

Rules





Rules section consists of three subsections: **Forwarding**, **Permitted addresses**, and **Forbidden addresses**.

Forwarding

Allows you to configure mail forwarding on the server using mail aliases. Aliases, unlike mailboxes, do not require logins and passwords, they are assigned to a mailbox and serve as its copy with a different name, or, if an alias is assigned to several mailboxes, it can serve as a mailing group. Mail incoming to the alias is automatically forwarded to all real mailboxes associated with this alias. If forwarding is done to a mailbox in another domain on the Internet, then the mailbox registered in the **Recipient** column must actually exist.

You can read more about setting up mail aliases on SafeUTM in the article [Mail forwarding](#).

Rules











Forwarding

Permitted addresses

Forbidden addresses

+ Add

Rows per page: 10 1-4 of 4

Recipient	Forwarding addresses ↑	Operations
ceo	ceo@gmail.com	 
sales	j.smith r.johnson	 
r.johnson	j.smith r.johnson	 
j.smith	r.johnson	 

Permitted addresses

Allows you to specify mail domains, IP addresses of mail servers and mailboxes, and emails from which will not be checked for spam.



If the mailbox is simultaneously specified in **Forbidden addresses** and **Permitted addresses**, then the **Permitted address** has the highest priority.

Forwarding Permitted addresses Forbidden addresses

The added addresses will be excluded from spam checks. Permitted addresses are more important than prohibited ones.

+ Add

Rows per page: 10 ▾ 1-3 of 3 < > 🔍

Senders	Comment	Operations
10.128.0.3		 
192.168.130.3		 
example.com		 

When you add overlapping sources to both lists, there is no correlation between the sources. Priority will be given first to IP addresses, then to mailboxes, and then to domains. That is, if the IP address of the mail server is forbidden and the domain it serves is permitted, then emails from it will be blocked (blocking by IP address is prioritized). Reverse example: An IP address is permitted, but a domain is forbidden. Emails are blocked, just at a later stage, when checking the mail domain.

Another example: the domain is in **Permitted addresses**, a mailbox from this domain is in **Forbidden addresses**, then emails from the mailbox will be blocked.

Reverse example: emails from a mailbox listed in **Permitted addresses** will be allowed even if the domain that the mailbox belongs to is listed in **Forbidden addresses**.

The scheme of letter processing in the mail server is presented in the article [Mail traffic filtering scheme](#). Please note that Permitted and Forbidden addresses are triggered after several preliminary filtering steps.

Forbidden addresses

Allows you to specify mail domains and mailboxes from which emails will not be accepted by the server.

Rules



Forwarding Permitted addresses **Forbidden addresses**

Reception of mail from the added addresses will be banned. Permitted addresses are more priority than prohibited ones.

+ Add

Rows per page: 10 1-2 of 2 < > 🔍

Senders	Comment	Operations
192.168.130.3		 
j.smith@test.com		 

Revision #5
Created 27 August 2022 19:09:19 by Val Redman
Updated 13 October 2022 16:03:59 by Val Redman