SANGFOR

IAM

Policy-Based Routing Configuration Guide

Version 12.0.41

Change Log

Date	Change Description
Jan 13, 2020	Version 12.0.41 document release.

CONTENT

Chapter 1 Overview

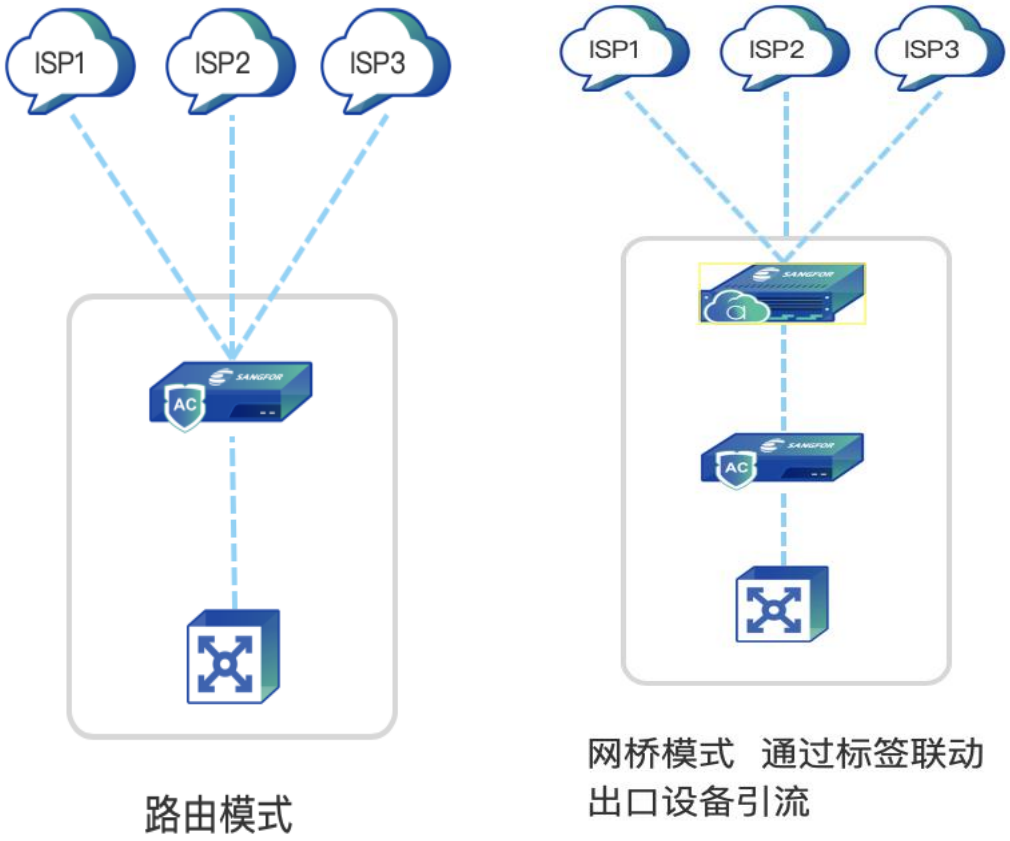
With the reduction of the cost of the Internet bandwidth of the operators, some customers will have multiple operator Internet exit links. The reason for multiple lines is that on the one hand, the problem of link redundancy backup is considered, and on the other hand, it is due to cost considerations (there are large price differences between different operator links). In this case, how to make good use of multiple links of different quality is an urgent problem.

In order to ensure the core user and core application online experience, and at the same time limited by limited high-quality bandwidth resources, users urgently hope to be able to use applications with low real-time and stability requirements (such as: P2P, P2P streaming media, web streaming media, games, etc.) Diversion to high-bandwidth, general-quality links, and diversion of core users (such as management) and core applications (such as video conferencing) that require high real-time and stability to high-quality lines. Those applications that require high real-time performance greatly improve work efficiency.

IAM traffic routing supports traffic optimization functions such as IP, protocol, user routing, application routing, bridge scenario routing, and DNS proxy to improve customer bandwidth utilization.

Chapter 2 Solution Description

Sangfor's application routing solution supports multiple flexible deployment methods, which can be routed to implement application drainage, and can also be combined with mainstream manufacturers' routers / firewalls. Support label-based routing to meet customer scenarios of different link access.



Sangfor IAM uses technologies such as routing technology, DNS transparent proxy technology, and link busy control to implement link allocation mechanisms based on load conditions, time periods, user groups, access objects, and other factors to further improve link optimization. rate.

Sangfor IAM supports setting the diversion range according to factors such as end-user groups, Internet applications, access domain names, source address segments, destination address segments, transmission protocols, IP layer DSCP / TOS tags, etc., and supports dynamic loads (high priority lines are preferred) Designated lines, load by operator, load by line bandwidth, load by remaining bandwidth, VPN dedicated line backup and other load methods to improve the drainage effect.

2.1 Application Software Routing Technology

Sangfor IAM uses application routing technology to implement the link allocation mechanism based on factors such as link load conditions, time periods, user groups, access objects, and access application types to further improve link optimization utilization.

2.2 Dynamic drainage technology

Sangfor IAM adopts dynamic drainage technology. When high-quality lines are idle, other users and traffic can also run high-quality lines. When high-quality lines are about to be busy, non-core application traffic and non-core user traffic are diverted. This guarantees the core users and core applications' online experience premise. Next, make full use of high-quality lines to avoid vacant waste.

Chapter3 Routing instructions

Routing mode and bridge mode support Policy-Based Routing. Support DSCP and tos mark.

Default Policy-based Routing

Prefer the line with highest priority

Based on dst ISP

Based on remaining bandwidth

Weighted Round Robin

Even load assignment

Disable Default policy

Preferred Policy-based Routing

Specified

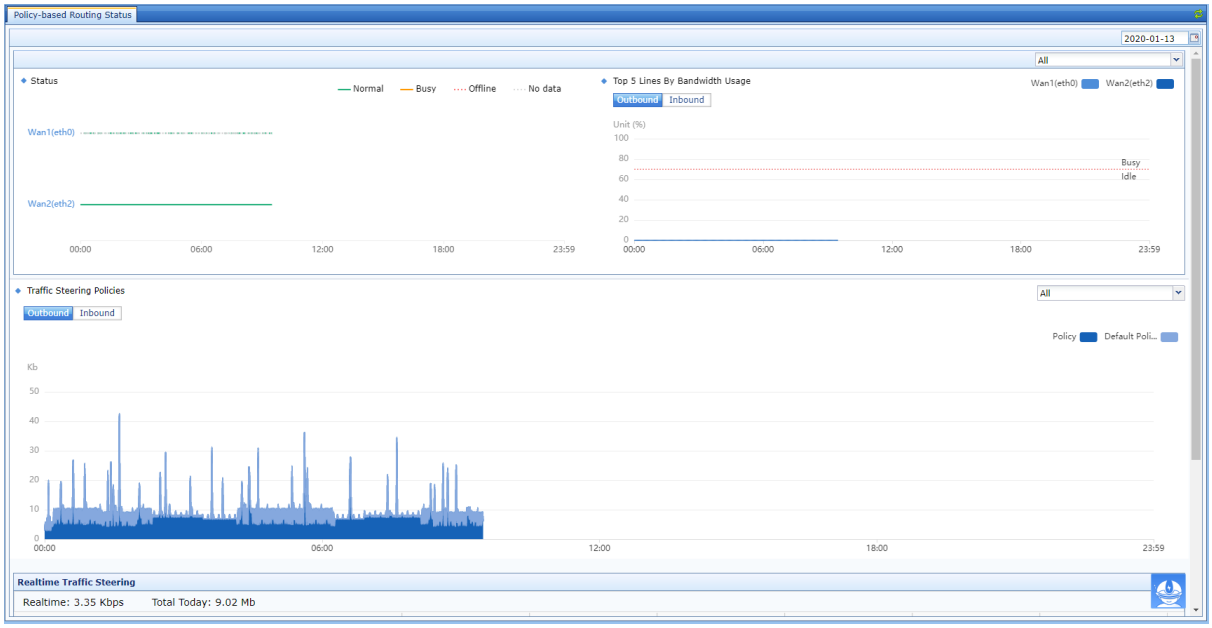
- Based on remaining bandwidth
- Prefer the link at top
- Weighted Round Robin

Even load assignment

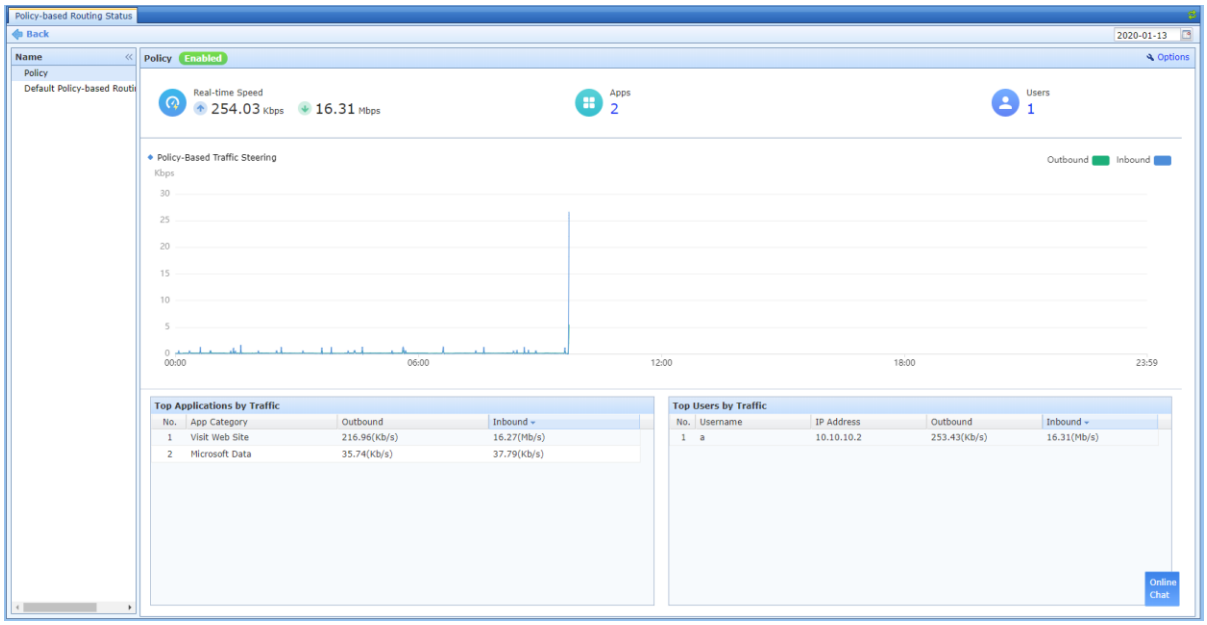
Chapter 4 Link Load Status

The previous version does not support link load status viewing. Starting from 12.0.41, link load visualization is supported. [Status]-[Traffic Statistics]-[Link Load Status].

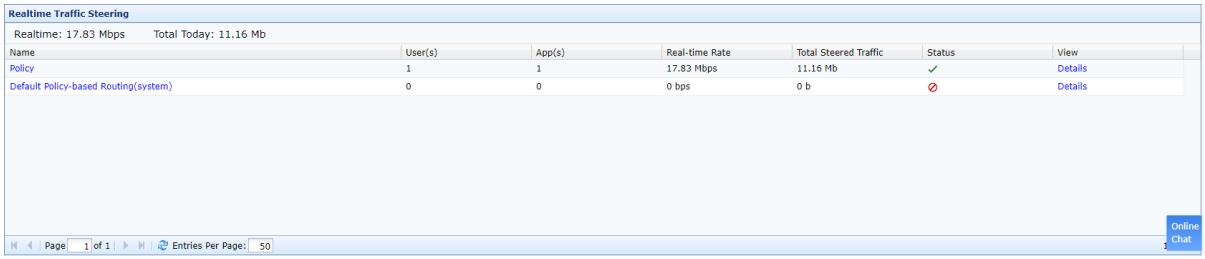
View the status of the line, know the bandwidth utilization, and know the distribution of the traffic diversion policy:



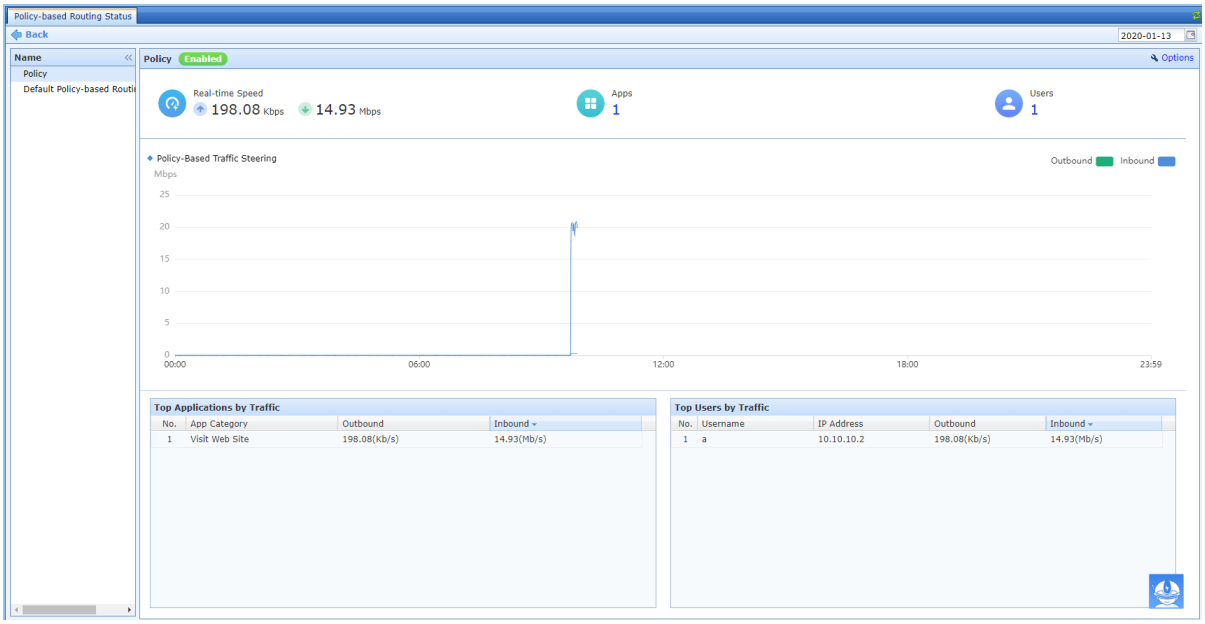
Click “Lines” to display the details of line drainage:



Real-time information for rendering strategy drainage:



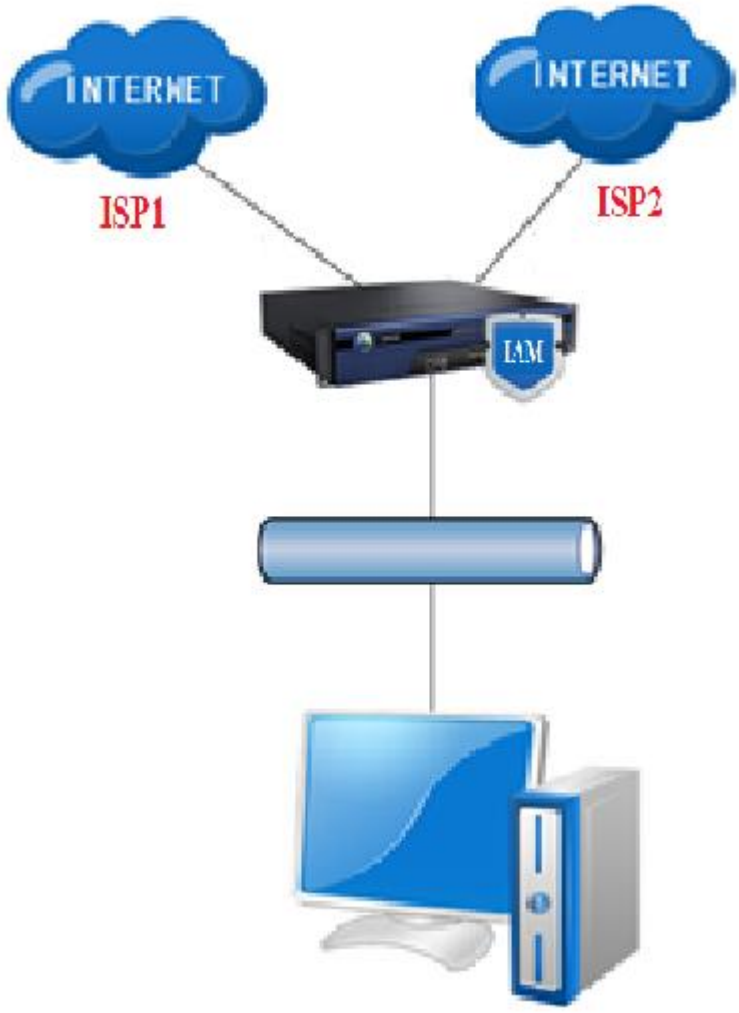
Click "Policy Name" to display the details of each drainage strategy:



Chapter 5 Configuration

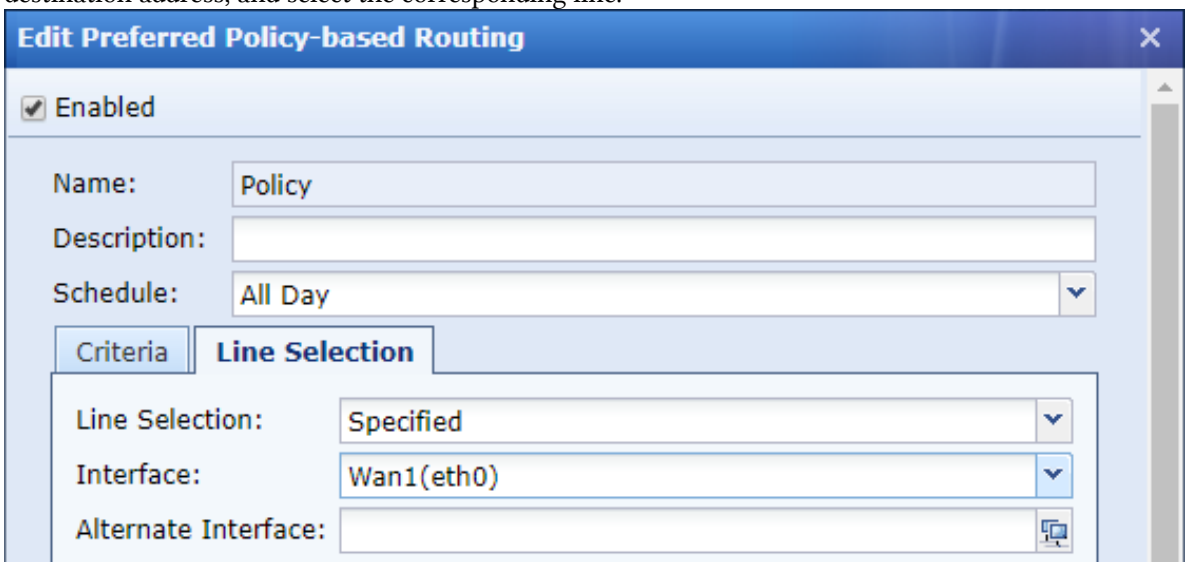
5.1 Designated Route Selection

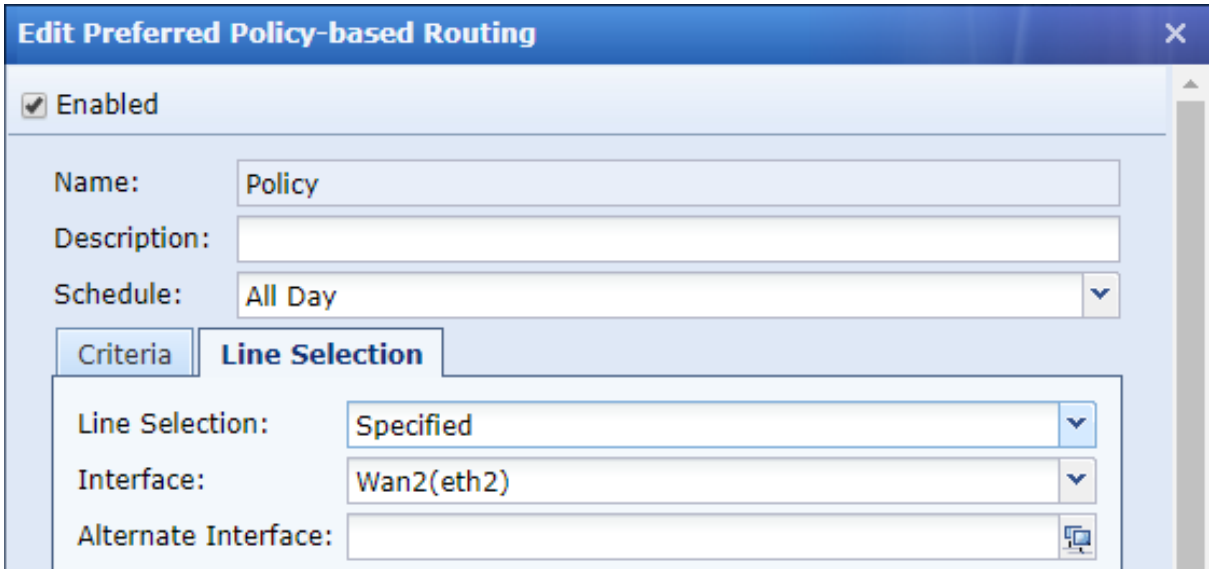
The customer has two external network lines, one China Unicom and one China Telecom, and now wants to achieve data access to China Telecom on the internal network via the China Telecom line, and China Unicom's data access to China Unicom



.

Solution: Configure Policy-Based Routing, the source address of the internal network, set the specified destination address, and select the corresponding line.

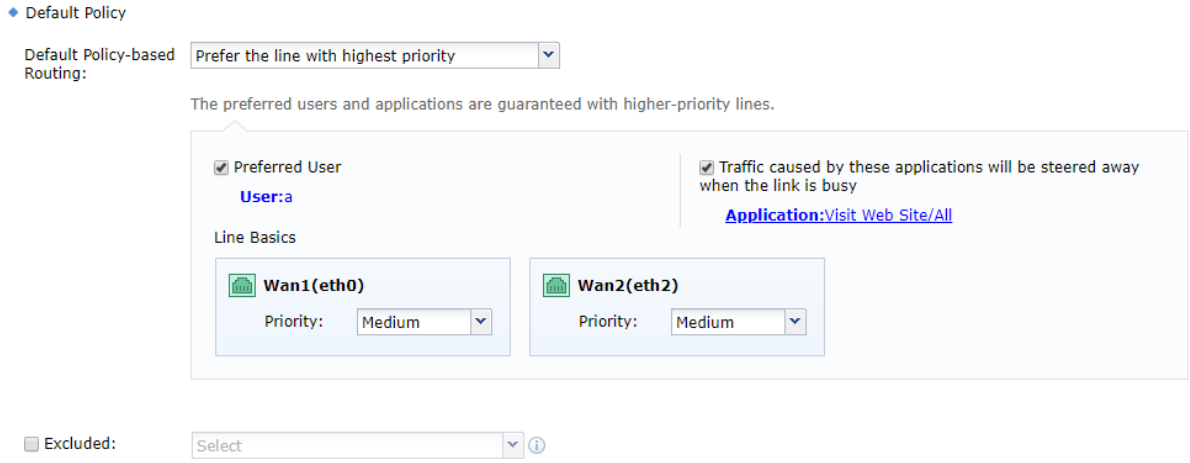




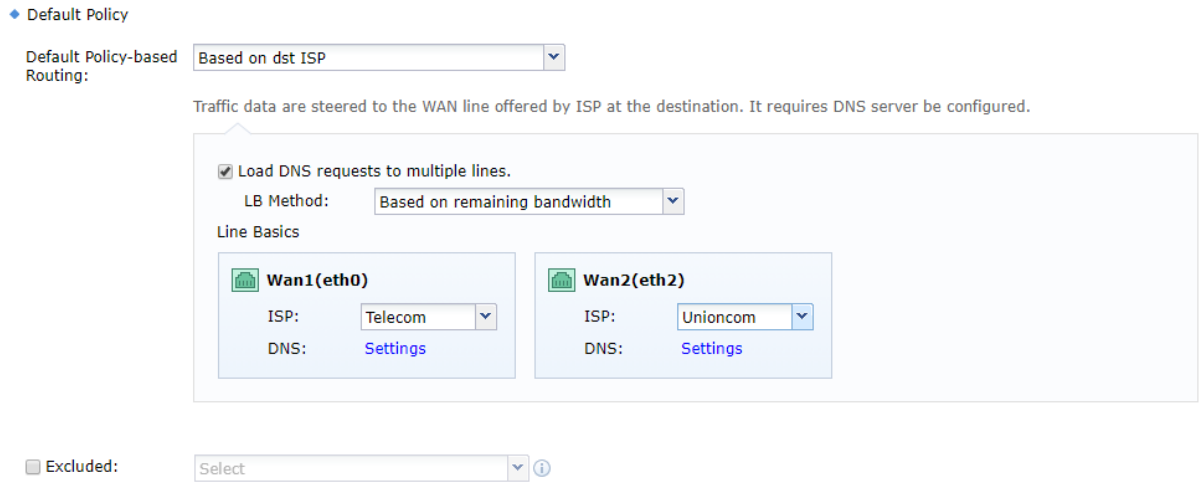
5.2 Multi-line load

5.2.1 Load Method Description

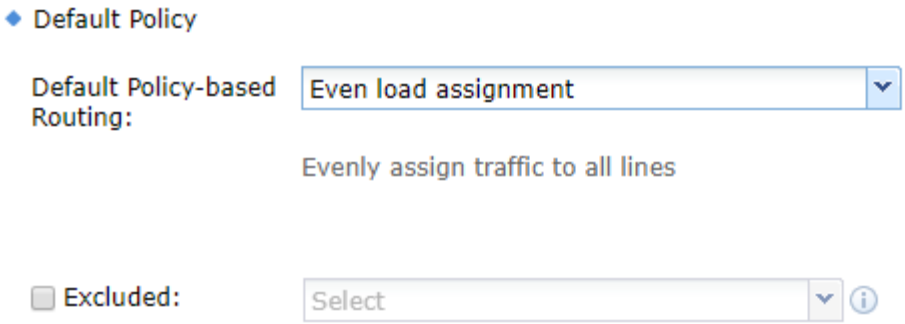
Prefer the line with highest priority: With multiple lines, the device will show the status of each line. The administrator defines the priority according to the line status and preferentially walks the line with the higher priority. When the line is busy, it supports the configuration to protect core users and divert non-core applications.



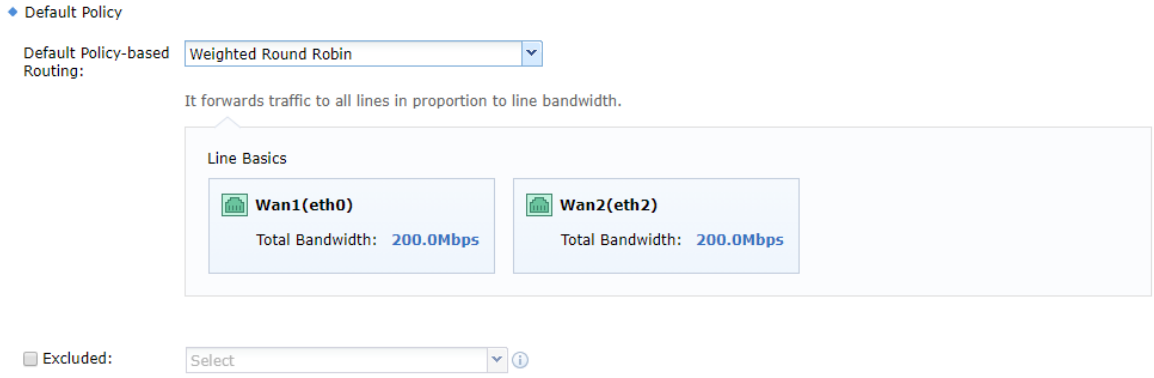
Based on dst ISP： With multiple lines, the device will show the status of each line. The administrator defines the priority according to the line status and preferentially walks the line with the higher priority. When the line is busy, it supports the configuration to protect core users and divert non-core applications.



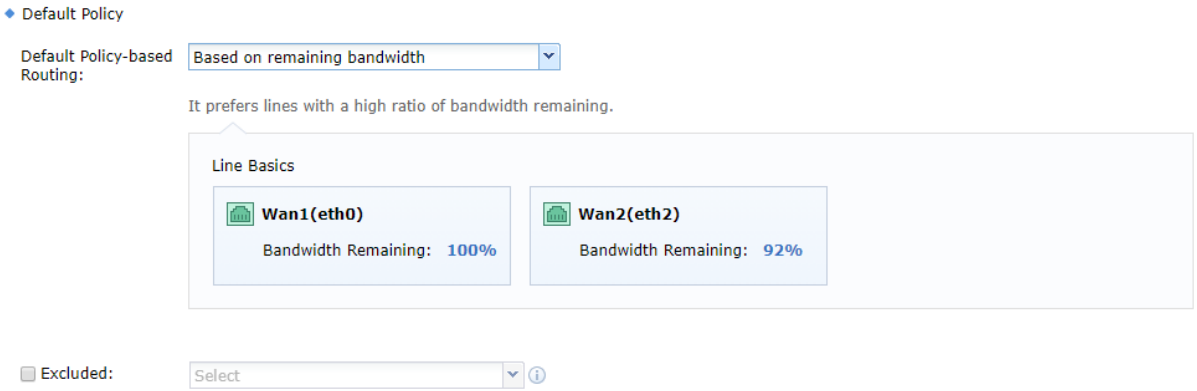
Even load assignment: Each link has an equal opportunity and is selected in turn.



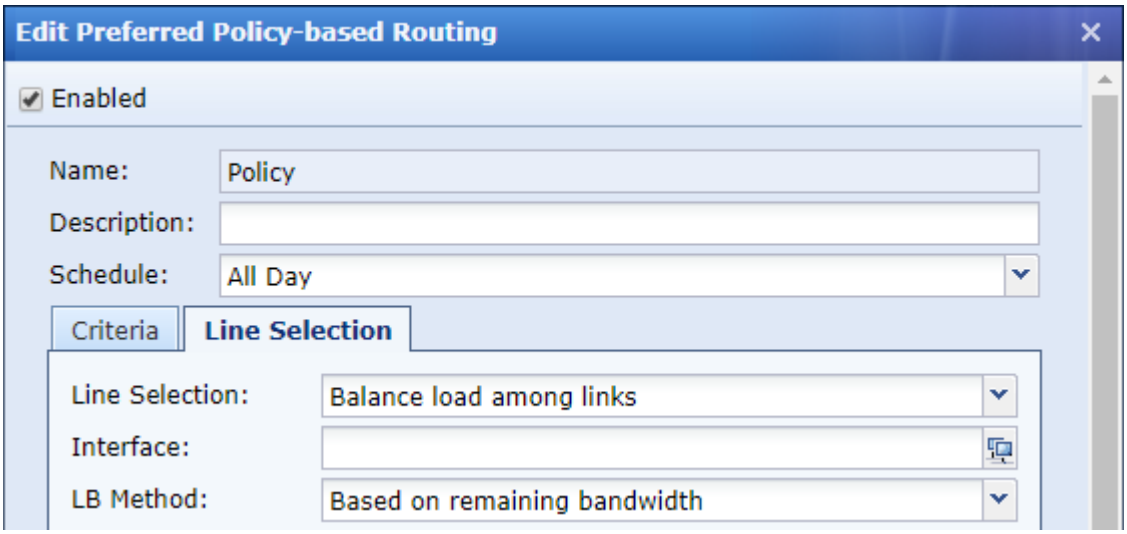
Based on remaining bandwidth: Each link is selected according to the ratio of weights. The chances of a large weight selection are high, and the chances of a small weight selection are small. The weight of a link is based on the bandwidth of the link.



Weighted Round Robin: Allocate traffic according to weight ratio and select the link with the smallest traffic weight ratio



Preferred Policy-based Routing: To implement link backup, for example, there are link one, link two, and link three, and the first surviving link will be found as the exit. Only the priority load policy supports this routing method.

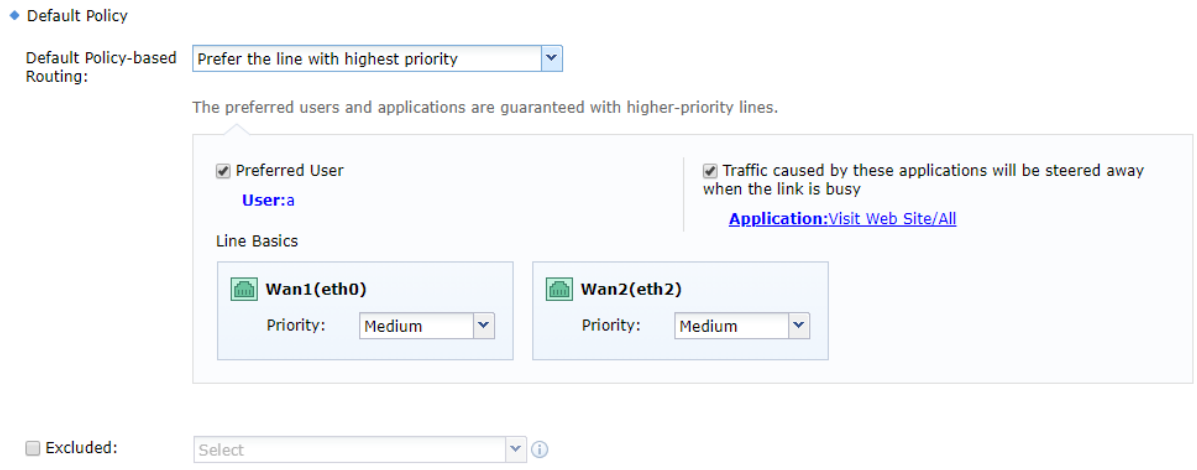


Excluded: It is unique to the default load policy and does not need to be a load line. It supports exclusion.

5.2.2 Default Policy-based Routing

Multi-line scenario, can monitor the status of each line; configure the default load policy according to different needs

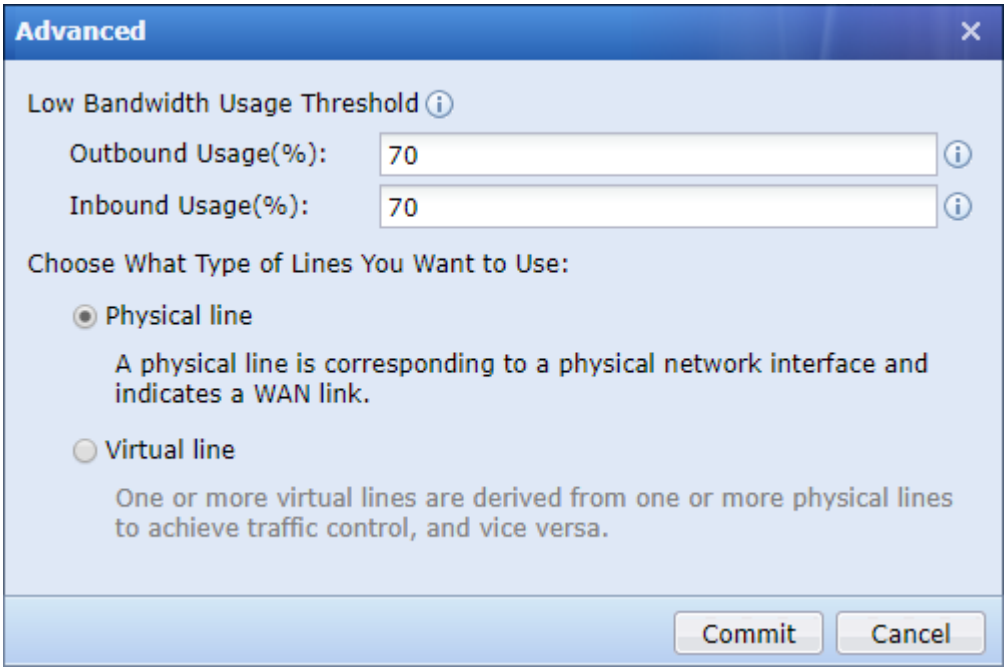
Note: The default load policy cannot customize the user / application / validation time.



There are three lines, depending on the line status

(1) Guarantee the user group "67.67" first and take the best quality line (assuming wan1 is the best, wan2 is the second, and wan3 is the worst)

(2) When the line is busy (traffic configuration-line configuration-advanced settings), the "p2p" application is taken away (busy definition: upstream or downstream, if one is busy, it enters the busy state)



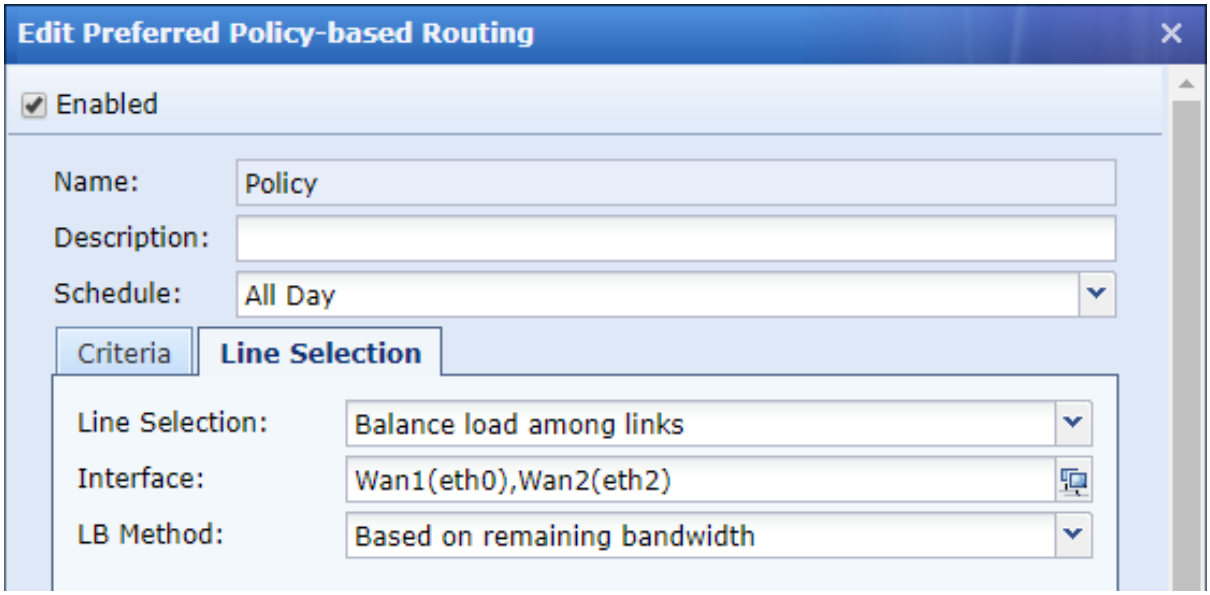
(3) Traffic diversion: Define line one-priority: very high, line two-priority: medium, line three-priority: low;

When line one is full, it will divert unimportant applications (in this case, p2p traffic) to line two; but line two is also busy and divert to line three ... recursively

5.3 Preferred Policy-based Routing

The customer has several external network lines, and now wants to achieve internal network access to the external network based on the remaining bandwidth of the line evenly distributed.

Solution: Configure the link load, select the multi-line load for the routing scheme, and select the corresponding load strategy.



5.4 Policy-based Routing and DNS Proxy

Requirement:

(1) For user A, match the redirection to the specified line policy in the DNS proxy policy, visit www.baidu.com, and go to line 2.

(2) Load strategy, user A, visit www.baidu.com, configure route 3

Which line does User A take to access Baidu?

answer:

Priority: DNS proxy> Priority load policy> Default load policy> Default policy routing

Going Line 2

5.5 DNS proxy escape

The "redirect to DNS server" and "redirect to designated line" scenarios of DNS proxy provide escape mechanisms.

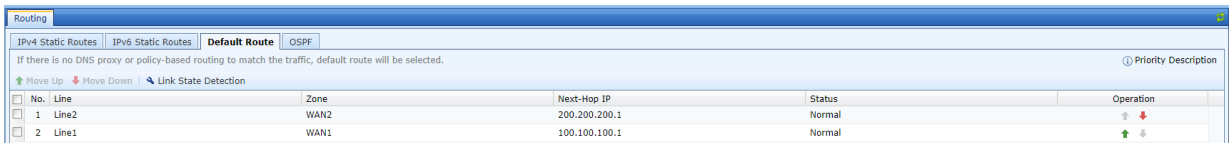
When a line goes down, the DNS proxy policy fails:

The link load is not enabled, and the default route is directly taken.

The link load is enabled, and the load policy is adopted; if the load is abnormal, the default route is used.

New default routing page, support adjustment of default routing order

Default route escape mechanism, based on line failure detection (DNS and ping)



Chapter 6 Precautions

(1) Routing mode, link load routing, DNS proxy, default routing function, and visualization of load link status.

(2) Bridge mode, link load routing, DNS proxy, visualization of load link status.

(3) When the SG is in the proxy mode, it cannot be used as a DNS proxy. SG starts the proxy. The DNS

request is initiated by the local proxy. The function of the DNS proxy cannot proxy the local packet.

(4) Under the SG opening proxy mode, it is not supported to select the line according to the DNS load for the carrier load. Operators routing based on DNS load actually needs to proxy the DNS. After the SG starts the proxy, DNS requests are initiated by the local proxy, and the proxy cannot be driven again.

(5) Application routing is not supported when SG is in proxy mode (TCP proxy is not supported, the effect is unreachable).

(6) The main mode will not synchronize the network related configuration. Link load and DSCP are network configurations. It will only take effect on a single node.

(7) Turn on global exclusion and pass-through. The link load function does not lose packets, and the function is still effective.

(8) Link load function does not support alarm

(9) The link load is not supported when the SG has enabled the display proxy or SSL decryption.

(10) In the application routing scenario, some applications have been identified and subdivided. Each segmented application is considered to be an application. It is recommended to check all of the first-type applications, otherwise it will affect the routing effect, such as WeChat and Facebook.

(11) Priority description of routing mode: direct route> static route> dynamic route> DNS proxy [redirect to specified line]> priority load policy> default load policy> default route. (No VPN configuration, no dedicated line backup scenario)

Direct route> Static route> Dynamic route> DNS proxy [Redirect to specified line]> Preferred load policy> Default load policy> Default route> System default route

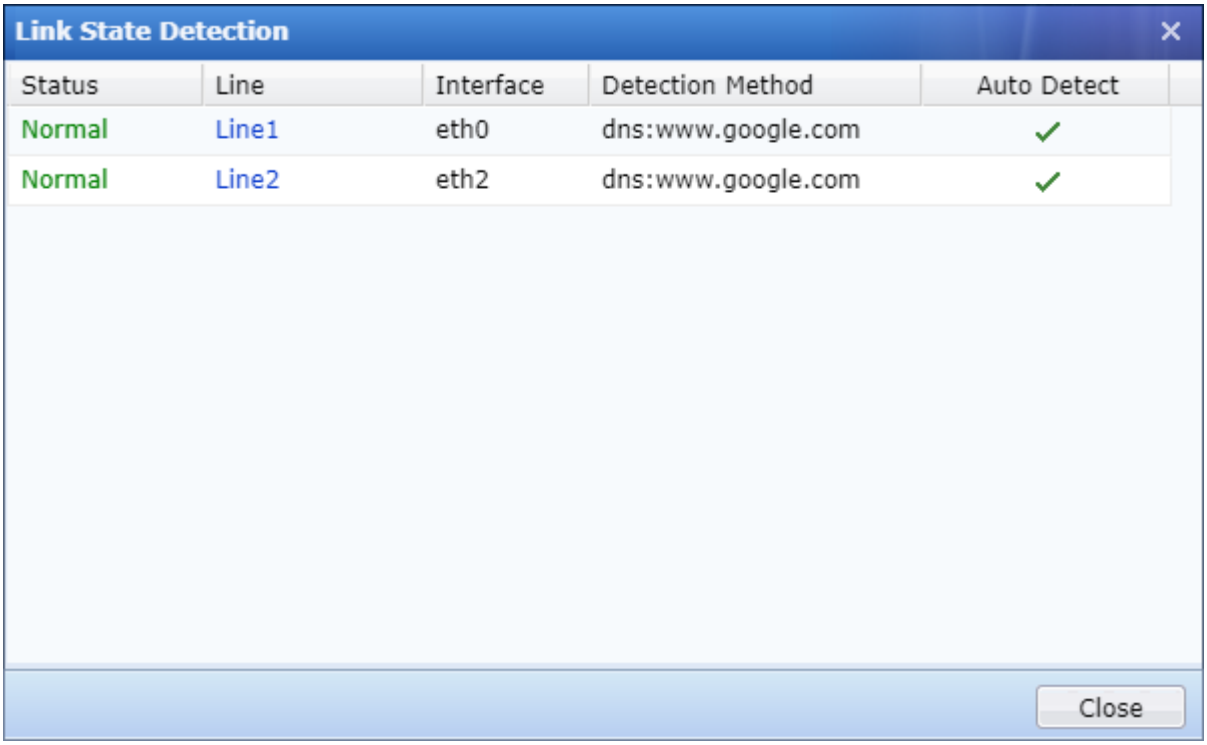
VPN routing> Direct routing> Static routing> Dynamic routing> DNS proxy [Redirect to specified line]> Preferred load policy> Default load policy> Default route> System default route

(12) Priority description of bridge mode: DNS proxy [Redirect to specified line]> Priority load policy> Default load policy.

(13) The DNS proxy policy conflicts with the link load policy only when the configuration is redirected to the specified line. When the two configurations conflict, the DNS proxy policy takes precedence, and the redirection line configured by the DNS proxy policy prevails.

(14) Intranet-AC (bridge)-proxy server-F5 scenario, does not support link load function

(15) Configure the link load. As long as there are multiple external network lines, you need to configure the "link failure detection" function. Otherwise, the link load policy does not take effect.



The default load policy cannot customize the user / application / validation time.