Proxmox Mail Gateway Administration Guide

Release 5.0

January 12, 2018

Proxmox Server Solutions Gmbh

www.proxmox.com

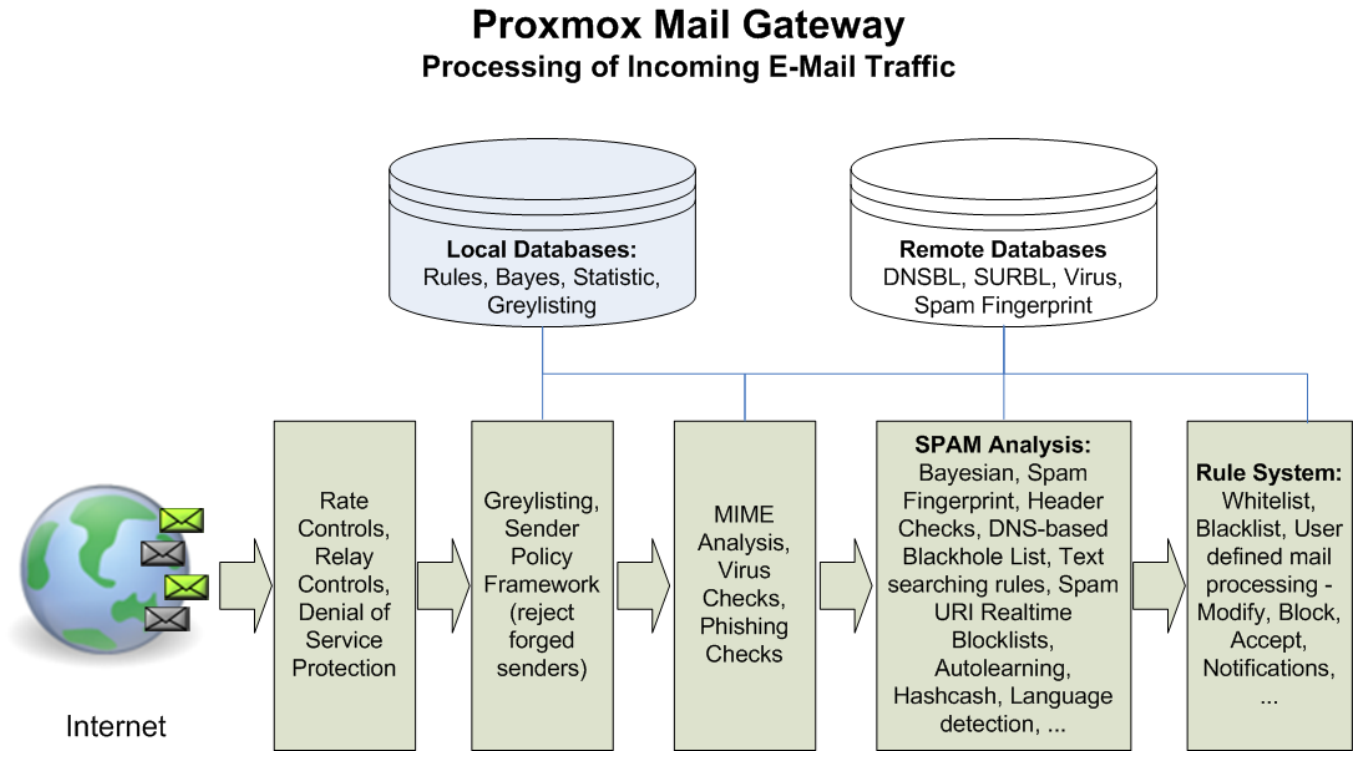
Contents

Chapter 1

Introduction

1.1 What is Proxmox Mail Gateway?

E-mail security begins at the gateway by controlling all incoming and outgoing e-mail messages. Proxmox Mail Gateway addresses the full spectrum of unwanted e-mail traffic, focusing spam and virus detection. Proxmox Mail Gateway provides a powerful and affordable server solution to eliminate spam, viruses and blocking undesirable content from your e-mail system. All products are self-installing and can be used without deep knowledge of Linux.



1.2 Features

1.2.1 Spam detection

Proxmox Mail Gateway uses a wide variety of local and network tests to identify spam mail. Here is a short list of used filtering methods:

Receiver Verification
Many of the junk messages reaching your network are emails to non-existent users. Proxmox Mail Gateway detects these emails on SMTP level, which means before they are transferred to your networks. This reduces the traffic to be analyzed for spam and viruses up to 90% and reduces the working load on your mail servers and scanners.

Sender policy framework (SPF)
Sender Policy Framework (SPF) is an open standard for validating emails and to prevent sender IP address forgery. SPF allows the administrator of an Internet domain to specify which computers are authorized to send emails with a given domain by creating a specific SPF record in the Domain Name System (DNS).

DNS-based Blackhole List
A DNS-based Blackhole List (DNSBL) is a means by which an Internet site may publish a list of IP addresses, in a format which can be easily queried by computer programs on the internet. The technology is built on top of the Domain Name System. DNSBLs are used to publish lists of addresses linked to spamming.

SMTP Whitelist
Exclude senders from SMTP blocking. To prevent all SMTP checks (Greylisting, Receiver Verification, SPF and RBL) and accept all e-mails for the analysis in the filter rule system, you can add the following to this list: Domains (Sender/Receiver), Mail address (Sender/Receiver), Regular Expression (Sender/Receiver), IP address (Sender), IP network (Sender)

Bayesian Filter - Automatically trained statistical filters
Some particular words have a higher probability of occurring in spam emails rather than in legitimate emails. By being trained to recognize those words, the Bayesian checks every email and adjusts the probabilities of it being a spam word or not in its database. This is done automatically.

Black- and Whitelists
Black- and Whitelists are an access control mechanism to accept, block, or quarantine emails to recipients. This allows you to tune the rule-system by applying different objects like domains, email address, regular expression, IP Network, LDAP Group, and others.

Autolearning algorithm
Proxmox Mail Gateway gathers statistical information about spam emails. This information is used by an autolearning algorithm, so the system becomes smarter over time.

Spam Uri Realtime BlockList (SURBL)
SURBLs are used to detect spam based on message body URIs (usually web sites). This makes them

different from most other Real-time Blocklists, because SURBLs are not used to block spam senders. SURBLs allow you to block messages that have spam hosts which are mentioned in message bodies.

Greylisting
Greylisting an email from a sender your system does not recognize, means, that it will be temporarily rejected. Since temporary failures are built into the RFC specifications for mail delivery, a legitimate server will try to resend the email later on. This is an effective method because spammers do not queue and reattempt mail delivery as is normal for a regular Mail Transport Agent.

Greylisting can reduce e-mail traffic up to 50%. A greylisted email never reaches your mail server and thus your mail server will not send useless "Non Delivery Reports" to spammers.

SMTP Protocol Tests
Postfix is able to do some sophisticated SMTP protocol tests (see `man postscreen`). Most spam is sent out by zombies (malware on compromised end-user computers), and those zombies often try to maximize the amount of mails delivered. In order to do that, many of them violates the SMTP protocol specification and can thus be detected by these tests.

1.2.2 Virus detection

Proxmox Mail Gateway integrates ClamAV®, which is an open-source (GPL) antivirus engine designed for detecting Trojans, viruses, malware and other malicious threats.

It provides a high performance mutli-threaded scanning daemon, command line utilities for on demand file scanning, and an intelligent tool for automatic signature updates.

1.2.3 Object-Oriented Rule System

The object-oriented rule system enables custom rules for your domains. It's an easy but very powerful way to define filter rules by user, domains, time frame, content type and resulting action. Proxmox Mail Gateway offers a lot of powerful objects to configure your own custom system.

WHO - objects
Who is the sender or receiver of the e-mail?

WHAT - objects
What is in the e-mail?

WHEN - objects
When is the e-mail received by Proxmox Mail Gateway?

ACTIONS - objects
Defines the final actions.

Every rule has five categories FROM, TO, WHEN, WHAT and ACTION. Every of these categories can contain several objects and a direction (in, out or both).

Options range from simple spam and virus filter setups to sophisticated, highly customized configurations blocking certain types of e-mails and generating notifications.

1.2.4 Spam Quarantine

Identified Spam mails can be stored to the user accessible Spam quarantine. Thus users can view and manage there Spam mails by themselves.

1.2.5 Tracking and Logging

The innovative Proxmox Message Tracking Center tracks and summarizes all available logs. With the web-based and user friendly management interface, the IT admins can easily overview and control all functions from a single screen.

The Message Tracking Center is very fast and powerful, tested on Proxmox Mail Gateway sites processing over a million emails per day. All different log files from the last 7 days can be queried and the results are summarized by an intelligent algorithm.

- Arrival of the email
- Proxmox filtering processing with results
- Internal queue to your email server
- Status of final delivery

1.2.6 High Availability with Proxmox HA Cluster

To provide a 100% secure email system for your business, we developed Proxmox High Availability (HA) Cluster. The Proxmox HA Cluster uses a unique application level clustering scheme, which provides extremely good performance. Fast set-up within minutes and a simple, intuitive management keep resource needs low. After temporary failures, nodes automatically reintegrate without any operator interaction.

1.2.7 LDAP integration

It is possible to query user and group data from LDAP servers. This may be used to build special filter rules, or just to provide authentication services for the Spam quarantine GUI.

1.2.8 Fetchmail integration

Proxmox Mail Gateway allows you to fetch mail from other IMAP or POP3 servers.

1.2.9 Flexible User Management

The administration interface uses a role based access control scheme, using the following roles:

Superuser
: This role is allowed to do everything (reserved for user *root*).

Administrator
Full access to mail filter setup, but not allowed to change network setup.

Quarantine Manager
Is able to view and manage the Spam Quarantine.

Auditor
Has read-only access to the whole configuration, can access logs and view statistics.

1.3 Your benefit with Proxmox Mail Gateway

- Open source software
- No vendor lock-in
- Linux kernel
- Fast installation and easy-to-use
- Web-based management interface
- REST API
- Huge active community
- Low administration costs and simple deployment

1.4 Getting Help

1.4.1 Community Support Forum

Proxmox Mail Gateway itself is fully open source, so we always encourage our users to discuss and share their knowledge using the Proxmox Community Forum. The forum is fully moderated by the Proxmox support team, and has a quite large user base around the whole world. Needless to say that such a large forum is a great place to get information.

1.4.2 Commercial Support

Proxmox Server Solutions Gmbh also offers commercial Proxmox Mail Gateway Subscription Service Plans. System Administrators with a standard subscription plan can access a dedicated support portal with guaranteed reponse time, where Proxmox Mail Gateway developers help them should an issue appear. Please contact the Proxmox sales team for more information or volume discounts.

1.4.3 Bug Tracker

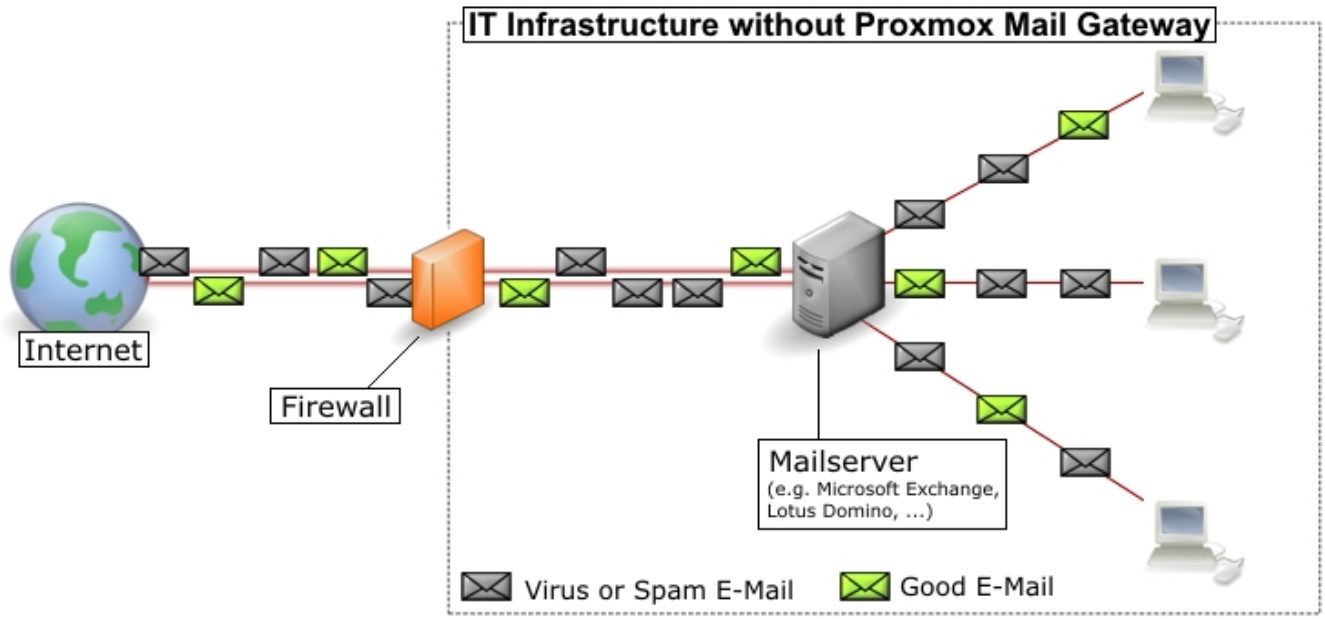
We also run a public a public bug tracker at https://bugzilla.proxmox.com. If you ever detect a bug, you can file an bug entry there. This makes it easy to track the bug status, and you will get notified as soon as the bug is fixed.

Chapter 2

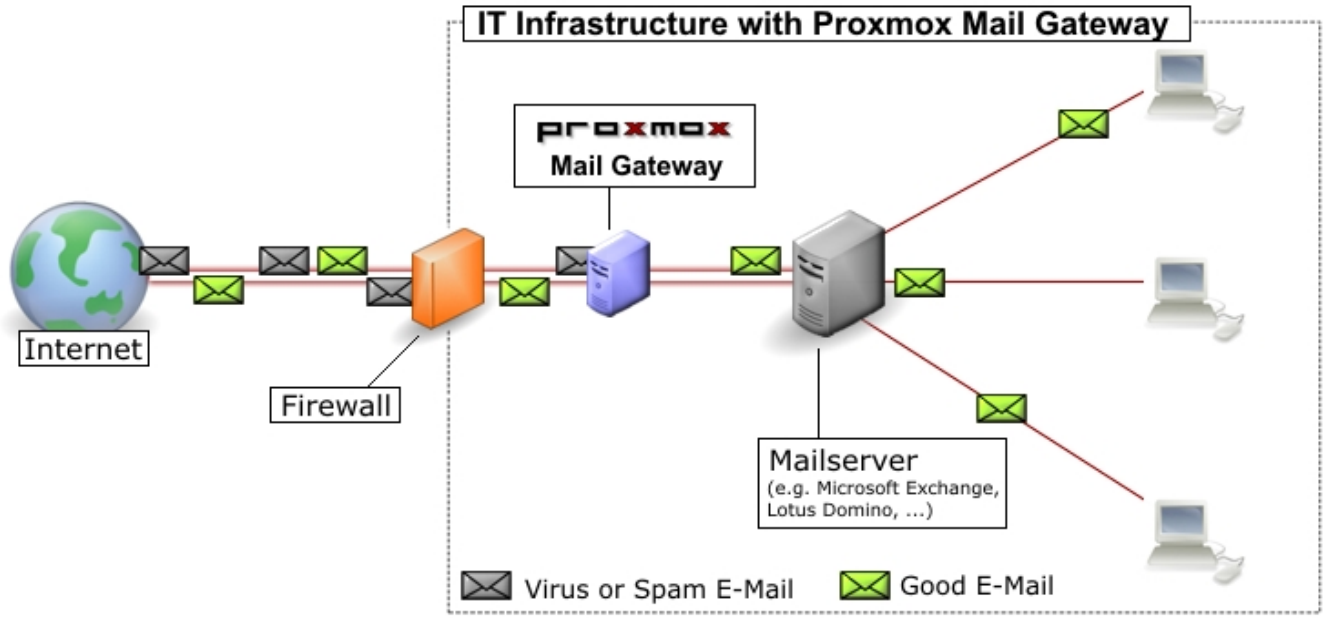
Planning for Deployment

2.1 Easy integration into existing e-mail server architecture

In this sample configuration, your e-mail traffic (SMTP) arrives on the firewall and will be directly forwarded to your e-mail server.



By using the Proxmox Mail Gateway, all your e-mail traffic is forwarded to the Proxmox Mail Gateway, which filters the whole e-mail traffic and removes unwanted e-mails. You can manage incoming and outgoing mail traffic.



2.2 Filtering outgoing e-mails

Many e-mail filter solutions do not scan outgoing mails. Opposed to that Proxmox Mail Gateway is designed to scan both incoming and outgoing e-mails. This has two major advantages:

1. Proxmox Mail Gateway is able to detect viruses sent from an internal host. In many countries you are liable for not sending viruses to other people. Proxmox Mail Gateway outgoing e-mail scanning feature is an additional protection to avoid that.

2. Proxmox Mail Gateway can gather statistics about outgoing e-mails too. Statistics about incoming e-mails looks nice, but they are quite useless. Consider two users, user-1 receives 10 e-mails from news portals and wrote 1 e-mail to a person you never heard from. While user-2 receives 5 e-mails from a customer and sent 5 e-mails back. Which user do you consider more active? I am sure its user-2, because he communicates with your customers. Proxmox Mail Gateway advanced address statistics can show you this important information. Solution which does not scan outgoing e-mail cannot do that.

To enable outgoing e-mail filtering you just need to send all outgoing "smarthost" on your e-mail server.

2.3 Firewall settings

In order to pass e-mail traffic to the Proxmox Mail Gateway you need to allow traffic on the SMTP the port. Our servers use the Network Time Protocol (NTP) for time synchronization, RAZOR, DNS, SSH, HTTP and port 8006 for the web based management interface.

Service	Port	Protocol	From	To
SMTP	25	TCP	Proxmox	Internet
SMTP	25	TCP	Internet	Proxmox
SMTP	26	TCP	Mailserver	Proxmox

Service	Port	Protocol	From	To
NTP	123	TCP/UDP	Proxmox	Internet
RAZOR	2703	TCP	Proxmox	Internet
DNS	53	TCP/UDP	Proxmox	DNS Server
HTTP	80	TCP	Proxmox	Internet
GUI/API	8006	TCP	Intranet	Proxmox

Caution
It is advisable to restrict access to the GUI/API port as far as possible.

The outgoing HTTP connection is mainly used by virus pattern updates, and can be configured to use a proxy instead of a direct internet connection.

You can use the *nmap* utility to test your firewall settings (see section port scans Section 9.9).

2.4 System Requirements

Proxmox Mail Gateway needs dedicated server hardware but can also run inside a virtual machine on any of the following plattforms:

- Proxmox VE (KVM)
- VMWare vSphere™ (open-vm tools are integrated in the ISO)
- Hyper-V™ (Hyper-V Linux integration tools are integrated in the ISO)
- KVM (virtio drivers are integrated, great performance)
- Virtual box™
- Citrix XenServer™

Please see http://www.proxmox.com for details.

In order to get a benchmark from your hardware, just run *pmgperf* after installation.

2.4.1 Minimum System Requirements

- CPU: 64bit (Intel EMT64 or AMD64)
- 2 GB RAM
- bootable CD-ROM-drive or USB boot support
- 1024x768 capable VGA/Monitor for Installer
- Hard disk 8 GB - ATA/SATA/SCSI/NVME
- Ethernet Network interface card

2.4.2 Recommended System Requirements

- Multicore CPU: 64bit (Intel EMT64 or AMD64)
- 4 GB RAM
- bootable CD-ROM-drive or USB boot support
- 1024x768 capable VGA/Monitor for Installer
- 1 GBps Ethernet Network interface card
- Hardware RAID1 or RAID10, Raid Controllers need write cache with batteries backup module for best performance
- Enterprise class SSD with power loss protection (e.g. Intel SSD DC 35xx/36xx/37xx)

Chapter 3

Installation

Proxmox Mail Gateway is based on Debian and comes with an installation CD-ROM which includes a complete Debian ("stretch" for version 5.x) system as well as all necessary Proxmox Mail Gateway packages.

The installer just asks you a few questions, then partitions the local disk(s), installs all required packages, and configures the system including a basic network setup. You can get a fully functional system within a few minutes. This is the preferred and recommended installation method.

Alternatively, Proxmox Mail Gateway can be installed on top of an existing Debian system. This option is only recommended for advanced users since it requires more detailed knowledge about Proxmox Mail Gateway and Debian.

3.1 Using the Proxmox Mail Gateway Installation CD-ROM

You can download the ISO from http://www.proxmox.com. It includes the following:

- Complete operating system (Debian Linux, 64-bit)
- The Proxmox Mail Gateway installer, which partitions the hard drive(s) with ext4, ext3, xfs or ZFS and installs the operating system.
- Linux kernel
- Postfix MTA, ClamAV, Spamassassin and the Proxmox Mail Gateway toolset
- Web based management interface for using the toolset

Please burn the downloaded ISO image to a CD or create a bootable USB stick Section 3.2.

Then insert the installation CD-ROM on the physical host where you want to install Proxmox Mail Gateway and boot from that drive. Immediately afterwards you can choose the following menu options:

Install Proxmox Mail Gateway
Start normal installation.

Install Proxmox Mail Gateway (Debug mode)
Start installation in debug mode. It opens a shell console at several installation steps, so that you can debug things if something goes wrong. Please press `CTRL-D` to exit those debug consoles and continue installation. This option is mostly for developers and not meant for general use.

Rescue Boot
This option allows you to boot an existing installation. It searches all attached hard disks and, if it finds an existing installation, boots directly into that disk using the existing Linux kernel. This can be useful if there are problems with the boot block (grub), or the BIOS is unable to read the boot block from the disk.

Test Memory
Runs `memtest86+`. This is useful to check if your memory is functional and error free.

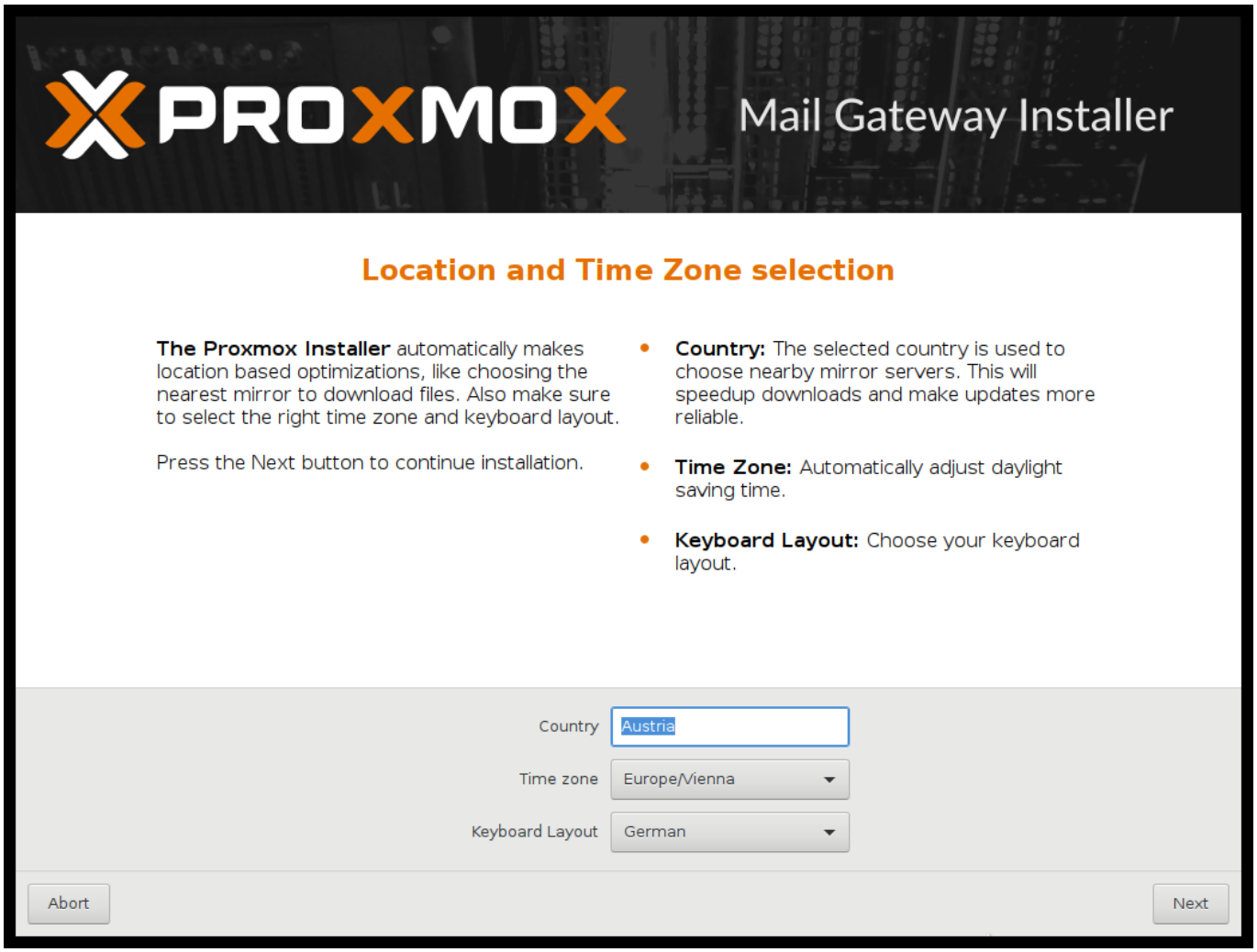
You normally select **Install Proxmox Mail Gateway** to start the installation.

First step ist to read our EULA (End User License Agreement). After that you get prompted to select the target hard disk(s).

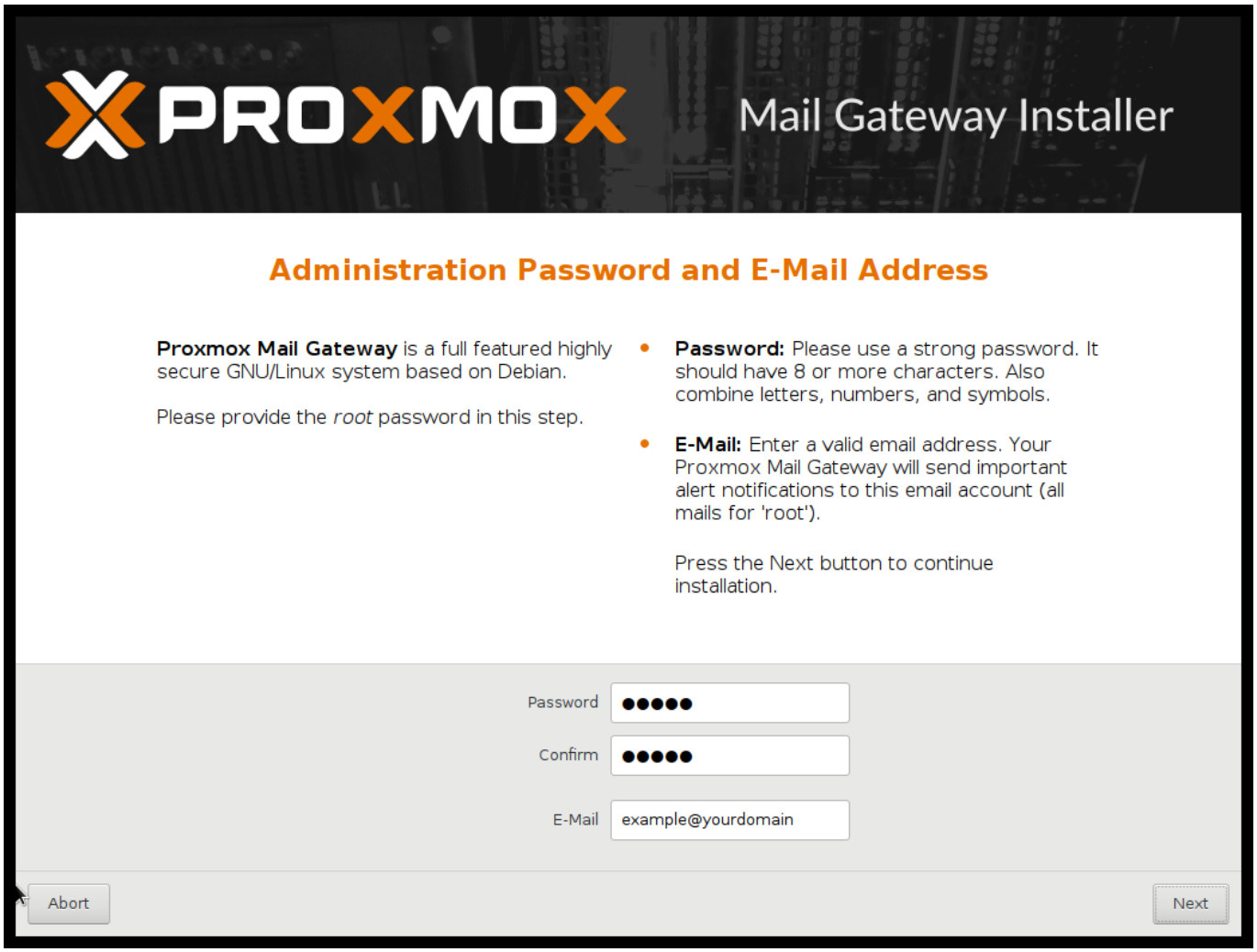
Note
By default, the complete server is used and all existing data is removed.

The `Options` button lets you select the target file system, which defaults to `ext4`. The installer uses LVM if you select `ext3`, `ext4` or `xfs` as file system, and offers additional option to restrict LVM space (see below)

If you have more than one disk, you can also use ZFS as file system. ZFS supports several software RAID levels, so this is specially useful if you do not have a hardware RAID controller. The `Options` button lets you select the ZFS RAID level, and you can choose disks there.



The next page just ask for basic configuration options like your location, the time zone and keyboard layout. The location is used to select a download server near you to speedup updates. The installer is usually able to auto detect those setting, so you only need to change them in rare situations when auto detection fails, or when you want to use some special keyboard layout not commonly used in your country.



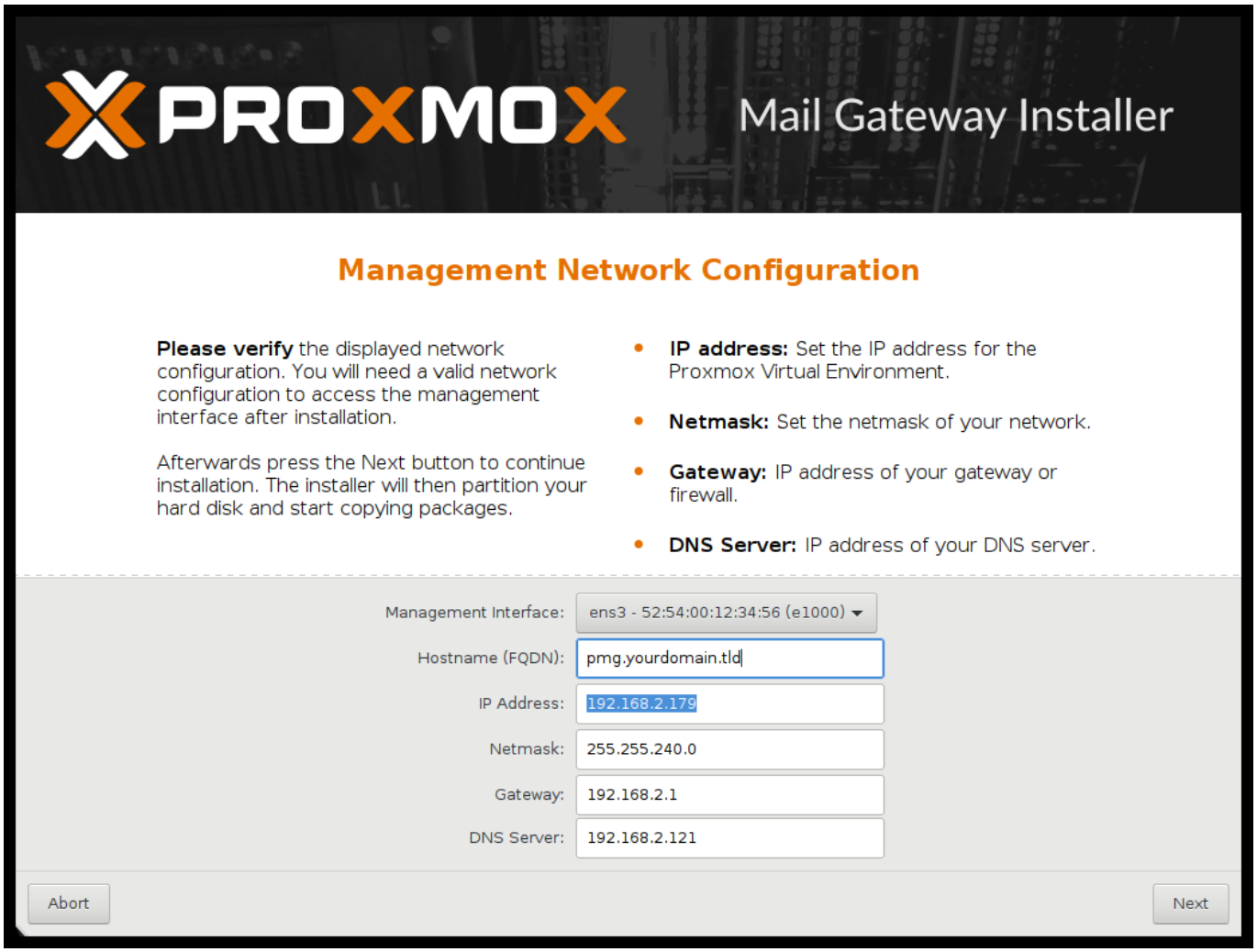
You then need to specify an email address and the superuser (root) password. The password must have at least 5 characters, but we highly recommend to use stronger passwords - here are some guidelines:

- Use a minimum password length of 12 to 14 characters.
- Include lowercase and uppercase alphabetic characters, numbers and symbols.
- Avoid character repetition, keyboard patterns, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past) and biographical information (e.g., ID numbers, ancestors' names or dates).

It is sometimes necessary to send notification to the system administrator, for example:

- Information about available package updates.
- Error messages from periodic CRON jobs.

All those notification mails will be sent to the specified email address.

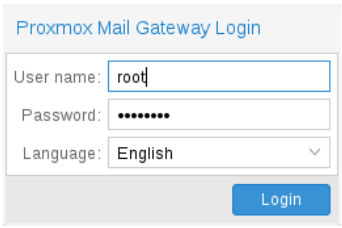


The last step is the network configuration. Please note that you can use either IPv4 or IPv6 here, but not both. If you want to configure a dual stack node, you can easily do that after installation.

If you press `Next` now, installation starts to format disks, and copies packages to the target.

Copying packages usually takes a few minutes. Please wait until that is finished, then reboot the server.

Further configuration is done via the Proxmox web interface. Just point your browser to the IP address given during installation (https://youripaddress:8006).



1. Login and upload subscription key.

   Note
   Default login is "root" and the root password is defined during the installation process.

2. Check the IP configuration and hostname.
3. Check and save the Time Zone.
4. Check your Firewall settings Section 2.3.

5. Configure Proxmox Mail Gateway to forward the incoming SMTP traffic to your Mail server (*Configuration/Mail Proxy/Default Relay*) - *Default Relay* is your e-mail server.

6. Configure your e-mail server to send all outgoing messages through your Proxmox Mail Gateway (*Smart Host*, port 26 by default).

For detailed deployment scenarios see chapter Planning for Deployment Chapter 2.

If the installation succeeds you have to route all your incoming and outgoing e-mail traffic to the Mail Gateway. For incoming traffic you have to configure your firewall and/or DNS settings. For outgoing traffic you need to change the existing e-mail server configuration.

3.1.1 Advanced LVM Configuration Options

The installer creates a Volume Group (VG) called `pmg`, and additional Logical Volumes (LVs) called `root` and `swap`. The size of those volumes can be controlled with:

`hdsize`
: Defines the total HD size to be used. This way you can save free space on the HD for further partitioning (i.e. for an additional PV and VG on the same hard disk that can be used for LVM storage).

`swapsize`
: Defines the size of the `swap` volume. The default is the size of the installed memory, minimum 4 GB and maximum 8 GB. The resulting value cannot be greater than `hdsize/8`.

`minfree`
: Defines the amount of free space left in LVM volume group `pmg`. With more than 128GB storage available the default is 16GB, else `hdsize/8` will be used.

> **Note**
> LVM requires free space in the VG for snapshot creation (not required for lvmthin snapshots).

3.1.2 ZFS Performance Tips

ZFS uses a lot of memory, so it is best to add additional RAM if you want to use ZFS. A good calculation is 4GB plus 1GB RAM for each TB RAW disk space.

ZFS also provides the feature to use a fast SSD drive as write cache. The write cache is called the ZFS Intent Log (ZIL). You can add that after installation using the following command:

```
zpool add <pool-name> log </dev/path_to_fast_ssd>
```

3.2 Install from USB Stick

The Proxmox Mail Gateway installation media is now a hybrid ISO image, working in two ways:

- An ISO image file ready to burn on CD
- A raw sector (IMG) image file ready to directly copy to flash media (USB Stick)

Using USB sticks is faster and more environmental friendly and therefore the recommended way to install Proxmox Mail Gateway.

3.2.1 Prepare a USB flash drive as install medium

In order to boot the installation media, copy the ISO image to a USB media.

First download the ISO image from https://www.proxmox.com/en/downloads/category/proxmox-mail-gateway

You need at least a 1 GB USB media.

Note
Using UNetbootin or Rufus does not work.

Important
Make sure that the USB media is not mounted and does not contain any important data.

3.2.2 Instructions for GNU/Linux

You can simply use `dd` on UNIX like systems. First download the ISO image, then plug in the USB stick. You need to find out what device name gets assigned to the USB stick (see below). Then run:

```
dd if=proxmox-mailgateway_*.iso of=/dev/XYZ bs=1M
```

Note
Be sure to replace /dev/XYZ with the correct device name.

Caution
Be very careful, and do not overwrite the hard disk!

Find Correct USB Device Name

You can compare the last lines of *dmesg* command before and after the insertion, or use the *lsblk* command. Open a terminal and run:

```
lsblk
```

Then plug in your USB media and run the command again:

```
lsblk
```

A new device will appear, and this is the USB device you want to use.

3.2.3 Instructions for OSX

Open the terminal (query Terminal in Spotlight).

Convert the .iso file to .img using the convert option of hdiutil for example.

```
hdiutil convert -format UDRW -o proxmox-mailgateway_*.dmg proxmox- ↩
   mailgateway_*.iso
```

Tip
OS X tends to put the .dmg ending on the output file automatically.

To get the current list of devices run the command again:

```
diskutil list
```

Now insert your USB flash media and run this command again to determine the device node assigned to your flash media (e.g. /dev/diskX).

```
diskutil list

diskutil unmountDisk /dev/diskX
```

Note
replace X with the disk number from the last command.

```
sudo dd if=proxmox-mailgateway_*.dmg of=/dev/rdiskN bs=1m
```

3.2.4 Instructions for Windows

Download Etcher from https://etcher.io , select the ISO and your USB Drive.

If this doesn't work, alternatively use the OSForensics USB installer from http://www.osforensics.com/portability.htm

3.2.5 Boot your server from USB media

Connect your USB media to your server and make sure that the server boots from USB (see server BIOS). Then follow the installation wizard.

3.3 Install Proxmox Mail Gateway on Debian

Proxmox Mail Gateway ships as a set of Debian packages, so you can install it on top of a normal Debian installation. After configuring the repositories, you need to run:

```
apt-get update
apt-get install proxmox-mailgateway
```

Installing on top of an existing Debian installation looks easy, but it presumes that you have correctly installed the base system, and you know how you want to configure and use the local storage. Network configuration is also completely up to you.

Note
In general, this is not trivial, especially when you use LVM or ZFS.

Chapter 4

Configuration Management

Proxmox Mail Gateway is usually configured using the web-based Graphical User Interface (GUI), but it is also possible to directly edit the configuration files, use the REST API over *https* or the command line tool `pmgsh`.

The command line tool `pmgconfig` is used to simplify some common configuration tasks, i.e. to generate cerificates and to rewrite service configuration files.

Note
We use a Postgres database to store mail filter rules and statistic data. See chapter Database Management Section 9.1 for more information.

4.1 Configuration files overview

`/etc/network/interfaces`
Network setup. We never modify this files directly. Instead, we write changes to `/etc/network/interfaces.new`. When you reboot, we rename the file to `/etc/network/interfaces`, so any changes gets activated on the next reboot.

`/etc/resolv.conf`
DNS search domain and nameserver setup.

`/etc/hostname`
The system's host name.

`/etc/hosts`
Static table lookup for hostnames.

`/etc/pmg/pmg.conf`
Stores common administration options, i.e. the spam and mail proxy setup.

`/etc/pmg/cluster.conf`
The cluster setup.

/etc/pmg/domains
The list of relay domains.

/etc/pmg/fetchmailrc
Fetchmail configuration (POP3 and IMAP setup).

/etc/pmg/ldap.conf
LDAP configuration.

/etc/pmg/mynetworks
List of local (trusted) networks.

/etc/pmg/subscription
Stores your subscription key and status.

/etc/pmg/transports
Message delivery transport setup.

/etc/pmg/user.conf
GUI user configuration.

/etc/mail/spamassassin/custom.cf
Custom SpamAssassin™ setup.

4.2 Keys and Certificates

/etc/pmg/pmg-api.pem
Key and certificate (combined) used be the HTTPs server (API).

/etc/pmg/pmg-authkey.key
Privat key use to generate authentication tickets.

/etc/pmg/pmg-authkey.pub
Public key use to verify authentication tickets.

/etc/pmg/pmg-csrf.key
Internally used to generate CSRF tokens.

/etc/pmg/pmg-tls.pem
Key and certificate (combined) to encrypt mail traffic (TLS).

4.3 Service Configuration Templates

Proxmox Mail Gateway uses various services to implement mail filtering, for example the Postfix Mail Transport Agent (MTA), the ClamAV® antivirus engine and the Apache SpamAssassin™ project. Those services use separate configuration files, so we need to rewrite those files when configuration is changed.

We use a template based approach to generate those files. The Template Toolkit is a well known, fast and flexible template processing system. You can find the default templates in `/var/lib/pmg/templates/`. Please do not modify them directly, because your modification would get lost on the next update. Instead, copy them to `/etc/pmg/templates/`, then apply your changes there.

Templates can access any configuration setting, and you can use the `pmgconfig dump` command to get a list of all variable names:

```
# pmgconfig dump
...
dns.domain = yourdomain.tld
dns.hostname = pmg
ipconfig.int_ip = 192.168.2.127
pmg.admin.advfilter = 1
...
```

The same tool is used to force regeneration of all template based configuration files. You need to run that after modifying a template, or when you directly edit configuration files

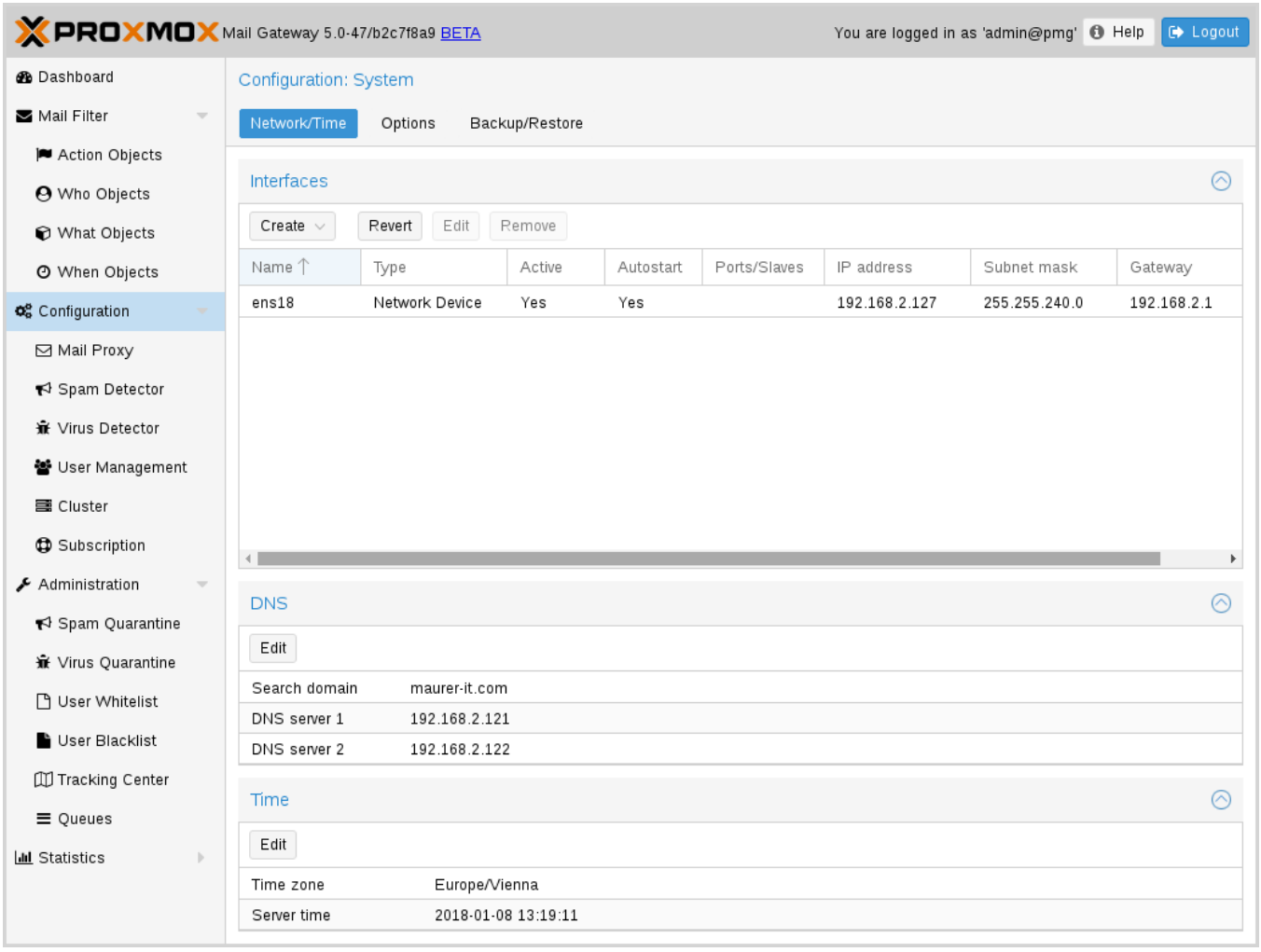
```
# pmgconfig sync --restart 1
```

Above commands also restarts services if underlying configuration files are changed. Please note that this is automatically done when you change the configuration using the GUI or API.

Note
Modified templates from `/etc/pmg/templates/` are automatically synced from the master node to all cluster members.

4.4 System Configuration

4.4.1 Network and Time



Normally the network and time is already configured when you visit the GUI. The installer asks for those setting and sets up the correct values.

The default setup uses a single Ethernet adapter and static IP assignment. The configuration is stored at */etc/network/interfaces*, and the actual network setup is done the standard Debian way using package *ifupdown*.

Example network setup /etc/network/interfaces

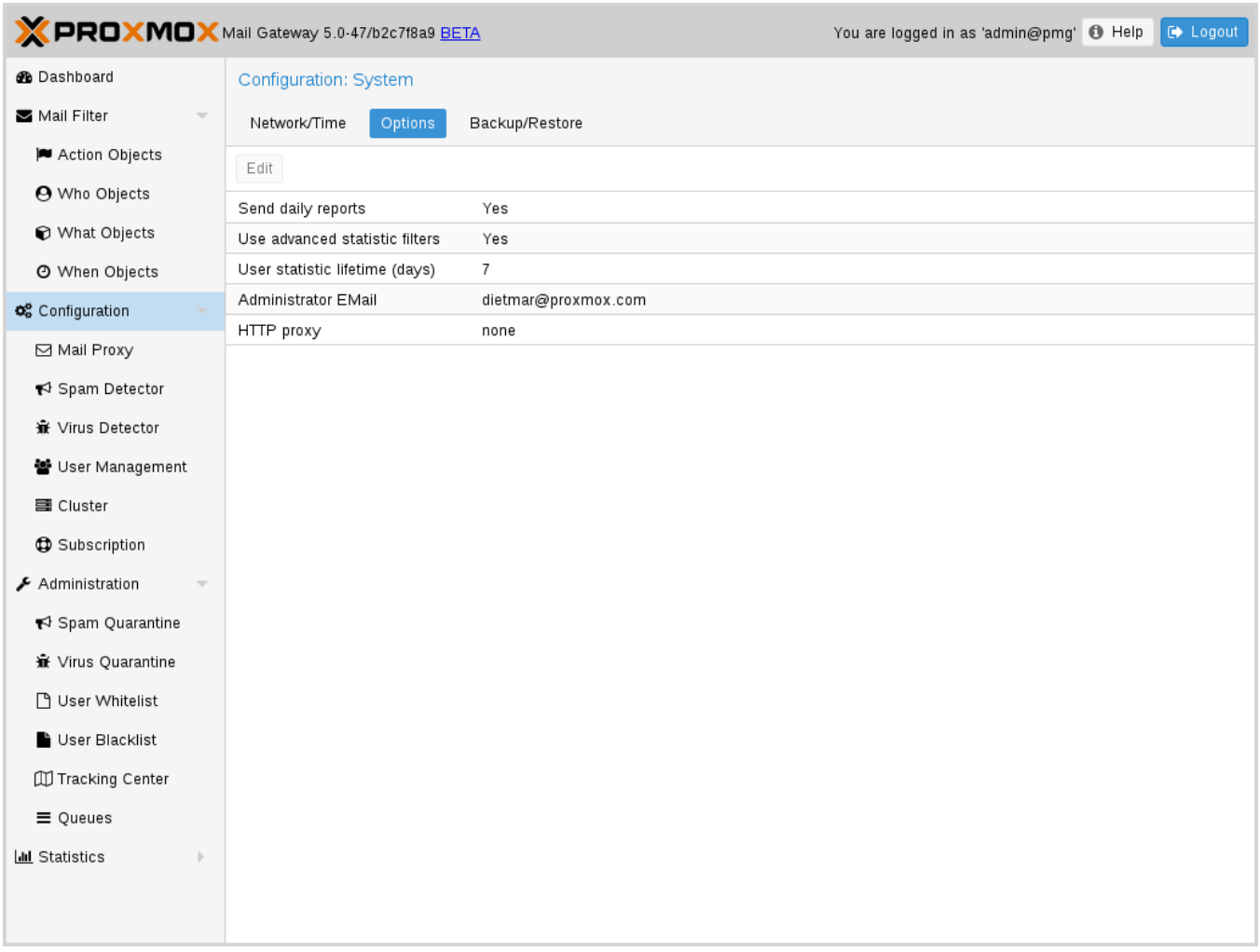
```
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto ens18
iface ens18 inet static
        address  192.168.2.127
        netmask  255.255.240.0
```

```
        gateway  192.168.2.1
```

DNS recommendations

Many tests to detect SPAM mails use DNS queries, so it is important to have a fast and reliable DNS server. We also query some public available DNS Blacklists. Most of them apply rate limits for clients, so they simply will not work if you use a public DNS server (because they are usually blocked). We recommend to use your own DNS server, which need to be configured in *recursive* mode.

4.4.2 Options



Those settings are saved to subsection *admin* in `/etc/pmg/pmg.conf`, using the following configuration keys:

`advfilter`: <boolean> (*default* = 1)
: Use advanced filters for statistic.

`dailyreport`: <boolean> (*default* = 1)
: Send daily reports.

demo: <boolean> (*default* = 0)
Demo mode - do not start SMTP filter.

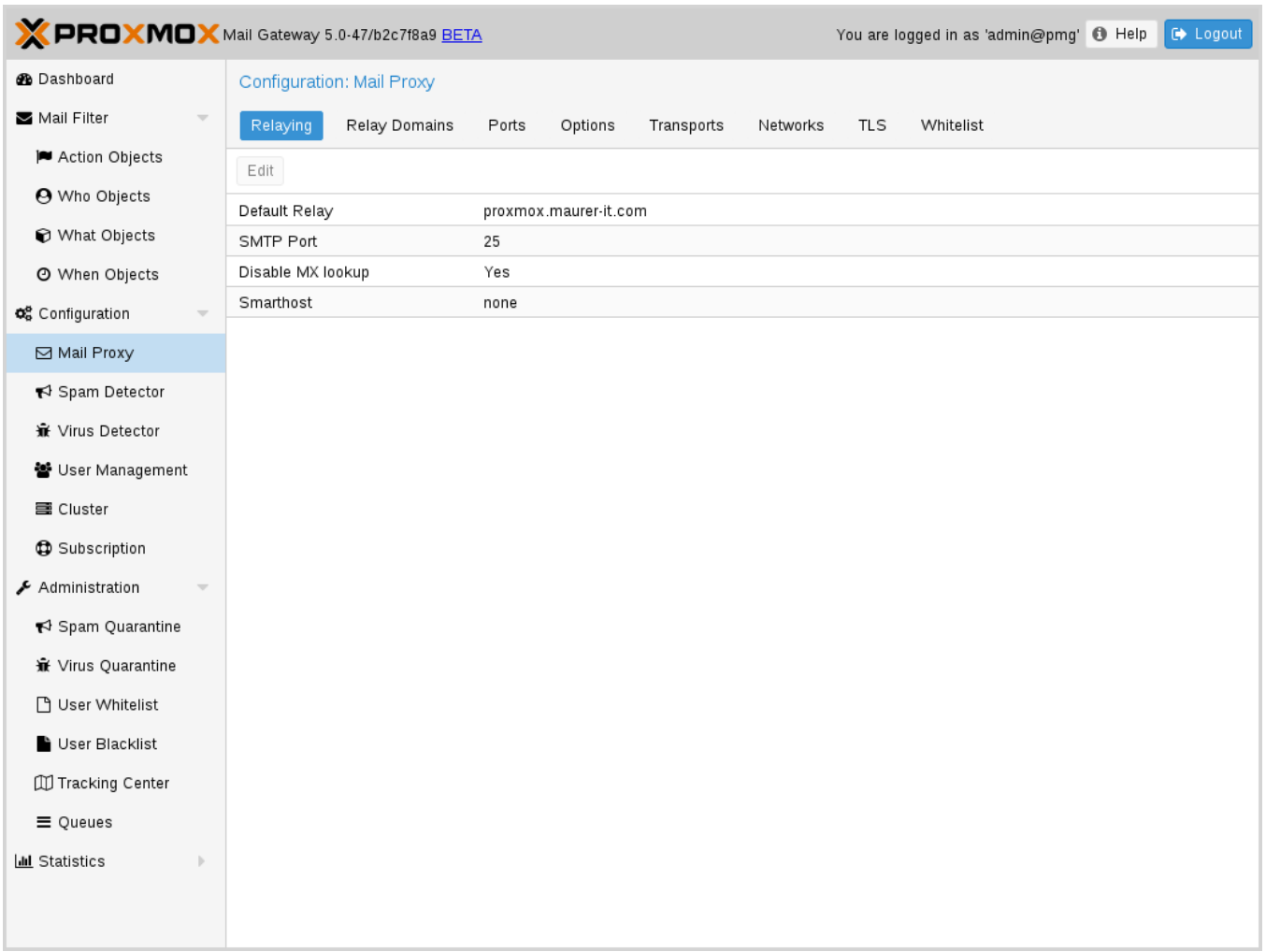
email: <string> (*default* = admin@domain.tld)
Administrator E-Mail address.

http_proxy: http://.*
Specify external http proxy which is used for downloads (example: *http://username:password@host:port/*)

statlifetime: <integer> (1 - N) (*default* = 7)
User Statistics Lifetime (days)

4.5 Mail Proxy Configuration

4.5.1 Relaying



Those settings are saved to subsection *mail* in `/etc/pmg/pmg.conf`, using the following configuration keys:

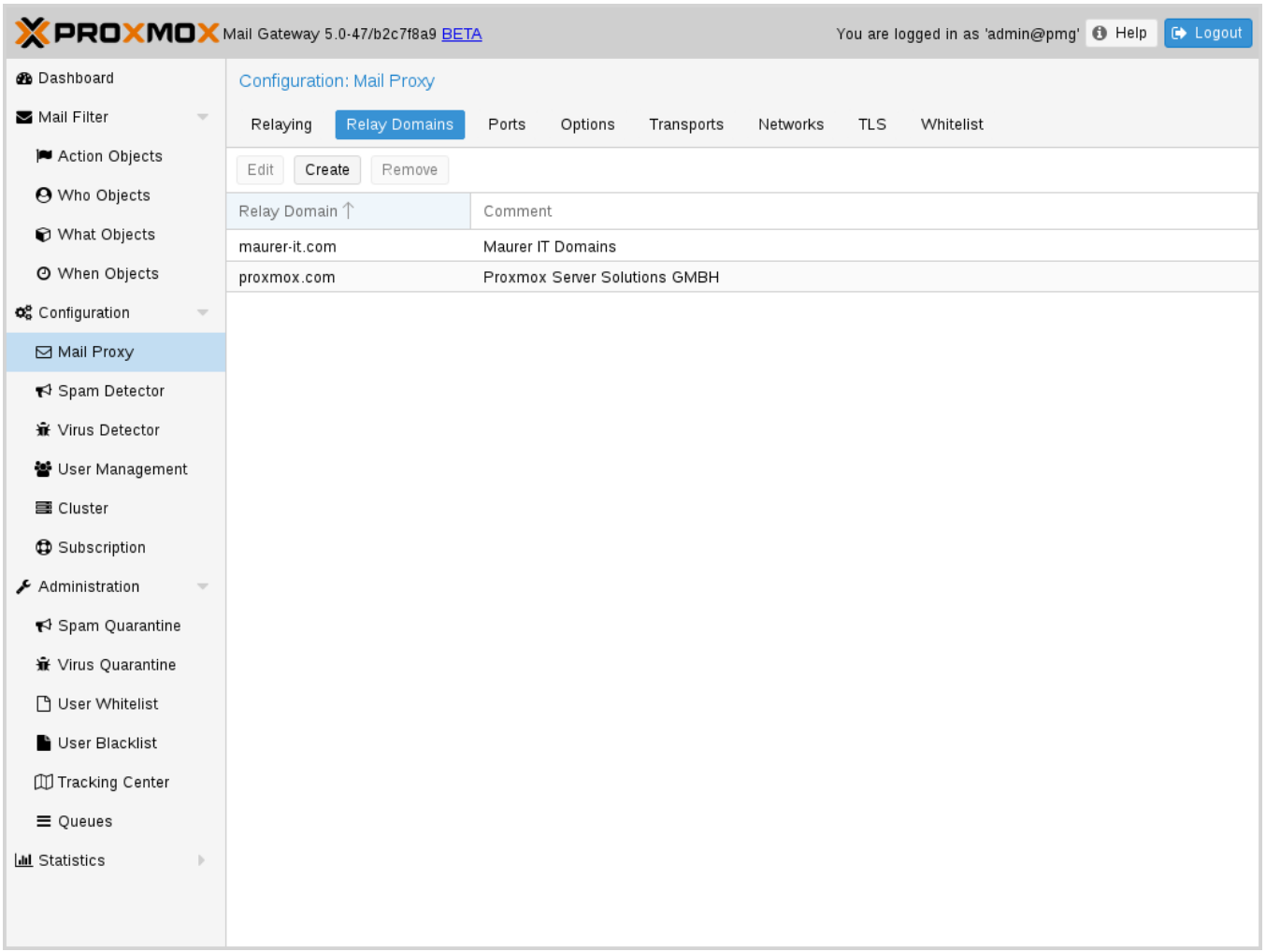
relay: <string>
The default mail delivery transport (incoming mails).

relaynomx: <boolean> (*default* = 0)
Disable MX lookups for default relay.

relayport: <integer> (1 - 65535) (*default* = 25)
SMTP port number for relay host.

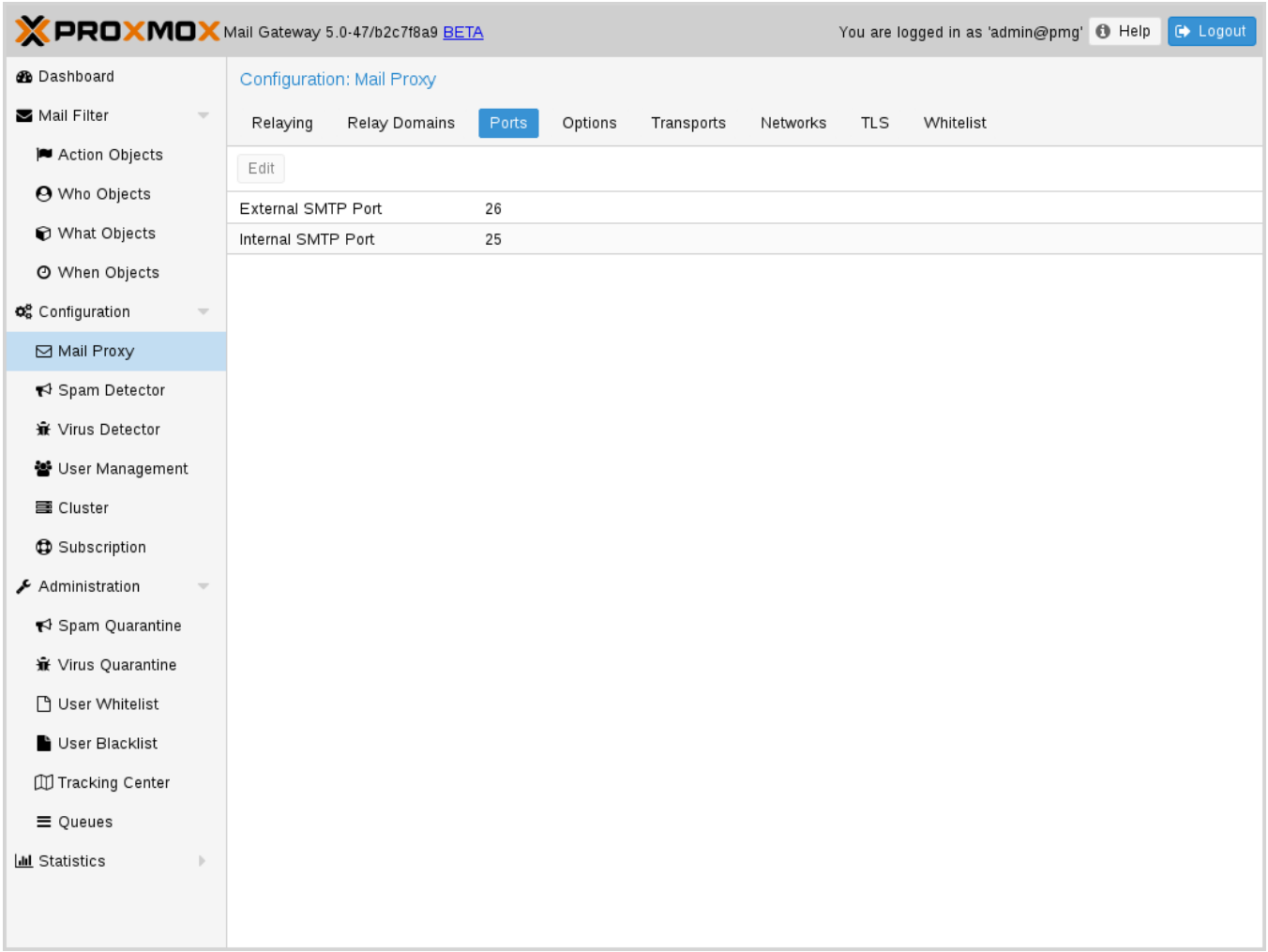
smarthost: <string>
When set, all outgoing mails are deliverd to the specified smarthost.

4.5.2 Relay Domains



List of relayed mail domains, i.e. what destination domains this system will relay mail to. The system will reject incoming mails to other domains.

4.5.3 Ports

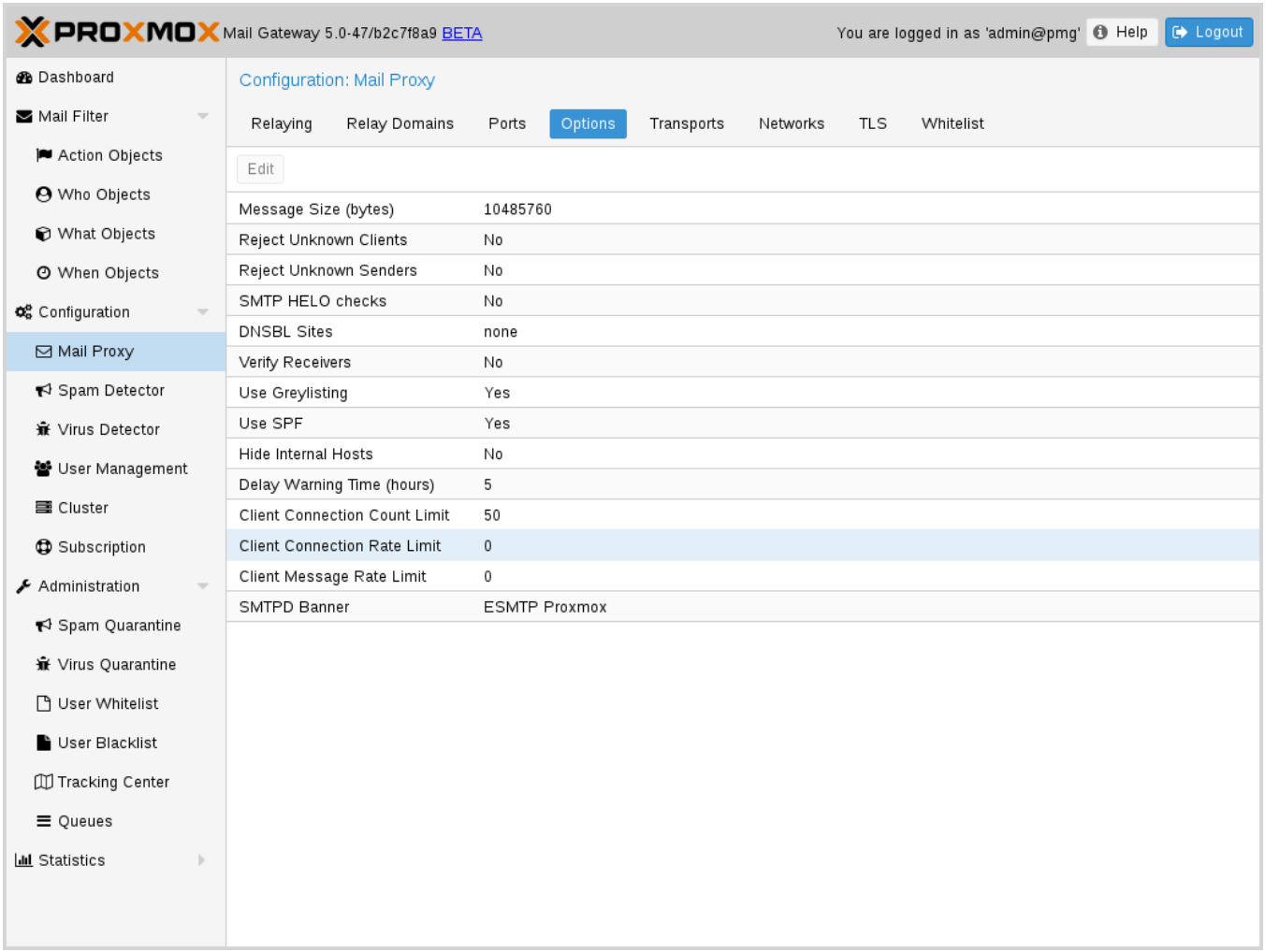


Those settings are saved to subsection *mail* in `/etc/pmg/pmg.conf`, using the following configuration keys:

ext_port: <integer> (1 - 65535) (*default* = 26)
: SMTP port number for incoming mail (untrusted). This must be a different number than *int_port*.

int_port: <integer> (1 - 65535) (*default* = 25)
: SMTP port number for outgoing mail (trusted).

4.5.4 Options



Those settings are saved to subsection *mail* in `/etc/pmg/pmg.conf`, using the following configuration keys:

banner: <string> (*default* = ESMTP Proxmox)
: ESMTP banner.

conn_count_limit: <integer> (0 - N) (*default* = 50)
: How many simultaneous connections any client is allowed to make to this service. To disable this feature, specify a limit of 0.

conn_rate_limit: <integer> (0 - N) (*default* = 0)
: The maximal number of connection attempts any client is allowed to make to this service per minute. To disable this feature, specify a limit of 0.

dnsbl_sites: <string>
: Optional list of DNS white/blacklist domains (see postscreen_dnsbl_sites parameter).

dwarning: <integer> (0 - N) (*default* = 4)
: SMTP delay warning time (in hours).

greylist: <boolean> (*default =* 1)
Use Greylisting.

helotests: <boolean> (*default =* 0)
Use SMTP HELO tests.

hide_received: <boolean> (*default =* 0)
Hide received header in outgoing mails.

maxsize: <integer> (1024 - N) (*default =* 10485760)
Maximum email size. Larger mails are rejected.

message_rate_limit: <integer> (0 - N) (*default =* 0)
The maximal number of message delivery requests that any client is allowed to make to this service per minute.To disable this feature, specify a limit of 0.

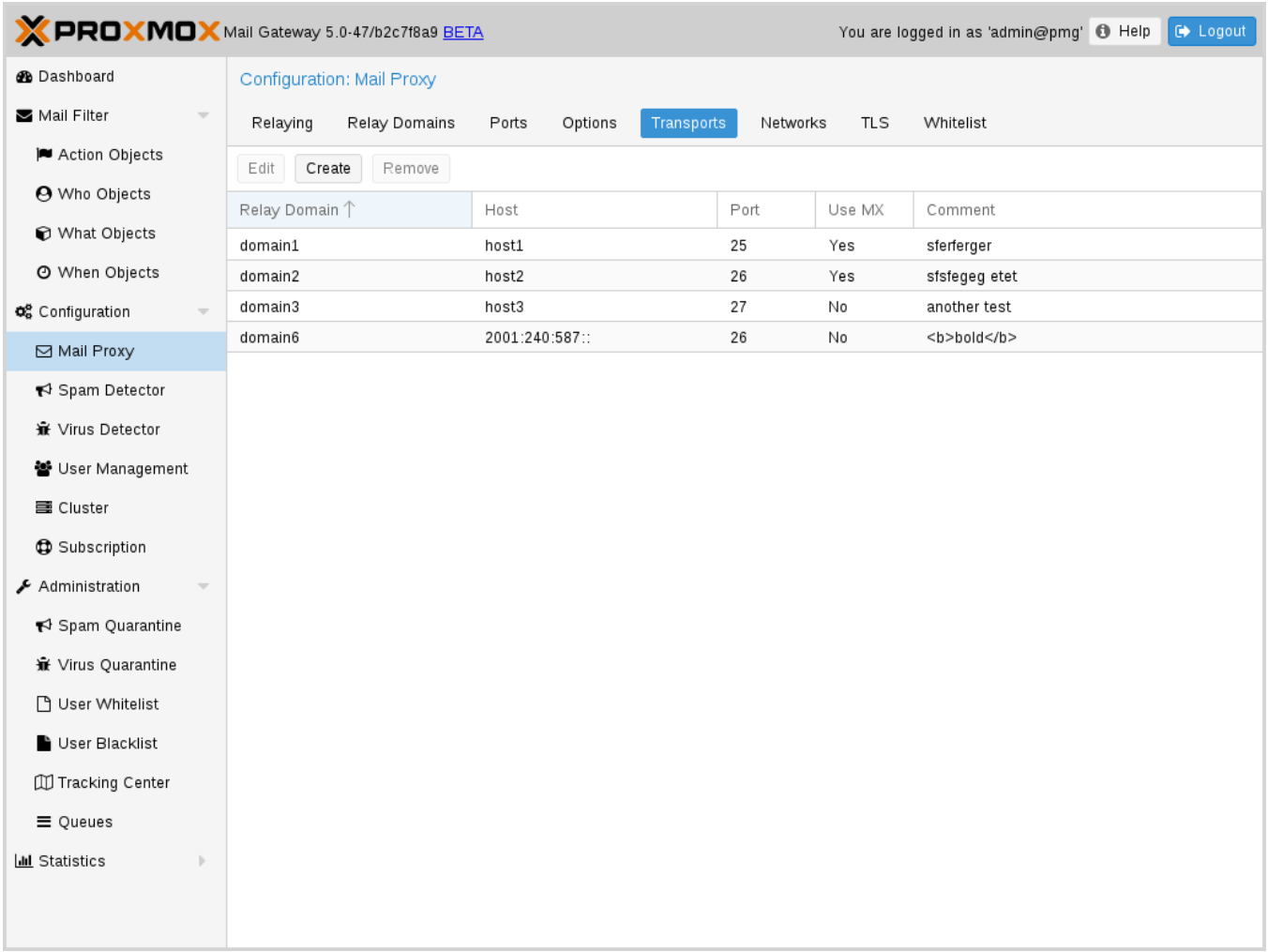
rejectunknown: <boolean> (*default =* 0)
Reject unknown clients.

rejectunknownsender: <boolean> (*default =* 0)
Reject unknown senders.

spf: <boolean> (*default =* 1)
Use Sender Policy Framework.

verifyreceivers: <450 | 550>
Enable receiver verification. The value spefifies the numerical reply code when the Postfix SMTP server rejects a recipient address.

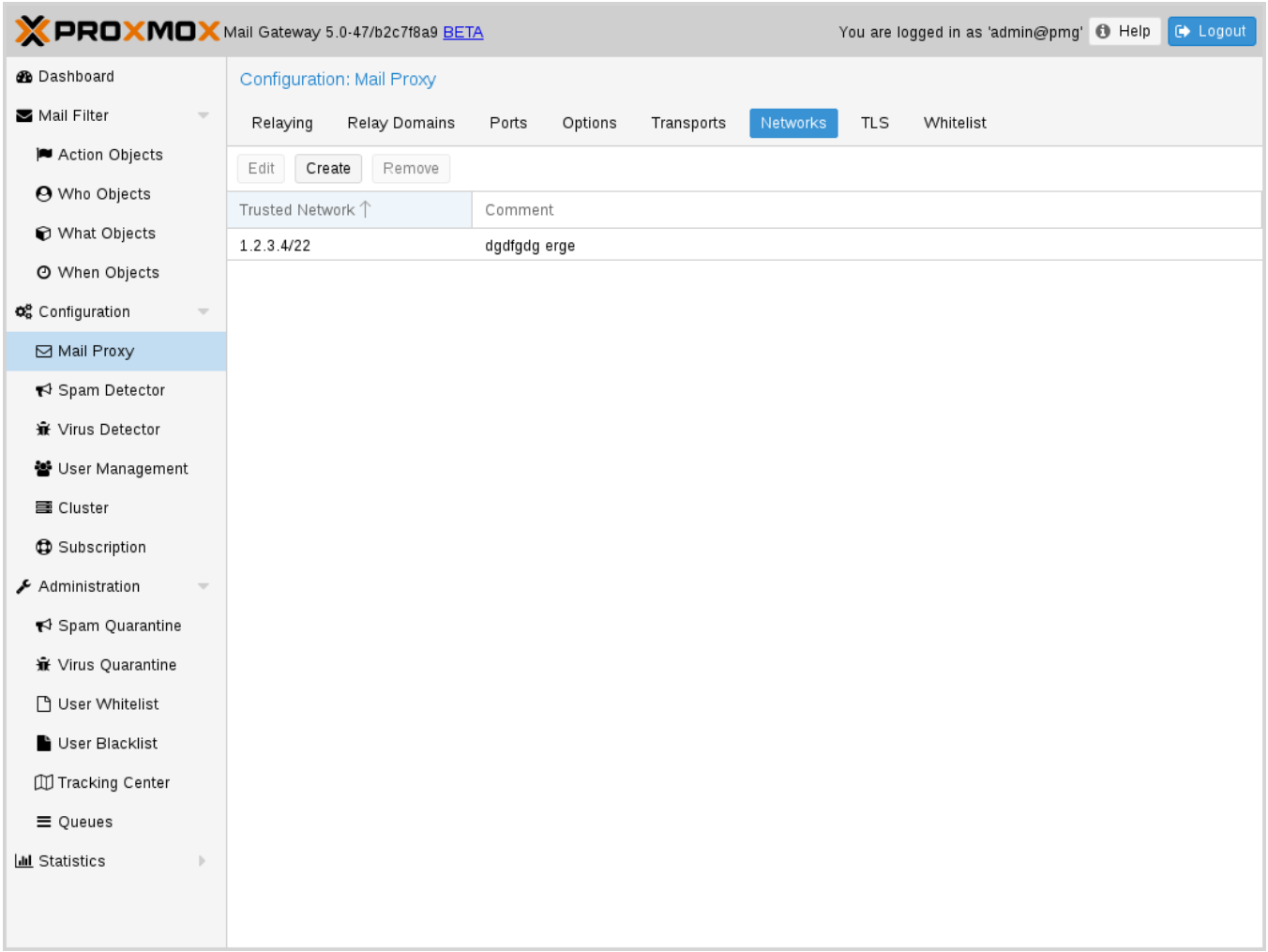
4.5.5 Transports



You can use Proxmox Mail Gateway to send e-mails to different internal e-mail servers. For example you can send e-mails addressed to domain.com to your first e-mail server, and e-mails addressed to subdomain.domain.com to a second one.

You can add the IP addresses, hostname and SMTP ports and mail domains (or just single email addresses) of your additional e-mail servers.

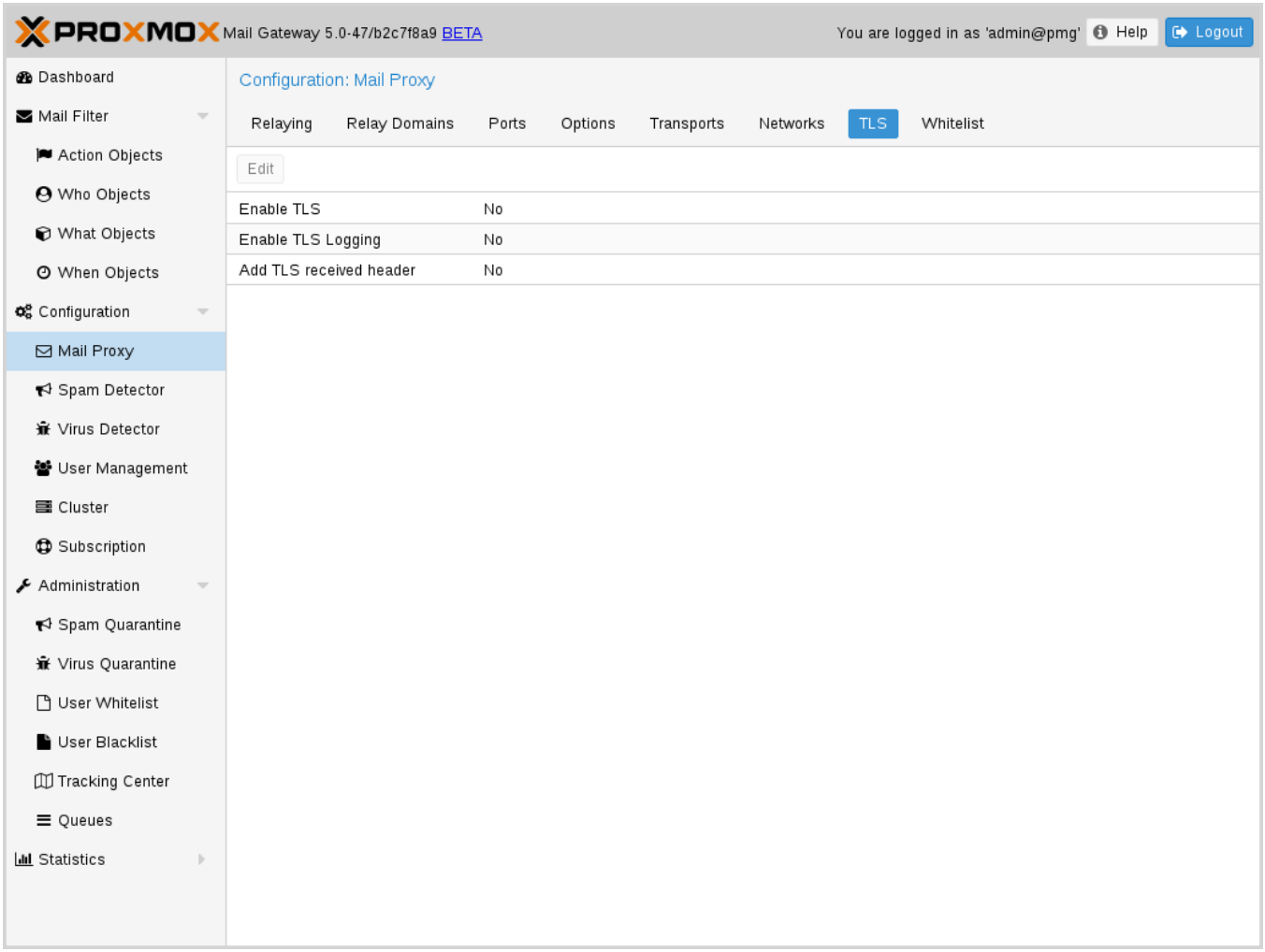
4.5.6 Networks



You can add additional internal (trusted) IP networks or hosts. All hosts in this list are allowed to relay.

Note
Hosts in the same subnet with Proxmox can relay by default and it's not needed to add them in this list.

4.5.7 TLS



Transport Layer Security (TLS) provides certificate-based authentication and encrypted sessions. An encrypted session protects the information that is transmitted with SMTP mail. When you activate TLS, Proxmox Mail Gateway automatically generates a new self signed certificate for you (`/etc/pmg/pmg-tls.pem`).

Proxmox Mail Gateway uses opportunistic TLS encryption. The SMTP transaction is encrypted if the *STARTTLS* ESMTP feature is supported by the remote server. Otherwise, messages are sent in the clear.

Enable TLS logging
: To get additional information about SMTP TLS activity you can enable TLS logging. That way information about TLS sessions and used certificate's is logged via syslog.

Add TLS received header
: Set this option to include information about the protocol and cipher used as well as the client and issuer CommonName into the "Received:" message header.

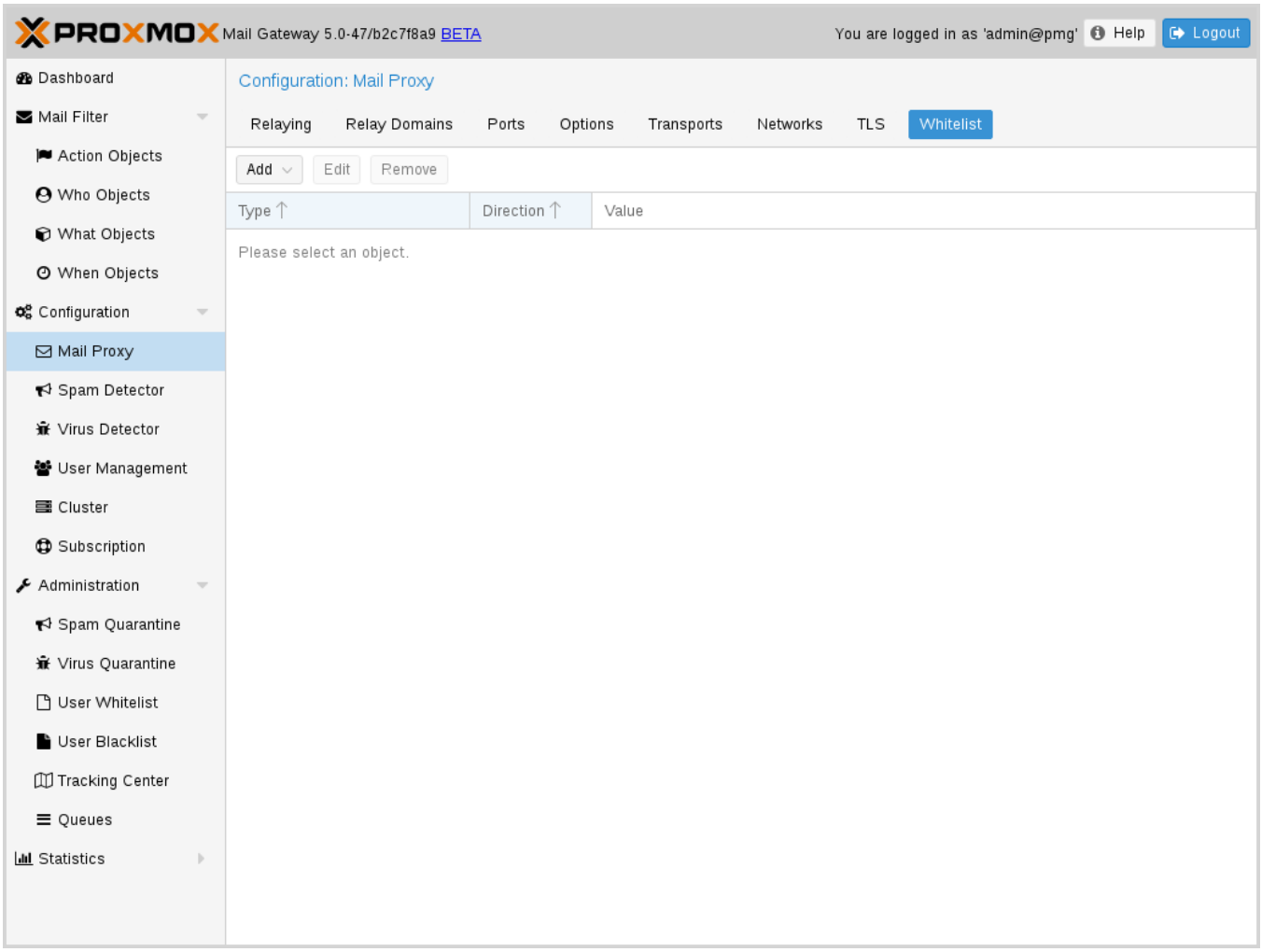
Those settings are saved to subsection *mail* in `/etc/pmg/pmg.conf`, using the following configuration keys:

`tls`: `<boolean>` (*default* = 0)
: Enable TLS.

`tlsheader`: <boolean> (*default* = 0)
Add TLS received header.

`tlslog`: <boolean> (*default* = 0)
Enable TLS Logging.

4.5.8 Whitelist

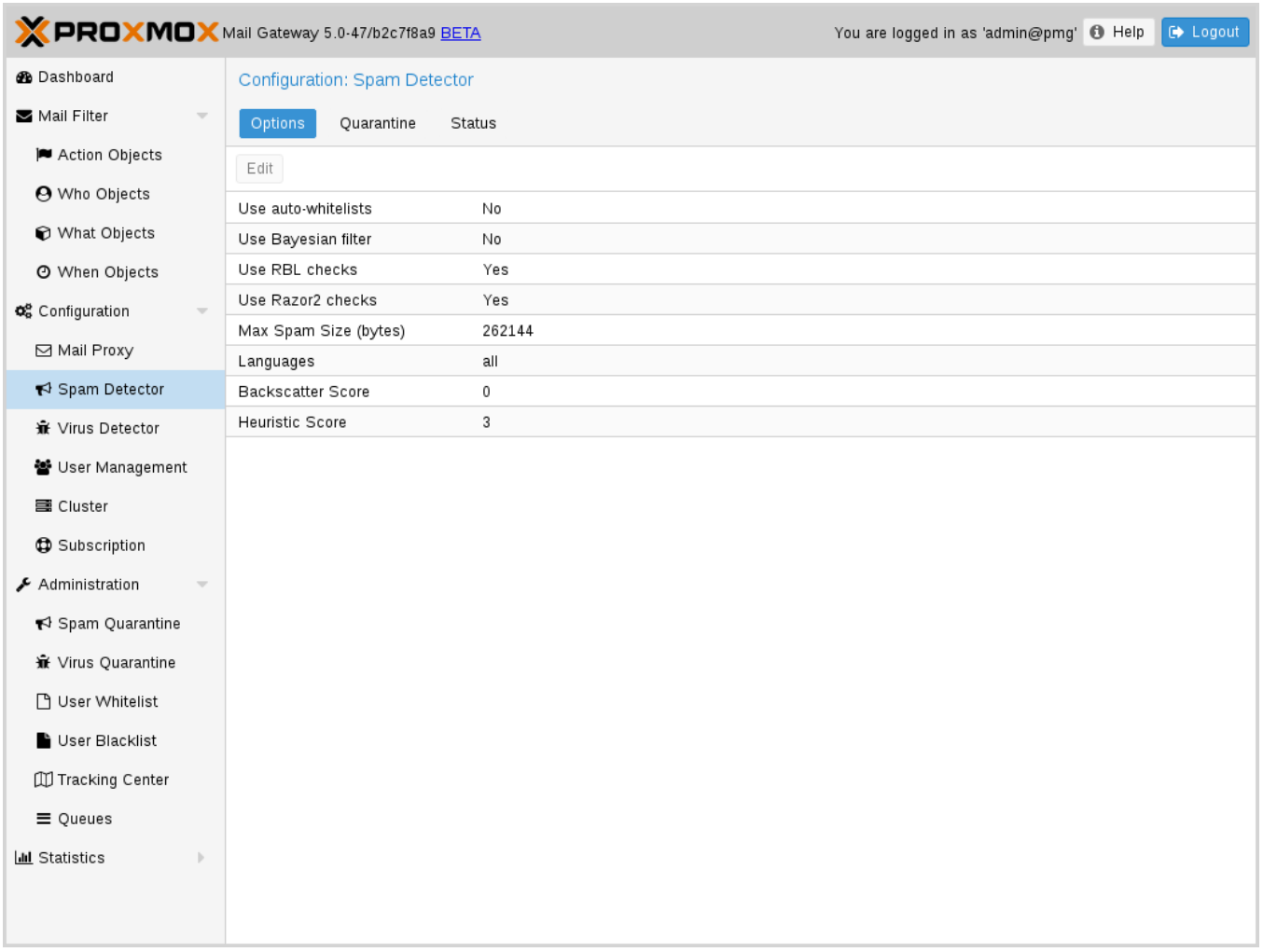


All SMTP checks are disabled for those entries (e. g. Greylisting, SPF, RBL, . . .)

Note
If you use a backup MX server (e.g. your ISP offers this service for you) you should always add those servers here.

4.6 Spam Detector Configuration

4.6.1 Options



Proxmox Mail Gateway uses a wide variety of local and network tests to identify spam signatures. This makes it harder for spammers to identify one aspect which they can craft their messages to work around the spam filter.

Every single e-mail will be analyzed and gets a spam score assigned. The system attempts to optimize the efficiency of the rules that are run in terms of minimizing the number of false positives and false negatives.

`bounce_score`: `<integer> (0 - 1000)` (*default* = 0)
: Additional score for bounce mails.

`clamav_heuristic_score`: `<integer> (0 - 1000)` (*default* = 3)
: Score for ClamaAV heuristics (Google Safe Browsing database, PhishingScanURLs, . . .).

`languages`: `(all|([a-z][a-z])+( ([a-z][a-z])+)*)` (*default* = `all`)
: This option is used to specify which languages are considered OK for incoming mail.

maxspamsize: <integer> (64 - N) (*default* = 262144)
Maximum size of spam messages in bytes.

rbl_checks: <boolean> (*default* = 1)
Enable real time blacklists (RBL) checks.

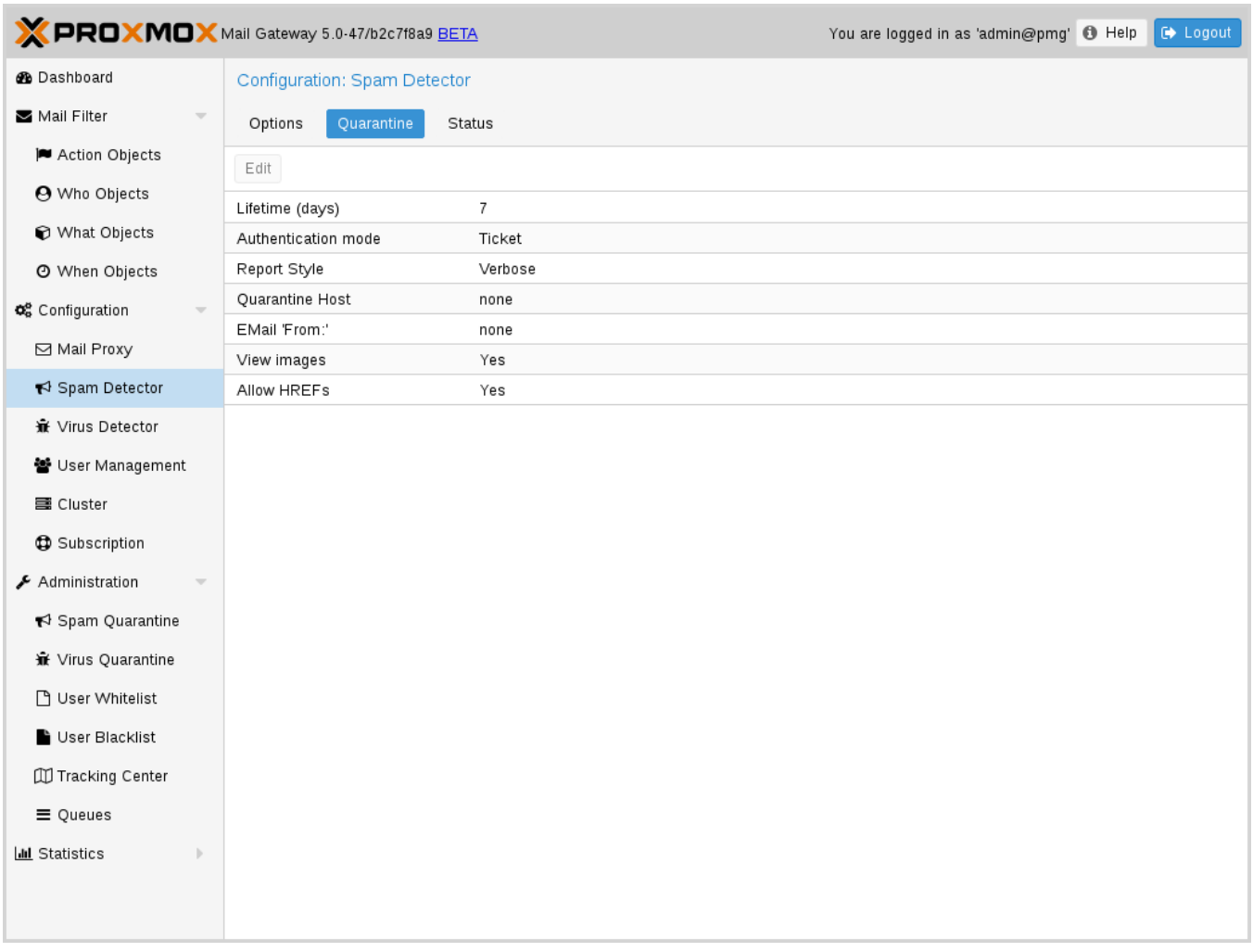
use_awl: <boolean> (*default* = 1)
Use the Auto-Whitelist plugin.

use_bayes: <boolean> (*default* = 1)
Whether to use the naive-Bayesian-style classifier.

use_razor: <boolean> (*default* = 1)
Whether to use Razor2, if it is available.

wl_bounce_relays: <string>
Whitelist legitimate bounce relays.

4.6.2 Quarantine



Proxmox analyses all incoming e-mail messages and decides for each e-mail if its ham or spam (or virus). Good e-mails are delivered to the inbox and spam messages can be moved into the spam quarantine.

The system can be configured to send daily reports to inform users about the personal spam messages received the last day. That report is only sent if there are new messages in the quarantine.

allowhrefs: <boolean> (*default =* 1)
Allow to view hyperlinks.

authmode: <ldap | ldapticket | ticket> (*default =* ticket)
Authentication mode to access the quarantine interface. Mode *ticket* allows login using tickets sent with the daily spam report. Mode *ldap* requires to login using an LDAP account. Finally, mode *ldapticket* allows both ways.

hostname: <string>
Quarantine Host. Usefule if you run a Cluster and want users to connect to a specific host.

lifetime: <integer> (1 - N) (*default =* 7)
Quarantine life time (days)

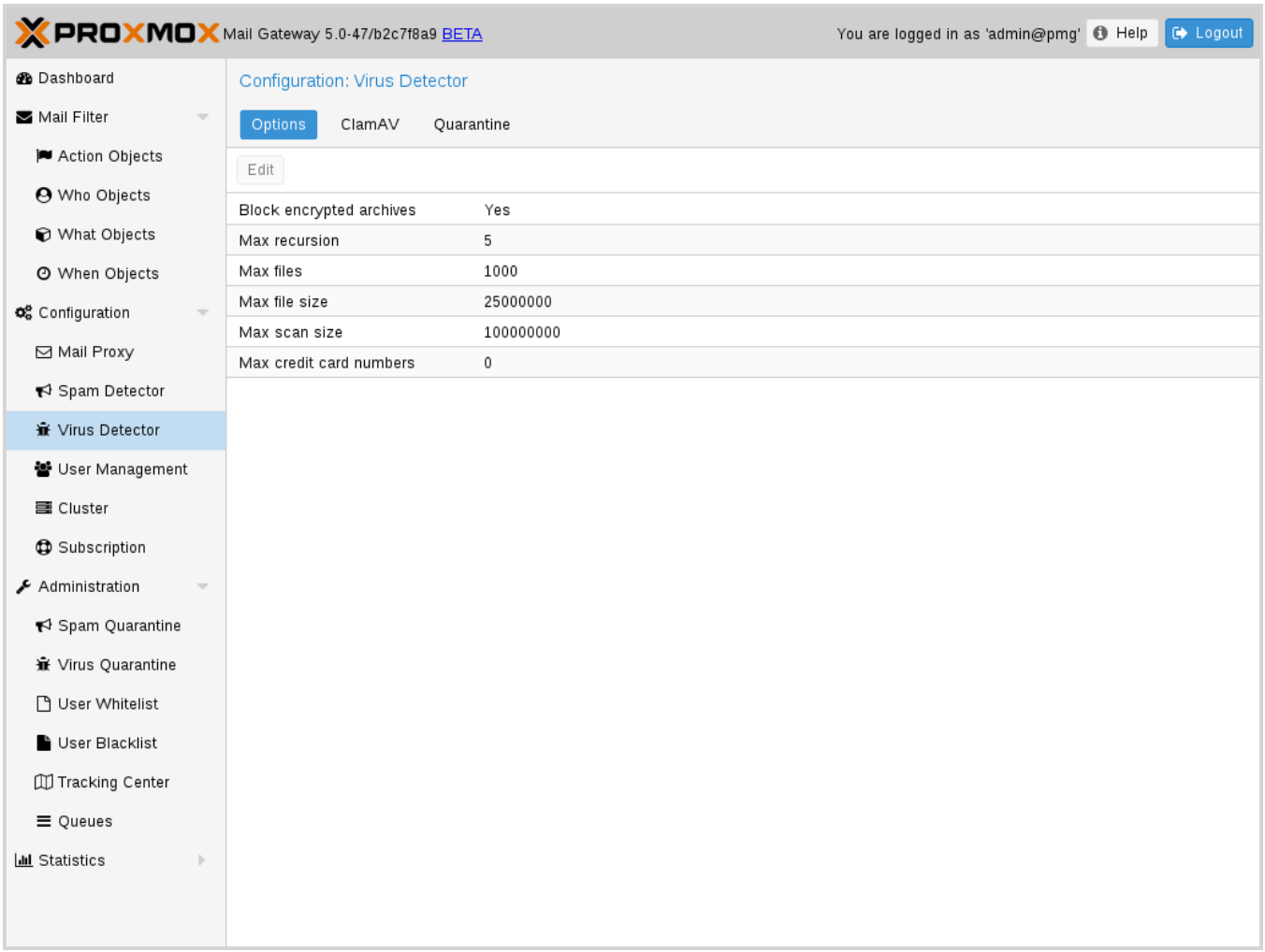
mailfrom: <string>
Text for *From* header in daily spam report mails.

reportstyle: <custom | none | short | verbose> (*default =* verbose)
Spam report style.

viewimages: <boolean> (*default =* 1)
Allow to view images.

4.7 Virus Detector Configuration

4.7.1 Options



All mails are automatically passed to the included virus detector (ClamAV®). The default setting are considered safe, so it is usually not required to change them.

ClamAV® related settings are saved to subsection *clamav* in `/etc/pmg/pmg.conf`, using the following configuration keys:

`archiveblockencrypted`: `<boolean>` (*default* = 0)
: Wether to block encrypted archives. Mark encrypted archives as viruses.

`archivemaxfiles`: `<integer> (0 - N)` (*default* = 1000)
: Number of files to be scanned within an archive, a document, or any other kind of container. Warning: disabling this limit or setting it too high may result in severe damage to the system.

`archivemaxrec`: `<integer> (1 - N)` (*default* = 5)
: Nested archives are scanned recursively, e.g. if a ZIP archive contains a TAR file, all files within it will also be scanned. This options specifies how deeply the process should be continued. Warning: setting this limit too high may result in severe damage to the system.

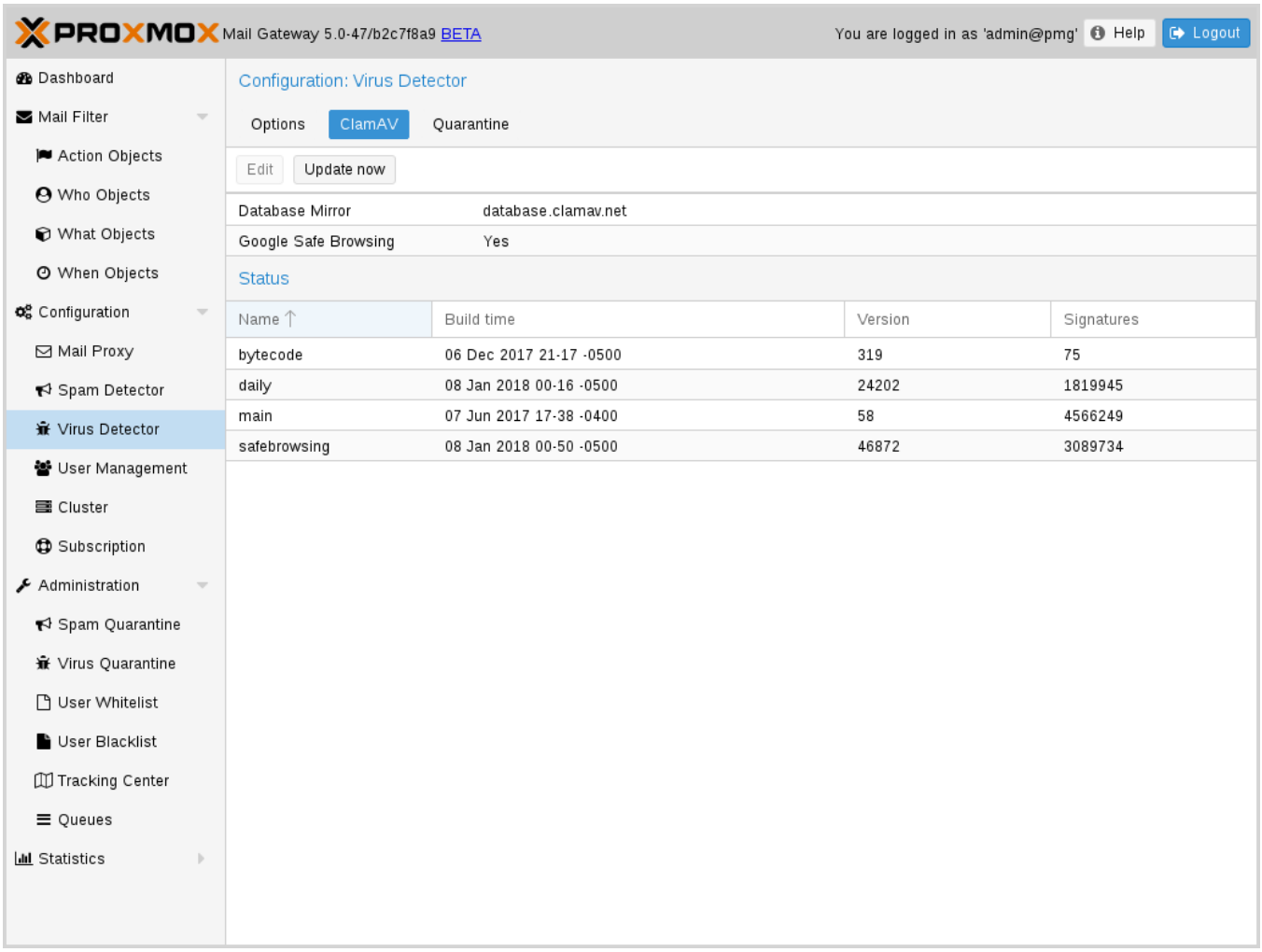
archivemaxsize: <integer> (1000000 - N) (*default* = 25000000)
Files larger than this limit won't be scanned.

dbmirror: <string> (*default* = database.clamav.net)
ClamAV database mirror server.

maxcccount: <integer> (0 - N) (*default* = 0)
This option sets the lowest number of Credit Card or Social Security numbers found in a file to generate a detect.

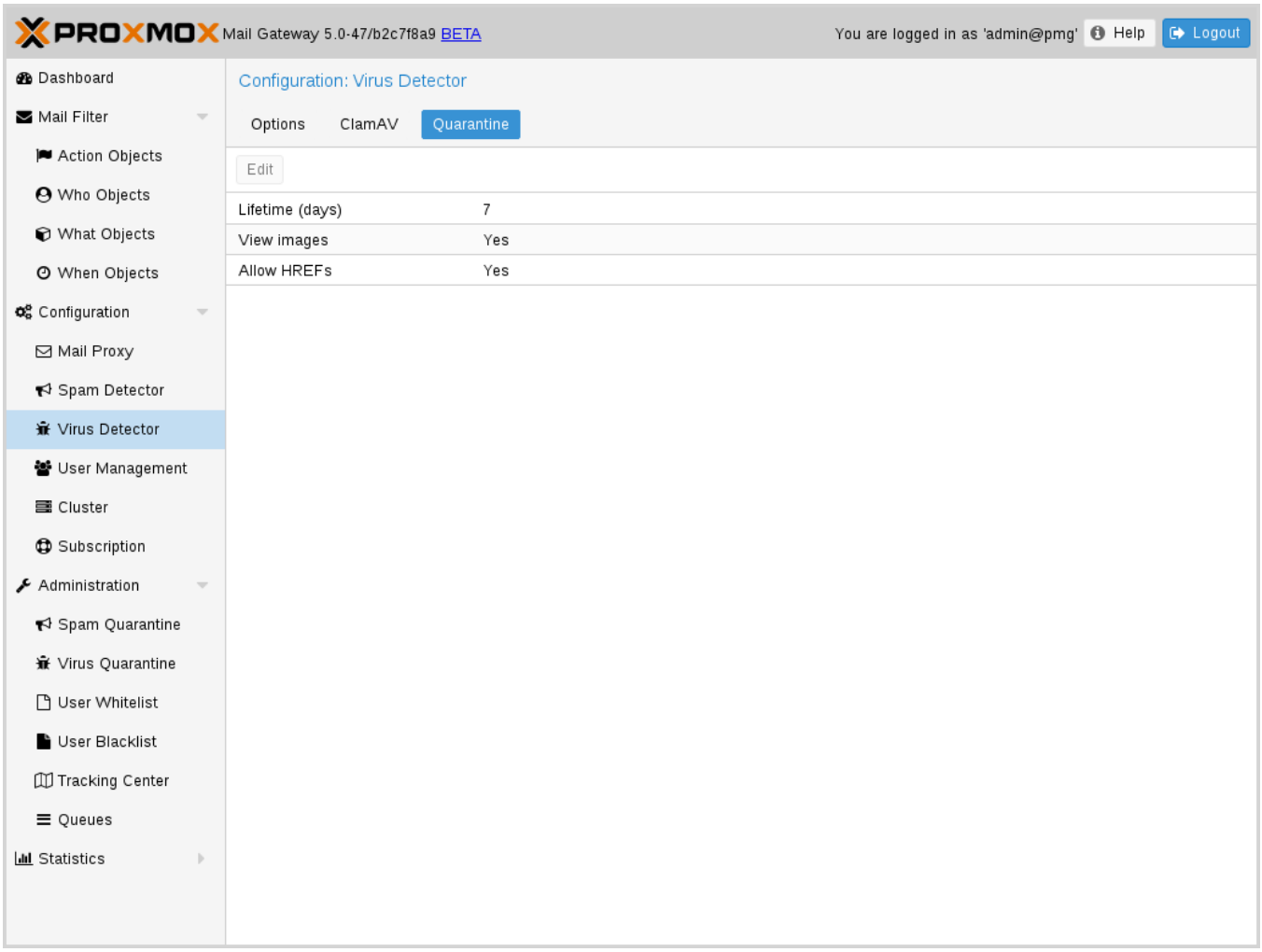
maxscansize: <integer> (1000000 - N) (*default* = 100000000)
Sets the maximum amount of data to be scanned for each input file.

safebrowsing: <boolean> (*default* = 1)
Enables support for Google Safe Browsing.



Please note that the virus signature database it automatically updated. But you can see the database status on the GUI, and you can trigger manual updates there.

4.7.2 Quarantine



Indentified virus mails are automatically moved to the virus quarantine. The administartor can view those mails using the GUI, or deliver them in case of false positives. Proxmox Mail Gateway does not notify individual users about received virus mails.

Virus quarantine related settings are saved to subsection *virusquar* in `/etc/pmg/pmg.conf`, using the following configuration keys:

`allowhrefs`: `<boolean>` (*default* = 1)
: Allow to view hyperlinks.

`lifetime`: `<integer>` (1 - N) (*default* = 7)
: Quarantine life time (days)

`viewimages`: `<boolean>` (*default* = 1)
: Allow to view images.

4.8 Custom SpamAssassin configuration

This is only for advanced users. To add or change the Proxmox SpamAssassin™ configuration please login to the console via SSH. Go to directory `/etc/mail/spamassasin/`. In this directory there are several

files (`init.pre`, `local.cf`, ...) – do not change them.

To add your special configuration, you have to create a new file and name it `custom.cf` (in this directory), then add your configuration there. Be aware to use the SpamAssassin™ syntax, and test with

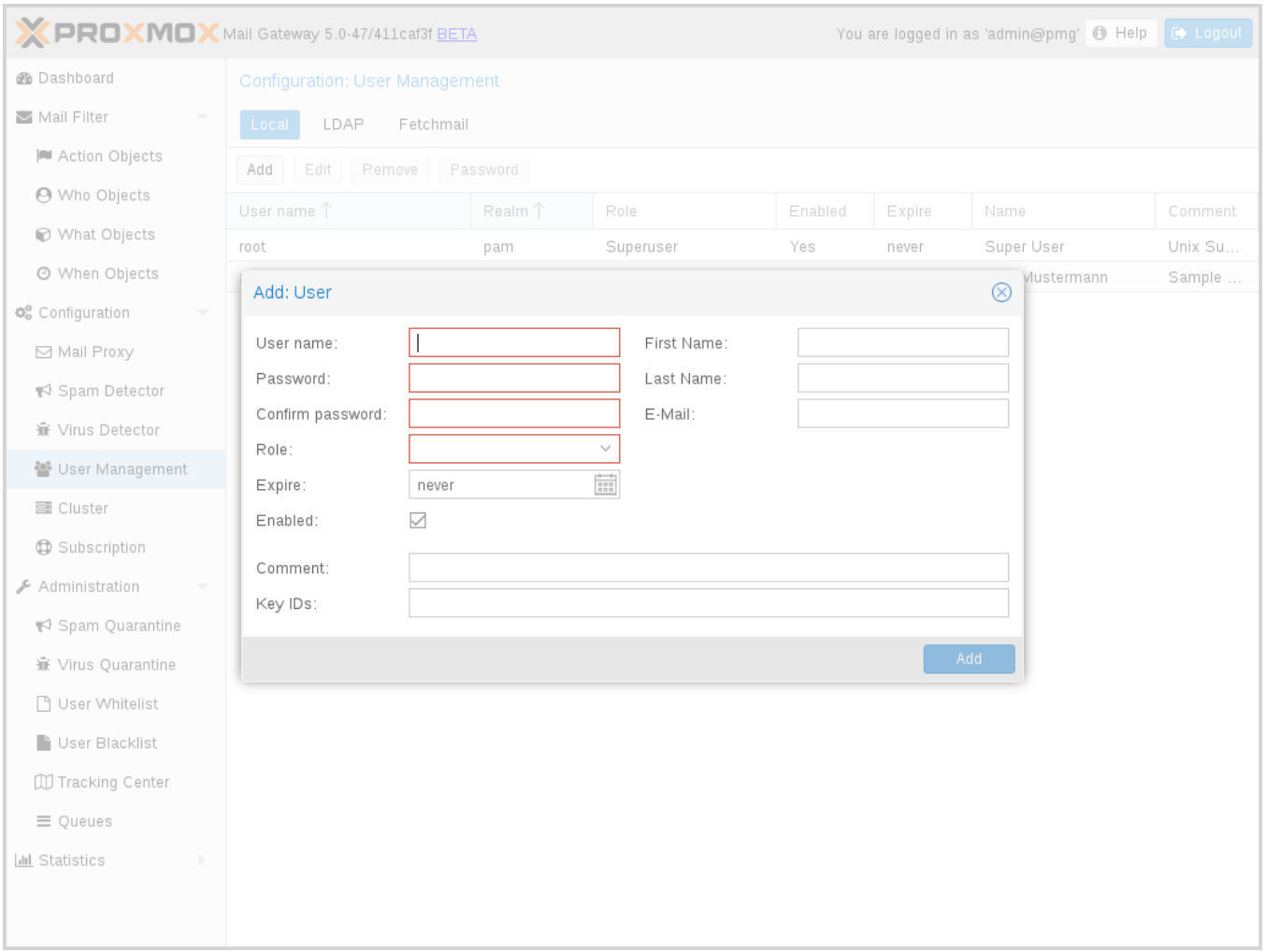
```
# spamassassin -D --lint
```

If you run a cluster, the `custom.cf` file is synchronized from the master node to all cluster members.

4.9 User Management

User management in Proxmox Mail Gateway consists of three types of users/accounts:

4.9.1 Local Users



Local users are used to manage and audit Proxmox Mail Gateway. Those users can login on the management web interface.

There are three roles:

- Administrator

  Is allowed to manage settings of Proxmox Mail Gateway, except some tasks like network configuration and upgrading.

- Quarantine manager

  Is allowed to manage quarantines, blacklists and whitelists, but not other settings. Has no right to view any other data.

- Auditor

  With this role, the user is only allowed to view data and configuration, but not to edit it.

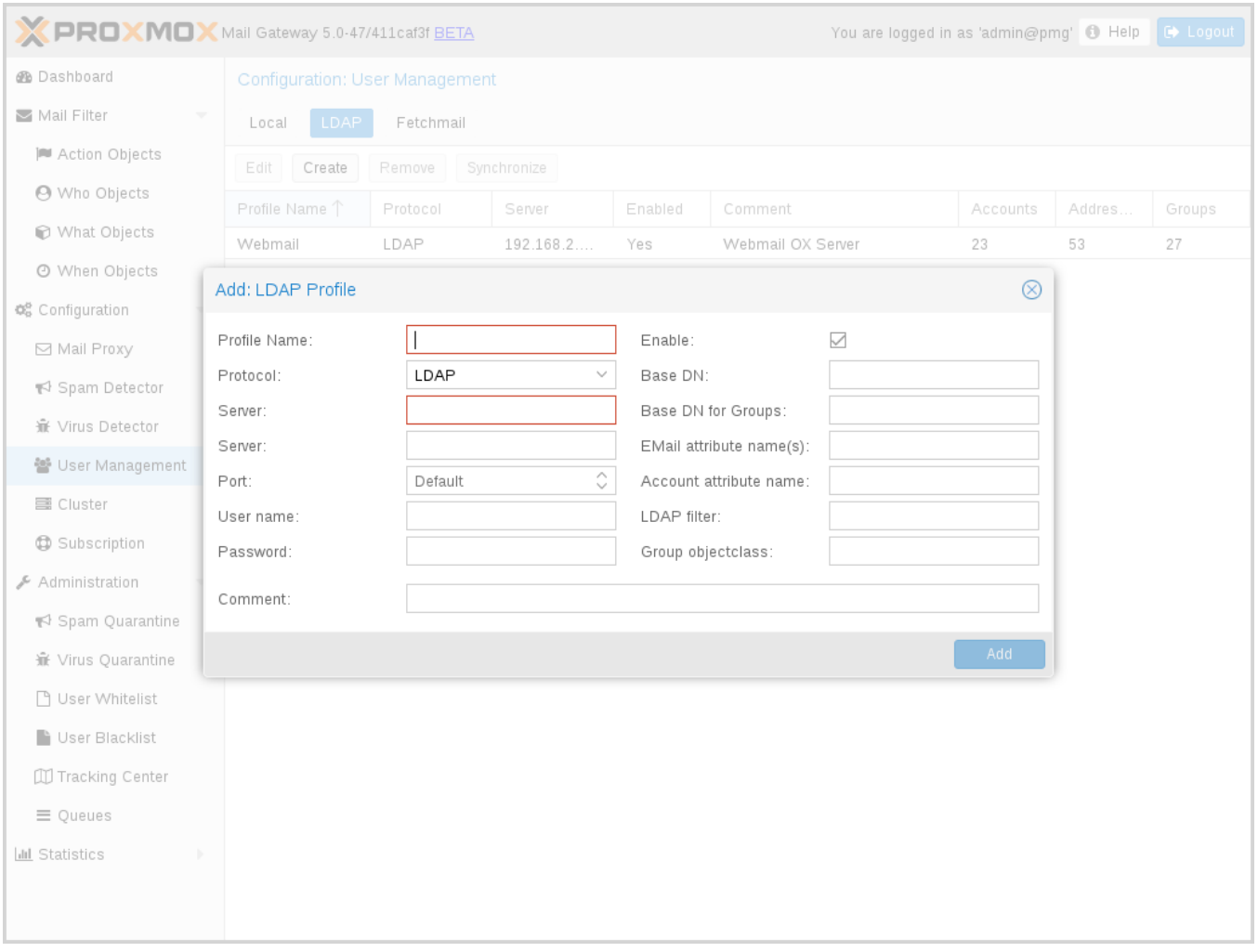
In addition there is always the *root* user, which is used to perform special system administrator tasks, such as updgrading a host or changing the network configuration.

Note
Only pam users are able to login via the webconsole and ssh, which the users created with the web interface are not. Those users are created for Proxmox Mail Gateway administration only.

Local user related settings are saved in `/etc/pmg/user.conf`.

For details of the fields see user.conf Section E.3

4.9.2 LDAP/Active Directory



You can specify multiple LDAP/Active Directory profiles, so that you can create rules matching those users and groups.

Creating a profile requires (at least) the following:

- profile name
- protocol (LDAP or LDAPS; LDAPS is recommended)
- at least one server
- a user and password (if your server does not support anonymous binds)

All other fields should work with the defaults for most setups, but can be used to customize the queries.

The settings are saved to `/etc/pmg/ldap.conf`. Details for the options can be found here: ldap.conf Section E.4

Bind user

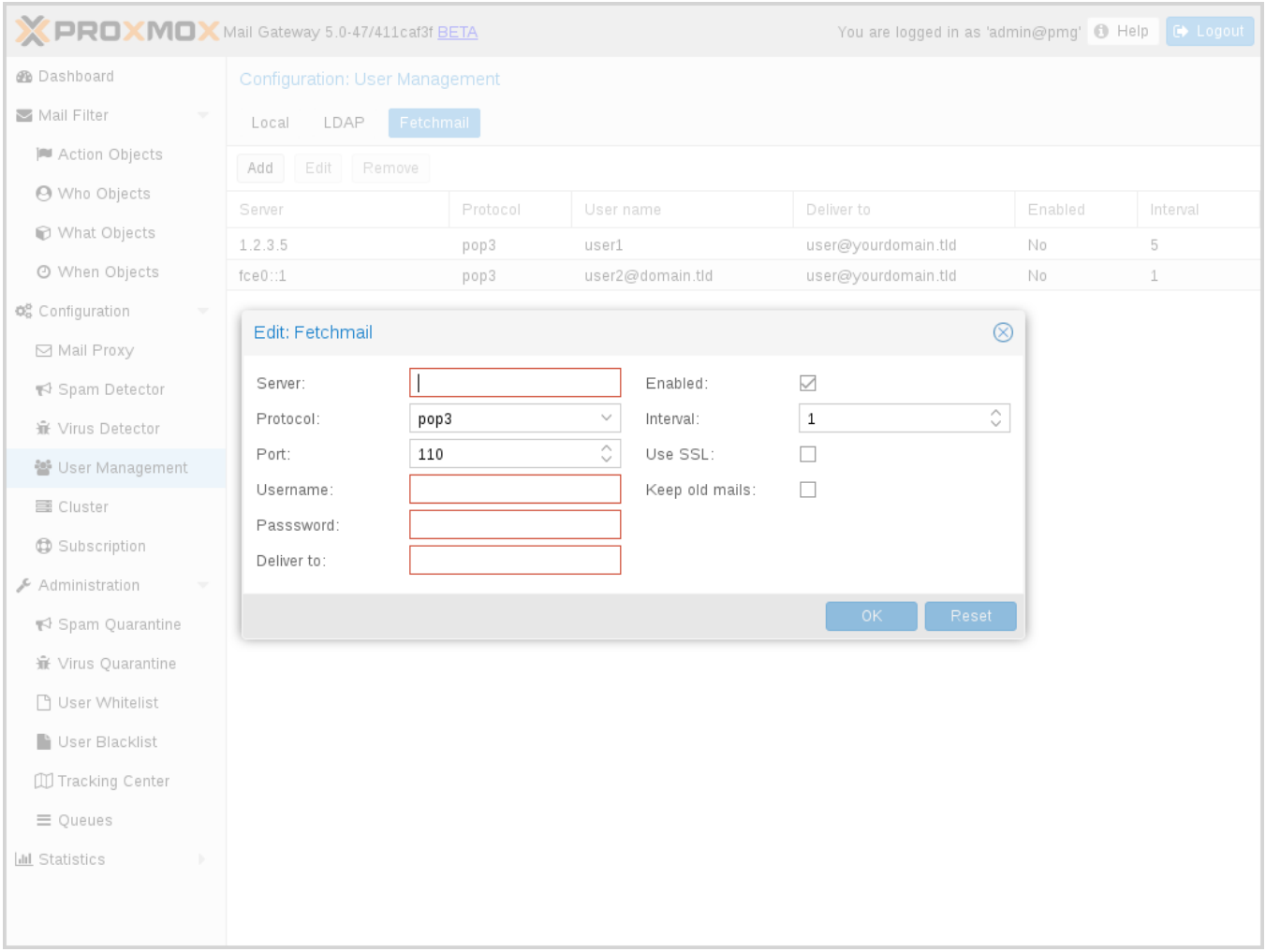
It is highly recommended that the user which you use for connecting to the LDAP server only has the permission to query the server. For LDAP servers (for example OpenLDAP or FreeIPA), the username has to be of a format like *uid=username,cn=users,cn=accounts,dc=domain* , where the specific fields are depending on your setup. For Active Directory servers, the format should be like *username@domain* or *domain\username*.

Sync

Proxmox Mail Gateway synchronizes the relevant user and group info periodically, so that that information is available in a fast manner, even when the LDAP/AD server is temporarily not accessible.

After a successfull sync, the groups and users should be visible on the web interface. After that, you can create rules targeting LDAP users and groups.

4.9.3 Fetchmail



Fetchmail is utility for polling and forwarding e-mails. You can define e-mail accounts, which will then be fetched and forwarded to the e-mail address you defined.

You have to add an entry for each account/target combination you want to fetch and forward. Those will then be regularly polled and forwarded, according to your configuration.

The API and web interface offer following configuration options:

`enable`: `<boolean>` (*default* = 0)
: Flag to enable or disable polling.

`interval`: `<integer> (1 - 2016)`
: Only check this site every <interval> poll cycles. A poll cycle is 5 minutes.

`keep`: `<boolean>` (*default* = 0)
: Keep retrieved messages on the remote mailserver.

`pass`: `<string>`
: The password used tfor server login.

port: **<integer> (1 - 65535)**
Port number.

protocol: **<imap | pop3>**
Specify the protocol to use when communicating with the remote mailserver

server: **<string>**
Server address (IP or DNS name).

ssl: **<boolean>** **(*default =* 0)**
Use SSL.

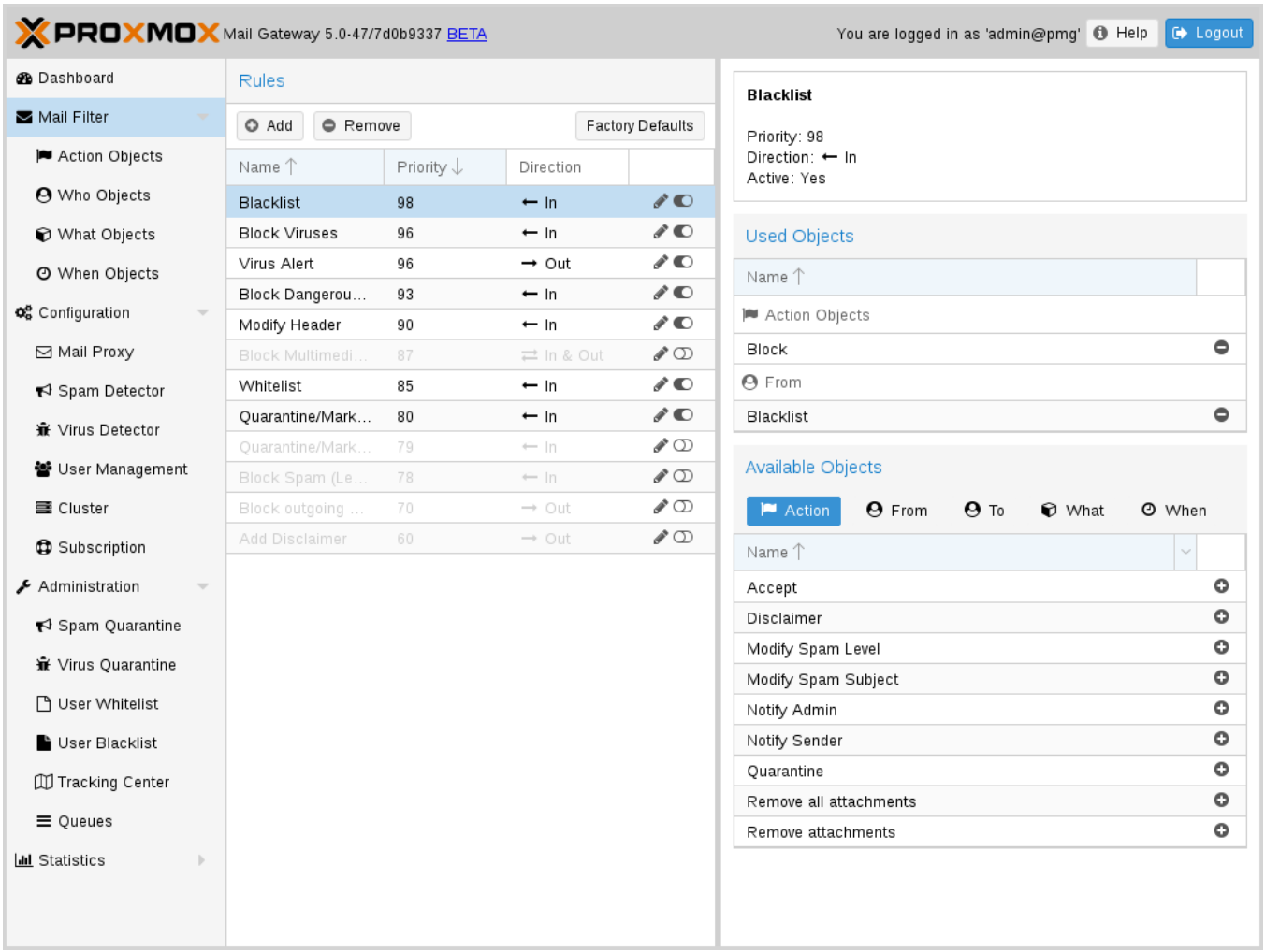
target: **(?:|[^\s\/\@]+\@[^\s\/\@]+)**
The target email address (where to deliver fetched mails).

user: **<string>**
The user identification to be used when logging in to the server

Chapter 5

Mail Filter

Proxmox Mail Gateway ships with a highly configurable mail filter. It's an easy but powerful way to define filter rules by user, domains, time frame, content type and resulting action.



Every rule has 5 categories (*FROM*, *TO*, *WHEN*, *WHAT* and *ACTION*), and each category may contain several objects to match certain criteria:

WHO - objects

Who is the sender or receiver of the e-mail? Those objects can be used for the *TO* and/or *FROM* category.

Example: EMail-object - Who is the sender or receiver of the e-mail?

WHAT - objects
What is in the e-mail?

Example: Does the e-mail contain spam?

WHEN - objects
When is the e-mail received by Proxmox Mail Gateway?

Example: Office Hours - Mail is received between 8:00 and 16:00.

ACTIONS - objects
Defines the final actions.

Example: Mark e-mail with “SPAM:” in the subject.

Rules are ordered by priority, so rules with higher priority are executed first. It is also possible to set a processing direction:

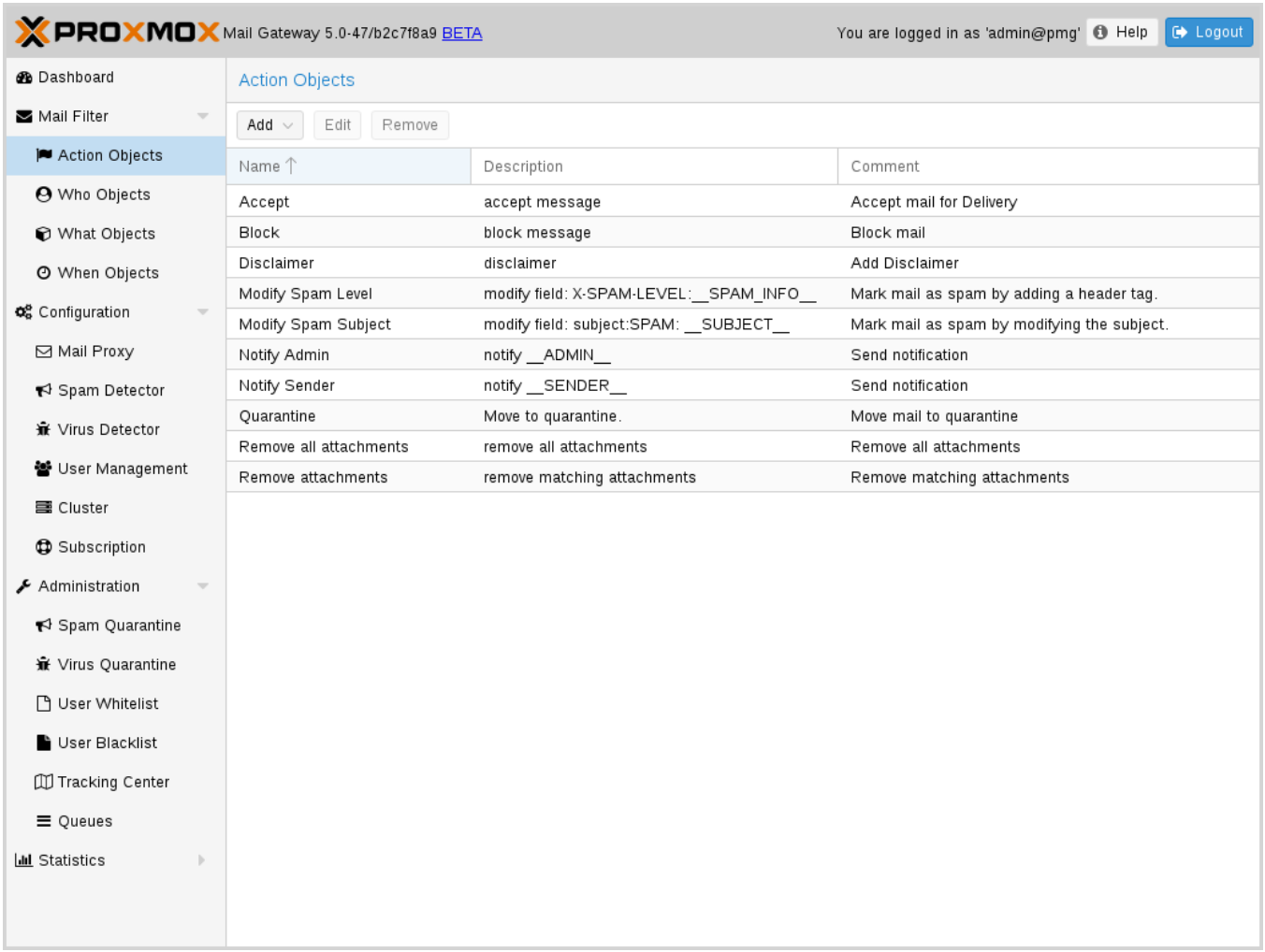
In
Rule applies for all incoming e-mails

Out
Rule applies for all outgoing e-mails

In & Out
Rule applies for both directions

And you can also disable a rule completely, which is mostly useful for testing and debugging. The *Factory Defaults* button alows you to reset the filter rules.

5.1 Actions



Please note that some actions stops further rule precessing. We call such actions *final*.

5.1.1 Accept

Accept mail for Delivery. This is a *final* action.

5.1.2 Block

Block mail. This is a *final* action.

5.1.3 Quarantine

Move to quarantine (virus mails are moved to the “virus quarantine”, other mails are moved to “spam quarantine”). This is also a *final* action.

5.1.4 Notification

Send notifications. Please note that object configuration can use macros Appendix D, so it is easy to include additional information. For example, the default *Notify Admin* object sends the following information:

Sample notification action body:

```
Proxmox Notification:
Sender:   __SENDER__
Receiver: __RECEIVERS__
Targets:  __TARGETS__
Subject: __SUBJECT__
Matching Rule: __RULE__

__RULE_INFO__

__VIRUS_INFO__
__SPAM_INFO__
```

Notification can also include a copy of the original mail.

5.1.5 Blind Carbon Copy (BCC)

The BCC object simply sends a copy to another target. It is possible to send the original unmodified mail, or the processed result. Please note that this can be quite different, i.e. when a previous rule removed attachments.

5.1.6 Header Attributes

This object is able to add or modify mail header attributes. As notice above, you can use macros Appendix D, making this a very powerful object. For example, the *Modify Spam Level* actions adds detailed infomation about detected Spam characteristics to the ` X-SPAM-LEVEL` header.

Modify Spam Level Header Attribute

```
Field: X-SPAM-LEVEL
Value: __SPAM_INFO__
```

Another prominent example is the *Modify Spam Subject* action. This simply adds the *SPAM:* prefix to the original mail subject:

Modify Spam Subject Header Attribute

```
Field: subject
Value: SPAM: __SUBJECT__
```

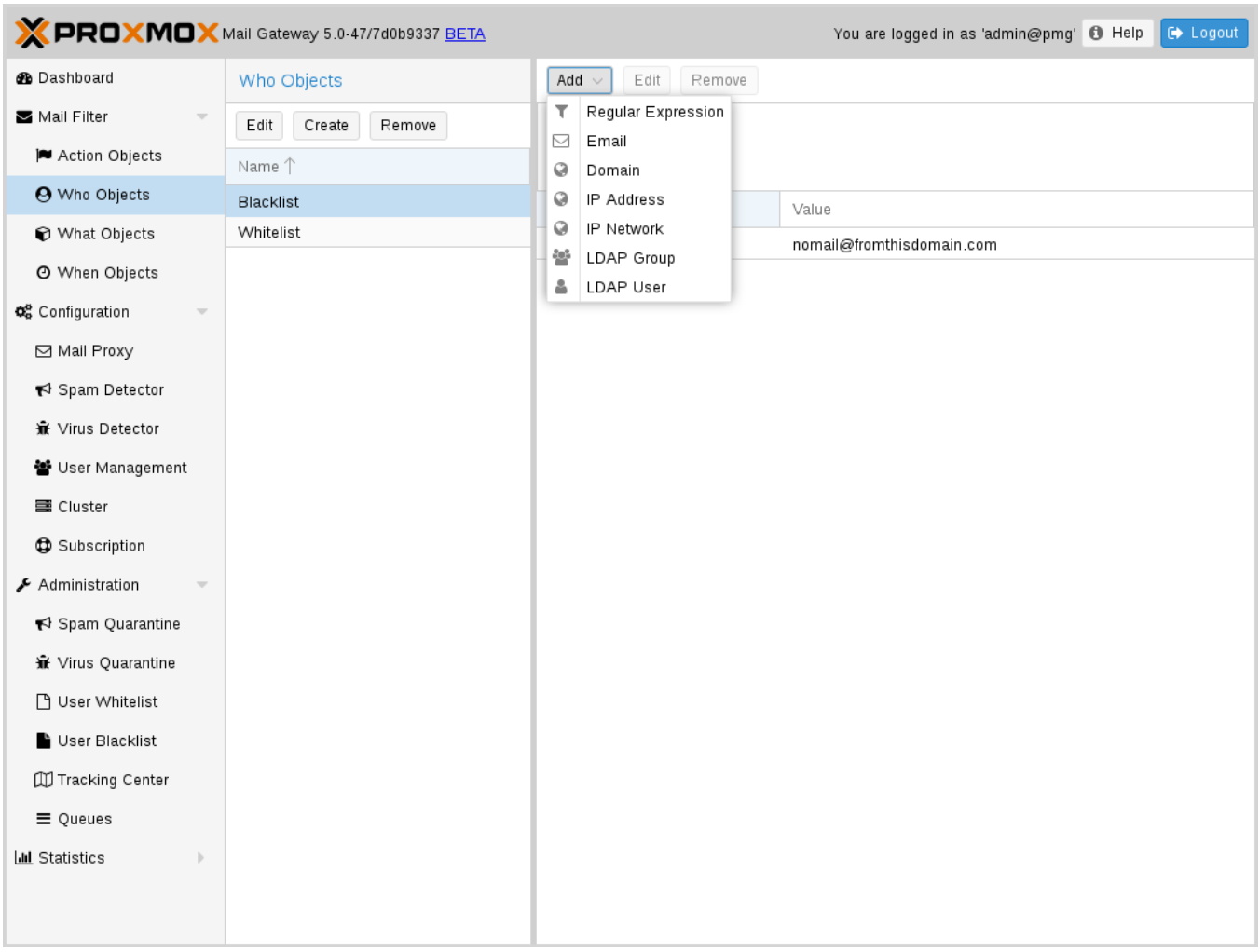
5.1.7 Remove attachments

Remove attachments can either remove all attachments, or only those matched by the rules *WHAT* object. You can also specify the replacement text if you want.

5.1.8 Disclaimer

Add a Disclaimer.

5.2 WHO - objects



This type of objects can be used for the *TO* and/or *FROM* category, and macth the sender or receiver of the e-mail. A single object can combine multiple items, and the following item types are available:

EMail
: Allows you to match a single mail address.

Domain
: Only match the domain part of the mail address.

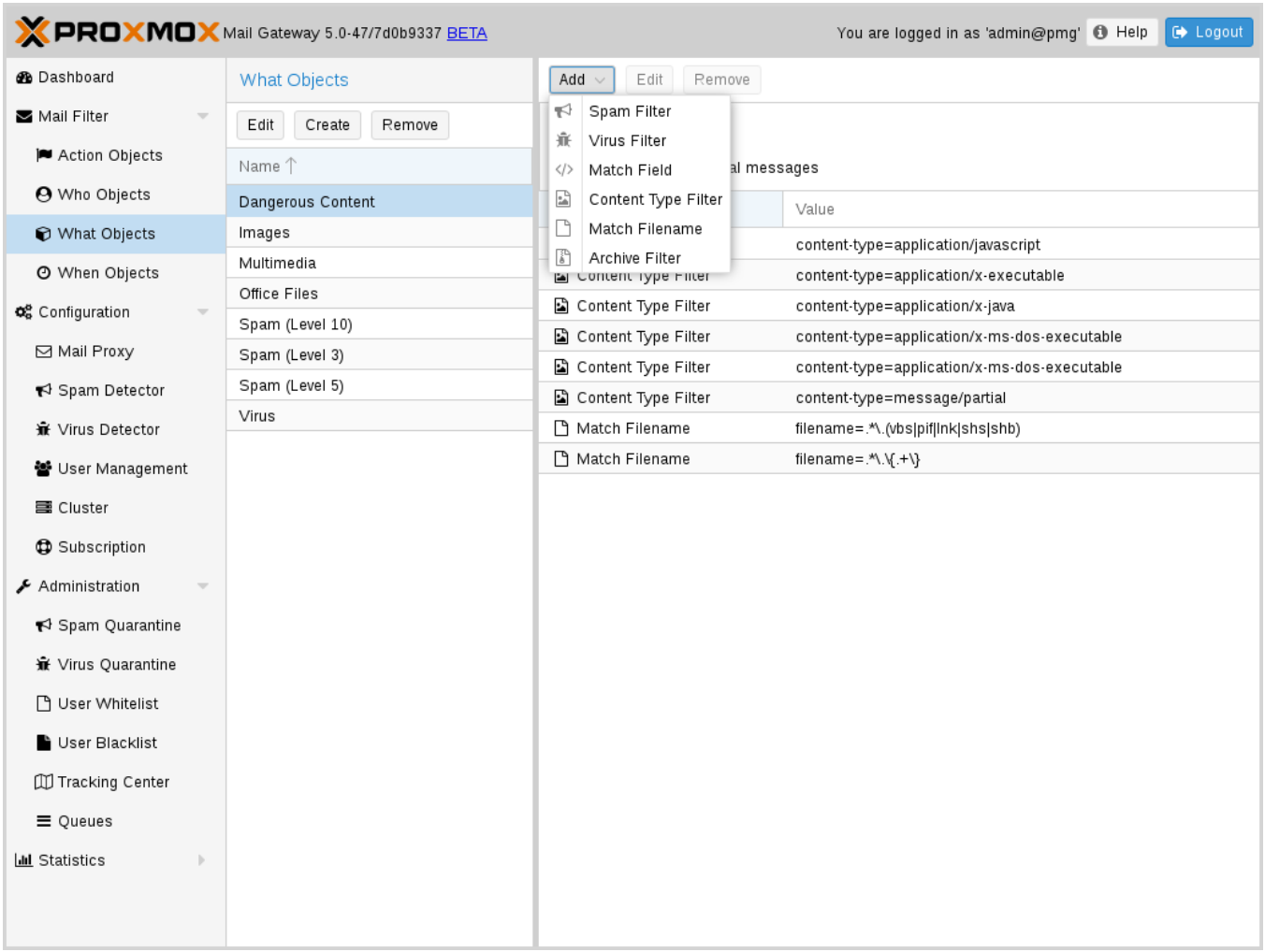
Regular Expression
This one uses a regular expression to match the whole mail address.

IP Address or Network
This can be used to match the senders IP address.

LDAP User or Group
Test if the mail address belong to a specific LDAP user or group.

We have two important WHO objects called *Blacklist* and *Whitelist*. Those are used in the default ruleset to globally block or allow specific senders.

5.3 WHAT - objects



WHAT - objects are used to classify the mail content. A single object can combine multiple items, and the following item types are available:

Spam Filter
Matches if configured value if greater than the detected spam level.

Virus Filter
Matches on infected mails.

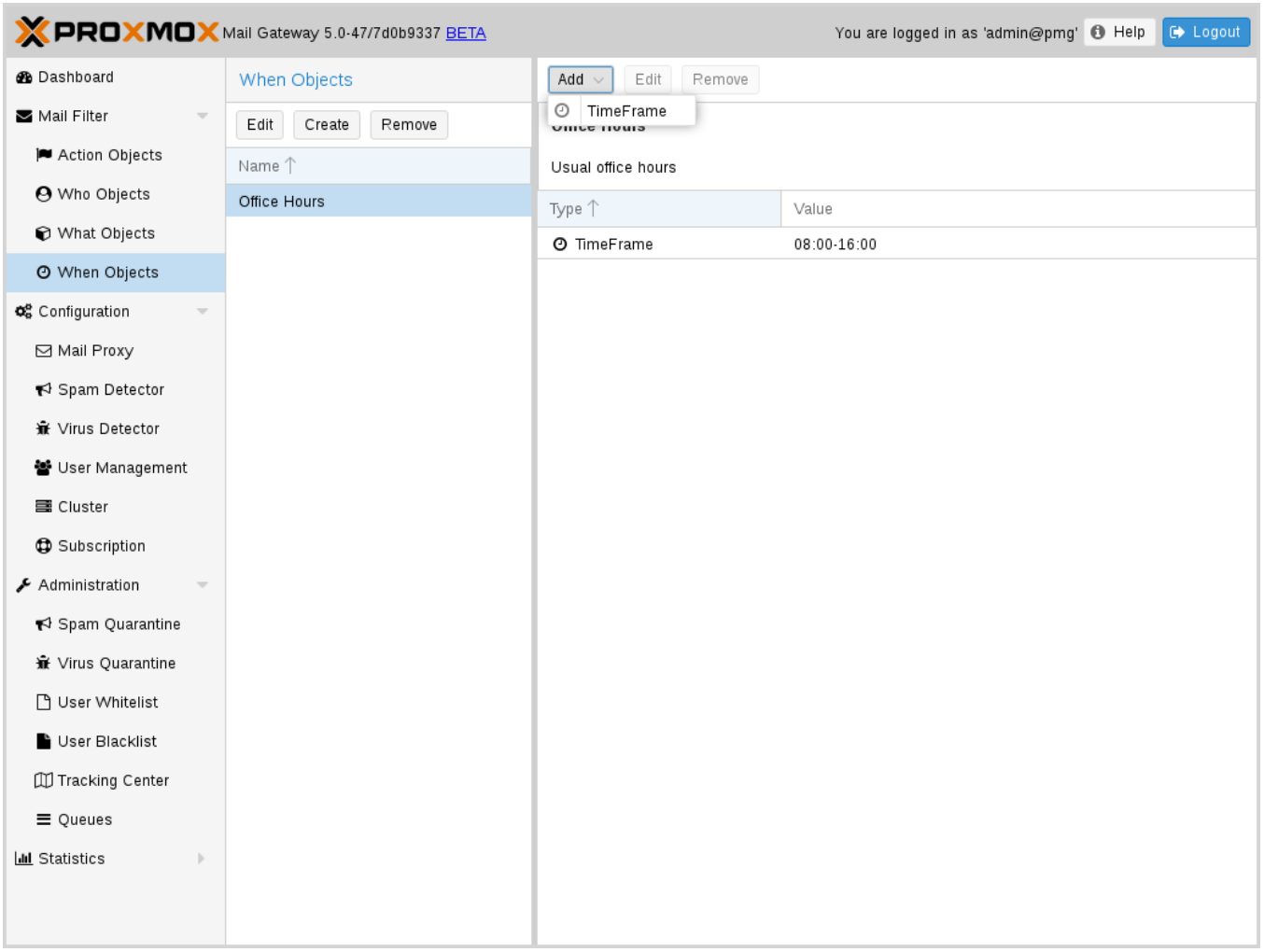
Match Field
Match specified mail header fields (eg. `Subject:`, `From:`, ...)

Content Type Filter
Can be used to match specific content types.

Match Filename
Uses regular expressions to match attachment filenames.

Archive Filter
Can be used to match specific content types inside archives.

5.4 WHEN - objects



WHEN - objects are use to activate rules at specific daytimes. You can compose them of one or more time-frame items.

The default ruleset defines *Office Hours*, but this is not used by the default rules.

5.5 Using regular expressions

A regular expression is a string of characters which tells us which string you are looking for. The following is a short introduction in the syntax of regular expressions used by some objects. If you are familiar with Perl, you already know the syntax.

5.5.1 Simple regular expressions

In its simplest form, a regular expression is just a word or phrase to search for. `Mail` would match the string "Mail". The search is case sensitive so "MAIL", "Mail", "mail" would not be matched.

5.5.2 Metacharacters

Some characters have a special meaning. These characters are called metacharacters. The Period (`.`) is a commonly used metacharacter. It matches exactly one character, regardless of what the character is. `e.mail` would match either "e-mail" or "e-mail" or "e2mail" but not "e-some-mail".

The question mark (`?`) indicates that the character immediately preceding it either zero or one time. `e?mail` would match either "email" or "mail" but not "e-mail".

Another metacharacter is the star (`*`). This indicates that the character immediately to its left may repeated any number of times, including zero. `e*mail` would match either "email" or "mail" or "eeemail".

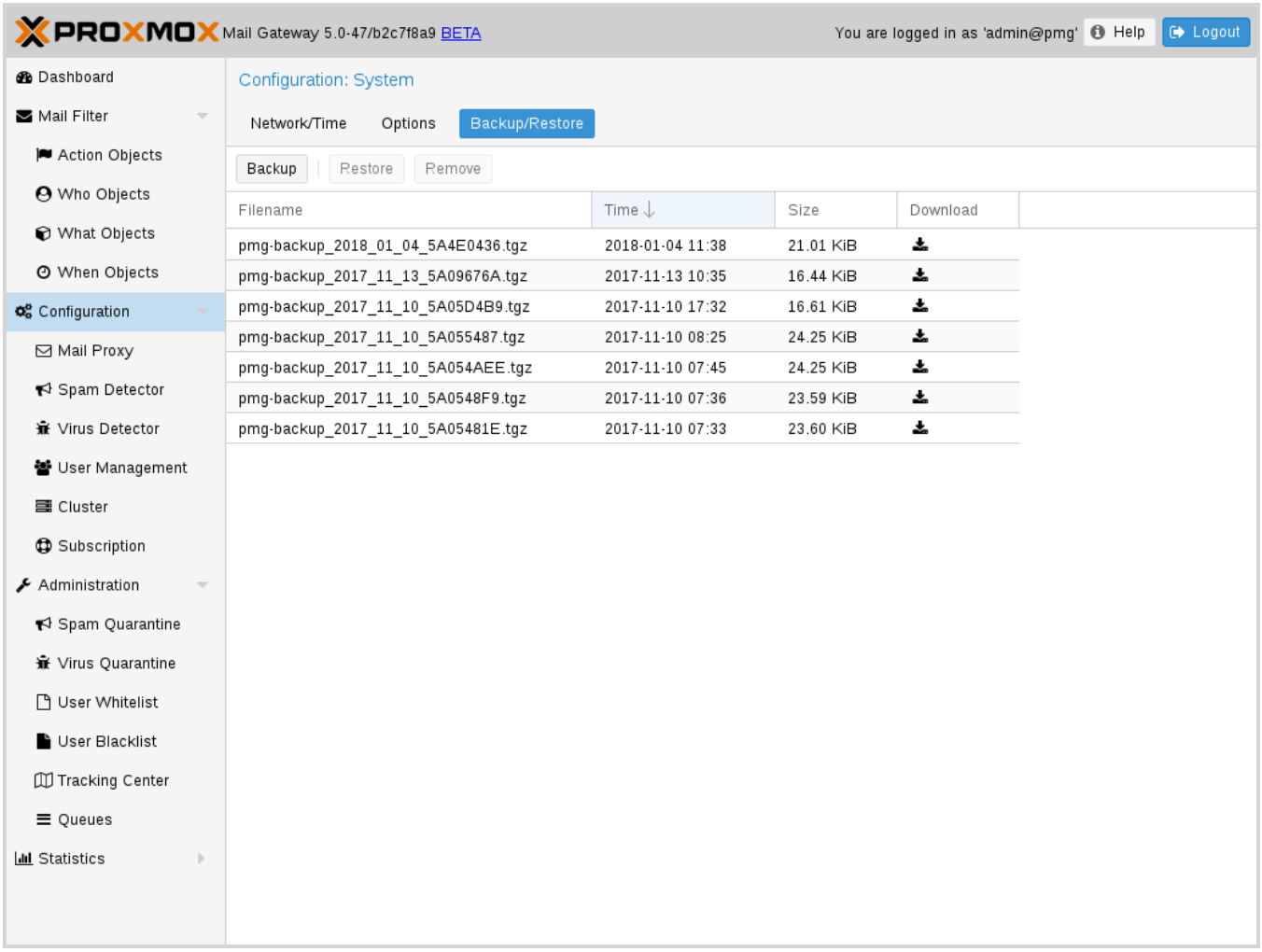
The plus (+) metacharacter does the same as the star (*) excluding zero. So `e+mail` does not match "mail".

Metacharacters may be combined. A common combination includes the period and star metacharacters (`.*`), with the star immediately following the period. This is used to match an arbitrary string of any length, including the null string. For example: `.*company.*` matches "company@domain.com" or "company@domain.co.uk" or "department.company@domain.com".

The book [Friedl97] provides a more comprehensive introduction.

Chapter 6

Backup and Restore



Proxmox Mail Gateway includes the ability to backup and restore the configuration. This includes the complete config from `/etc/pmg/`, the mail filter rules and the statistic database.

Note
The backup does not include the network setup, and also no mail data from the postfix queue or the spam or virus quarantine.

You can create a backup by simply pressing the *Backup* button on the GUI, or by using the command line interface:

```
# pmgbackup backup
starting backup to: /var/lib/pmg/backup/pmg-backup_2018_01_04_5A4E0436.tgz
backup finished
```

Backups are stored inside directory `/var/lib/pmg/backup/`. It is usually best to mount a remote file system to that directory, so that the resulting backups gets stored remotely.

You can list the contents of that directory with:

```
# pmgbackup list
....
pmg-backup_2017_11_10_5A05D4B9.tgz      17012
pmg-backup_2017_11_13_5A09676A.tgz      16831
pmg-backup_2018_01_04_5A4E0436.tgz      21514
```

Restores are also possible using the GUI or command line, and you can select what parts you want to restore:

System Configuration
: Basically the contents of `/etc/pmg/`.

Rule Database
: The mail filter rule database.

Statistic
: All statistical data.

For examply, you can selectively restore the mail filter rules from an older backup:

```
# pmgbackup restore --filename pmg-backup_2018_01_04_5A4E0436.tgz -- ↩
   database
starting restore: /var/lib/pmg/backup/pmg-backup_2018_01_04_5A4E0436.tgz
config_backup.tar: OK
Proxmox_ruledb.sql: OK
Proxmox_statdb.sql: OK
version.txt: OK
Destroy existing rule database
Create new database
run analyze to speed up database queries
Analyzing/Upgrading existing Databases...done
restore finished
```

Chapter 7

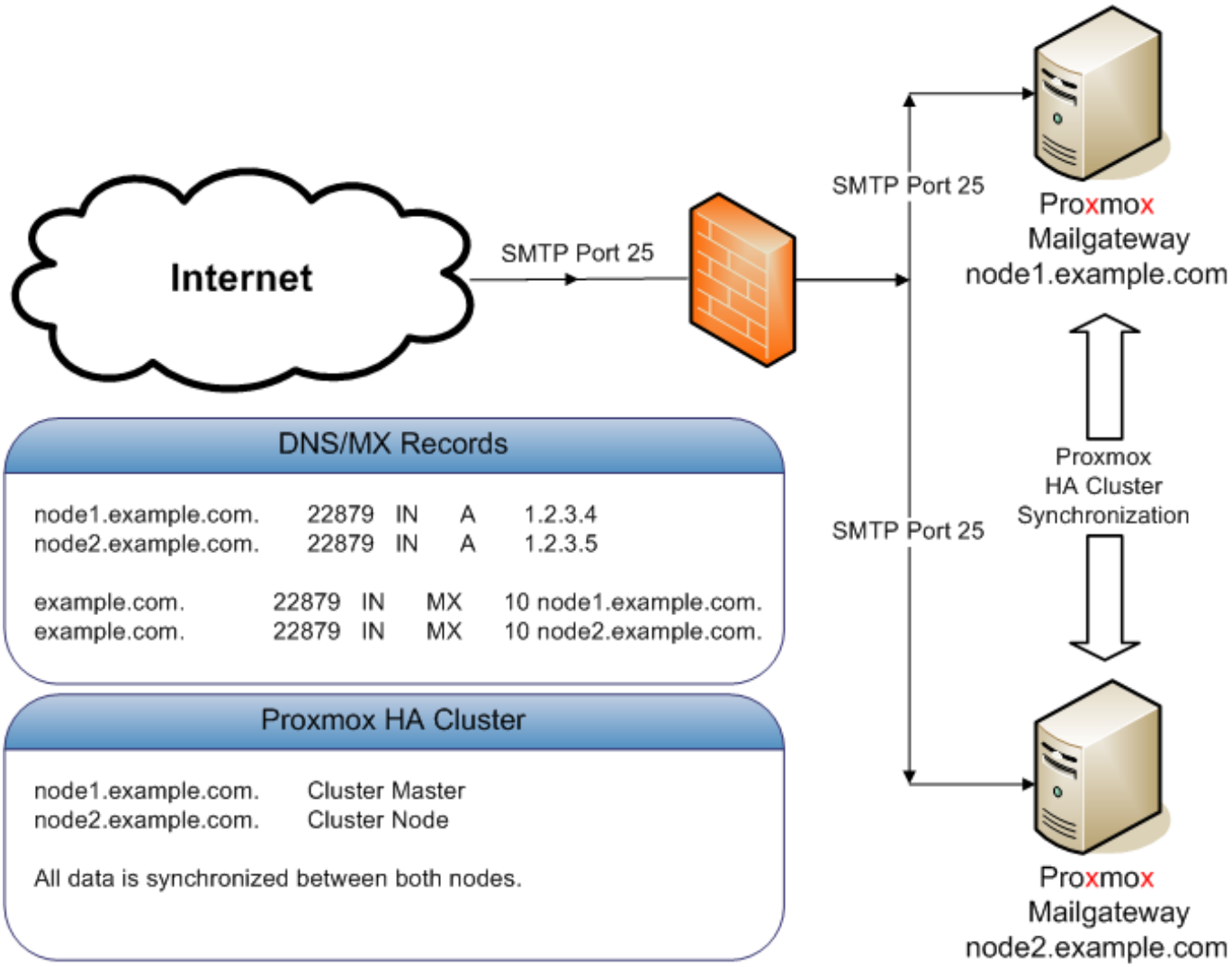
Cluster Management

We are living in a world where email becomes more and more important - failures in email systems are just not acceptable. To meet these requirements we developed the Proxmox HA (High Availability) Cluster.

The Proxmox Mail Gateway HA Cluster consists of a master and several slave nodes (minimum one node). Configuration is done on the master. Configuration and data is synchronized to all cluster nodes over a VPN tunnel. This provides the following advantages:

- centralized configuration management
- fully redundant data storage
- high availability
- high performance

We use a unique application level clustering scheme, which provides extremely good performance. Special considerations where taken to make management as easy as possible. Complete Cluster setup is done within minutes, and nodes automatically reintegrate after temporary failures without any operator interaction.



7.1 Hardware requirements

There are no special hardware requirements, although it is highly recommended to use fast and reliable server with redundant disks on all cluster nodes (Hardware RAID with BBU and write cache enabled).

The HA Cluster can also run in virtualized environments.

7.2 Subscriptions

Each host in a cluster has its own subscription. If you want support for a cluster, each cluster node needs to have a valid subscription. All nodes must have the same subscription level.

7.3 Load balancing

It is usually advisable to distribute mail traffic among all cluster nodes. Please note that this is not always required, because it is also reasonable to use only one node to handle SMTP traffic. The second node is used as quarantine host, and only provides the web interface to the user quarantine.

The normal mail delivery process looks up DNS Mail Exchange (MX) records to determine the destination host. A MX record tells the sending system where to deliver mail for a certain domain. It is also possible to have several MX records for a single domain, they can have different priorities. For example, our MX record looks like that:

```
# dig -t mx proxmox.com

;; ANSWER SECTION:
proxmox.com.            22879   IN      MX      10 mail.proxmox.com.

;; ADDITIONAL SECTION:
mail.proxmox.com.       22879   IN      A       213.129.239.114
```

Please notice that there is one single MX record for the Domain proxmox.com, pointing to mail.proxmox.com. The dig command automatically puts out the corresponding address record if it exists. In our case it points to 213.129.239.114. The priority of our MX record is set to 10 (preferred default value).

7.3.1 Hot standby with backup MX records

Many people do not want to install two redundant mail proxies, instead they use the mail proxy of their ISP as fall-back. This is simply done by adding an additional MX Record with a lower priority (higher number). With the example above this looks like that:

```
proxmox.com.            22879   IN      MX      100 mail.provider.tld.
```

Sure, your provider must accept mails for your domain and forward received mails to you. Please note that such setup is not really advisable, because spam detection needs to be done by that backup MX server also, and external servers provided by ISPs usually don't do that.

You will never lose mails with such a setup, because the sending Mail Transport Agent (MTA) will simply deliver the mail to the backup server (mail.provider.tld) if the primary server (mail.proxmox.com) is not available.

Note
Any resononable mail server retries mail devivery if the target server is not available, i.e. Proxmox Mail Gateway stores mail and retries delivery for up to one week. So you will not loose mail if you mail server is down, even if you run a single server setup.

7.3.2 Load balancing with MX records

Using your ISPs mail server is not always a good idea, because many ISPs do not use advanced spam prevention techniques, or do not filter SPAM at all. It is often better to run a second server yourself to avoid lower spam detection rates.

Anyways, it's quite simple to set up a high performance load balanced mail cluster using MX records. You just need to define two MX records with the same priority. I will explain this using a complete example to make it clearer.

First, you need to have at least 2 working Proxmox Mail Gateway servers (mail1.example.com and mail2.example.co configured as cluster (see section Cluster administration Section 7.4 below), each having its own IP address. Let us assume the following addresses (DNS address records):

```
mail1.example.com.        22879   IN      A       1.2.3.4
mail2.example.com.        22879   IN      A       1.2.3.5
```

Btw, it is always a good idea to add reverse lookup entries (PTR records) for those hosts. Many email systems nowadays reject mails from hosts without valid PTR records. Then you need to define your `MX` records:

```
example.com.              22879   IN      MX      10 mail1.example.com.
example.com.              22879   IN      MX      10 mail2.example.com.
```

This is all you need. You will receive mails on both hosts, more or less load-balanced using round-robin scheduling. If one host fails the other is used.

7.3.3 Other ways

Multiple address records

Using several DNS `MX` record is sometime clumsy if you have many domains. It is also possible to use one `MX` record per domain, but multiple address records:

```
example.com.              22879   IN      MX      10 mail.example.com.
mail.example.com.         22879   IN      A       1.2.3.4
mail.example.com.         22879   IN      A       1.2.3.5
```

Using firewall features

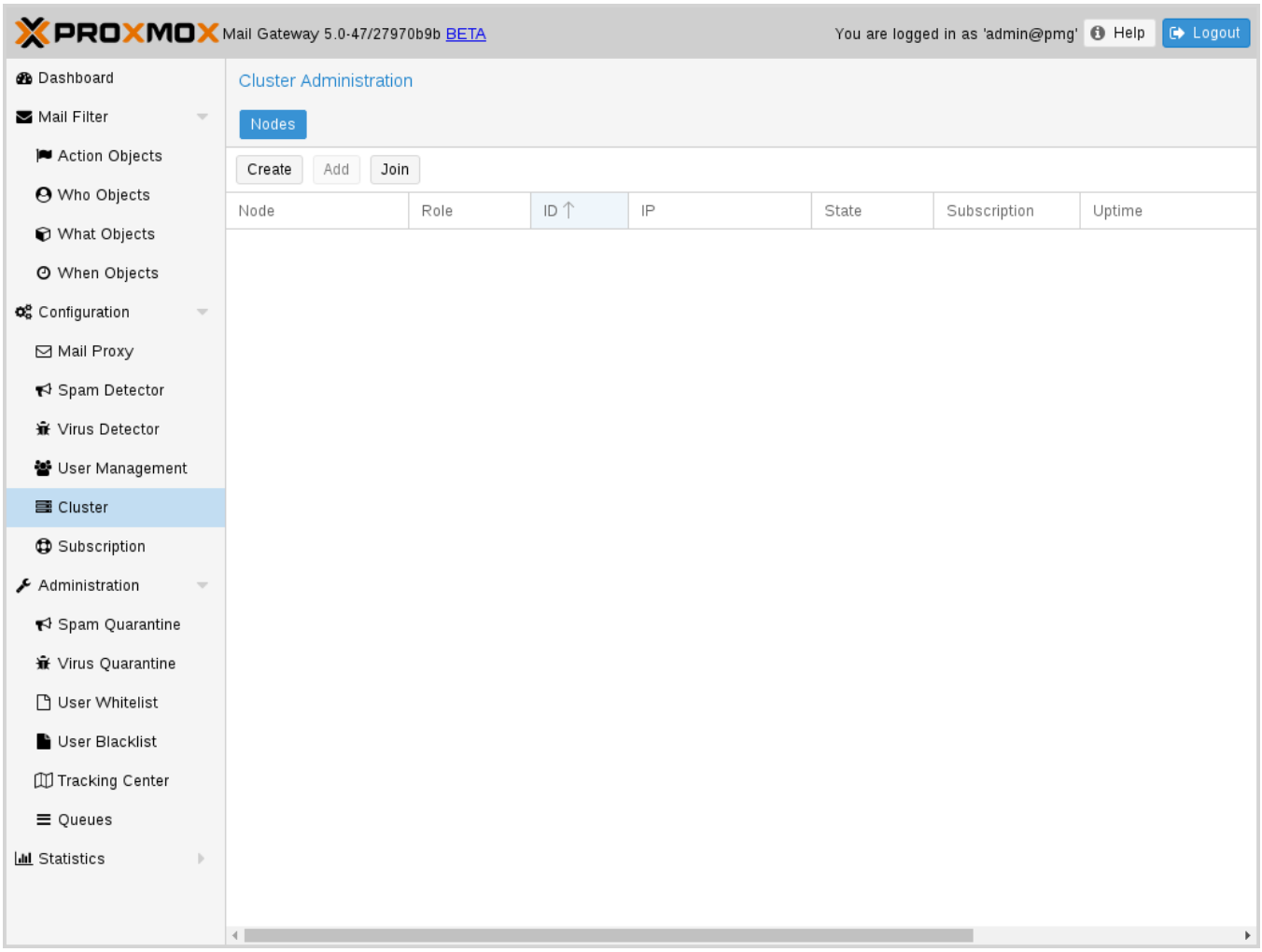
Many firewalls can do some kind of RR-Scheduling (round-robin) when using DNAT. See your firewall manual for more details.

7.4 Cluster administration

Cluster administration can be done on the GUI or using the command line utility `pmgcm`. The CLI tool is a bit more verbose, so we suggest to use that if you run into problems.

Note
Always setup the IP configuration before adding a node to the cluster. IP address, network mask, gateway address and hostname can't be changed later.

7.4.1 Creating a Cluster



You can create a cluster from any existing Proxmox host. All data is preserved.

- make sure you have the right IP configuration (IP/MASK/GATEWAY/HOSTNAME), because you cannot change that later
- press the create button on the GUI, or run the cluster creation command:

```
pmgcm create
```

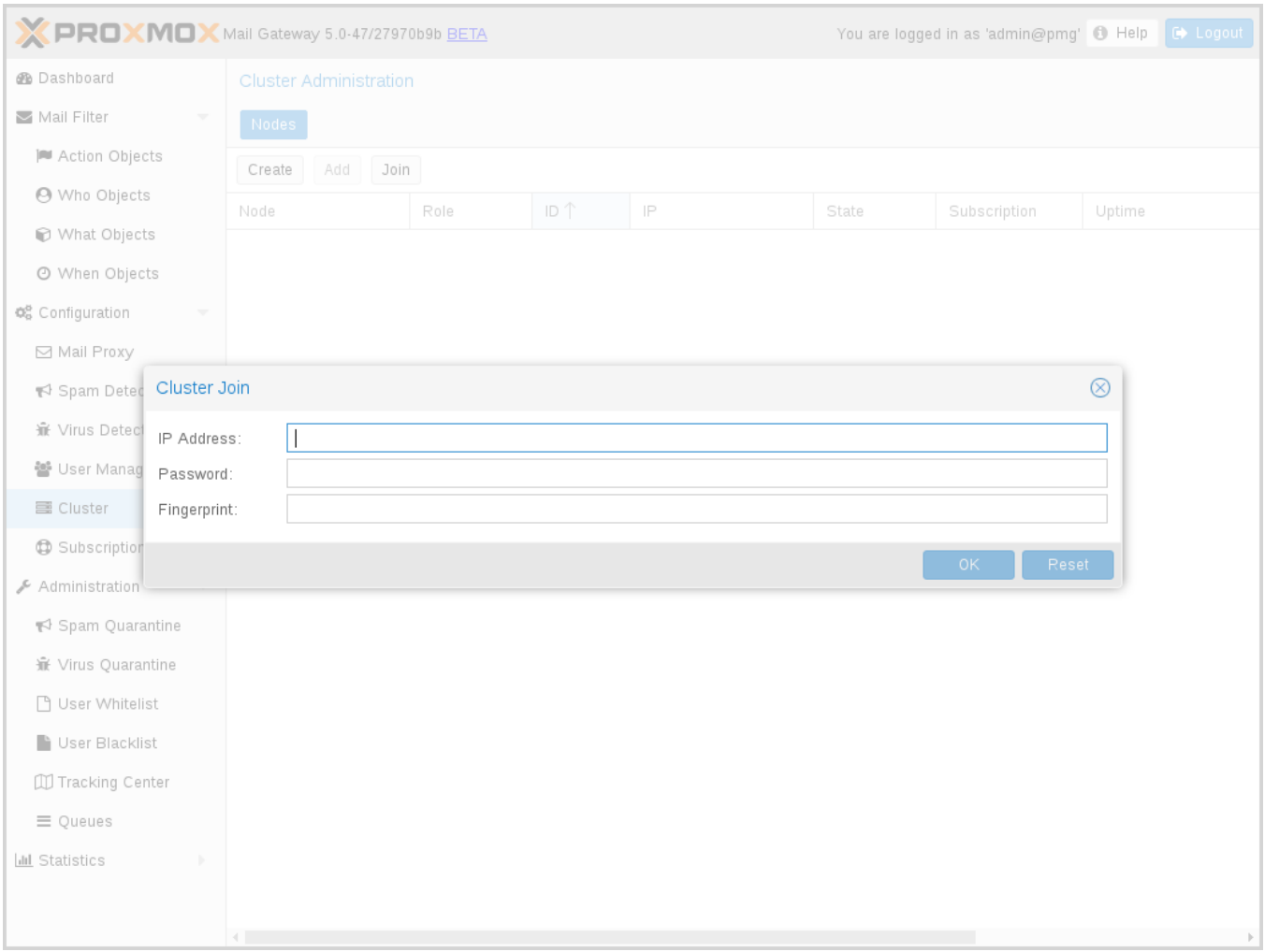
Note
The node where you run the cluster create command will be the *master* node.

7.4.2 Show Cluster Status

The GUI shows the status of all cluster nodes, and it is also possible to use the command line tool:

```
pmgcm status
--NAME(CID)--------------IPADDRESS----ROLE-STATE---------UPTIME---LOAD---- ↩
   MEM---DISK
pmg5(1)                192.168.2.127   master A       1 day 21:18    0.30     ↩
   80%    41%
```

7.4.3 Adding Cluster Nodes



When you add a new node to a cluster (join) all data on that node is destroyed. The whole database is initialized with cluster data from the master.

- make sure you have the right IP configuration
- run the cluster join command (on the new node):

```
pmgcm join <master_ip>
```

You need to enter the root password of the master host when asked for a password. When joining a cluster using the GUI, you also need to enter the *fingerprint* of the master node. You get that information by pressing the `Join` button on the master node.

Caution
Node initialization deletes all existing databases, stops and then restarts all services accessing the database. So do not add nodes which are already active and receive mails.

Also, joining a cluster can take several minutes, because the new node needs to synchronize all data from the master (although this is done in the background).

Note
If you join a new node, existing quarantined items from the other nodes are not synchronized to the new node.

7.4.4 Deleting Nodes

Please detach nodes from the cluster network before removing them from the cluster configuration. Then run the following command on the master node:

```
pmgcm delete <cid>
```

Parameter `<cid>` is the unique cluster node ID, as listed with `pmgcm status`.

7.4.5 Disaster Recovery

It is highly recommended to use redundant disks on all cluster nodes (RAID). So in almost any circumstances you just need to replace the damaged hardware or disk. Proxmox Mail Gateway uses an asynchronous clustering algorithm, so you just need to reboot the repaired node, and everything will work again transparently.

The following scenarios only apply when you really loose the contents of the hard disk.

Single Node Failure

- delete failed node on master

```
pmgcm delete <cid>
```

- add (re-join) a new node

```
pmgcm join <master_ip>
```

Master Failure

- force another node to be master

```
pmgcm promote
```

- tell other nodes that master has changed

```
pmgcm sync --master_ip <master_ip>
```

Total Cluster Failure

- restore backup (Cluster and node information is not restored, you have to recreate master and nodes)
- tell it to become master

```
pmgcm create
```

- install new nodes
- add those new nodes to the cluster

```
pmgcm join <master_ip>
```

Chapter 8

Important Service Daemons

8.1 pmgdaemon - Proxmox Mail Gateway API Daemon

This daemon exposes the whole Proxmox Mail Gateway API on `127.0.0.1:85`. It runs as `root` and has permission to do all privileged operations.

Note
The daemon listens to a local address only, so you cannot access it from outside. The `pmgproxy` daemon exposes the API to the outside world.

8.2 pmgproxy - Proxmox Mail Gateway API Proxy Daemon

This daemon exposes the whole Proxmox Mail Gateway API on TCP port 8006 using HTTPS. It runs as user `www-data` and has very limited permissions. Operation requiring more permissions are forwarded to the local `pmgdaemon`.

Requests targeted for other nodes are automatically forwarded to those nodes. This means that you can manage your whole cluster by connecting to a single Proxmox Mail Gateway node.

8.2.1 Alternative HTTPS certificate

By default, pmgproxy uses the certificate `/etc/pmg/pmg-api.pem` for HTTPS connections. This certificate is a self signed certificate, and therefor not trusted by browsers and operating systems by default. You can simply replace this certificate with your own (please include the key inside the *.pem* file).

8.3 pmg-smtp-filter - Proxmox SMTP Filter Daemon

This is the Proxmox SMTP filter daemon, which does the actual SPAM filtering using the SpamAssassin and the rule database. It listens on 127.0.0.1:10023 and 127.0.0.1:10024. The daemon listens to a local address only, so you cannot access it from outside.

With our postfix configuration, incoming mails are sent to 127.0.0.1:10024. Outgoing (trusted) mails are sent to 127.0.0.1:10023. After filtering, mails are reinjected into postfix at 127.0.0.1:10025.

8.4 pmgpolicy - Proxmox Mail Gateway Policy Daemon

This daemon implements the Postfix SMTP access policy delegation protocol on `127.0.0.1:10022`. The daemon listens to a local address only, so you cannot access it from outside. We configure Postfix to use this service for greylisting and as SPF policy server.

8.5 pmgtunnel - Cluster Tunnel Daemon

This daemon creates a ssh tunnel to the postgres database in other cluster nodes (port 5432). The tunnel is used to synchronize the database using an application specific asynchronous replication algorythm.

8.6 pmgmirror - Database Mirror Daemon

Proxmox Mail Gateway use an application specific asynchronous replication algorythm to replicate the database to all cluster nodes.

The daemon uses the ssh tunnel provided by *pmgtunnel* to access the database on remote nodes.

Chapter 9

Useful Command Line Tools

9.1 Database Management Toolkit

Toolkit to simplify common database management tasks.

9.2 API Shell

Toolkit to access the Proxmox Mail Gateway API via the command line.

9.2.1 Examples

List entries:

```
# pmgsh ls /
```

Call method *GET* on an specific API path:

```
# pmgsh get /version
```

View current mail configuration:

```
# pmgsh get /config/mail
```

Get help for a specific path:

```
# pmgsh help /config/mail  -v
```

Disable option *spf* in */config/mail*

```
# pmgsh set /config/mail  -spf 0
```

Delete *spf* setting from */config/mail*

```
# pmgsh set /config/mail  -delete spf
```

9.3 Proxmox Mail Gateway Version Info

Print version information for Proxmox Mail Gateway packages.

9.3.1 Examples

Print Proxmox Mail Gateway version:

```
# pmgversion
```

List version details for important packages:

```
# pmgversion -v
```

Please use the Debian package management for details about other packages

```
# dpkg -l
```

9.4 pmgsubscription - Subscription Management

This tool is used to handle Proxmox Mail Gateway subscriptions.

9.5 Proxmox Simple Performance Benchmark

The command line tool `pmgperf` tries to gather some general performance data. This is mostly useful for debugging and to identify performance bottlenecks. It computes the following metrics:

CPU BOGOMIPS	bogomips sum of all CPUs
REGEX/SECOND	regular expressions per second (perl performance test), should be above 1000000.
HD SIZE	harddisk size
BUFFERED READS	simple HD read test. Modern HDs should reach at least 100 MB/sec
AVERAGE SEEK TIME	tests average seek time. Fast SCSI HDs reach values < 8 milliseconds. Common IDE/SATA disks get values from 15 to 20 ms. SSD seek times should be below 1ms.
FSYNCS/SECOND	value should be greater than 200 (you should enable *write back* cache mode on you RAID controller - needs a battery backed cache (BBWC)).
DNS EXT	average time to resolve an external DNS name
DNS INT	average time to resolve a local DNS name

Here is an example output generated by the tool:

```
# pmgperf
CPU BOGOMIPS:      16759.60
REGEX/SECOND:      1186304
HD SIZE:           60.78 GB (/dev/sda1)
BUFFERED READS:    209.84 MB/sec
AVERAGE SEEK TIME: 1.24 ms
FSYNCS/SECOND:     2198.79
DNS EXT:           35.69 ms
DNS INT:           1.41 ms (yourdomain.tld)
```

9.6 Quarantine Management Toolkit

Toolkit to manage spam an virus quarantine, and send spam report mails.

9.7 Send daily system report email

This binary generates and send daily system report email.

9.8 Upgrade Proxmox Mail Gateway

This is a small wrapper around `apt-get dist-upgrade`. We use this to print additional information (kernel restart required?), and optionally run an interactive shell after the update. This binary is invoked when starting an upgrade using the web GUI.

If you are already logged in on the console, it is peferable to invoke `apt-get` directly.

```
# apt-get dist-upgrade
```

9.9 `nmap` - Port Scans

`nmap` is designed to allow system administrators to scan large networks to determine which hosts are up and what services they are offering. You can use nmap to test your firewall setting, for example to see if the required ports are open.

Test Razor port (tcp port 2703):

```
# nmap -P0 -sS -p 2703 c301.cloudmark.com

Starting Nmap 5.00 ( http://nmap.org ) at 2012-07-31 11:10 CEST
Interesting ports on c301.cloudmark.com (208.83.137.114):
PORT     STATE SERVICE
2703/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

See the manual page (`man nmap`) for more information about nmap.

Chapter 10

Bibliography

10.1 Books about mail processing technology

[1] [KyleDDent04] Kyle D Dent. Postfix: The Definitive Guide. O'Reilly & Associates, 2004. ISBN 978-0596002121

[2] [Schwartz04] Alan Schwartz. SpamAssassin. O'Reilly & Associates, 2004. ISBN 978-0596007072

10.2 Books about related technology

[3] [Hertzog13] Raphaël Hertzog & Roland Mas. The Debian Administrator's Handbook: Debian Jessie from Discovery to Mastery, Freexian, 2013. ISBN 979-1091414050

[4] [Bir96] Kenneth P. Birman. Building Secure and Reliable Network Applications. Manning Publications Co, 1996. ISBN 978-1884777295

[5] [Walsh10] Norman Walsh. DocBook 5: The Definitive Guide. O'Reilly & Associates, 2010. ISBN 978-0596805029

[6] [Richardson07] Leonard Richardson & Sam Ruby. RESTful Web Services. O'Reilly Media, 2007. ISBN 978-0596529260

[7] [Friedl97] Jeffrey E. F. Friedl. Mastering Regular Expressions. O'Reilly & Associates, 2006. ISBN 978-0596528126

[8] [Mauerer08] Wolfgang Mauerer. Professional Linux Kernel Architecture. John Wiley & Sons, 2008. ISBN 978-0470343432

[9] [Loshin03] Pete Loshin, IPv6: Theory, Protocol, and Practice, 2nd Edition. Morgan Kaufmann, 2003. ISBN 978-1558608108

[10] [Loeliger12] Jon Loeliger & Matthew McCullough. Version Control with Git: Powerful tools and techniques for collaborative software development. O'Reilly and Associates, 2012. ISBN 978-1449316389

[11] [Ahmed16] Wasim Ahmed. Mastering Proxmox - Second Edition. Packt Publishing, 2016. ISBN 978-1785888243

10.3 Books about related topics

[12] [Bessen09] James Bessen & Michael J. Meurer, Patent Failure: How Judges, Bureaucrats, and Lawyers Put Innovators at Risk. Princeton Univ Press, 2009. ISBN 978-0691143217

Appendix A

SSL certificate

Access to the administration web interface is always done via `https`. The default certificate is never valid for your browser and you get always warnings.

If you want to get rid of these warnings, you have to generate a valid certificate for your server.

Login to your Proxmox via ssh or use the console:

```
openssl req -newkey rsa:2048 -nodes -keyout key.pem -out req.pem
```

Follow the instructions on the screen, see this example:

```
Country Name (2 letter code) [AU]: AT
State or Province Name (full name) [Some-State]:Vienna
Locality Name (eg, city) []:Vienna
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Proxmox GmbH
Organizational Unit Name (eg, section) []:Proxmox Mail Gateway
Common Name (eg, YOUR name) []: yourproxmox.yourdomain.com
Email Address []:support@yourdomain.com

Please enter the following 'extra' attributes to be sent with your ↩
   certificate request
A challenge password []: not necessary
An optional company name []: not necessary
```

After you finished this certificate request you have to send the file `req.pem` to your Certification Authority (CA). The CA will issue the certificate (BASE64 encoded) based on your request – save this file as `cert.pem` to your Proxmox.

To activate the new certificate, do the following on your Proxmox:

```
cat key.pem cert.pem >/etc/pmg/pmg-api.pem
```

The restart the API servers

```
systemctl restart pmgproxy
```

Test your new certificate by using your browser.

Note
To transfer files from and to your Proxmox, you can use secure copy: If you desktop is Linux, you can use the `scp` command line tool. If your desktop PC is windows, please use a scp client like WinSCP (see http://winscp.net/).

Appendix B

Command Line Interface

B.1 pmgbackup - Proxmox Mail Gateway Backup and Restore Utility

pmgbackup `<COMMAND> [ARGS] [OPTIONS]`

pmgbackup backup `[OPTIONS]`

Backup the system configuration.

`--statistic <boolean>` (*default =* `1`)
: Backup statistic databases.

pmgbackup help `[<cmd>] [OPTIONS]`

Get help about specified command.

`<cmd>: <string>`
: Command name

`--verbose <boolean>`
: Verbose output format.

pmgbackup list

pmgbackup restore `--filename <string> [OPTIONS]`

Restore the system configuration.

`--config <boolean>` (*default =* `0`)
: Restore system configuration.

`--database <boolean>` (*default =* `1`)
: Restore the rule database. This is the default.

`--filename pmg-backup_[0-9A-Za-z_-]+\.tgz`
: The backup file name.

`--statistic <boolean>` (*default =* `0`)
: Restore statistic databases. Only considered when you restore the *database*.

B.2 pmgcm - Proxmox Mail Gateway Cluster Management Toolkit

pmgcm <COMMAND> [ARGS] [OPTIONS]

pmgcm create

Create initial cluster config with current node as master.

pmgcm help [<cmd>] [OPTIONS]

Get help about specified command.

<cmd>: <string>
Command name

--verbose <boolean>
Verbose output format.

pmgcm join <master_ip> [OPTIONS]

Join a new node to an existing cluster.

<master_ip>: <string>
IP address.

--fingerprint ^(:?[A-Z0-9][A-Z0-9]:){31}[A-Z0-9][A-Z0-9]$
SSL certificate fingerprint.

pmgcm join_cmd

Prints the command for joining an new node to the cluster. You need to execute the command on the new node.

pmgcm status [OPTIONS]

Cluster node status.

--list_single_node <boolean> (*default =* 0)
List local node if there is no cluster defined. Please note that RSA keys and fingerprint are not valid in that case.

pmgcm sync [OPTIONS]

Synchronize cluster configuration.

--master_ip <string>
Optional IP address for master node.

B.3 pmgsh - API Shell

Interactive session:

pmgsh

Directly call API functions:

pmgsh (get|set|create|help) <path> [OPTIONS]

B.4 pmgperf - Proxmox Simple Performance Benchmark

pmgperf `help`

pmgperf `[<path>]`

Proxmox benchmark.

<path>: <string> (*default = /*)
File system location to test.

B.5 pmgconfig - Configuration Management Toolkit

pmgconfig `<COMMAND> [ARGS] [OPTIONS]`

pmgconfig apicert `[OPTIONS]`

Generate /etc/pmg/pmg-api.pem (self signed certificate for GUI and REST API).

--force <boolean> (*default =* 0)
Overwrite existing certificate.

pmgconfig dump

Print configuration setting which can be used in templates.

pmgconfig help `[<cmd>] [OPTIONS]`

Get help about specified command.

<cmd>: <string>
Command name

--verbose <boolean>
Verbose output format.

pmgconfig init

Generate required files in /etc/pmg/

pmgconfig ldapsync

Syncronize the LDAP database.

pmgconfig sync `[OPTIONS]`

Syncronize Proxmox Mail Gateway configurations with system configuration.

--restart <boolean> (*default =* 0)
Restart services if necessary.

pmgconfig tlscert `[OPTIONS]`

Generate /etc/pmg/pmg-tls.pem (self signed certificate for encrypted SMTP traffic).

--force <boolean> (*default =* 0)
Overwrite existing certificate.

B.6 pmgdb - Database Management Toolkit

pmgdb <COMMAND> [ARGS] [OPTIONS]

pmgdb delete

Delete PMG rule database.

pmgdb dump

Print the PMG rule database.

pmgdb help [<cmd>] [OPTIONS]

Get help about specified command.

<cmd>: <string>
Command name

--verbose <boolean>
Verbose output format.

pmgdb init [OPTIONS]

Initialize/Upgrade the PMG rule database.

--force <boolean> (***default =*** 0)
Delete existing database.

--statistics <boolean> (***default =*** 0)
Reset and update statistic database.

pmgdb reset

Reset PMG rule database back to factory defaults.

pmgdb update

Update the PMG statistic database.

Appendix C

Service Daemons

C.1 pmgdaemon - Proxmox Mail Gateway API Daemon

pmgdaemon <COMMAND> [ARGS] [OPTIONS]

pmgdaemon help [<cmd>] [OPTIONS]

Get help about specified command.

<cmd>: <string>
Command name

--verbose <boolean>
Verbose output format.

pmgdaemon restart

Restart the daemon (or start if not running).

pmgdaemon start [OPTIONS]

Start the daemon.

--debug <boolean> (*default =* 0)
Debug mode - stay in foreground

pmgdaemon status

Get daemon status.

pmgdaemon stop

Stop the daemon.

C.2 pmgproxy - Proxmox Mail Gateway API Proxy Daemon

pmgproxy <COMMAND> [ARGS] [OPTIONS]

pmgproxy help [<cmd>] [OPTIONS]

Get help about specified command.

<cmd>: <string>
Command name

--verbose <boolean>
Verbose output format.

pmgproxy restart

Restart the daemon (or start if not running).

pmgproxy start [OPTIONS]

Start the daemon.

--debug <boolean> (*default =* 0)
Debug mode - stay in foreground

pmgproxy status

Get daemon status.

pmgproxy stop

Stop the daemon.

C.3 pmg-smtp-filter - Proxmox SMTP Filter Daemon

Please use systemd tools to manage this service.

systemctl (start|stop|restart|reload|status) pmg-smtp-filter

C.4 pmgpolicy - Proxmox Mail Gateway Policy Daemon

Please use systemd tools to manage this service.

systemctl (start|stop|restart|reload|status) pmgpolicy

C.5 pmgtunnel - Cluster Tunnel Daemon

pmgtunnel <COMMAND> [ARGS] [OPTIONS]

pmgtunnel help [<cmd>] [OPTIONS]

Get help about specified command.

<cmd>: <string>
Command name

--verbose <boolean>
Verbose output format.

pmgtunnel restart

Restart the Cluster Tunnel Daemon

pmgtunnel start `[OPTIONS]`

Start the Cluster Tunnel Daemon

`--debug <boolean>` (*default =* 0)
Debug mode - stay in foreground

pmgtunnel status

Print cluster tunnel status.

pmgtunnel stop

Stop the Cluster Tunnel Daemon

C.6 pmgmirror - Database Mirror Daemon

pmgmirror `<COMMAND> [ARGS] [OPTIONS]`

pmgmirror help `[<cmd>] [OPTIONS]`

Get help about specified command.

`<cmd>: <string>`
Command name

`--verbose <boolean>`
Verbose output format.

pmgmirror restart

Restart the Database Mirror Daemon

pmgmirror start `[OPTIONS]`

Start the Database Mirror Daemon

`--debug <boolean>` (*default =* 0)
Debug mode - stay in foreground

pmgmirror stop

Stop the Database Mirror Daemon

Appendix D

Available Macros for the Rule System

It is possible to use macros inside most fields of action objects. That way it is possible to access and include data contained in the original mail, get envelope sender and receivers addresses or include additional information about Viruses and Spam. Currently the following macros are defined:

Macro	Comment
__SENDER__	(envelope) sender mail address
__RECEIVERS__	(envelope) receiver mail address list
__ADMIN__	Email address of the administrator
__TARGETS__	Subset of receivers matched by the rule
__SUBJECT__	Subject of the message
__MSGID__	The message ID
__RULE__	Name of the matching rule
__RULE_INFO__	Additional information about the matching rule

Macro	Comment
__VIRUS_INFO__	Additional information about detected viruses
__SPAMLEVEL__	Computed spam level
__SPAM_INFO__	Additional information why message is spam
__SENDER_IP__	IP address of sending host
__VERSION__	The current software version (proxmox mail gateway)
__FILENAME__	Attachment file name
__SPAMSTARS__	A series of "*" charactes where each one represents a full score (*SPAMLEVEL*) point

Appendix E

Configuration Files

E.1 Proxmox Mail Gateway Main Configuration

The file `/etc/pmg/pmg.conf` is the main configuration.

E.1.1 File Format

The file is divided into several section. Each section has the following format:

```
section: NAME
         OPTION value
         ...
```

Blank lines in the file separates sections, and lines starting with a # character are treated as comments and are also ignored.

E.1.2 Options

SECTION *admin*

advfilter: <boolean> (*default =* 1)
Use advanced filters for statistic.

dailyreport: <boolean> (*default =* 1)
Send daily reports.

demo: <boolean> (*default =* 0)
Demo mode - do not start SMTP filter.

email: <string> (*default =* admin@domain.tld)
Administrator E-Mail address.

http_proxy: http://.*
Specify external http proxy which is used for downloads (example: *http://username:password@host:port/*)

statlifetime: <integer> (1 - N) (*default =* 7)
User Statistics Lifetime (days)

SECTION *clamav*

archiveblockencrypted: <boolean> (*default =* 0)
Wether to block encrypted archives. Mark encrypted archives as viruses.

archivemaxfiles: <integer> (0 - N) (*default =* 1000)
Number of files to be scanned within an archive, a document, or any other kind of container. Warning: disabling this limit or setting it too high may result in severe damage to the system.

archivemaxrec: <integer> (1 - N) (*default =* 5)
Nested archives are scanned recursively, e.g. if a ZIP archive contains a TAR file, all files within it will also be scanned. This options specifies how deeply the process should be continued. Warning: setting this limit too high may result in severe damage to the system.

archivemaxsize: <integer> (1000000 - N) (*default =* 25000000)
Files larger than this limit won't be scanned.

dbmirror: <string> (*default =* database.clamav.net)
ClamAV database mirror server.

maxcccount: <integer> (0 - N) (*default =* 0)
This option sets the lowest number of Credit Card or Social Security numbers found in a file to generate a detect.

maxscansize: <integer> (1000000 - N) (*default =* 100000000)
Sets the maximum amount of data to be scanned for each input file.

safebrowsing: <boolean> (*default =* 1)
Enables support for Google Safe Browsing.

SECTION *mail*

banner: <string> (*default =* ESMTP Proxmox)
ESMTP banner.

conn_count_limit: <integer> (0 - N) (*default =* 50)
How many simultaneous connections any client is allowed to make to this service. To disable this feature, specify a limit of 0.

conn_rate_limit: <integer> (0 - N) (*default =* 0)
The maximal number of connection attempts any client is allowed to make to this service per minute. To disable this feature, specify a limit of 0.

dnsbl_sites: <string>
Optional list of DNS white/blacklist domains (see postscreen_dnsbl_sites parameter).

dwarning: <integer> (0 - N) (*default* = 4)
SMTP delay warning time (in hours).

ext_port: <integer> (1 - 65535) (*default* = 26)
SMTP port number for incoming mail (untrusted). This must be a different number than *int_port*.

greylist: <boolean> (*default* = 1)
Use Greylisting.

helotests: <boolean> (*default* = 0)
Use SMTP HELO tests.

hide_received: <boolean> (*default* = 0)
Hide received header in outgoing mails.

int_port: <integer> (1 - 65535) (*default* = 25)
SMTP port number for outgoing mail (trusted).

max_filters: <integer> (3 - 40) (*default* = 15)
Maximum number of pmg-smtp-filter processes.

max_policy: <integer> (2 - 10) (*default* = 5)
Maximum number of pmgpolicy processes.

max_smtpd_in: <integer> (3 - 100) (*default* = 99)
Maximum number of SMTP daemon processes (in).

max_smtpd_out: <integer> (3 - 100) (*default* = 99)
Maximum number of SMTP daemon processes (out).

maxsize: <integer> (1024 - N) (*default* = 10485760)
Maximum email size. Larger mails are rejected.

message_rate_limit: <integer> (0 - N) (*default* = 0)
The maximal number of message delivery requests that any client is allowed to make to this service per minute.To disable this feature, specify a limit of 0.

rejectunknown: <boolean> (*default* = 0)
Reject unknown clients.

rejectunknownsender: <boolean> (*default* = 0)
Reject unknown senders.

relay: <string>
The default mail delivery transport (incoming mails).

relaynomx: <boolean> (*default =* 0)
Disable MX lookups for default relay.

relayport: <integer> (1 - 65535) (*default =* 25)
SMTP port number for relay host.

smarthost: <string>
When set, all outgoing mails are deliverd to the specified smarthost.

spf: <boolean> (*default =* 1)
Use Sender Policy Framework.

tls: <boolean> (*default =* 0)
Enable TLS.

tlsheader: <boolean> (*default =* 0)
Add TLS received header.

tlslog: <boolean> (*default =* 0)
Enable TLS Logging.

verifyreceivers: <450 | 550>
Enable receiver verification. The value spefifies the numerical reply code when the Postfix SMTP server rejects a recipient address.

SECTION *spam*

bounce_score: <integer> (0 - 1000) (*default =* 0)
Additional score for bounce mails.

clamav_heuristic_score: <integer> (0 - 1000) (*default =* 3)
Score for ClamaAV heuristics (Google Safe Browsing database, PhishingScanURLs, . . .).

languages: (all|([a-z][a-z])+(([a-z][a-z])+)*) (*default =* all)
This option is used to specify which languages are considered OK for incoming mail.

maxspamsize: <integer> (64 - N) (*default =* 262144)
Maximum size of spam messages in bytes.

rbl_checks: <boolean> (*default =* 1)
Enable real time blacklists (RBL) checks.

use_awl: <boolean> (*default =* 1)
Use the Auto-Whitelist plugin.

use_bayes: <boolean> (*default =* 1)
Whether to use the naive-Bayesian-style classifier.

use_razor: <boolean> (*default =* 1)
Whether to use Razor2, if it is available.

wl_bounce_relays: <string>
Whitelist legitimate bounce relays.

SECTION *spamquar*

allowhrefs: <boolean> (*default =* 1)
Allow to view hyperlinks.

authmode: <ldap | ldapticket | ticket> (*default =* ticket)
Authentication mode to access the quarantine interface. Mode *ticket* allows login using tickets sent with the daily spam report. Mode *ldap* requires to login using an LDAP account. Finally, mode *ldapticket* allows both ways.

hostname: <string>
Quarantine Host. Usefule if you run a Cluster and want users to connect to a specific host.

lifetime: <integer> (1 - N) (*default =* 7)
Quarantine life time (days)

mailfrom: <string>
Text for *From* header in daily spam report mails.

reportstyle: <custom | none | short | verbose> (*default =* verbose)
Spam report style.

viewimages: <boolean> (*default =* 1)
Allow to view images.

SECTION *virusquar*

allowhrefs: <boolean> (*default =* 1)
Allow to view hyperlinks.

lifetime: <integer> (1 - N) (*default =* 7)
Quarantine life time (days)

viewimages: <boolean> (*default =* 1)
Allow to view images.

E.2 Cluster Configuration

The file `/etc/pmg/cluster.conf` contains the cluster configuration.

E.2.1 File Format

The file is divided into several section. There is one *master* and several *node* sections.

```
master: <cid>
         OPTION value
         ...

node: <cid>
         OPTION value
         ...
```

Blank lines in the file separates sections, and lines starting with a # character are treated as comments and are also ignored.

E.2.2 Options

cid: **<integer> (1 - N)**
: Cluster Node ID.

fingerprint: **^(:?[A-Z0-9][A-Z0-9]:){31}[A-Z0-9][A-Z0-9]$**
: SSL certificate fingerprint.

hostrsapubkey: **^[A-Za-z0-9\.\/\+]{200,}$**
: Public SSH RSA key for the host.

ip: **<string>**
: IP address.

maxcid: **<integer> (1 - N)**
: Maximum used cluster node ID (used internally, do not modify).

name: **<string>**
: Node name.

rootrsapubkey: **^[A-Za-z0-9\.\/\+]{200,}$**
: Public SSH RSA key for the root user.

E.3 User Configuration

The file `/etc/pmg/user.conf` contains the user configuration.

E.3.1 File Format

The file has the following format for each user:

```
# comment
userid:enable:expire:crypt_pass:role:email:firstname:lastname:keys
```

E.3.2 Options

comment: **<string>**
: Comment.

crypt_pass: **\$\d\$[a-zA-Z0-9\.\/]+\$[a-zA-Z0-9\.\/]+**
: Encrypted password (see `man crypt`)

email: **<string>**
: Users E-Mail address.

enable: **<boolean>** (***default =*** **0**)
: Flag to enable or disable the account.

expire: **<integer> (0 - N)** (***default =*** **0**)
: Account expiration date (seconds since epoch). *0* means no expiration date.

firstname: **<string>**
: First name.

keys: **<string>**
: Keys for two factor auth (yubico).

lastname: **<string>**
: Last name.

password: **<string>**
: Password

role: **<admin | audit | qmanager | root>**
: User role. Role *root* is reseved for the Unix Superuser.

userid: **<string>**
: User ID

E.4 LDAP Configuration

The file `/etc/pmg/ldap.conf` contains the LDAP configuration.

E.4.1 File Format

The file is divided into a section for each LDAP profile. Each section has the following format:

```
ldap: NAME
        OPTION value
        ...
```

Blank lines in the file separates sections, and lines starting with a # character are treated as comments and are also ignored.

E.4.2 Options

accountattr: <string> (*default* = sAMAccountName, uid)
Account attribute name name.

basedn: <string>
Base domain name.

binddn: <string>
Bind domain name.

bindpw: <string>
Bind password.

comment: <string>
Description.

disable: <boolean>
Flag to disable/deactivate the entry.

filter: <string>
LDAP filter.

groupbasedn: <string>
Base domain name for groups.

groupclass: <string> (*default* = group, univentionGroup, ipausergroup)
List of objectclasses for groups.

mailattr: <string> (*default* = mail, userPrincipalName, proxyAddresses, othermailbox, mailAlternativeAddress)
List of mail attribute names.

mode: <ldap | ldaps> (*default* = ldap)
LDAP protocol mode (*ldap* or *ldaps*).

port: **<integer> (1 - 65535)**
Specify the port to connect to.

profile: **<string>**
Profile ID.

server1: **<string>**
Server address.

server2: **<string>**
Fallback server address. Userd when the first server is not available.

Appendix F

GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a worldwide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or

to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document

are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into

the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.