IP Firewall

Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

To the certification exam

IP Firewall is a mechanism of filtering packets crossing an IP network node, according to different criteria. System administrator may define a set of incoming filters and a set of outgoing filters. The incoming filters determine which packets may be accepted by the node. The outgoing filters determine which packets may be forwarded by the node as a result of routing. Each filter describes a class of packets and defines how these packets should be processed (reject and log, accept, accept and log).

Packets can be filtered based on the following criteria:

- Protocol (IP, TCP, UDP, ICMP, ARP)
- Source address and/or destination address (and port numbers for TCP and UDP)
- The inbound network interface
- Whether the packet is a TCP/IP connection request (a packet attempting to initiate a TCP/IP session) or not
- Whether the packet is a head, tail or intermediate IP fragment
- Whether the packet has certain IP options defined or not
- The MAC address of the destination station or of the source station.

The figure below illustrates how packets are processed by the filtering mechanism of the router:

There are two classes (sets) of filters - prohibiting (reject) and permitting (accept).

Furthermore, a filter may be applied to all inbound packets or only to packets arriving via a specific interface. Each received packet is checked against all filters in the order they are put in the set.

The first filter that matches the received packet determines how the packet are treated. If the filter is an accept filter, the packet is accepted, otherwise it is rejected. If the packet matches no filter in the set, or if the set is empty, the packet is accepted.

NOTE

The rejected packet are discarded without notification to the sender.

Packet filtering rules

Every packet entering a router passes through a set of input filters (blocking filters). The packets accepted by the input filter set are further processed by the IP layer of the router kernel. If the IP layer determines that the packet should go further and not landing here, it hands the packet to the set of outgoing filters (forwarding filters).

Information on packets rejected by any filter is displayed on the operator's terminal and the packets themselves are discarded without any notice to their sender.

A packet, "advancing through" a set of filters, is checked by every filter in the set, from the first one till the end of the set, or until the first matching filter. The algorithm is the following:

1. If the filter set is empty, the packet is accepted
2. Otherwise, the first matching filter decides what to do with the packet. If it is an accept filter, the packet is accepted. If it's a reject filter, the packet is rejected (discarded)
3. If no filter has been found that matches the packet, it is accepted.

IP Firewall parameters

In the "IP Firewall parameters" section, you can view the IP Firewall rules that are already created; you can create a new rule for the current switch group by clicking the "Add Rule" button, or you can permanently remove the rule from the configuration by clicking the "Remove Rule" button.

IP firewall rule parameter	Description

Action	• Set the action for the rule: permit/deny/pass:
	  • "*Permit*" - the packet is processed by the system (ignoring other firewall rules)
	  • "*Deny*" - the packet is dropped
	  • "*Pass*" - the packet is passed to the next rule in the list and logged in the system log (only if the log check box is marked)

Channel	• Allocate a logical channel if there are logical channels prior created in "Traffic Shaping" section (it is active only if the action "permit" is selected) • If you allocate a number for a logical channel that was not prior created in "Traffic Shaping" section, it has no effect in the rule configuration • For the indications how to create a logical channel, please refer to "Traffic Shaping" section below

Priority	• Set the priority for the packets going through the new rule of the filter:
	  • "*Up to*" - used to increase the packet priority to the specified value only if the processed packet has a lower priority
	  • "*Set*" - used to assign a new priority regardless of the value already assigned to the packet

Log	• Enable/disable filter actions logging in the system log

Direction	• Set the input/output direction for applying the new rule:
	  • "*Input*" - the rule is used to process inbound traffic
	  • "*Output*" - the rule is used to process outbound traffic and for post-routing packet filtering

Interface	• Set the interface for applying the new rule • All the available interfaces are displayed in the dropdown list (physical and logical) • If "*any*" option is used, the rule is applied to all available interfaces
Group	• Set the Switch Group number for the applying of the new rule • The Switch Group must be prior created
Rule	• Set the packet capture filter for IP firewall • It is the same syntax called "PCAP expression", as in the "Switching" section • Refer to the filter expression syntax description above • By clicking the "Validate" button, you can check the syntax in the expression in the "Rule" fie

Table - IP Firewall

The "Up/Down" arrows allow you to organize rules list. The rules are processed one by one in a top-down order.