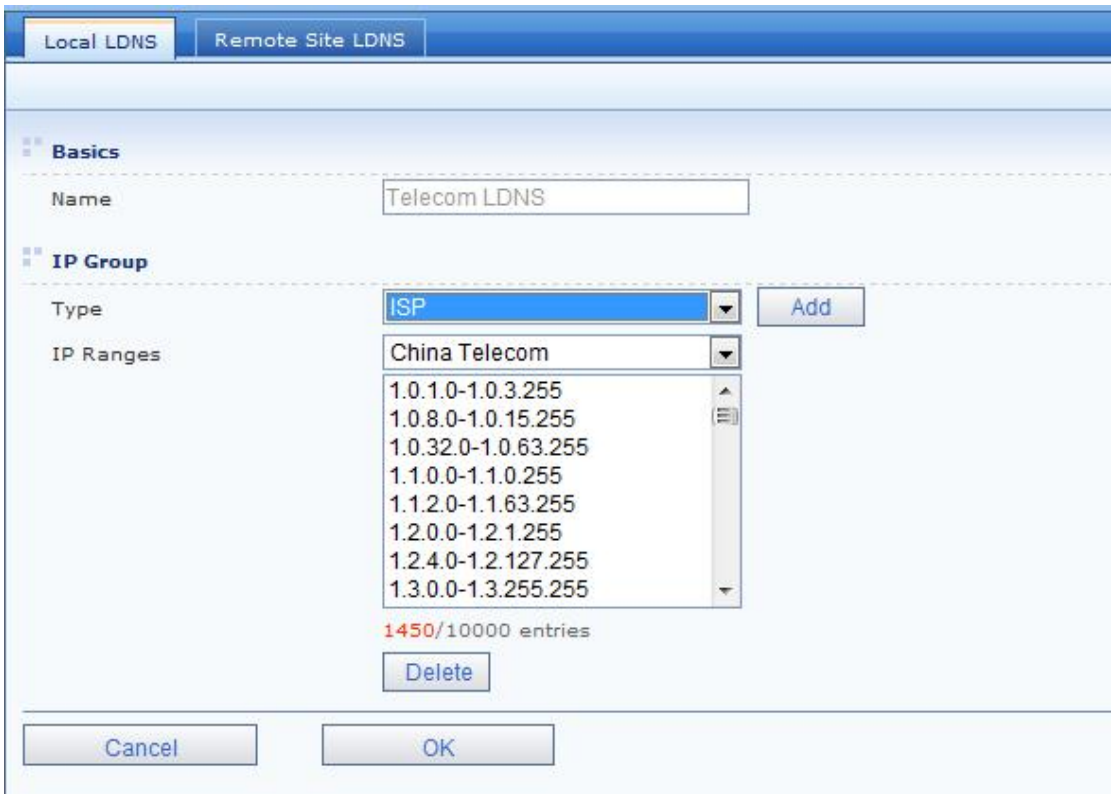
8. Go to **Intelligent DNS > DNS Mapping > Local DNS Mapping** page, and create a local DNS mapping. Enter the domain name which needs to be resolved and add it into **Domain names** field. Specify the IP pool which needs to be distributed in **Virtual IP Pool** field, as shown in the following figure:

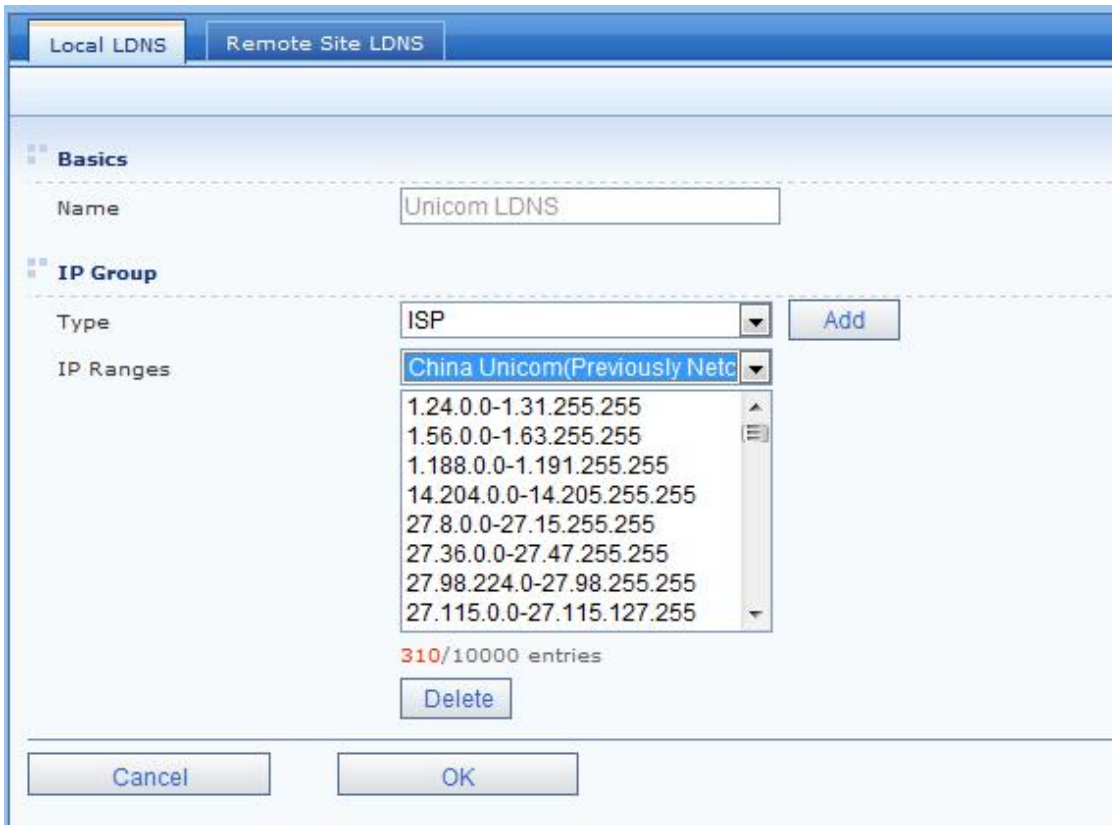
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com



9. Create two local LDNS on the **Intelligent DNS > LDNS > Local LDNS** page, one for adding IP range of Telecom, the other one for adding IP range of Unicom.

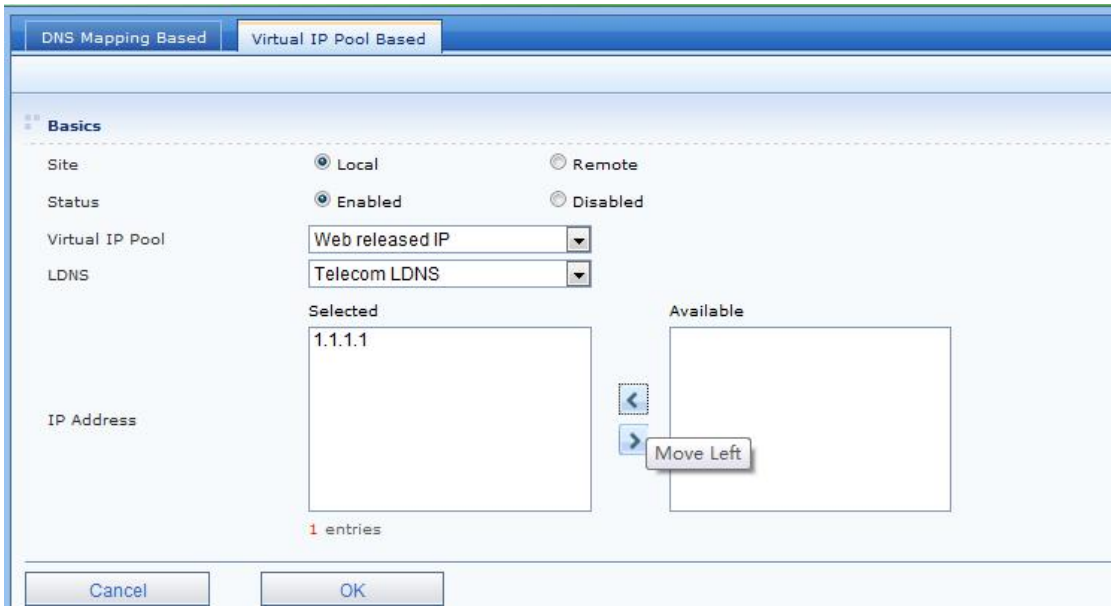
Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com

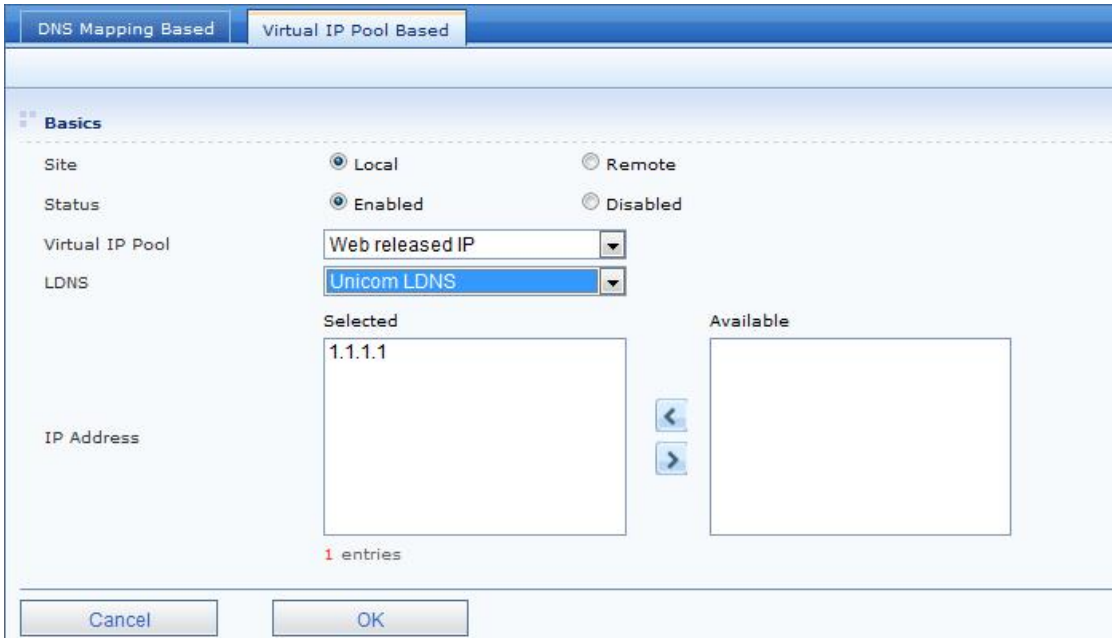




10. Go to the **Intelligent DNS > Static Proximity** page, **c**reate two static proximity policies. When external users access the domain name: www. sangfor. com, if the LDNS request is from Telecom link, return 212. 10. 204. 26 as resolved IP; if the LDNS request is from Unicom link, return 61. 139. 2. 34 as resolved IP.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com





11. The configuration is completed.

Copyright©Sangfor Technologies Co., Ltd. All Rights Reserved. www.sangfor.com