

How does Load-Balance Policy in Firewall rules work?

Load-Balance Policy in Firewall Policy is a new feature introduced since firmware version 3.3.5 (e.g, VigorPro 5300 series).

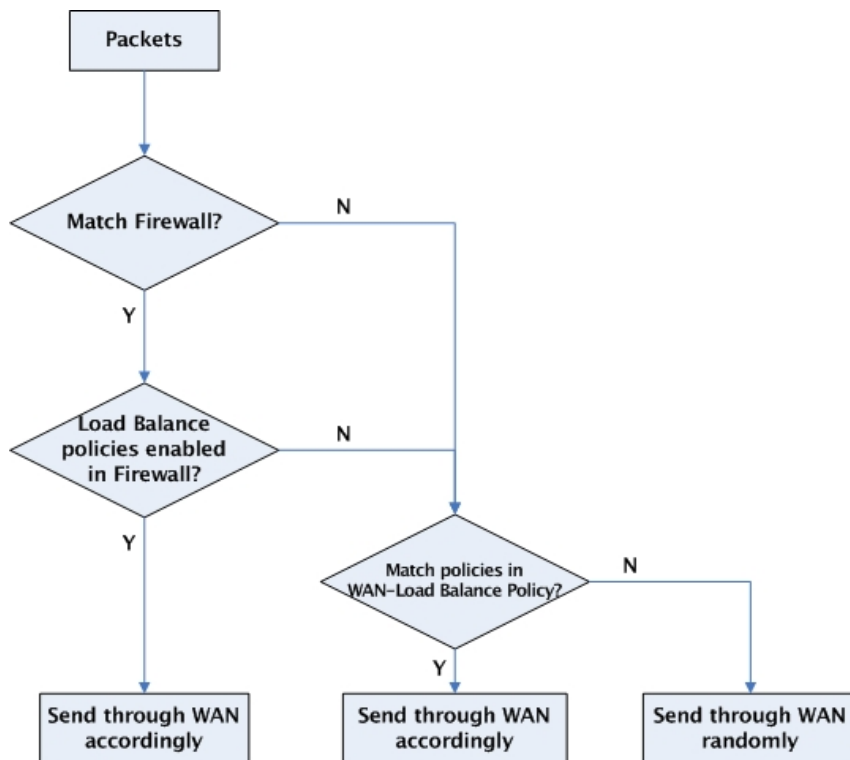
Why adding Load-balance Policy in Firewall Policy?

In old versions all traffic are first checked against Firewall rules. If the traffic is allowed to be passed to the Internet, Load-balance rules will be checked and used to determine which WAN to send the packets through. As you can see both Load-balance Policy and Firewall policy can use the Source IP, Destination IP and Destination Port to set a match condition. By combining Firewall Policy with Load-balance Policy, the traffic just needs to be checked against a rule once for firewall decision and Load-balance decision, making packet processing more efficient.

Load-Balance Policy in Firewall menu has more match conditions like Source Port and VLAN. IP Objects/Groups and Service Type Objects/Groups can also be selected here, which make the Load-Balance Policy more flexible.

How Load-balance Policy in Firewall Policy works?

The flow chart below explains how the Load Balance Policy feature works on Vigor 5300.



When a packet arrives at the router, the router will check the IP filter rules to see if it matches any rule (according to Direction, Source IP, Service Type and etc), and proceed the following checks.

Step 1

If the packet matches one of the IP filter rules, it will be sent through the specific WAN interface, according to the WAN interface selected in the **Load-Balance Policy** in this rule. According to the settings shown in the following picture, traffic from 192.168.30.11 ~ 192.168.30.50 will be sent through WAN1.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 3 Rule 4

Check to enable the Filter Rule

Comments:

Index(1-15) in Schedule Setup: , , ,

Direction: LAN -> WAN

Source IP: 192.168.30.11~192.168.30.50

Destination IP: Any

Service Type: Any

Fragments: Don't Care

VLAN: Don't Care

Application	Action/Profile	Syslog
Filter:	Pass Immediately <input type="button" value="v"/>	<input type="checkbox"/>
Branch to Other Filter Set:	None <input type="button" value="v"/>	
Sessions Control	0 / 10000	<input type="checkbox"/>
MAC Bind IP	Non-Strict <input type="button" value="v"/>	<input type="checkbox"/>
Quality of Service	None <input type="button" value="v"/>	<input type="checkbox"/>
Load-Balance policy	WAN1 <input type="button" value="v"/>	<input type="checkbox"/>
User Management	None <input type="button" value="v"/>	<input type="checkbox"/>
APP Enforcement:	None <input type="button" value="v"/>	<input type="checkbox"/>
URL Content Filter:	None <input type="button" value="v"/>	<input type="checkbox"/>
Web Content Filter:	None <input type="button" value="v"/>	<input type="checkbox"/>

If **Load-Balance policy** is set as **Auto-Select**, the router will proceed to check the policies set in the **WAN >> Load-Balance Policy** page.

Branch to Other Filter Set:	None <input type="button" value="v"/>	
Sessions Control	0 / 10000	<input type="checkbox"/>
MAC Bind IP	Non-Strict <input type="button" value="v"/>	<input type="checkbox"/>
Quality of Service	None <input type="button" value="v"/>	<input type="checkbox"/>
Load-Balance policy	Auto-Select <input type="button" value="v"/>	<input type="checkbox"/>
User Management	None <input type="button" value="v"/>	<input type="checkbox"/>
APP Enforcement:	None <input type="button" value="v"/>	<input type="checkbox"/>
URL Content Filter:	None <input type="button" value="v"/>	<input type="checkbox"/>

Step 2 setting

Following Step 1, if the packet does not match any of the IP filter rules but the default rule, it will be sent through the specific WAN according to the **Load-Balance Policy** in **Firewall >> General Setup >> Default Rule** page. According to the settings shown in the following picture, the packet that matches the Default Rule will be sent through WAN2.

Same as Step 1, if **Load-Balance policy** in this page is set as **Auto-Select**, the router will check the policies in **WAN >> Load-Balance Policy**.

Firewall >> General Setup

General Setup

General Setup | Default Rule

Actions for default rule:		
Application	Action/Profile	Syslog
Filter	Block	<input checked="" type="checkbox"/>
Sessions Control	0 / 8000	<input type="checkbox"/>
Quality of Service	None	<input type="checkbox"/>
Load-Balance policy	WAN2	<input type="checkbox"/>
User Management	None	<input type="checkbox"/>
APP Enforcement	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
Anti-Virus	1-Default	<input type="checkbox"/>
Anti-Intrusion	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/>
Anti-Spam	1-Default	<input type="checkbox"/>

Advance Setting

Note:

The Load-Balance policy in Firewall policy doesn't support the option for switching on/off **Auto failover to the other WAN** as in **WAN >> Load-Balance Policy**. If you want to bind the traffic to a specific WAN port and don't allow the traffic to pass through the other WAN interface even the specific WAN port is down. You must disable **Auto failover to the other WAN**. Since the Load-Balance policy in Firewall policy doesn't support such feature, when you configure the firewall policies, be careful and make sure the **Load-Balance policy** in Firewall policies is set with **Auto-Select**.

Index: 1

<input type="checkbox"/> Enable	
Protocol	any
Binding WAN Interface	WAN1
Src IP Start	
Src IP End	
Dest IP Start	
Dest IP End	
Dest Port Start	
Dest Port End	

Auto failover to the other WAN