Packet Filter

Disable Packet Filters

Packet Filter Rules

Order		Enabled	Delete
1	**Drop** packets that match:		Delete
	IP Version of "BothIPv4AndIPv6"		
	Ingress Interface of "LAN"		Delete
	Egress Interface of "WAN"		Delete
	Destination IP Address of "1.2.3.4"		Delete
	Protocol of "TCP"		Delete
	Destination Port of "80"		Delete
	Add Match...		
2	**Drop** packets that match:		Delete
	IP Version of "BothIPv4AndIPv6"		
	Ingress Interface of "LAN"		Delete
	Egress Interface of "WAN"		Delete
	Destination IP Address of "1:2:3::4"		Delete
	Protocol of "TCP"		Delete
	Destination Port of "80"		Delete
	Add Match...		
3	**Drop** packets that match:		Delete
	IP Version of "IPv4"		
	Ingress Interface of "LAN"		Delete
	Egress Interface of "WAN"		Delete
	Protocol of "TCP"		Delete
	Destination Port of "21"		Delete
	Add Match...		
4	**Drop** packets that match:		Delete
	IP Version of "IPv6"		
	Ingress Interface of "WAN"		Delete
	Egress Interface of "LAN"		Delete
	Protocol of "TCP"		Delete
	Destination Port of "80"		Delete
	Add Match...		
5	**Drop** packets that match:		Delete
	IP Version of "IPv6"		

Help

Packet filters can drastically effect the operation of the device. Do not make changes to this page unless instructed by your service provider.

You can create packet filter rules to pass or drop packets. Packets will be dropped or passed (forwarded) if they match the rest of the criteria in this rule. If there is no specified match item for the rule, that aspect of the rule will match for all packets.

Once a rule is enabled, you must disable it before making any changes to it. Changes to a rule include adding, editing, or deleting matches.

The 'Disable Packet Filters' button disables all of the rules on this page. The rules will continue to be displayed and can be re-enabled by pushing the button again.

Add a 'Drop' Rule: Create a rule by clicking the button. A Drop rule will discard all traffic that matches.

Add a 'Pass' Rule: Create a rule by clicking the button. A Pass rule will pass all traffic that matches.

Order: Rules are processed in the order shown. You can move rules up or down one at a time by clicking the buttons next to the rule order number.

Add Match: To create a match, hit the Add Match button associated with one of your Rules. Then select the Match Type and Match Value in the Match entry section and hit Enter Match.

IP Version: This match designates which versions of IP will be matched. If 'IPv4' is specified, the rest of the matches must not contain any IPv6 protocols or addresses. If 'IPv6' is specified, the rest of the matches must not contain any IPv4 protocols or addresses. If 'IPv4 or IPv6' is specified, the other matches determine if the rule is IPv4 specific, IPv6 specific, or matches both types of packets.

Source IP Address: This field accepts a single IPv4/IPv6 address, a range of IPv4 addresses in the form "start address - end address", or an IPv4/IPv6 range in the form ipaddress/mask, where mask should be of variable length subnet mask format ranging from 0 to 32/64. If the packet source ip address falls in this range and the rest of the criteria matches, the rule is processed. This field is the IP address of a device on the Internet.

Destination IP Address: Specify this field as described above for the Source IP Address Range. This field is the IP address of a LAN device.

Protocol: Packets will be inspected for the specified protocol. If the protocol matches, this rule is processed.

Protocol by number: To specify a protocol by number, select "by Number" in the Protocol pulldown and enter the number in this field.

Protocol by name: To specify a protocol by name, select "by Name" in the Protocol pulldown and enter the name in this field. Click here for a list of valid iana assignments that you can copy/paste into this field.

Source Port: Packets will be inspected for the source port if the protocol is TCP or UDP. If the source port is within the port range, this rule is processed.

Destination Port: Packets will be inspected for the destination port if the protocol is TCP or UDP. If the destination port is within the port range, this rule is processed.

Source MAC Address: For a given rule, you can choose to create a match by either Source MAC Address or Source IP Address. You can specify a matching Source MAC address for LAN-side

	Ingress Interface of "WAN"	Delete
	Egress Interface of "LAN"	Delete
	Add Match...	

Add a 'Drop' Rule Add a 'Pass' Rule

devices only; the destination MAC address of packets destined for the Internet will not contain the recipient's MAC address.

Destination MAC Address: For a given rule, you can choose to create a match by either Destination MAC Address or Destination IP Address. You can specify a matching Destination MAC address for LAN-side devices only; the source MAC address of packets arriving from the Internet will not contain the originator's MAC address.

Ingress Interface: The rule is applied only to packets that are received on this interface.

Egress Interface: The rule is applied only to packets that are transmitted on this interface.

TCP Flags: The selected TCP Flags are examined and set on if the rule matches.

ICMP Type: If the protocol is icmp, this field adds another criteria which must match in order for the rule to be processed.