

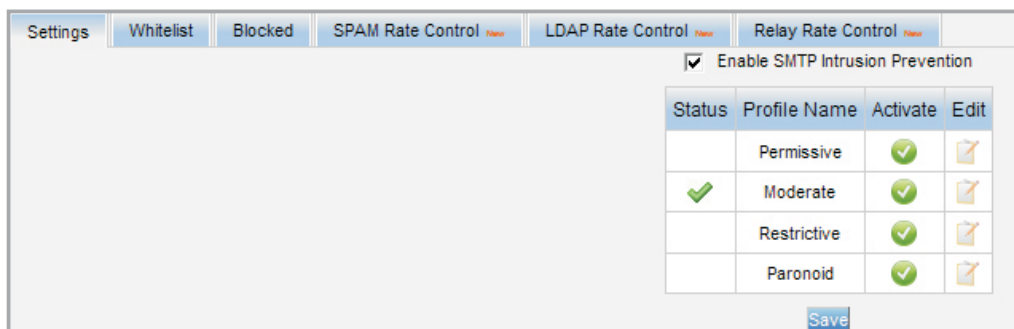
Overview

As a highly engineered product Surgate offers greater control on messaging traffic more than its competitors with unique SMTP IPS / FW module and provides ability to deal with attackers and abusive users. Since legacy firewalls are not aware of Layer-7, they are not able to help you to keep your messaging traffic secure. For that reason, Surgate is the best player for your messaging infrastructure.

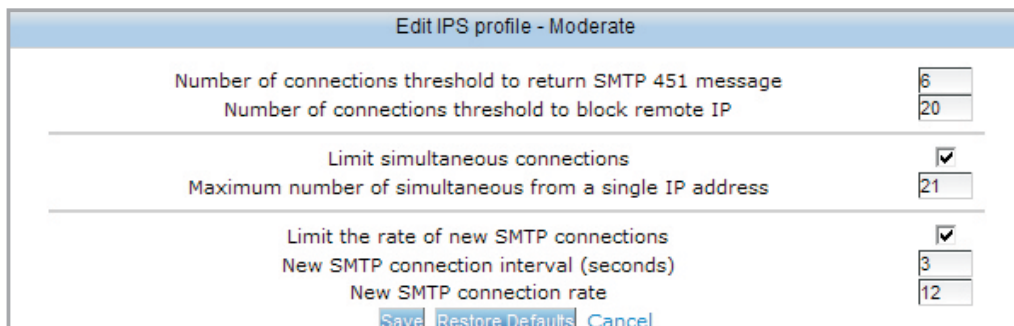
Pre-defined Ready-to-Use Security Profiles

Surgate provides ready-to-use security profiles to quickly set up the features offered by SMTP IPS/FW module. These profiles enable you to set security level of your messaging traffic with just a single click. In case of changing conditions, this option helps you to get convenience in consumption system resources .

Thanks to SMTP IPS/FW module, you can shape and control your network traffic.



Security profiles allow you to control messaging traffic and protect your system resources to be used by intruders. The options which you can limit using security profile are as follows:



For example the IPs want to make more connections than a specified number will be blocked. Since in practice, a real user is not able to send simultaneous email, the programs that automatically send email will be blocked.

Whether the email comes from the same IP or a different IP, you can specify a certain time between two requests. In the above example, 12 new connections are allowed within three seconds.

Your trusted users you received email often from will not be bothered by these limitations. Surgate offers special whitelists for each module individually. You are able to inform Surgate about your trusted IPs which you want to exempt from IPS/FW module limitations by using the whitelist tab. For instance, since Hotmail sends millions of emails, the number of connections from the same IP would be too many as the interval would be too short. You can add this kind of mass and trusted senders to the whitelist.

While traditional firewalls are not able to detect threats that come via email, Surgate detects the threats in Layer-7 and blocks in Layer-2.

SMTP/ FW

Surgate appliance includes an SMTP firewall running on layer2- layer7. While traditional firewalls cannot detect threats that come via email, Surgate is able to detect the attacks in Layer-7 and block in Layer-2.



Access Rate Controls

SMTP IPS / FW module offers great flexibility serving its controls separately for each subsystem in Surgate.

