

How to Block Traffic from WAN on Vigor2130/Vigor2750

For Vigor2130 and Vigor2750 adopt firewall settings built in the chip, the rules of firewall for both two routers are different with other models. Firewall rules are done in the specified interface. However, the TCP protocol is still based on the connection. Therefore, specifying the interface to be blocked would influence other connections. It is necessary to separate TCP connection with other network connections.

TCP connection is carried out with Three-Way Handshake protocol. First of all, SYN packet will be sent out to express one side wants to build connection with the peer. If the port of the peer has been opened, the peer will answer and return SYN ACK packet back. Finally, the initiator will send out the ACK packet to indicate the connection between both ends is successful. During the process, the initial connection will use SYN (1) and ACK (0) to represent the successful initial connection.

If, at present, you want to block the connection via WAN to Vigor2130 or Vigor2750 but allow the connection via SSH protocol to Vigor2130 or Vigor2750 without affecting the network accessing in LAN, please configure as the following:

1. Configure to allow the connection with SSH protocol

- Choose **WAN** as the **Ingress Port**.
- Choose **TCP** as the **IP Protocol Filter** and choose **Host** as the **Dest IP**. Then fill the IP address for the host.
- Choose **Allow** for **Action**.
- Choose **Specific** as **Dest. Port Filter** and fill in the port number, **22**, in the field of **Dest. Port No.**

Firewall >> Access Control List

ACE Configuration

Enable

Ingress Port	WAN
Frame Type	IPv4

Action	Allow
Rate Limiter	Disabled

IP Parameters

IP Protocol Filter	TCP
Source IP	Any
Dest IP	Host
Dest IP Address	212.112.130.242

TCP Parameters

Source Port Filter	Any
Dest. Port Filter	Specific
Dest. Port No.	22
TCP FIN	Any
TCP SYN	Any
TCP RST	Any
TCP PSH	Any
TCP ACK	Any
TCP URG	Any

2. Configure to block the connection from WAN port

- Choose **WAN** as the **Ingress Port**.
- Choose **TCP** as the **IP Protocol Filter**
- Choose **Deny** for **Action**.
- Set **TCP SYN** with 1 and **TCP ACK** with 0.

Firewall >> Access Control List

ACE Configuration

Enable

Ingress Port	WAN	Action	Deny
Frame Type	IPv4	Rate Limiter	Disabled

IP Parameters		TCP Parameters	
IP Protocol Filter	TCP	Source Port Filter	Any
Source IP	Any	Dest. Port Filter	Any
Dest IP	Any	TCP FIN	Any
		TCP SYN	1
		TCP RST	Any
		TCP PSH	Any
		TCP ACK	0
		TCP URG	Any

OK Cancel

TCP FIN	Used to release the connection to tell the user that there is no data transmitted from the peer side any more.
TCP SYN	Used to establish the connection. In the request of connection, set SYN with 1 and ACK with 0. If you want to receive the answer from the peer side, please set SYN with 1 and ACK with 1.
TCP RST	Used to retrieve the connection cause by error due to some reason. Also, it can be used to refuse illegal request and data transmission.
TCP PSH	If you choose 1, the requested data will be sent to the application program directly when the receiver gets it.
TCP ACK	1 means legal. 0 means the data does not contain the authentication message. The authentication number will be ignored.
TCP URG	Used to prevent from the TCP data stream interrupted by some reason.

3. In the page of Firewall>>Access Control List, the configuration result for above settings can be seen.

Firewall >> Access Control List

Access Control List Configuration

Auto-refresh Refresh Clear Delete All

Status	Ingress Port	Frame Type	Action	Rate Limiter	Counter	
✓	WAN	IPv4 / TCP / In SrcIP = Any DesIP = 212.112.130.242/32 SrcPort = Any DesPort = 22	Permit	Disabled	0	
✓	WAN	IPv4 / TCP SrcIP = Any DesIP = Any SrcPort = Any DesPort = Any	Deny	Disabled	0	

Note: This hardware-based feature is available for wired connection only.

If you want to block the connection via UDP protocol, you cannot configure with the same settings on TCP protocol for such protocol is connectionless.

In addition to specify WAN port, we also can use Rate Limiter to block the connection for such protocol. Please configure as the following:

- Choose **UDP** as **IP Protocol Filter**.
 - Choose **Allow** for **Action**.
- * It is necessary to put the packet inside the specified interface due to the request of Rate Limiter activated.
- Set the value for **Rate Limiter** and specify the number of the packets allowed per second.

Enable

Ingress Port: WAN
Frame Type: IPv4

Action: Allow
Rate Limiter: 1

IP Parameters

IP Protocol Filter: UDP
Source IP: Any
Dest IP: Any

UDP Parameters

Source Port Filter: Any
Dest. Port Filter: Any