



PROXMOX MAIL GATEWAY ADMINISTRATION GUIDE

RELEASE 7.2



November 29, 2022
Proxmox Server Solutions GmbH
www.proxmox.com

Copyright © 2022 Proxmox Server Solutions GmbH

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

A copy of the license is included in the section entitled "GNU Free Documentation License".

Contents

1	Introduction	1
1.1	What is Proxmox Mail Gateway?	1
1.2	Features	2
1.2.1	Spam detection	2
1.2.2	Virus detection	3
1.2.3	Object-Oriented Rule System	3
1.2.4	Web-based Management Interface	4
1.2.5	Spam Quarantine	5
1.2.6	Tracking and Logging	5
1.2.7	DKIM Signing	5
1.2.8	High Availability with Proxmox HA Cluster	5
1.2.9	LDAP Integration	5
1.2.10	Fetchmail Integration	5
1.2.11	Flexible User Management	6
1.3	Your benefit with Proxmox Mail Gateway	6
1.4	Getting Help	6
1.4.1	Community Support Forum	6
1.4.2	Commercial Support	7
1.4.3	Bug Tracker	7
2	Planning for Deployment	8
2.1	Easy Integration into Existing Email Server Architecture	8
2.2	Filtering Outgoing Emails	9
2.3	Firewall Settings	9
2.4	System Requirements	10
2.4.1	Minimum System Requirements	11
2.4.2	Recommended System Requirements	11
2.4.3	Supported web browsers for accessing the web interface	11

3	Installation	12
3.1	Prepare Installation Media	12
3.1.1	Prepare a USB Flash Drive as an Installation Medium	12
3.1.2	Instructions for GNU/Linux	13
3.1.3	Instructions for macOS	13
3.1.4	Instructions for Windows	14
3.2	Using the Proxmox Mail Gateway Installation CD-ROM	15
3.2.1	Advanced LVM Configuration Options	22
3.2.2	ZFS Performance Tips	22
3.3	Install Proxmox Mail Gateway on Debian	22
3.4	Install Proxmox Mail Gateway as a Linux Container Appliance	23
3.5	Package Repositories	23
3.5.1	Repositories in Proxmox Mail Gateway	23
3.5.2	Proxmox Mail Gateway Enterprise Repository	25
3.5.3	Proxmox Mail Gateway No-Subscription Repository	25
3.5.4	Proxmox Mail Gateway Test Repository	26
3.5.5	SecureApt	26
3.5.6	Other Repository Sources	26
4	Configuration Management	28
4.1	Configuration files overview	28
4.2	Keys and Certificates	29
4.3	Service Configuration Templates	30
4.4	White- and Blacklists	31
4.4.1	SMTP Whitelist	31
4.4.2	Rule-based White-/Blacklist	31
4.4.3	User White-/Blacklist	31
4.5	System Configuration	32
4.5.1	Network and Time	32
4.5.2	Options	33
4.6	Certificate Management	34
4.6.1	Certificates for the API and SMTP	34
4.6.2	Upload Custom Certificate	35
4.6.3	Trusted certificates via Let's Encrypt (ACME)	35
4.6.4	ACME HTTP Challenge Plugin	37
4.6.5	ACME DNS API Challenge Plugin	37

4.6.6	Automatic renewal of ACME certificates	39
4.6.7	Manually Change Certificate over Command-Line	39
4.6.8	Change Certificate for Cluster Setups	40
4.7	Mail Proxy Configuration	40
4.7.1	Relaying	40
4.7.2	Relay Domains	41
4.7.3	Ports	42
4.7.4	Options	43
4.7.5	Before and After Queue scanning	45
4.7.6	Greylisting	45
4.7.7	Transports	46
4.7.8	Networks	47
4.7.9	TLS	48
4.7.10	DKIM Signing	49
4.7.11	Whitelist	51
4.8	Spam Detector Configuration	52
4.8.1	Options	52
4.8.2	Quarantine	53
4.8.3	Customization of Rulescores	55
4.9	Virus Detector Configuration	56
4.9.1	Options	56
4.9.2	Quarantine	58
4.10	Custom SpamAssassin configuration	58
4.11	Custom Check Interface	59
4.12	User Management	61
4.12.1	Local Users	61
4.12.2	LDAP/Active Directory	62
4.12.3	Fetchmail	64
4.13	Two-Factor Authentication	65
4.13.1	Available Second Factors	65
4.13.2	Configuration of Two-Factor	66
4.13.3	TOTP	66
4.13.4	WebAuthn	66
4.13.5	Recovery Keys	66
4.13.6	WebAuthn Configuration	67

5	Rule-Based Mail Filter	68
5.1	<i>Action</i> - objects	70
5.1.1	Accept	70
5.1.2	Block	70
5.1.3	Quarantine	70
5.1.4	Notification	71
5.1.5	Blind Carbon Copy (BCC)	71
5.1.6	Header Attributes	71
5.1.7	Remove attachments	72
5.1.8	Disclaimer	72
5.2	<i>Who</i> objects	72
5.3	<i>What</i> objects	74
5.4	<i>When</i> objects	75
5.5	Using regular expressions	75
5.5.1	Simple regular expressions	76
5.5.2	Metacharacters	76
6	Administration	77
6.1	Server Administration	78
6.1.1	Status	78
6.1.2	Services	79
6.1.3	Updates	80
6.1.4	Syslog and Tasks	81
6.2	Quarantine	82
6.2.1	Spam	82
6.2.2	Virus	82
6.2.3	Attachment	83
6.2.4	User White- and Blacklist	83
6.3	Tracking Center	83
6.4	Postfix Queue Administration	85
6.4.1	Deferred Mail	86
7	Backup and Restore	87
7.1	Local Backups	88
7.2	Proxmox Backup Server	88
7.2.1	Remotes	89
7.2.2	Backup Jobs	90

8 Cluster Management	93
8.1 Hardware Requirements	94
8.2 Subscriptions	94
8.3 Load Balancing	94
8.3.1 Hot standby with backup MX records	95
8.3.2 Load balancing with MX records	95
8.3.3 Other ways	96
8.4 Cluster Administration	96
8.4.1 Creating a Cluster	97
8.4.2 Show Cluster Status	97
8.4.3 Adding Cluster Nodes	98
8.4.4 Deleting Nodes	99
8.4.5 Disaster Recovery	99
9 Important Service Daemons	101
9.1 pmgdaemon - Proxmox Mail Gateway API Daemon	101
9.2 pmgproxy - Proxmox Mail Gateway API Proxy Daemon	101
9.2.1 Alternative HTTPS certificate	101
9.2.2 Host based Access Control	101
9.2.3 Listening IP	102
9.2.4 SSL Cipher Suite	103
9.2.5 Supported TLS versions	103
9.2.6 Diffie-Hellman Parameters	104
9.2.7 COMPRESSION	104
9.3 pmg-smtp-filter - Proxmox SMTP Filter Daemon	104
9.4 pmgpolicy - Proxmox Mail Gateway Policy Daemon	104
9.5 pmgtunnel - Cluster Tunnel Daemon	104
9.6 pmgmirror - Database Mirror Daemon	104
10 Useful Command Line Tools	105
10.1 pmgdb - Database Management Toolkit	105
10.2 pmgsh - API Shell	105
10.3 pmgversion - Version Info	106
10.4 pmgsubscription - Subscription Management	106
10.5 pmgperf - Proxmox Simple Performance Benchmark	107
10.6 pmgqm - Quarantine Management Toolkit	107

10.7 pmgreport - Send daily system report email	108
10.8 pmgupgrade - Upgrade Proxmox Mail Gateway	108
10.9 pmg-log-tracker - Backend for the Tracking Center	108
10.10 nmap - Port Scans	109
11 Frequently Asked Questions	110
12 Bibliography	112
12.1 Books about mail processing technology	112
12.2 Books about related technology	112
12.3 Books about related topics	113
A Command Line Interface	114
A.1 pmgbackup - Proxmox Mail Gateway Backup and Restore Utility	114
A.2 pmgcm - Proxmox Mail Gateway Cluster Management Toolkit	119
A.3 pmgsh - API Shell	120
A.4 pmgperf - Proxmox Simple Performance Benchmark	121
A.5 pmgconfig - Configuration Management Toolkit	121
A.6 pmgdb - Database Management Toolkit	127
B Service Daemons	128
B.1 pmgdaemon - Proxmox Mail Gateway API Daemon	128
B.2 pmgproxy - Proxmox Mail Gateway API Proxy Daemon	128
B.3 pmg-smtp-filter - Proxmox SMTP Filter Daemon	129
B.4 pmgpolicy - Proxmox Mail Gateway Policy Daemon	129
B.5 pmgtunnel - Cluster Tunnel Daemon	129
B.6 pmgmirror - Database Mirror Daemon	130
C Available Macros for the Rule System	131
D Configuration Files	133
D.1 Proxmox Mail Gateway Main Configuration	133
D.1.1 File Format	133
D.1.2 Options	133
D.2 Cluster Configuration	139
D.2.1 File Format	139
D.2.2 Options	139
D.3 User Configuration	140

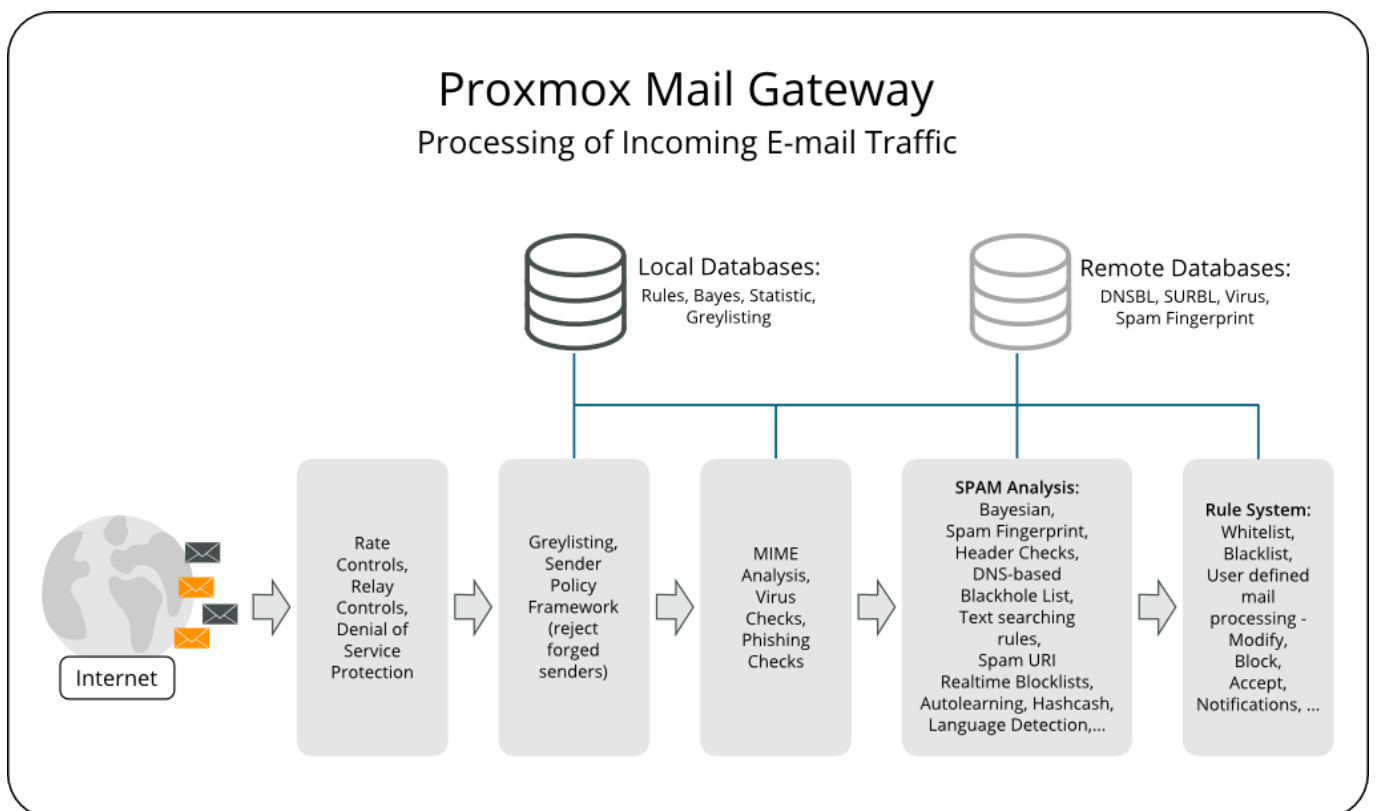
D.3.1	File Format	140
D.3.2	Options	140
D.4	LDAP Configuration	141
D.4.1	File Format	141
D.4.2	Options	141
E	GNU Free Documentation License	143

Chapter 1

Introduction

1.1 What is Proxmox Mail Gateway?

Email security begins at the gateway, by controlling all incoming and outgoing email messages. Proxmox Mail Gateway addresses the full spectrum of unwanted email traffic, focusing on spam and virus detection. Proxmox Mail Gateway provides a powerful and affordable server solution to eliminate spam and viruses, and block undesirable content from your email 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 the SMTP level, before they are transferred to your network. This reduces the traffic to be analyzed for spam and viruses by 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 preventing 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 DNSBL) and accept all emails for 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

Certain words have a higher probability of occurring in spam emails than in legitimate emails. By being trained to recognize those words, the Bayesian filter 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.

Auto-learning algorithm

Proxmox Mail Gateway gathers statistical information about spam emails. This information is used by an auto-learning algorithm, meaning the system becomes smarter over time.

Spam URI Real-time Block List (SURBL)

SURBLs are used to detect spam, based on the URIs in the message body (usually websites). 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 means that unknown senders are intentionally temporarily rejected. Since temporary failures are part of the specifications for mail delivery, a legitimate server will try to resend the email later on. Spammers, on the other hand, do not queue and reattempt mail delivery. A greylisted email never reaches your mail server and thus your mail server will not send useless "Non Delivery Reports" to spammers. Additionally, greylisted mail is not analyzed by the antivirus and spam-detector engines, which saves resources.

A mail is greylisted if it is the first mail from a sender to a receiver coming from a particular IP network. You can configure which IP addresses belong to the same network, by setting an appropriate netmask for greylisting.

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 violate the SMTP protocol specification and thus can be detected by these tests.

Before and After Queue Filtering

Proxmox Mail Gateway can be configured to either accept the mail, by sending a response of *250 OK*, and scan it afterwards, or alternatively inspect the mail directly after it has the content and respond with a reject *554* if the mail is blocked by the rule system. These options are known as After Queue and Before Queue filtering respectively (see [Before and After Queue Scanning](#) Section 4.7.5).

Configurable NDR policy

In certain environments, it can be unacceptable to discard an email, without informing the sender about that decision. You can decide whether you want to inform the senders of blocked emails or not.

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, multi-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 email?

WHAT - objects

What is in the email?

WHEN - objects

When was the email received by Proxmox Mail Gateway?

ACTIONS - objects

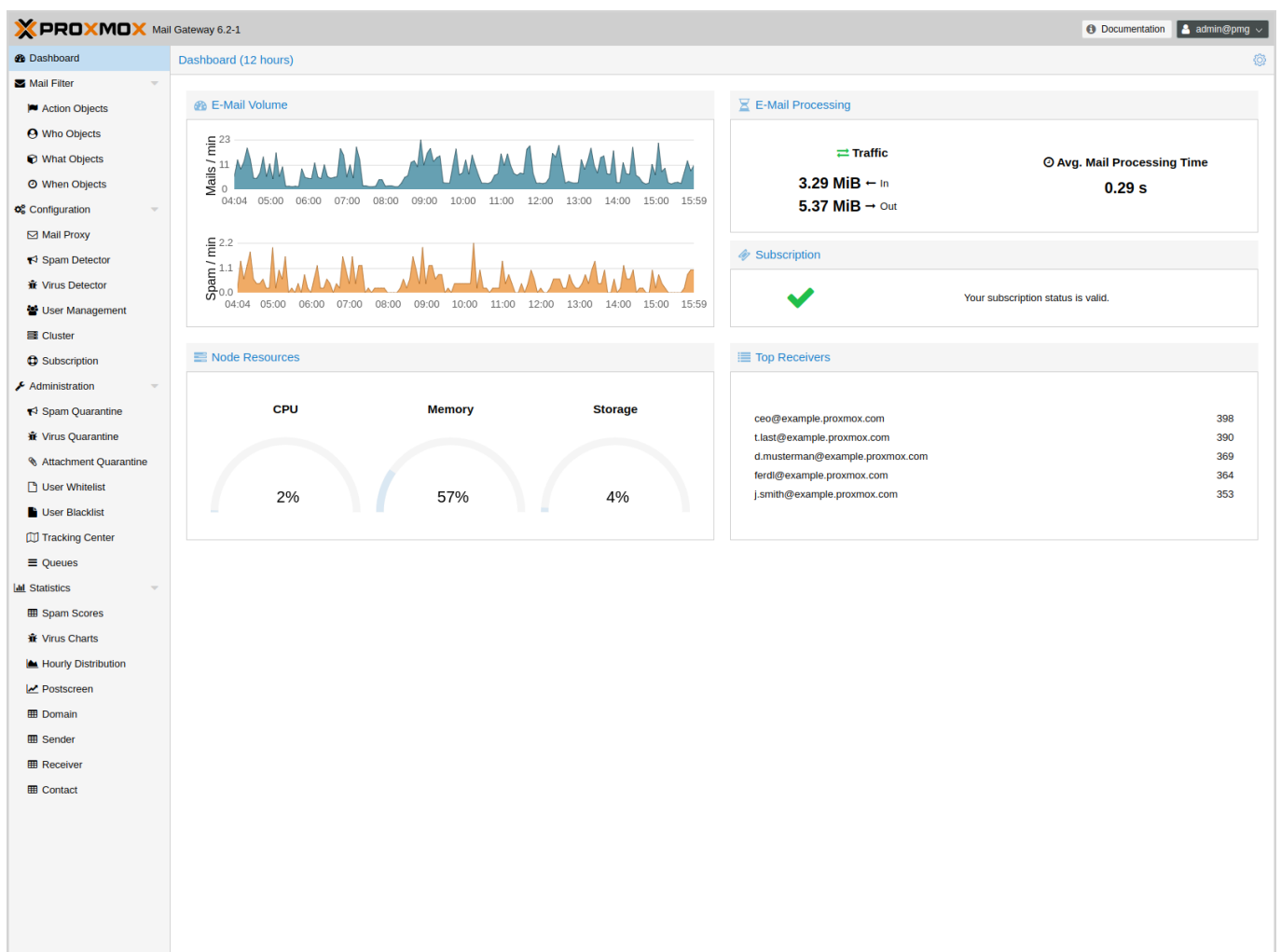
Defines the final actions.

Every rule has five categories FROM, TO, WHEN, WHAT and ACTION. Each 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 emails and generating notifications.

1.2.4 Web-based Management Interface

Proxmox Mail Gateway makes email security and filtering simple to manage. The web-based management interface allows you to set up and maintain even a complex mail system with ease.



There is no need to install a separate management tool. Any modern internet browser is sufficient.

1.2.5 Spam Quarantine

Identified spam mails can be stored in the user-accessible Spam Quarantine. Thus, users can view and manage their spam mails by themselves.

1.2.6 Tracking and Logging

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

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

The logged information includes:

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

1.2.7 DKIM Signing

Proxmox Mail Gateway offers the possibility to optionally sign outgoing emails with [DKIM](#) Section [4.7.10](#).

1.2.8 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. It is quick to set-up and the simple, intuitive management interface keeps resource requirements low. After temporary failures, nodes automatically reintegrate without any operator interaction.

1.2.9 LDAP Integration

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

1.2.10 Fetchmail Integration

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

1.2.11 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 the mail filter setup, but not allowed to alter the 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.

Helpdesk

Combines permissions of the *Auditor* and the *Quarantine Manager* role.

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 moderated by the Proxmox support team, and has a large user base around the world. Needless to say, 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](#). Users with a Basic subscription or above have access to a dedicated support portal with guaranteed response times, where Proxmox Mail Gateway developers can help them, should an issue appear. Please contact the [Proxmox sales team](#) for more information or volume discounts.

1.4.3 Bug Tracker

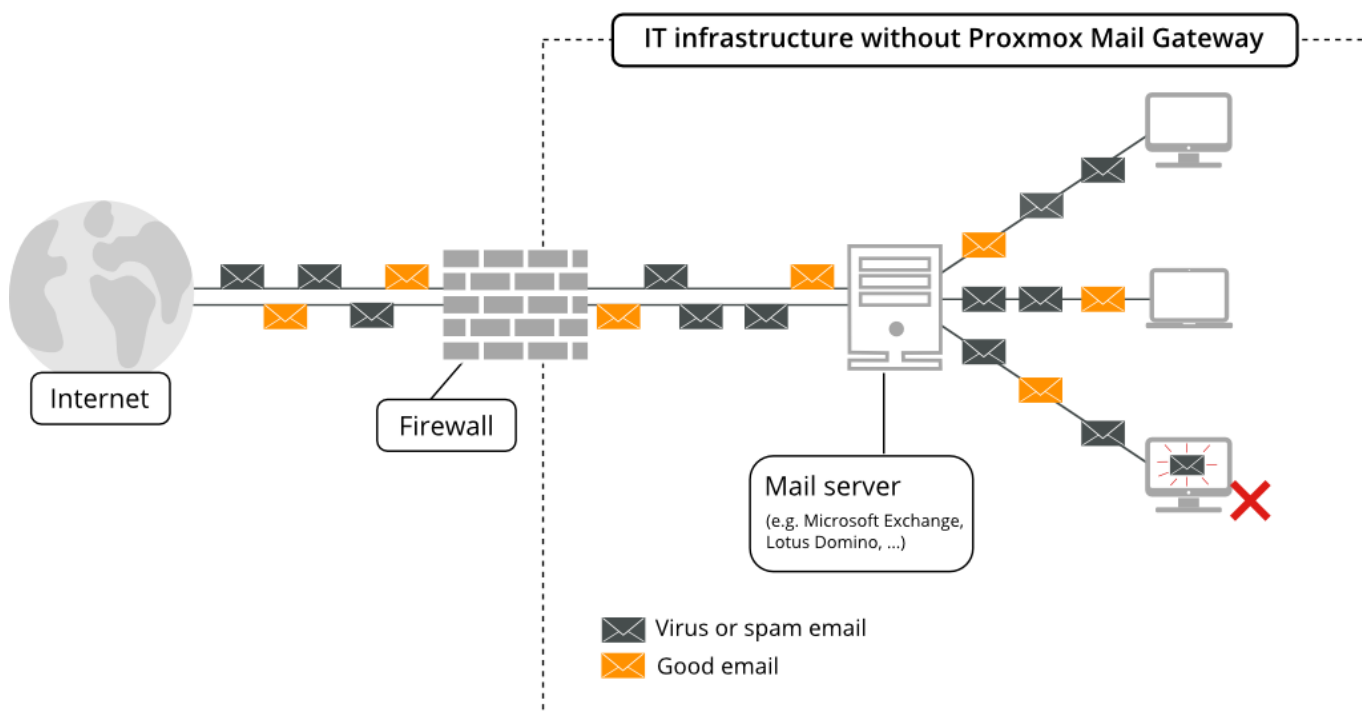
We also run a public bug tracker at <https://bugzilla.proxmox.com>. If you ever detect a bug, you can file a bug entry there. This makes it easy to track the bug's status and get notified as soon as the bug is fixed.

Chapter 2

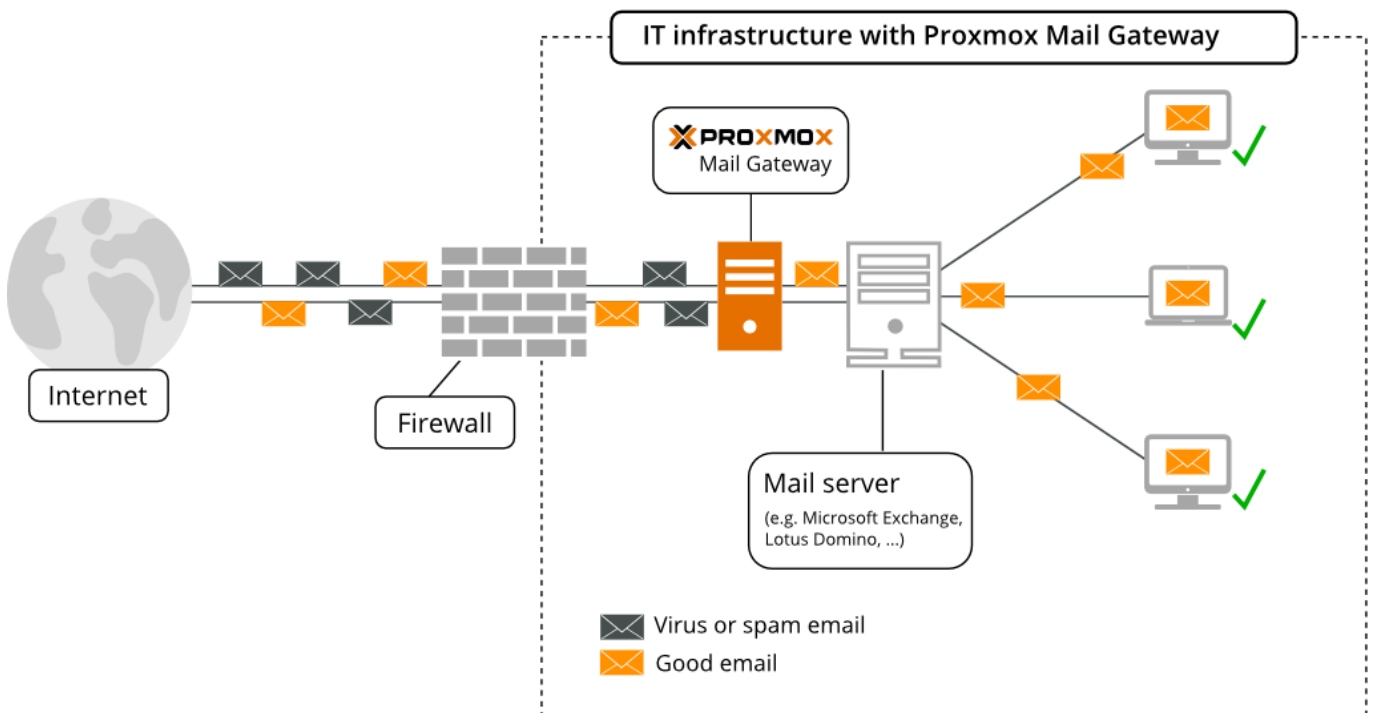
Planning for Deployment

2.1 Easy Integration into Existing Email Server Architecture

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



By using Proxmox Mail Gateway, all your email traffic is forwarded to the Proxmox Mail Gateway instance, which filters the email traffic and removes unwanted emails. This allows you to manage incoming and outgoing mail traffic.



2.2 Filtering Outgoing Emails

Many email filtering solutions do not scan outgoing mails. In contrast, Proxmox Mail Gateway is designed to scan both incoming and outgoing emails. 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 sending viruses to other people. The outgoing email scanning feature is an additional protection to avoid that.
2. Proxmox Mail Gateway can gather statistics about outgoing emails too. Statistics about incoming emails may look nice, but they aren't necessarily helpful. Consider two users; user-1 receives 10 emails from news portals and writes 1 email to an unknown individual, while user-2 receives 5 emails from customers and sends 5 emails in return. With this information, user-2 can be considered as the more active user, because they communicate more with your customers. Proxmox Mail Gateway advanced address statistics can show you this important information, whereas a solution which does not scan outgoing email cannot do this.

To enable outgoing email filtering, you simply need to send all outgoing emails through your Proxmox Mail Gateway (usually by specifying Proxmox Mail Gateway as "smarthost" on your email server).

2.3 Firewall Settings

In order to pass email traffic to Proxmox Mail Gateway, you need to allow traffic on the SMTP port. Our software uses the Network Time Protocol (NTP), RAZOR, DNS, SSH, and HTTP, as well as 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
NTP	123	TCP/UDP	Proxmox	Internet
RAZOR	2703	TCP	Proxmox	Internet
DNS	53	TCP/UDP	Proxmox	DNS Server
HTTP	80	TCP	Proxmox	Internet
HTTPS	443	TCP	Proxmox	Internet
GUI/API	8006	TCP	Intranet	Proxmox

**Caution**

It is recommended 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 10.10).

2.4 System Requirements

Proxmox Mail Gateway can run on dedicated server hardware or inside a virtual machine on any of the following platforms:

- 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)
- VirtualBox™
- Citrix Hypervisor™ (former XenServer™)
- LXC container
- and others that support Debian Linux as a guest OS

Please see <https://www.proxmox.com> for details.

To benchmark your hardware, 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
- Monitor with a minimum resolution of 1024x768 for the installation
- Hard disk with at least 8 GB of disk space
- Ethernet network interface card (NIC)

2.4.2 Recommended System Requirements

- Multi-core CPU: 64bit (Intel EMT64 or AMD64),
 - for use in a virtual machine, activate Intel VT/AMD-V CPU flag
- 4 GB RAM
- Bootable CD-ROM-drive or USB boot support
- Monitor with a minimum resolution of 1024x768 for the installation
- 1 Gbps Ethernet network interface card (NIC)
- Storage: at least 8 GB free disk space, best set up with redundancy, using a hardware RAID controller with battery backed write cache (“BBU”) or ZFS. ZFS is not compatible with hardware RAID controllers. For best performance, use enterprise-class SSDs with power loss protection.

2.4.3 Supported web browsers for accessing the web interface

To use the web interface, you need a modern browser. This includes:

- Firefox, a release from the current year, or the latest Extended Support Release
 - Chrome, a release from the current year
 - Microsoft’s currently supported version of Edge
 - Safari, a release from the current year
-

Chapter 3

Installation

Proxmox Mail Gateway is based on Debian. This is why the install disk images (ISO files) provided by Proxmox include a complete Debian system as well as all necessary Proxmox Mail Gateway packages.

Tip

See the [support table in the FAQ](#) [?informaltable] for the relationship between Proxmox Mail Gateway releases and Debian releases.

The installer will guide you through the setup, allowing you to partition the local disk(s), apply basic system configurations (for example, timezone, language, network) and install all required packages. This process should not take more than a few minutes. Installing with the provided ISO is the recommended method for new and existing users.

Alternatively, Proxmox Mail Gateway can be installed on top of an existing Debian system. This option is only recommended for advanced users because detailed knowledge about Proxmox Mail Gateway is required.

3.1 Prepare Installation Media

Download the installer ISO image from: <https://www.proxmox.com/en/downloads/category/proxmox-mail-gateway>

The Proxmox Mail Gateway installation media is a hybrid ISO image. It works in two ways:

- An ISO image file ready to burn to a CD or DVD.
- A raw sector (IMG) image file ready to copy to a USB flash drive (USB stick).

Using a USB flash drive to install Proxmox Mail Gateway is the recommended way, because it is the faster option.

3.1.1 Prepare a USB Flash Drive as an Installation Medium

The flash drive needs to have at least 1 GB of storage available.

Note

Do not use UNetbootin. It does not work with the Proxmox Mail Gateway installation image.

**Important**

Make sure that the USB flash drive is not mounted and does not contain any important data.

3.1.2 Instructions for GNU/Linux

On a Unix-like operating system, you can use the `dd` command to copy the ISO image to the USB flash drive. To do this, find the device name of the USB flash drive (see below), then run the `dd` command.

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

Note

Be sure to replace `/dev/XYZ` with the correct device name and adapt the input filename (*if*) path.

**Caution**

Be very careful, and do not overwrite the wrong disk!

Find the USB Device Name

There are multiple ways to find out the name of the USB flash drive. One is to compare the last lines of the `dmesg` command output before and after plugging in the flash drive. Another way is to compare the output of the `lsblk` command. Open a terminal and run:

```
# lsblk
```

Then plug in your USB flash drive and run the command again:

```
# lsblk
```

A new device will appear. This is the one you want to use. As an additional precaution, check that the reported size matches your USB flash drive.

3.1.3 Instructions for macOS

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-ve_*.iso ↵
```

Tip

macOS tends to automatically add `.dmg` to the output filename.

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

```
# diskutil list
```

Now insert the USB flash drive and run this command again to determine which device node has been assigned to it. (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/rdiskX bs=1m
```

Note

`rdiskX`, instead of `diskX`, in the last command is intended. This will increase the write speed.

3.1.4 Instructions for Windows

Using Etcher

Etcher works out of the box. Download Etcher from <https://etcher.io>. It will guide you through the process of selecting the ISO and your USB drive.

Using Rufus

Rufus is a more lightweight alternative, but you need to use the **DD mode** to make it work. Download Rufus from <https://rufus.ie/>. Either install it or use the portable version. Select the destination drive and the Proxmox Mail Gateway ISO file.

**Important**

After you *Start*, you have to click *No* on the dialog asking to download a different version of GRUB. In the next dialog select the *DD* mode.

3.2 Using the Proxmox Mail Gateway Installation CD-ROM

The installer ISO image includes the following:

- Complete operating system (Debian Linux, 64-bit)
- The Proxmox Mail Gateway installer, which partitions the hard drive(s) with ext4, 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 insert the [prepared installation media](#) Section 3.1 (for example, USB flash drive or CD-ROM) and boot from it.

Tip

Make sure that booting from the installation medium (for example, USB) is enabled in your servers firmware settings.

After choosing the correct entry (for example, Boot from USB) the Proxmox Mail Gateway menu will be displayed, and one of the following options can be selected:



Install Proxmox Mail Gateway

Start normal installation.

Install Proxmox Mail Gateway (Debug mode)

Start installation in debug mode. This opens a shell console at various stages throughout the installation, so that you can debug issues, if something goes wrong. You can press `CTRL-D` to exit the debug console and continue the 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.



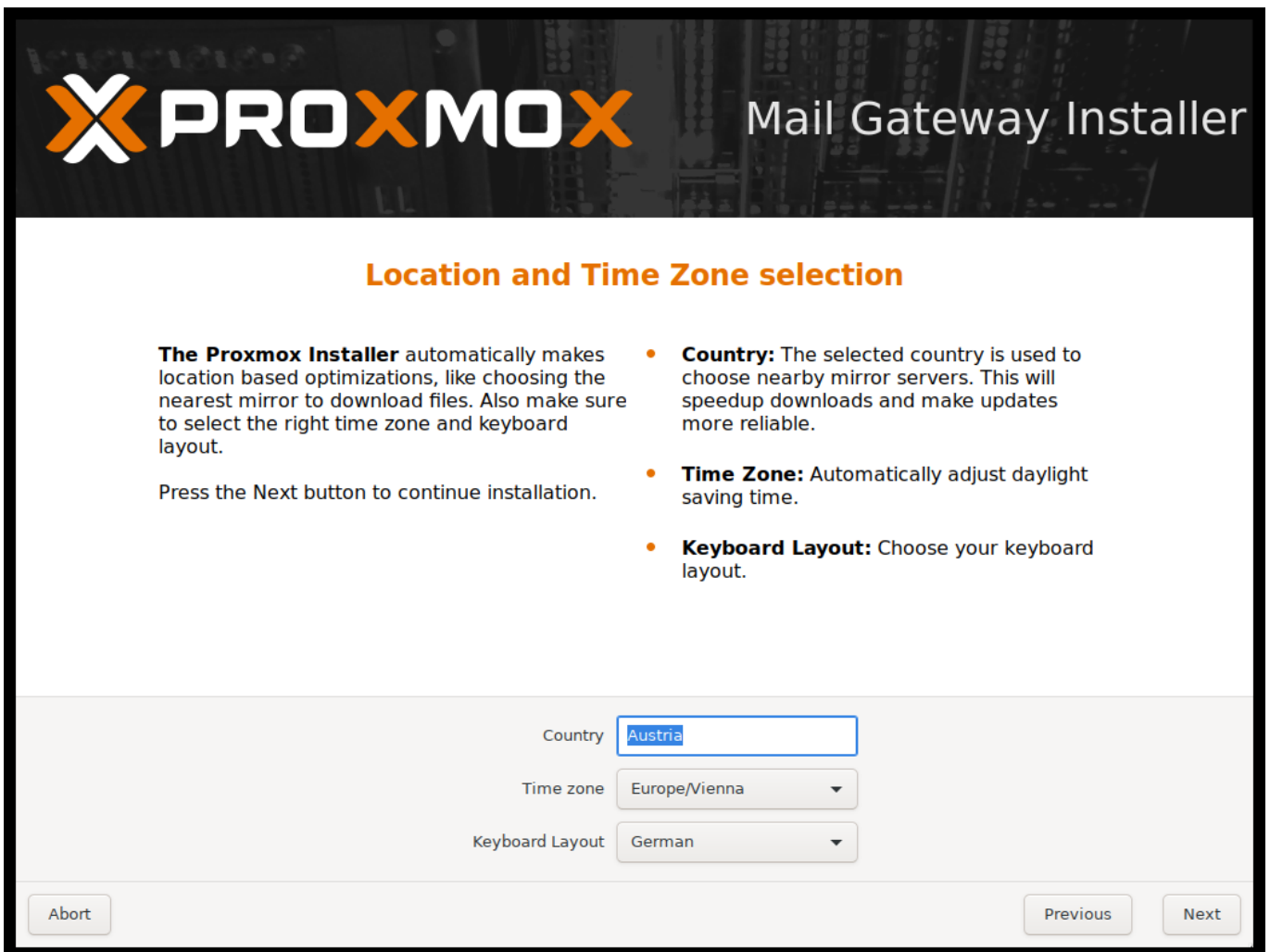
The first step is to read our EULA (End User License Agreement). Following this, you can select the target hard disk(s) for the installation.

**Caution**

By default, the whole server is used and all existing data is removed. Make sure there is no important data on the server before proceeding with the installation.

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

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



The next page asks for basic configuration options like your location, timezone, and keyboard layout. The location is used to select a nearby download server, in order to increase the speed of updates. The installer is usually able to auto-detect these settings, so you only need to change them in rare situations when auto-detection fails, or when you want to use a keyboard layout not commonly used in your country.

The screenshot shows the 'Administration Password and E-Mail Address' step of the Proxmox Mail Gateway installer. The title bar at the top features the Proxmox logo and the text 'Mail Gateway Installer'. The main heading is 'Administration Password and E-Mail Address'. Below this, there is a paragraph describing Proxmox Mail Gateway as a full-featured, highly secure GNU/Linux system based on Debian. To the right, two bullet points provide instructions: 'Password' (strong password, 8+ characters, letters, numbers, symbols) and 'E-Mail' (valid email address for alerts). A note asks for the root password and instructs to press 'Next'. The form below has three fields: 'Password' (masked with dots), 'Confirm' (masked with dots), and 'E-Mail' (containing 'mailadmin@example.com'). At the bottom are 'Abort', 'Previous', and 'Next' buttons.

Administration Password and E-Mail Address

Proxmox Mail Gateway is a full featured highly secure GNU/Linux system based on Debian.

Please provide the *root* password in this step.

- **Password:** Please use a strong password. It should have 8 or more characters. Also combine letters, numbers, and symbols.
- **E-Mail:** Enter a valid email address. Your Proxmox Mail Gateway will send important alert notifications to this email account (all mails for 'root').

Press the Next button to continue installation.

Password

Confirm

E-Mail

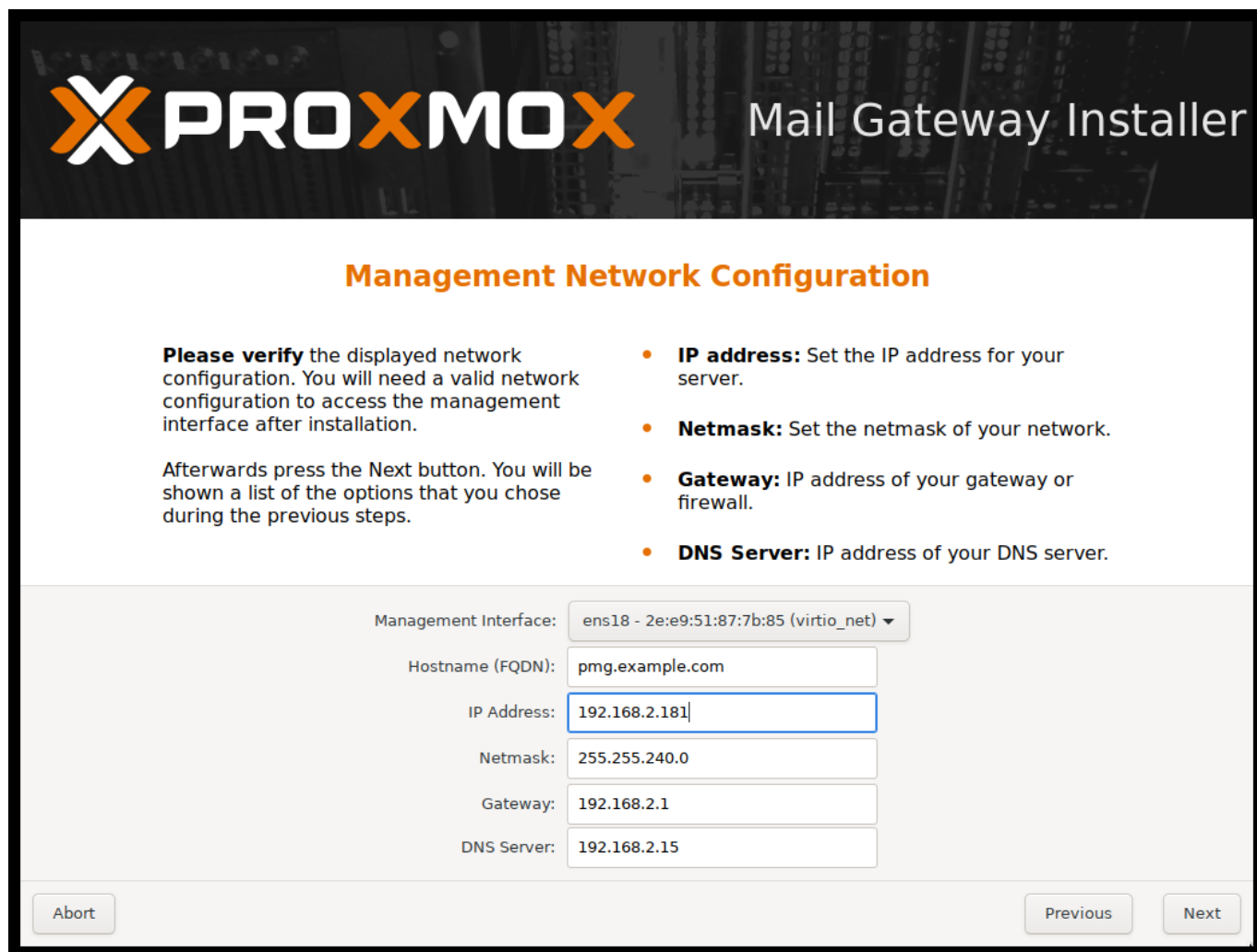
You then need to specify an email address and the superuser (root) password. The password must have at least 5 characters, but we highly recommend to use stronger passwords - here are some guidelines:

- 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 screenshot shows the 'Management Network Configuration' step of the Proxmox Mail Gateway Installer. The interface includes a header with the Proxmox logo and the title 'Mail Gateway Installer'. Below the header, there is a section for instructions and a list of configuration items. The configuration items are presented as a form with input fields for each parameter.

Management Network Configuration

Please verify the displayed network configuration. You will need a valid network configuration to access the management interface after installation.

Afterwards press the Next button. You will be shown a list of the options that you chose during the previous steps.

- **IP address:** Set the IP address for your server.
- **Netmask:** Set the netmask of your network.
- **Gateway:** IP address of your gateway or firewall.
- **DNS Server:** IP address of your DNS server.

Management Interface:

Hostname (FQDN):

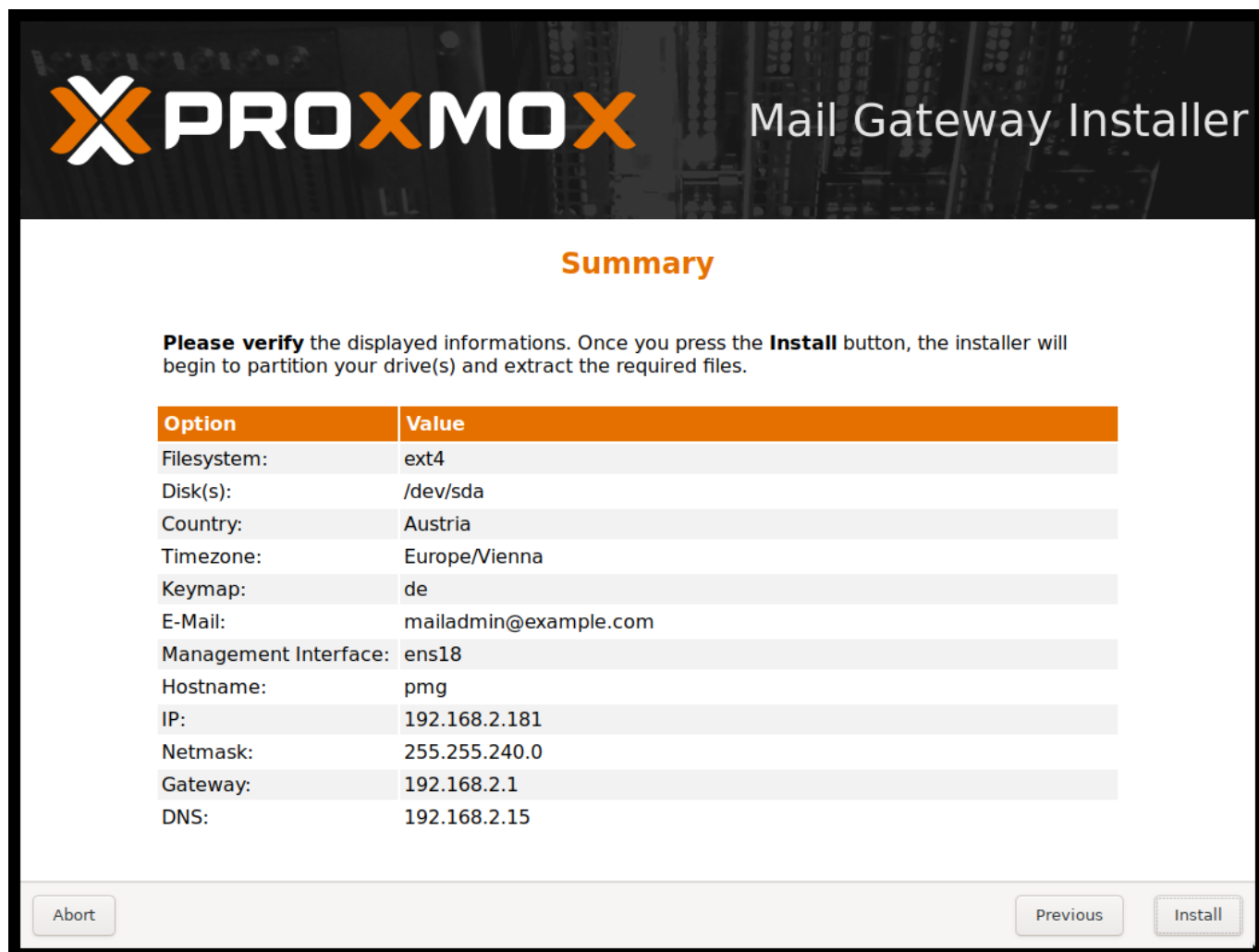
IP Address:

Netmask:

Gateway:

DNS Server:

The next 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 the installation.



Summary

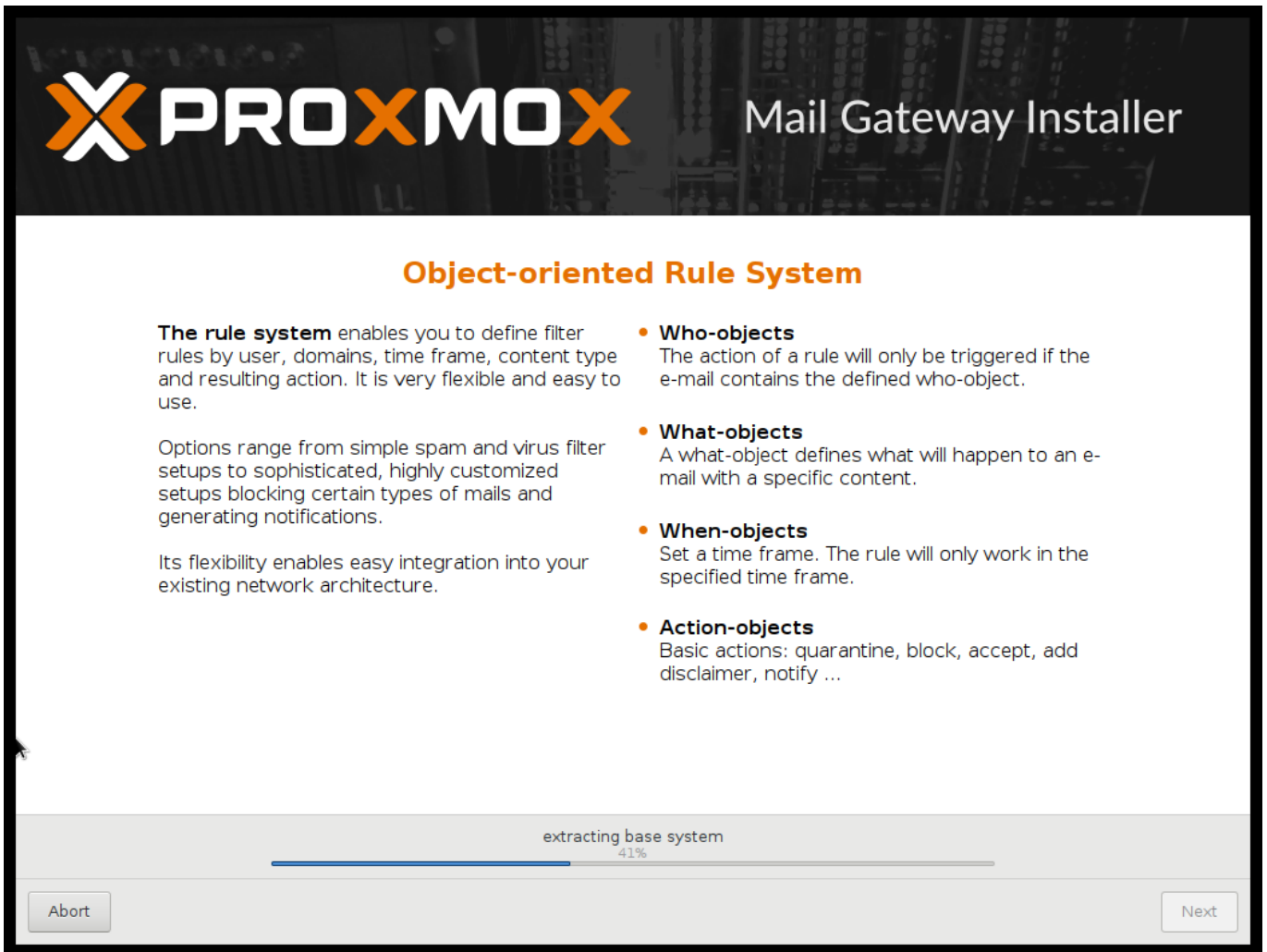
Please verify the displayed informations. Once you press the **Install** button, the installer will begin to partition your drive(s) and extract the required files.

Option	Value
Filesystem:	ext4
Disk(s):	/dev/sda
Country:	Austria
Timezone:	Europe/Vienna
Keymap:	de
E-Mail:	mailadmin@example.com
Management Interface:	ens18
Hostname:	pmg
IP:	192.168.2.181
Netmask:	255.255.240.0
Gateway:	192.168.2.1
DNS:	192.168.2.15

Abort Previous Install

When you press `Next`, you will see an overview of your entered configuration. Please re-check every setting, you can still use the `Previous` button to go back and edit any settings.

After clicking `Install`, the installer will begin to format and copy packages to the target disk(s).



Copying the packages usually takes several minutes. When this is finished, you can reboot the server.

Further configuration is done via the Proxmox Mail Gateway web interface:

1. Point your browser to the IP address given during the installation (<https://youripaddress:8006>).
2. Log in and upload your subscription key.

Note

The default login is "root", and the password is the one chosen during the installation.

3. Check the IP configuration and hostname.
 4. Check the timezone.
 5. Check your [Firewall settings](#) Section 2.3.
 6. Configure Proxmox Mail Gateway to forward the incoming SMTP traffic to your mail server (*Configuration/Mail Proxy/Default Relay*) - *Default Relay* is your email server.
 7. Configure your email 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](#).

After the installation, you have to route all your incoming and outgoing email traffic to Proxmox Mail Gateway. For incoming traffic, you have to configure your firewall and/or DNS settings. For outgoing traffic you need to change the existing email server configuration.

3.2.1 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 disk size to be used. This way you can save free space on the disk for further partitioning (i.e. for an additional PV and VG on the same 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. The minimum is 4 GB and the maximum is 8 GB. The resulting value cannot be greater than `hdsize/8`.

minfree

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

Note

LVM requires free space in the VG for snapshot creation (not required for `lvmtthin` snapshots).

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

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

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 [package repositories](#) Section 3.5, you need to run:

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

Installing on top of an existing Debian installation seems easy, but it assumes 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.

3.4 Install Proxmox Mail Gateway as a Linux Container Appliance

Proxmox Mail Gateway can also run inside a Debian-based LXC instance. In order to keep the set of installed software, and thus the necessary updates minimal, you can use the `proxmox-mailgateway-container` meta-package. This does not depend on any Linux kernel, firmware, or components used for booting from bare-metal, like grub2.

A ready-to-use appliance template is available through the `mail` section of the **Proxmox VE** appliance manager, so if you already use Proxmox VE, you can set up a Proxmox Mail Gateway instance in minutes.

Note

It's recommended to use a static network configuration. If DHCP must be used, ensure that the container always leases the same IP, for example, by reserving one with the container's network MAC address.

Additionally, you can install this on top of a container-based Debian installation. After configuring the [package repositories](#) Section 3.5, you need to run:

```
apt update
apt install proxmox-mailgateway-container
```

3.5 Package Repositories

Proxmox Mail Gateway uses **APT** as its package management tool like any other Debian-based system.

3.5.1 Repositories in Proxmox Mail Gateway

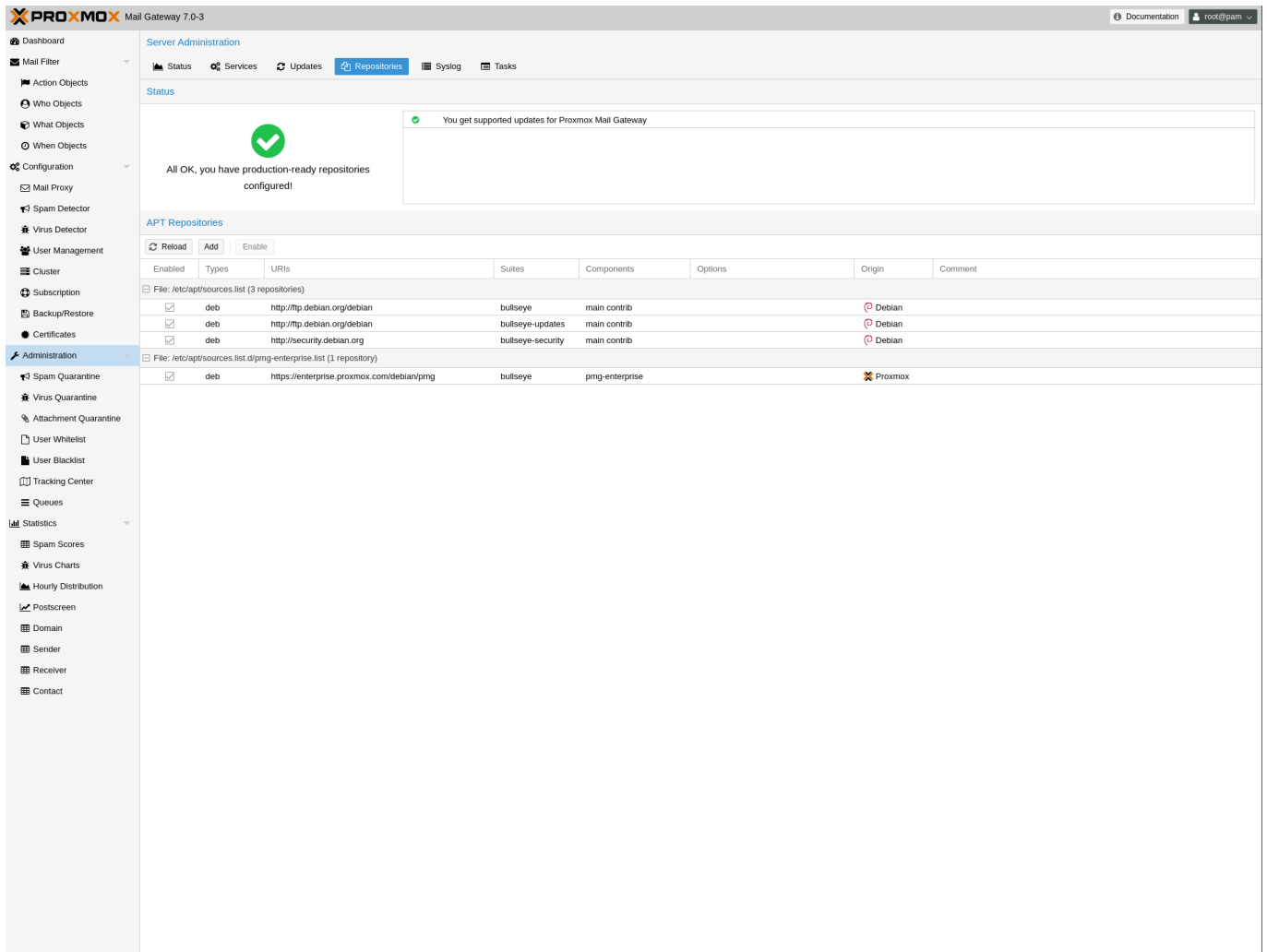
Repositories are a collection of software packages. They can be used to install new software, but are also important to get new updates.

Note

You need valid Debian and Proxmox repositories to get the latest security updates, bug fixes and new features.

APT Repositories are defined in the file `/etc/apt/sources.list` and in `.list` files placed in `/etc/apt/`

Repository Management



The screenshot shows the Proxmox Mail Gateway 7.0-3 web interface. The left sidebar contains navigation options like Dashboard, Mail Filter, Action Objects, Who Objects, What Objects, When Objects, Configuration, Mail Proxy, Spam Detector, Virus Detector, User Management, Cluster, Subscription, Backup/Restore, Certificates, Administration, Spam Quarantine, Virus Quarantine, Attachment Quarantine, User Whitelist, User Blacklist, Tracking Center, Queues, Statistics, Spam Scores, Virus Charts, Hourly Distribution, Postscreen, Domain, Sender, Receiver, and Contact. The main content area is titled 'Server Administration' and shows the 'Repositories' tab. A status message indicates that all repositories are production-ready. Below this, a table titled 'APT Repositories' lists the configured repositories.

Enabled	Types	URIs	Suites	Components	Options	Origin	Comment
File: /etc/apt/sources.list (3 repositories)							
<input checked="" type="checkbox"/>	deb	http://ftp.debian.org/debian	bullseye	main contrib		Debian	
<input checked="" type="checkbox"/>	deb	http://ftp.debian.org/debian	bullseye-updates	main contrib		Debian	
<input checked="" type="checkbox"/>	deb	http://security.debian.org	bullseye-security	main contrib		Debian	
File: /etc/apt/sources.list.d/pmg-enterprise.list (1 repository)							
<input checked="" type="checkbox"/>	deb	https://enterprise.proxmox.com/debian/pmg	bullseye	pmg-enterprise		Proxmox	

Since Proxmox Mail Gateway 7.0 you can check the repository state in the web interface. The *Dashboard* shows a high level status overview, while the separate *Repository* panel (accessible via *Administration*) shows in-depth status and list of all configured repositories.

Basic repository management, for example, activating or deactivating a repository, is also supported.

Sources.list

In a `sources.list` file, each line defines a package repository. The preferred source must come first. Empty lines are ignored. A `#` character anywhere on a line marks the remainder of that line as a comment. The available packages from a repository are acquired by running `apt update`. Updates can be installed directly using `apt`, or via the GUI (*Administration* → *Updates*).

File `/etc/apt/sources.list`

```
# basic Debian repositories:
deb http://ftp.debian.org/debian bullseye main contrib
deb http://ftp.debian.org/debian bullseye-updates main contrib

# security updates
```

```
deb http://security.debian.org/debian-security bullseye-security main ↔
  contrib

# Proxmox Mail Gateway repo required too - see below!
```

Proxmox Mail Gateway provides three different package repositories.

3.5.2 Proxmox Mail Gateway Enterprise Repository

This is the default, stable and recommended repository, available for all Proxmox Mail Gateway subscription users. It contains the most stable packages, and is suitable for production use. The `pmg-enterprise` repository is enabled by default:

File `/etc/apt/sources.list.d/pmg-enterprise.list`

```
deb https://enterprise.proxmox.com/debian/pmg bullseye pmg-enterprise
```

As soon as updates are available, the `root@pam` user is notified via email about the newly available packages. From the GUI, the change-log of each package can be viewed (if available), showing all details of the update. Thus, you will never miss important security fixes.

Please note that you need a valid subscription key to access this repository. We offer different support levels, which you can find further details about at <https://www.proxmox.com/en/proxmox-mail-gateway/pricing>.

Note

You can disable this repository by commenting out the above line using a `#` (at the start of the line). This prevents error messages, if you do not have a subscription key. Please configure the `pmg-no-subscription` repository in this case.

3.5.3 Proxmox Mail Gateway No-Subscription Repository

As the name suggests, you do not need a subscription key to access this repository. It can be used for testing and non-production use. It's not recommended to use this on production servers, as these packages are not always heavily tested and validated.

We recommend configuring this repository in `/etc/apt/sources.list`.

File `/etc/apt/sources.list`

```
deb http://ftp.debian.org/debian bullseye main contrib
deb http://ftp.debian.org/debian bullseye-updates main contrib

# security updates
deb http://security.debian.org/debian-security bullseye-security main ↔
  contrib

# PMG pmg-no-subscription repository provided by proxmox.com,
# NOT recommended for production use
deb http://download.proxmox.com/debian/pmg bullseye pmg-no-subscription
```

3.5.4 Proxmox Mail Gateway Test Repository

Finally, there is a repository called `pmgtest`. This contains the latest packages, and is heavily used by developers to test new features. As with before, you can configure this using `/etc/apt/sources.list` by adding the following line:

sources.list entry for pmgtest

```
deb http://download.proxmox.com/debian/pmg bullseye pmgtest
```



Warning

the `pmgtest` repository should only be used for testing new features or bug fixes.

3.5.5 SecureApt

We use GnuPG to sign the `Release` files inside these repositories, and APT uses these signatures to verify that all packages are from a trusted source.

The key used for verification is already installed, if you install from our installation CD. If you install via another means, you can manually download the key with:

```
# wget https://enterprise.proxmox.com/debian/proxmox-release-bullseye.gpg -O /etc/apt/trusted.gpg.d/proxmox-release-bullseye.gpg ↔
```

Verify the checksum afterwards with the `sha512sum` CLI tool:

```
# sha512sum /etc/apt/trusted.gpg.d/proxmox-release-bullseye.gpg
7 ↔
fb03ec8a1675723d2853b84aa4fdb49a46a3bb72b9951361488bfd19b29aab0a789a4f8c7406e71
/etc/apt/trusted.gpg.d/proxmox-release-bullseye.gpg
```

or the `md5sum` CLI tool:

```
# md5sum /etc/apt/trusted.gpg.d/proxmox-release-bullseye.gpg
bcc35c7173e0845c0d6ad6470b70f50e /etc/apt/trusted.gpg.d/proxmox-release- ↔
bullseye.gpg
```

3.5.6 Other Repository Sources

Certain software cannot be made available in the `main` and `contrib` areas of the [Debian](#) archives, since it does not adhere to the Debian Free Software Guidelines (DFSG). These are distributed in the [Debian's non-free archive area](#). For Proxmox Mail Gateway two packages from the `non-free` area are needed in order to support the RAR archive format:

- `p7zip-rar` for matching [Archive Objects](#) Section 5.3 in the [Rule system](#) Chapter 5
 - `libclamunrar` for detecting viruses in RAR archives.
-

Additional sources.list entry for non-free

```
deb http://deb.debian.org/debian/ bullseye non-free
deb http://security.debian.org/debian-security bullseye-security non-free
deb http://deb.debian.org/debian/ bullseye-updates non-free
```

Following this, you can install the required packages with:

```
apt update
apt install libclamunrar p7zip-rar
```

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, using the REST API over *https* or the command line tool `pmgsh`.

The command line tool `pmgconfig` is used to simplify some common configuration tasks, such as generating certificates and rewriting service configuration files.

Note

We use a Postgres database to store mail filter rules and statistical data. See chapter [Database Management](#) Section 10.1 for more information.

4.1 Configuration files overview

`/etc/network/interfaces`

Network setup. We never modify this file directly. Instead, we write changes to `/etc/network/interfaces.d`. When you reboot, Proxmox Mail Gateway renames the file to `/etc/network/interfaces`, thus applying the changes.

`/etc/resolv.conf`

DNS search domain and nameserver setup. Proxmox Mail Gateway uses the search domain setting to create the FQDN and domain name used in the postfix configuration.

`/etc/hostname`

The system's hostname. Proxmox Mail Gateway uses the hostname to create the FQDN used in the postfix configuration.

`/etc/hosts`

Static table lookup for hostnames.

`/etc/pmg/pmg.conf`

Stores common administration options, such as the spam and mail proxy configuration.

/etc/pmg/cluster.conf

The cluster setup.

/etc/pmg/domains

The list of relay domains.

/etc/pmg/dkim/domains

The list of domains for outbound DKIM signing.

/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/tls_policy

TLS policy for outbound connections.

/etc/pmg/transport

Message delivery transport setup.

/etc/pmg/user.conf

GUI user configuration.

/etc/mail/spamassassin/custom.cf

Custom **SpamAssassin™** setup.

/etc/mail/spamassassin/pmg-scores.cf

Custom **SpamAssassin™** rule scores.

4.2 Keys and Certificates

/etc/pmg/pmg-api.pem

Key and certificate (combined) used by the HTTPS server (API).

/etc/pmg/pmg-authkey.key

Private key used to generate authentication tickets.

/etc/pmg/pmg-authkey.pub

Public key used 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).

/etc/pmg/dkim/<selector>.private

Key for DKIM signing mails with selector <selector>.

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. These services use separate configuration files, so we need to rewrite those files when the configuration is changed.

We use a template-based approach to generate these 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 these directly, otherwise your modifications will be lost on the next update. Instead, copy the template you wish to change to `/etc/pmg/templates/`, then apply your changes there.

Templates can access any configuration settings, 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 the regeneration of all template-based configuration files. You need to run the following after modifying a template, or when you directly edit configuration files:

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

The above command also restarts services if the 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 White- and Blacklists

Proxmox Mail Gateway has multiple white- and blacklists. It differentiates between the [SMTP Whitelist](#) Section 4.7.4, the rule-based whitelist and the user whitelist. In addition to the whitelists, there are two separate blacklists: the rule-based blacklist and the user blacklist.

4.4.1 SMTP Whitelist

The [SMTP Whitelist](#) Section 4.7.4 is responsible for disabling greylisting, as well as SPF and DNSBL checks. These are done during the SMTP dialogue.

4.4.2 Rule-based White-/Blacklist

The [rule-based white- and blacklists](#) Chapter 5 are predefined rules. They work by checking the attached *Who* objects, containing, for example, a domain or a mail address for a match. If it matches, the assigned action is used, which by default is *Accept* for the whitelist rule and *Block* for the blacklist rule. In the default setup, the blacklist rule has priority over the whitelist rule and spam checks.

4.4.3 User White-/Blacklist

The user white- and blacklist are user specific. Every user can add mail addresses to their white- and blacklist. When a user adds a mail address to the whitelist, the result of the spam analysis will be discarded for that recipient. This can help in the mail being accepted, but what happens next still depends on the other rules. In the default setup, this results in the mail being accepted for this recipient.

For mail addresses on a user's blacklist, the spam score will be increased by 100. What happens when a high spam score is encountered still depends on the rule system. In the default setup, it will be recognized as spam and quarantined (spam score of 3 or higher).

4.5 System Configuration

4.5.1 Network and Time

The screenshot displays the Proxmox Mail Gateway 6.2-1 GUI. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area is titled 'Configuration: System' and has tabs for 'Network/Time', 'Options', and 'Backup/Restore'. The 'Network/Time' tab is active, showing three sections: 'Interfaces', 'DNS', and 'Time'.

Interfaces

Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
ens18	Network Device	Yes	Yes	No			192.168.30.12...	192.168.16.1	

DNS

Edit

Search domain: proxmox.com

DNS server 1: 192.168.2.15

Time

Edit

Time zone: Europe/Vienna

Server time: 2020-04-23 16:04:08

As network and time are configured in the installer, these generally do not need to be configured again in the GUI.

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 the 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 publicly 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 needs to be configured in *recursive* mode.

4.5.2 Options

The screenshot shows the Proxmox Mail Gateway 6.2-1 web interface. The top navigation bar includes the Proxmox logo, the version 'Mail Gateway 6.2-1', and a user profile 'admin@pmg'. The left sidebar contains a menu with categories like Mail Filter, Action Objects, Who Objects, What Objects, When Objects, Configuration, Mail Proxy, Spam Detector, Virus Detector, User Management, Cluster, Subscription, Administration, Spam Quarantine, Virus Quarantine, Attachment Quarantine, User Whitelist, User Blacklist, Tracking Center, Queues, and Statistics. The main content area is titled 'Configuration: System' and has three tabs: 'Network/Time', 'Options', and 'Backup/Restore'. The 'Options' tab is active, showing a table of settings:

Edit	
Send daily admin reports	Yes
Use advanced statistic filters	Yes
User statistic lifetime (days)	7
Administrator EMail	t.lamprecht@proxmox.com
HTTP proxy	none

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

advfilter: <boolean> (**default = 1**)

Use advanced filters for statistic.

avast: <boolean> (**default = 0**)

Use Avast Virus Scanner (`/usr/bin/scan`). You need to buy and install *Avast Core Security* before you can enable this feature.

clamav: <boolean> (**default = 1**)

Use ClamAV Virus Scanner. This is the default virus scanner and is enabled by default.

custom_check: <boolean> (*default = 0*)

Use Custom Check Script. The script has to take the defined arguments and can return Virus findings or a Spamscore.

custom_check_path: `^ / ([^ / \ 0] + \ /) + [^ / \ 0] + $` (*default = /usr/local/bin/pmg-custom-check*)

Absolute Path to the Custom Check Script

dailyreport: <boolean> (*default = 1*)

Send daily reports.

demo: <boolean> (*default = 0*)

Demo mode - do not start SMTP filter.

dkim_selector: <string>

Default DKIM selector

dkim_sign: <boolean> (*default = 0*)

DKIM sign outbound mails with the configured Selector.

dkim_sign_all_mail: <boolean> (*default = 0*)

DKIM sign all outgoing mails irrespective of the Envelope From domain.

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)

4.6 Certificate Management

Access to the web-based administration interface is always encrypted through `https`. Each Proxmox Mail Gateway host creates by default its own (self-signed) certificate. This certificate is used for encrypted communication with the host's `pmgproxy` service, for any API call between a user and the web-interface or between nodes in a cluster.

Certificate verification in a Proxmox Mail Gateway cluster is done based on pinning the certificate fingerprints in the cluster configuration and verifying that they match on connection.

4.6.1 Certificates for the API and SMTP

Proxmox Mail Gateway uses two different certificates:

- `/etc/pmg/pmg-api.pem`: the required certificate used for Proxmox Mail Gateway API requests.
- `/etc/pmg/pmg-tls.pem`: the optional certificate used for SMTP TLS connections, see [mailproxy TLS configuration](#) Section 4.7.9 for details.

You have the following options for these certificates:

1. Keep using the default self-signed certificate in `/etc/pmg/pmg-api.pem`.
2. Use an externally provided certificate (for example, signed by a commercial Certificate Authority (CA)).
3. Use an ACME provider like Let's Encrypt to get a trusted certificate with automatic renewal; this is also integrated in the Proxmox Mail Gateway API and web interface.

Certificates are managed through the Proxmox Mail Gateway web-interface/API or using the `pmgconfig` CLI tool.

4.6.2 Upload Custom Certificate

If you already have a certificate which you want to use for a Proxmox Mail Gateway host, you can simply upload that certificate over the web interface.

Upload Custom Certificate

Private Key (Optional):

No change

From File

Certificate Chain:

```
-----BEGIN CERTIFICATE-----
MIIFBzCCAu+gAwIBAgIUWesRZvSVZKb9pB4O+1ILk1F4o0wDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwlcG1nLWRibW8wHhcNMjAwNDIyMTMzOTA1WhcNMzAwNDIw
MTMzOTA1WiATMREwDwYDVOODDAhwbWctZGVtbzCCAILwDOYJKoZIhvcNAOEBOAD
```

From File

Upload

Note that any certificate key files must not be password protected.

4.6.3 Trusted certificates via Let's Encrypt (ACME)

Proxmox Mail Gateway includes an implementation of the **Automatic Certificate Management Environment (ACME)** protocol, allowing Proxmox Mail Gateway admins to use an ACME provider like Let's Encrypt for easy setup of TLS certificates, which are accepted and trusted by modern operating systems and web browsers out of the box.

Currently, the two ACME endpoints implemented are the [Let's Encrypt \(LE\)](#) production and staging environments. Our ACME client supports validation of `http-01` challenges using a built-in web server and validation of `dns-01` challenges using a DNS plugin supporting all the DNS API endpoints [acme.sh](#) does.

ACME Account

The screenshot shows a 'Register Account' dialog box with the following fields and values:

- Account Name: default
- E-Mail: admin@example.com
- ACME Directory: Let's Encrypt V2
- Accept TOS:

A link to the Let's Encrypt SA v1.2 document is provided below the directory selection. A 'Register' button is located at the bottom right of the form.

You need to register an ACME account per cluster, with the endpoint you want to use. The email address used for that account will serve as the contact point for renewal-due or similar notifications from the ACME endpoint.

You can register or deactivate ACME accounts over the web interface `Certificates -> ACME Accounts` or using the `pmgconfig` command line tool.

```
pmgconfig acme account register <account-name> <mail@example.com>
```

Tip

Because of **rate-limits** you should use `LE staging` for experiments or if you use ACME for the very first time until all is working there, and only then switch over to the production directory.

ACME Plugins

The ACME plugin's role is to provide automatic verification that you, and thus the Proxmox Mail Gateway cluster under your operation, are the real owner of a domain. This is the basic building block of automatic certificate management.

The ACME protocol specifies different types of challenges, for example the `http-01`, where a web server provides a file with a specific token to prove that it controls a domain. Sometimes this isn't possible, either because of technical limitations or if the address of a record is not reachable from the public internet. The `dns-01` challenge can be used in such cases. This challenge is fulfilled by creating a certain DNS record in the domain's zone.

The screenshot shows the 'Add: ACME DNS Plugin' configuration form with the following values:

- Plugin ID: pdns1
- Validation Delay: 30
- DNS API: PowerDNS server
- PDNS_ServerId: pdns1
- PDNS_Token: s11GDx8fbDPKX/UT6aDpHEGukUwWqVv1y3zFgODYBXM=
- PDNS_Ttl: 10
- PDNS_Url: 192.168.0.2

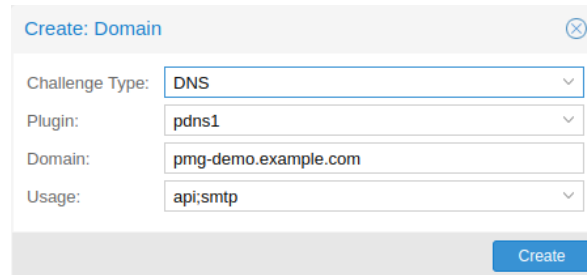
An 'Add' button is located at the bottom right of the form.

Proxmox Mail Gateway supports both of those challenge types out of the box, you can configure plugins either over the web interface under `Certificates -> ACME Challenges`, or using the `pmgconfig acme plugin add` command.

ACME Plugin configurations are stored in `/etc/pmg/acme/plugins.cfg`. A plugin is available for all nodes in the cluster.

Domains

You can add new or manage existing domain entries under `Certificates`, or using the `pmgconfig` command.



The screenshot shows a web form titled "Create: Domain". It contains four dropdown menus: "Challenge Type" (selected: DNS), "Plugin" (selected: pdns1), "Domain" (selected: pmg-demo.example.com), and "Usage" (selected: api:smtp). A blue "Create" button is located at the bottom right of the form.

After configuring the desired domain(s) for a node and ensuring that the desired ACME account is selected, you can order your new certificate over the web-interface. On success, the interface will reload after roughly 10 seconds.

Renewal will happen [automatically](#) Section 4.6.6.

4.6.4 ACME HTTP Challenge Plugin

There is always an implicitly configured `standalone` plugin for validating `http-01` challenges via the built-in web server spawned on port 80.

Note

The name `standalone` means that it can provide the validation on its own, without any third party service. So this plugin also works for cluster nodes.

There are a few prerequisites to use this for certificate management with Let's Encrypts ACME.

- You have to accept the ToS of Let's Encrypt to register an account.
- **Port 80** of the node needs to be reachable from the internet.
- There **must** be no other listener on port 80.
- The requested (sub)domain needs to resolve to a public IP of the Proxmox Mail Gateway host.

4.6.5 ACME DNS API Challenge Plugin

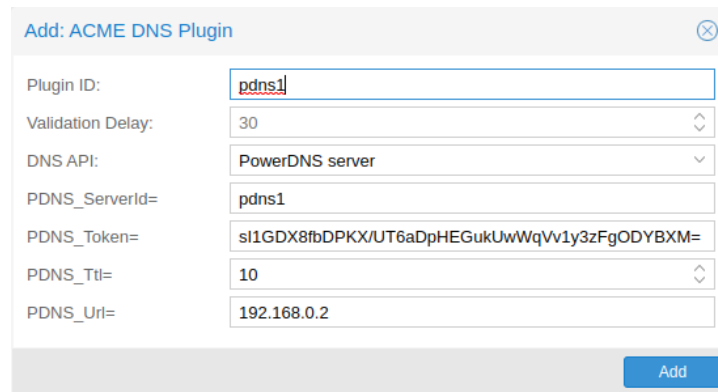
On systems where external access for validation via the `http-01` method is not possible or desired, it is possible to use the `dns-01` validation method. This validation method requires a DNS server that allows provisioning of `TXT` records via an API.

Configuring ACME DNS APIs for validation

Proxmox Mail Gateway re-uses the DNS plugins developed for the `acme.sh`¹ project. Please refer to its documentation for details on configuration of specific APIs.

¹acme.sh <https://github.com/acmesh-official/acme.sh>

The easiest way to configure a new plugin with the DNS API is using the web interface (Certificates -> ACME Accounts/Challenges).



Field	Value
Plugin ID:	pdns1
Validation Delay:	30
DNS API:	PowerDNS server
PDNS_ServerId=	pdns1
PDNS_Token=	s11GDX8fbDPKX/UT6aDpHEGukUwWqVv1y3zFgODYBXM=
PDNS_Ttl=	10
PDNS_Url=	192.168.0.2

Here you can add a new challenge plugin by selecting your API provider and entering the credential data to access your account over their API.

Tip

See the acme.sh [How to use DNS API](#) wiki for more detailed information about getting API credentials for your provider. Configuration values do not need to be quoted with single or double quotes; for some plugins that is even an error.

As there are many DNS providers and API endpoints, Proxmox Mail Gateway automatically generates the form for the credentials, but not all providers are annotated yet. For those you will see a bigger text area, into which you simply need to copy all the credential's KEY=VALUE pairs.

DNS Validation through CNAME Alias

A special `alias` mode can be used to handle validation on a different domain/DNS server, in case your primary/real DNS does not support provisioning via an API. Manually set up a permanent CNAME record for `_acme-challenge.domain1.example` pointing to `_acme-challenge.domain2.example`, and set the `alias` property in the Proxmox Mail Gateway node configuration file `/etc/pmg/node.conf` to `domain2.example` to allow the DNS server of `domain2.example` to validate all challenges for `domain1.example`.

Wildcard Certificates

Wildcard DNS names start with a `*.` prefix and are considered valid for all (one-level) subdomain names of the verified domain. So a certificate for `*.domain.example` is valid for `foo.domain.example` and `bar.domain.example`, but not for `baz.foo.domain.example`.

Currently, you can only create wildcard certificates with the [DNS challenge type](#).

Combination of Plugins

Combining `http-01` and `dns-01` validation is possible in case your node is reachable via multiple domains with different requirements / DNS provisioning capabilities. Mixing DNS APIs from multiple providers or instances is also possible by specifying different plugin instances per domain.

Tip

Accessing the same service over multiple domains increases complexity and should be avoided if possible.

4.6.6 Automatic renewal of ACME certificates

If a node has been successfully configured with an ACME-provided certificate (either via `pmgconfig` or via the web-interface/API), the certificate will be renewed automatically by the `pmg-daily.service`. Currently, renewal is triggered if the certificate either has already expired or if it will expire in the next 30 days.

4.6.7 Manually Change Certificate over Command-Line

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

Log in to your Proxmox Mail Gateway via `ssh` or use the console:

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

Follow the instructions on the screen, for 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 have finished the 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 Mail Gateway.

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

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

Then restart the API servers:

```
systemctl restart pmgproxy
```

Test your new certificate, using your browser.

Note

To transfer files to and from your Proxmox Mail Gateway, you can use secure copy: If your desktop runs Linux, you can use the `scp` command line tool. If your desktop PC runs windows, please use an `scp` client like WinSCP (see <https://winscp.net/>).

4.6.8 Change Certificate for Cluster Setups

If you change the API certificate of an active cluster node manually, you also need to update the pinned fingerprint inside the cluster configuration.

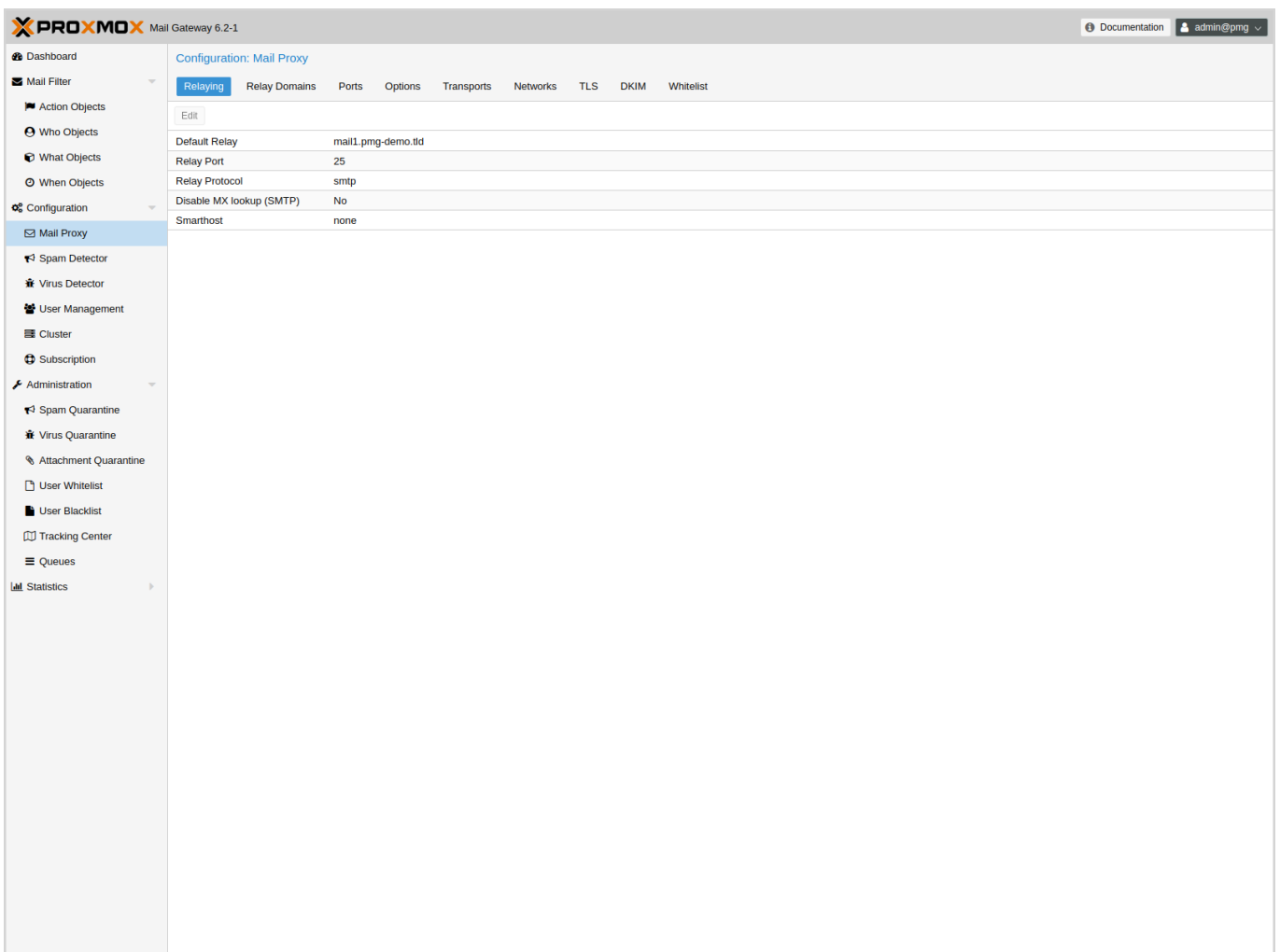
You can do that by executing the following command on the host where the certificate changed:

```
pmgcm update-fingerprints
```

Note, this will be done automatically if using the integrated ACME (for example, through Let's Encrypt) feature.

4.7 Mail Proxy Configuration

4.7.1 Relaying



The screenshot shows the Proxmox Mail Gateway 6.2-1 web interface. The left sidebar contains a navigation menu with categories like Mail Filter, Configuration, and Administration. The main content area is titled 'Configuration: Mail Proxy' and has a sub-tab 'Relaying' selected. Below the sub-tab is an 'Edit' button and a table of configuration settings.

Default Relay	mail1.pmg-demo.tld
Relay Port	25
Relay Protocol	smtp
Disable MX lookup (SMTP)	No
Smarthost	none

These settings are saved to the *mail* subsection 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 (SMTP only, ignored for LMTP).

relayport: <integer> (1 - 65535) (*default = 25*)

SMTP/LMTP port number for relay host.

relayprotocol: <lmtp | smtp> (*default = smtp*)

Transport protocol for relay host.

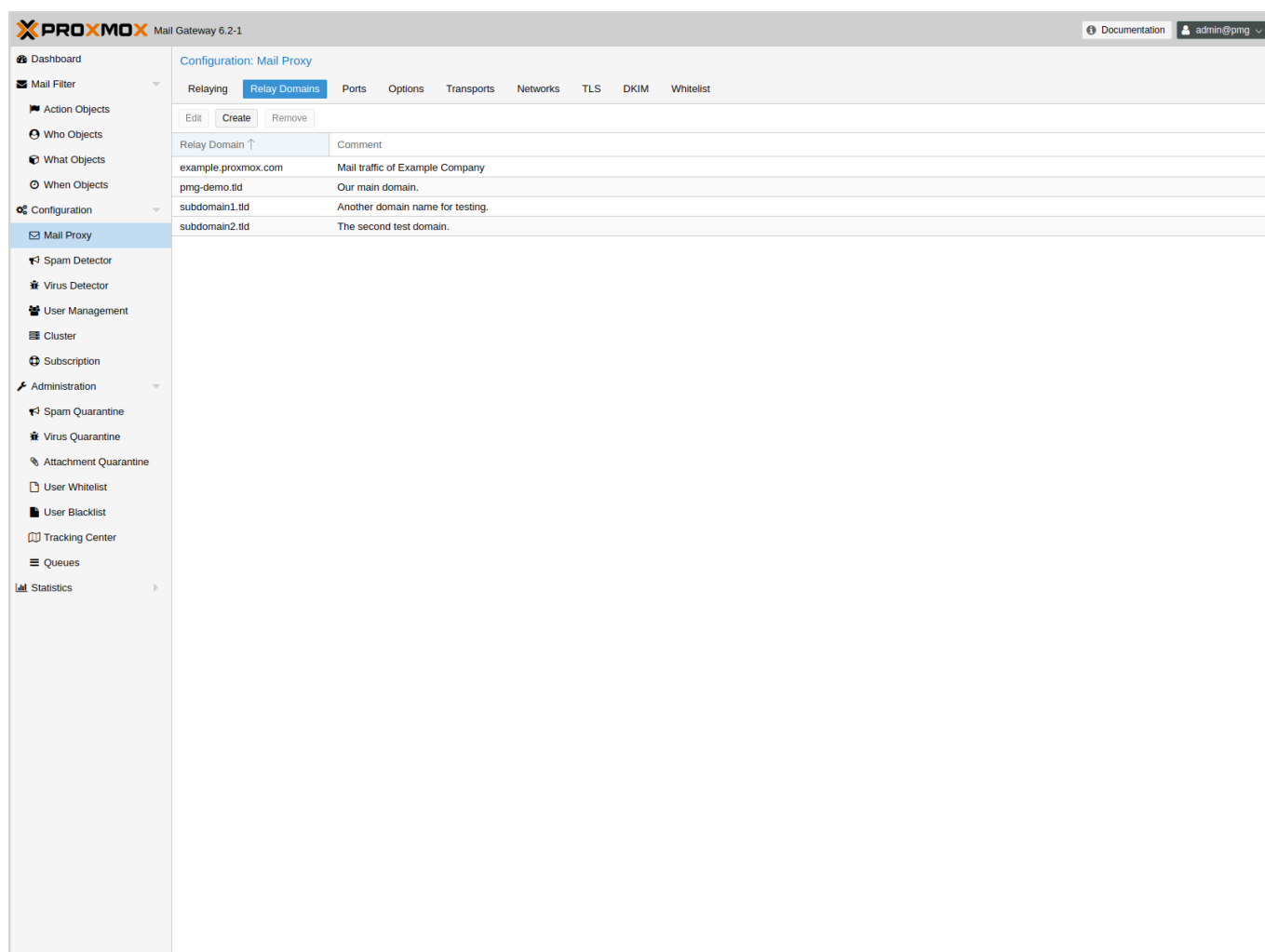
smarthost: <string>

When set, all outgoing mails are delivered to the specified smarthost.

smarthostport: <integer> (1 - 65535) (*default = 25*)

SMTP port number for smarthost.

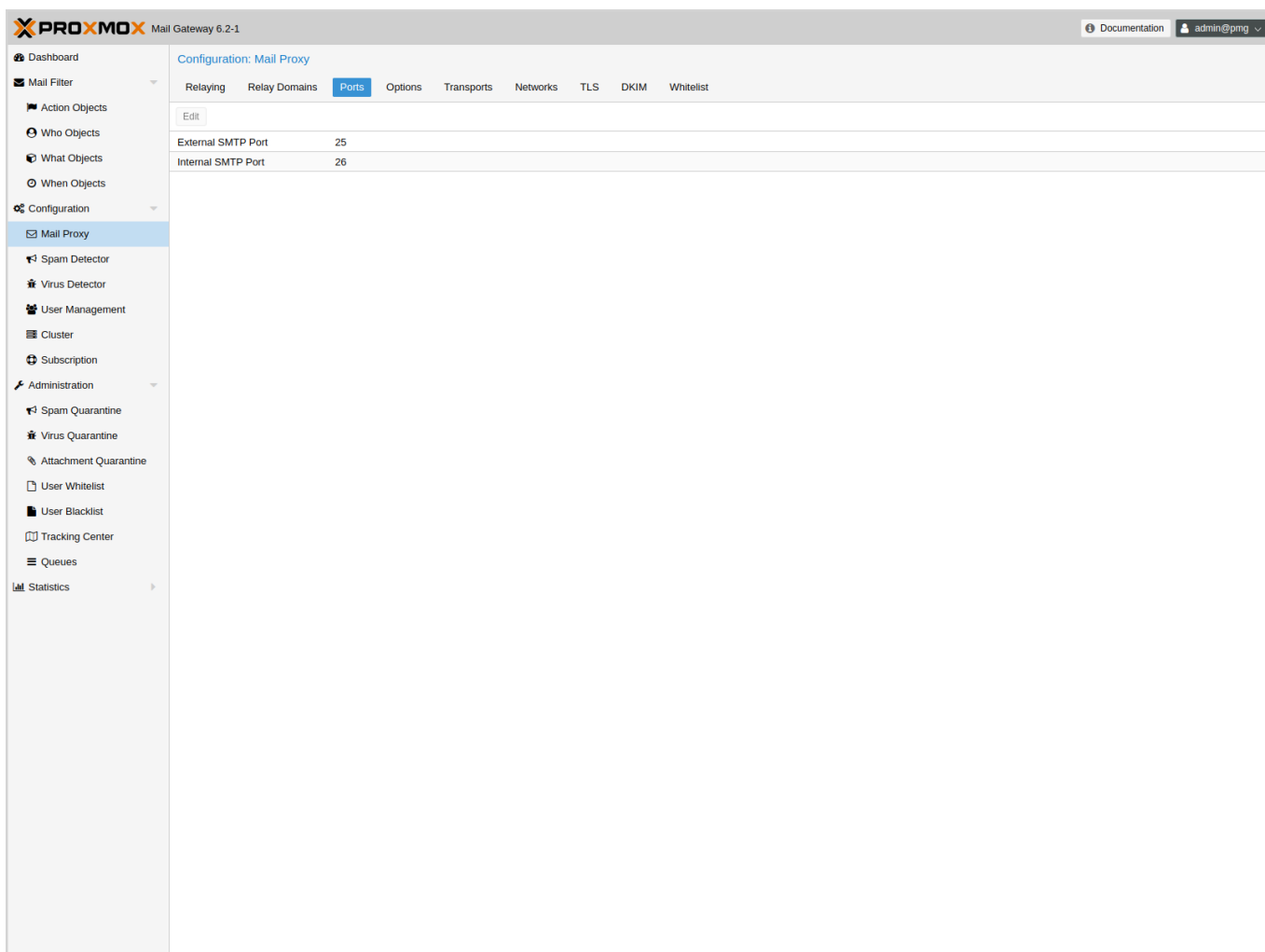
4.7.2 Relay Domains



Relay Domain	Comment
example.proxmox.com	Mail traffic of Example Company
pmg-demo.tld	Our main domain.
subdomain1.tld	Another domain name for testing.
subdomain2.tld	The second test domain.

A list of relayed mail domains, that is, what destination domains this system will relay mail to. The system will reject incoming mails to other domains.

4.7.3 Ports



Configuration: Mail Proxy	
External SMTP Port	25
Internal SMTP Port	26

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

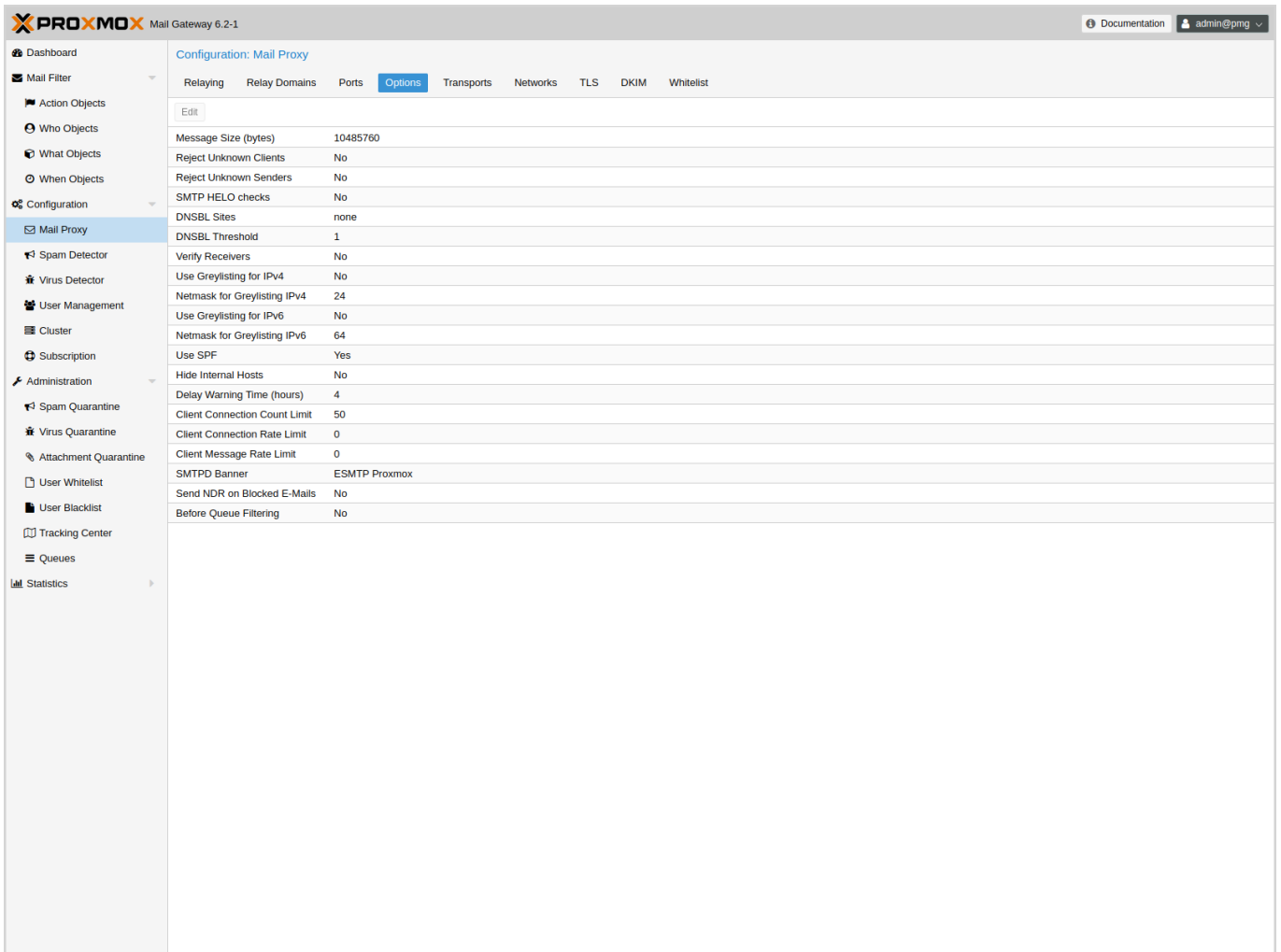
ext_port: <integer> (1 - 65535) (default = 25)

SMTP port number for incoming mail (untrusted). This must be a different number than *int_port*.

int_port: <integer> (1 - 65535) (default = 26)

SMTP port number for outgoing mail (trusted).

4.7.4 Options



The screenshot shows the Proxmox Mail Gateway Administration interface. The left sidebar contains a navigation menu with categories like Mail Filter, Configuration, Administration, and Statistics. The main content area is titled 'Configuration: Mail Proxy' and has tabs for Relaying, Relay Domains, Ports, Options (selected), Transports, Networks, TLS, DKIM, and Whitelist. Below the tabs is an 'Edit' button and a table of configuration options.

Option	Value
Message Size (bytes)	10485760
Reject Unknown Clients	No
Reject Unknown Senders	No
SMTP HELO checks	No
DNSBL Sites	none
DNSBL Threshold	1
Verify Receivers	No
Use Greylisting for IPv4	No
Netmask for Greylisting IPv4	24
Use Greylisting for IPv6	No
Netmask for Greylisting IPv6	64
Use SPF	Yes
Hide Internal Hosts	No
Delay Warning Time (hours)	4
Client Connection Count Limit	50
Client Connection Rate Limit	0
Client Message Rate Limit	0
SMTPD Banner	ESMTP Proxmox
Send NDR on Blocked E-Mails	No
Before Queue Filtering	No

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

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

before_queue_filtering: <boolean> (**default = 0**)
Enable before queue filtering by pmg-smtp-filter

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).

dnsbl_threshold: <integer> (0 - N) (default = 1)

The inclusive lower bound for blocking a remote SMTP client, based on its combined DNSBL score (see `postscreen_dnsbl_threshold` parameter).

dwarning: <integer> (0 - N) (default = 4)

SMTP delay warning time (in hours).

greylist: <boolean> (default = 1)

Use Greylisting for IPv4.

greylist6: <boolean> (default = 0)

Use Greylisting for IPv6.

greylistmask4: <integer> (0 - 32) (default = 24)

Netmask to apply for greylisting IPv4 hosts

greylistmask6: <integer> (0 - 128) (default = 64)

Netmask to apply for greylisting IPv6 hosts

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.

ndr_on_block: <boolean> (default = 0)

Send out NDR when mail gets blocked

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 specifies the numerical reply code when the Postfix SMTP server rejects a recipient address.

4.7.5 Before and After Queue scanning

Email scanning can happen at two different stages of mail-processing:

- Before-queue filtering: During the SMTP session, after the complete message has been received (after the *DATA* command).
- After-queue filtering: After initially accepting the mail and putting it on a queue for further processing.

Before-queue filtering has the advantage that the system can reject a mail (by sending a permanent reject code *554*), and leave the task of notifying the original sender to the other mail server. This is of particular advantage if the processed mail is a spam message or contains a virus and has a forged sender address. Sending out a notification in this situation leads to so-called *backscatter* mail, which might cause your server to get listed as spamming on RBLs (Real-time Blackhole List).

After-queue filtering has the advantage of providing faster delivery of mails for the sending servers, since queuing emails is much faster than analyzing them for spam and viruses.

If a mail is addressed to multiple recipients (for example, when multiple addresses are subscribed to the same mailing list), the situation is more complicated; your mail server can only reject or accept the mail for all recipients, after having received the complete message, while your rule setup might accept the mail for part of the recipients and reject it for others. This can be due to a complicated rule setup, or if your users use the *User White- and Blacklist* feature.

If the resulting action of the rule system is the same for all recipients, Proxmox Mail Gateway responds accordingly, if configured for before-queue filtering (sending *554* for a blocked mail and *250* for an accepted or quarantined mail). If some mailboxes accept the mail and some reject it, the system has to accept the mail.

Whether Proxmox Mail Gateway notifies the sender that delivery failed for some recipients by sending a non-delivery report, depends on the *ndr_on_block* setting in */etc/pmg/pmg.conf*. If enabled, an NDR is sent. Keeping this disabled prevents NDRs being sent to the (possibly forged) sender and thus minimizes the chance of getting your IP listed on an RBL. However in certain environments, it can be unacceptable not to inform the sender about a rejected mail.

The setting has the same effect if after-queue filtering is configured, with the exception that an NDR is always sent out, even if all recipients block the mail, since the mail already got accepted before being analyzed.

The details of integrating the mail proxy with [Postfix](#) in both setups are explained in [Postfix Before-Queue Content Filter](#) and [Postfix After-Queue Content Filter](#) respectively.

4.7.6 Greylisting

Greylisting is a technique for preventing unwanted messages from reaching the resource intensive stages of content analysis (virus detection and spam detection). By initially replying with a temporary failure code (*450*) to each new email, Proxmox Mail Gateway tells the sending server that it should queue the mail and retry delivery at a later point. Since certain kinds of spam get sent out by software which has no provisioning for queuing, these mails are dropped without reaching Proxmox Mail Gateway or your mailbox.

The downside of greylisting is the delay introduced by the initial deferral of the email, which usually amounts to less than 30 minutes.

In order to prevent unnecessary delays in delivery from known sources, emails coming from a source for a recipient, which have passed greylisting in the past are directly passed on: For each email the triple *<sender*

network, sender email, recipient email> is stored in a list, along with the time when delivery was attempted. If an email fits an already existing triple, the timestamp for that triple is updated, and the email is accepted for further processing.

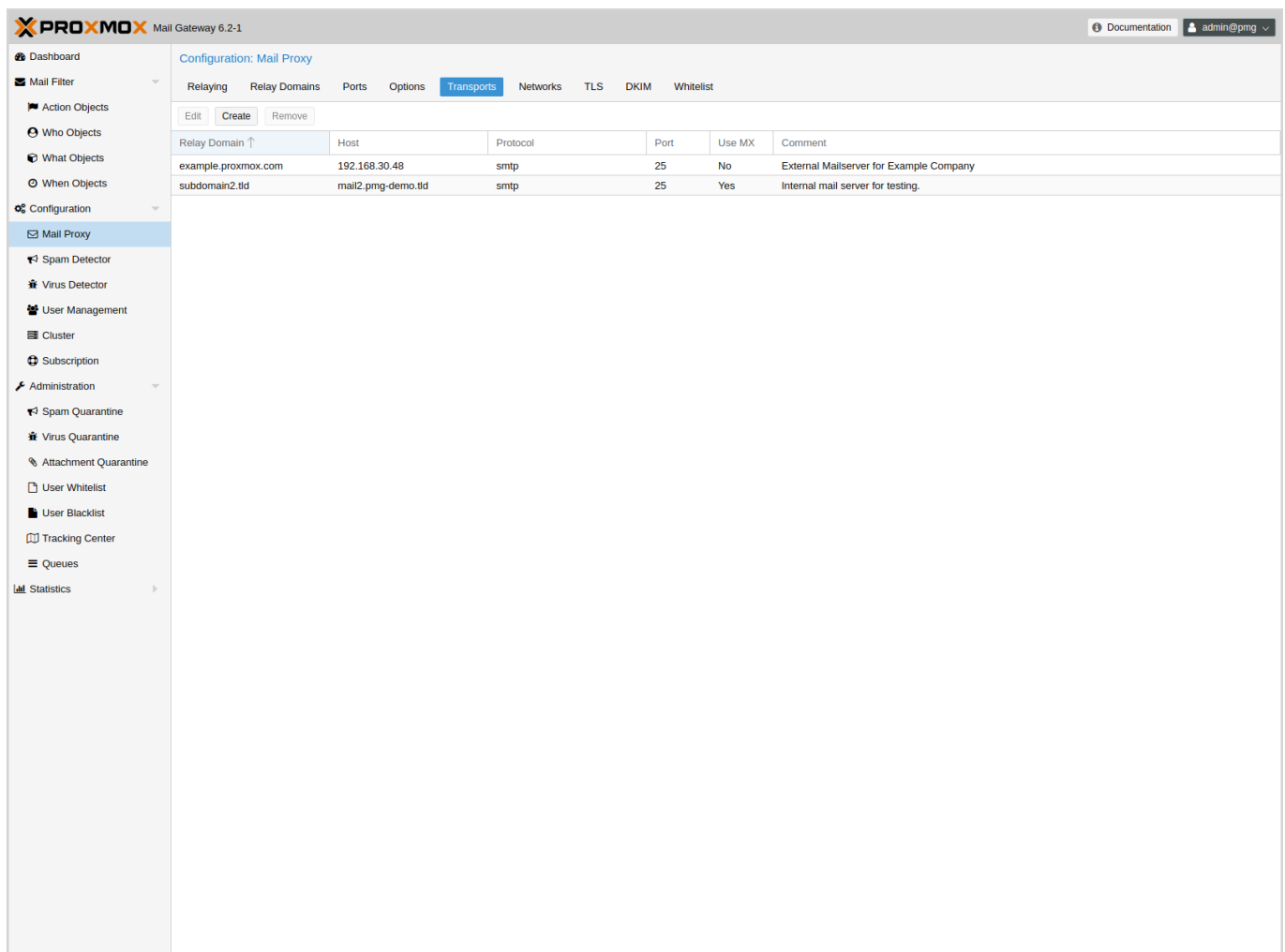
As long as a sender and recipient communicate frequently, there is no delay introduced by enabling greylisting. A triple is removed after a longer period of time, if no mail fitting that triple has been seen. The timeouts in Proxmox Mail Gateway are:

- 2 days for the retry of the first delivery
- 36 days for a known triple

Mails with an empty envelope sender are always delayed.

Some email service providers send out emails for one domain from multiple servers. To prevent delays due to an email coming in from two separate IPs of the same provider, the triples store a network (*cidr*) instead of a single IP. For certain large providers, the default network size might be too small. You can configure the netmask applied to an IP for the greylist lookup in */etc/pmg/pmg.conf* or in the GUI with the settings *greylistmask* for IPv4 and *greylistmask6* for IPv6 respectively.

4.7.7 Transports



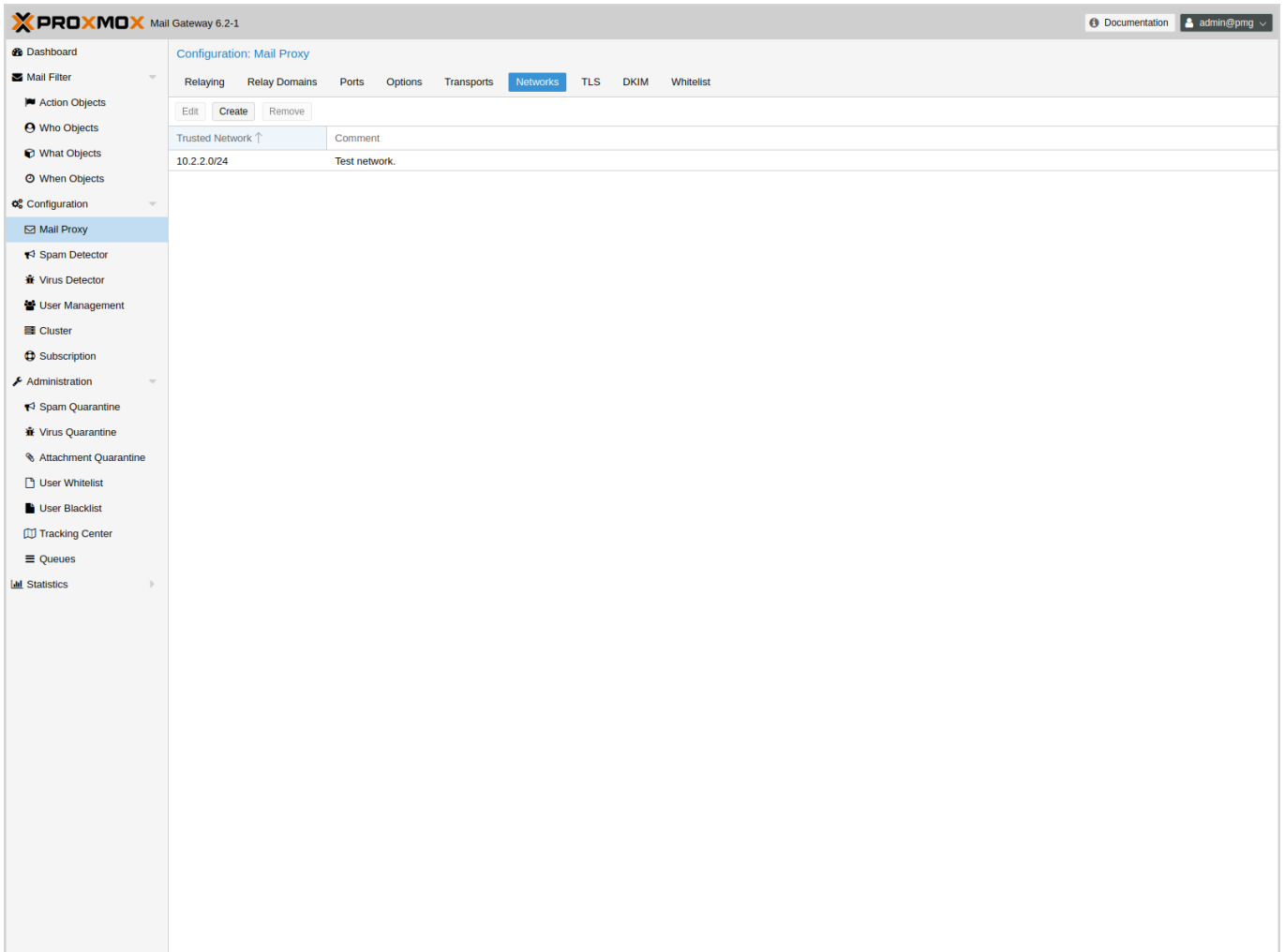
The screenshot shows the Proxmox Mail Gateway 6.2-1 GUI. The left sidebar contains a navigation menu with categories like Mail Filter, Configuration, and Administration. The main content area is titled 'Configuration: Mail Proxy' and has tabs for Relaying, Relay Domains, Ports, Options, Transports (selected), Networks, TLS, DKIM, and Whitelist. Below the tabs are buttons for 'Edit', 'Create', and 'Remove'. A table lists the configured transports:

Relay Domain ↑	Host	Protocol	Port	Use MX	Comment
example.proxmox.com	192.168.30.48	smtp	25	No	External Mailserver for Example Company
subdomain2.tld	mail2.pmg-demo.tld	smtp	25	Yes	Internal mail server for testing.

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

You can add the IP addresses, hostname, transport protocol (smtp/lmtp), transport ports and mail domains (or just single email addresses) of your additional email servers. When transport protocol is set to `lmtp`, the option *Use MX* is useless and will automatically be set to *No*.

4.7.8 Networks



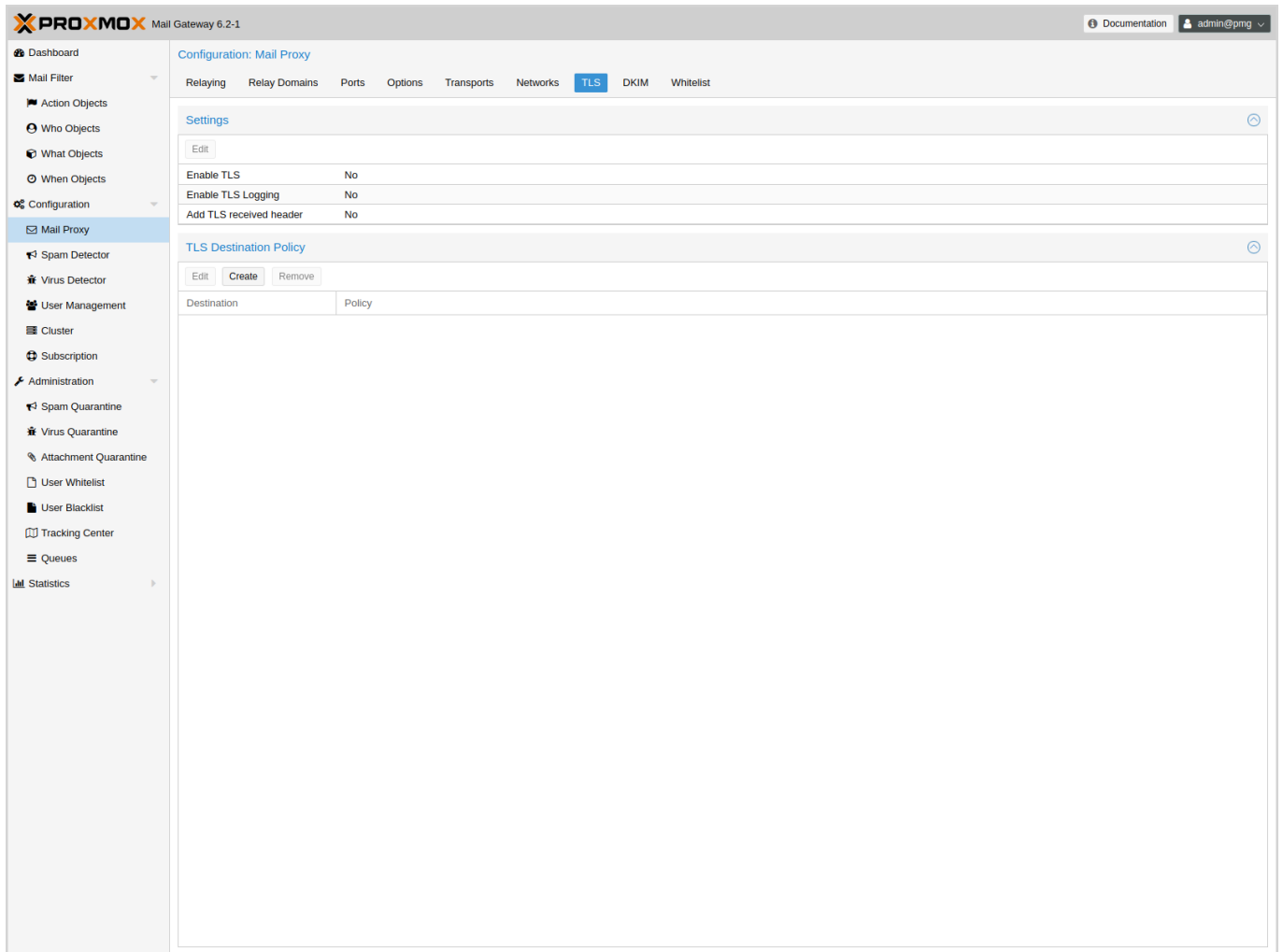
The screenshot displays the Proxmox Mail Gateway 6.2-1 web interface. The main content area is titled 'Configuration: Mail Proxy' and shows the 'Networks' configuration page. The page has a navigation menu on the left and a top navigation bar with tabs for 'Relaying', 'Relay Domains', 'Ports', 'Options', 'Transports', 'Networks', 'TLS', 'DKIM', and 'Whitelist'. The 'Networks' tab is active. Below the tabs, there are buttons for 'Edit', 'Create', and 'Remove'. A table lists trusted networks with two columns: 'Trusted Network' and 'Comment'. One entry is shown: '10.2.2.0/24' with the comment 'Test network.'

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 as Proxmox Mail Gateway can relay by default and don't need to be added to this list.

4.7.9 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 by default. The SMTP transaction is encrypted if the `STARTTLS` ESMTP feature is supported by the remote server. Otherwise, messages are sent unencrypted.

You can set a different TLS policy per destination. A destination is either a remote domain or a next-hop destination, as specified in `/etc/pmg/transport`. This can be used if you need to prevent email delivery without encryption, or to work around a broken `STARTTLS` ESMTP implementation. See [Postfix TLS Readme](#) for details on the supported policies.

Enable TLS logging

To get additional information about SMTP TLS activity, you can enable TLS logging. In this case, information about TLS sessions and used certificates 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.

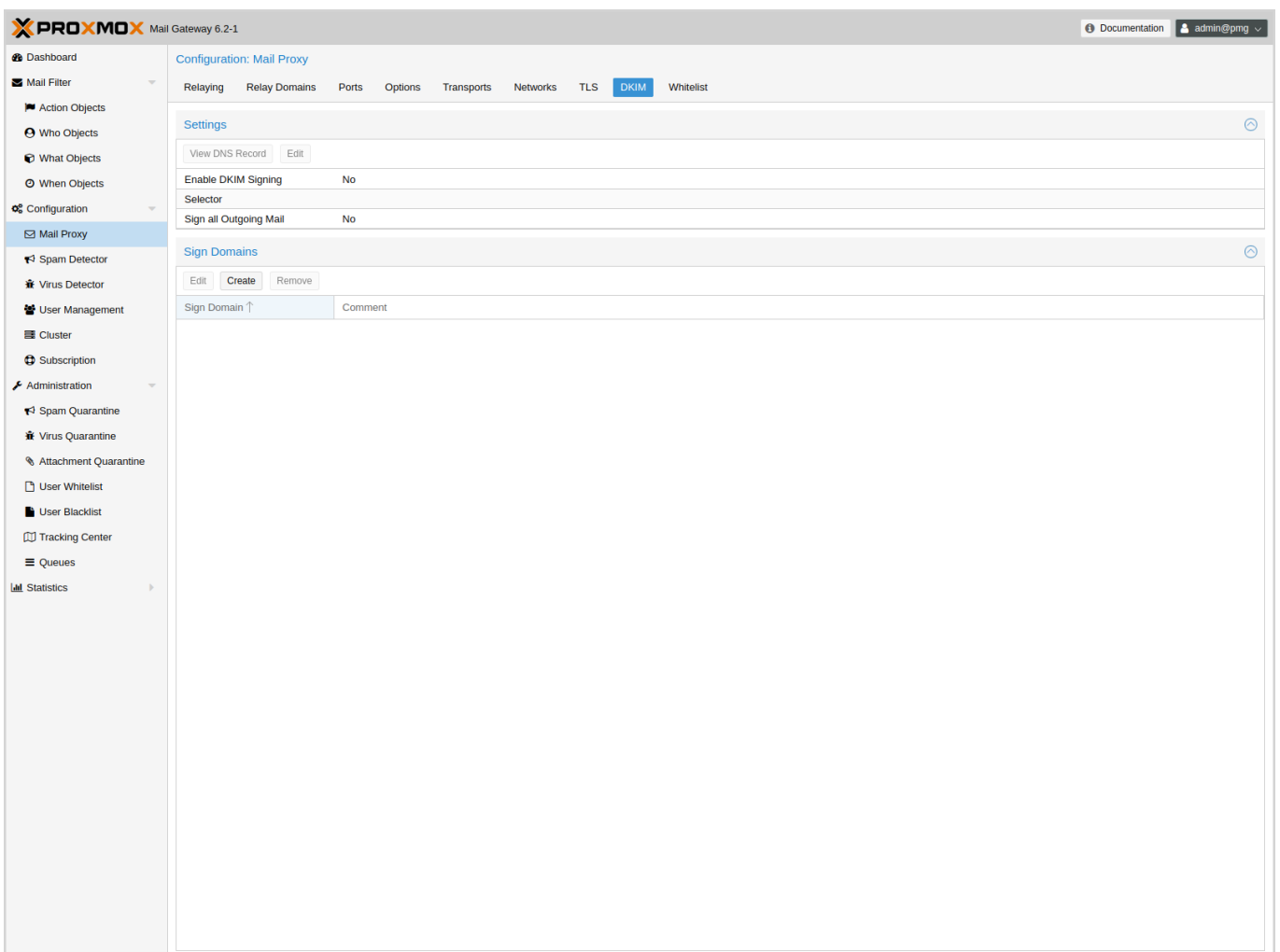
Those settings are saved to subsection *mail* in `/etc/pmg/pmg.conf`, using the following configuration keys:

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

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

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

4.7.10 DKIM Signing



The screenshot shows the Proxmox Mail Gateway 6.2-1 web interface. The top navigation bar includes 'PROXMOX Mail Gateway 6.2-1', 'Documentation', and 'admin@pmg'. The left sidebar contains a navigation menu with categories like 'Mail Filter', 'Configuration', 'Administration', and 'Statistics'. The main content area is titled 'Configuration: Mail Proxy' and has tabs for 'Relaying', 'Relay Domains', 'Ports', 'Options', 'Transports', 'Networks', 'TLS', 'DKIM', and 'Whitelist'. The 'DKIM' tab is selected. The 'Settings' section has a 'View DNS Record' and 'Edit' button. Below it, there are three rows: 'Enable DKIM Signing' (No), 'Selector' (empty), and 'Sign all Outgoing Mail' (No). The 'Sign Domains' section has 'Edit', 'Create', and 'Remove' buttons. Below that is a table with columns 'Sign Domain' and 'Comment', currently empty.

DomainKeys Identified Mail (DKIM) Signatures (see [RFC 6376](#)) is a method to cryptographically authenticate a mail as originating from a particular domain. Before sending the mail, a hash over certain header fields and the body is computed, signed with a private key and added in the `DKIM-Signature` header of the mail. The *selector* (a short identifier chosen by you, used to identify which system and private key were used for signing) is also included in the `DKIM-Signature` header.

The verification is done by the receiver. The public key is fetched via DNS TXT lookup for `yourselector._domainkey.yourdomain` and used for verifying the hash. You can publish multiple selectors for your domain, each used by a system which sends email from your domain, without the need to share the private key.

Proxmox Mail Gateway verifies DKIM Signatures for inbound mail in the Spam Filter by default.

Additionally, it supports conditionally signing outbound mail, if configured. It uses one private key and selector per Proxmox Mail Gateway deployment (all nodes in a cluster use the same key). The key has a minimal size of 1024 bits and `rsa-sha256` is used as the signing algorithm.

The headers included in the signature are taken from the list of `Mail::DKIM::Signer`. Additionally `Content-Type` (if present), `From`, `To`, `CC`, `Reply-To` and `Subject` get oversigned.

You can either sign all mails received on the internal port using the domain of the envelope sender address or create a list of domains, for which emails should be signed, defaulting to the list of relay domains.

Enable DKIM Signing

Controls whether outbound mail should get DKIM signed.

Selector

The selector used for signing the mail. The private key used for signing is saved under `/etc/pmg/dkim/yourselector`. You can display the DNS TXT record which you need to add to all domains signed by Proxmox Mail Gateway by clicking on the *View DNS Record* Button.

Sign all Outgoing Mail

Controls whether all outbound mail should get signed or only mails from domains listed in `/etc/pmg/dkim/sign_domains` if it exists and `/etc/pmg/domains` otherwise.

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

`dkim_selector: <string>`

Default DKIM selector

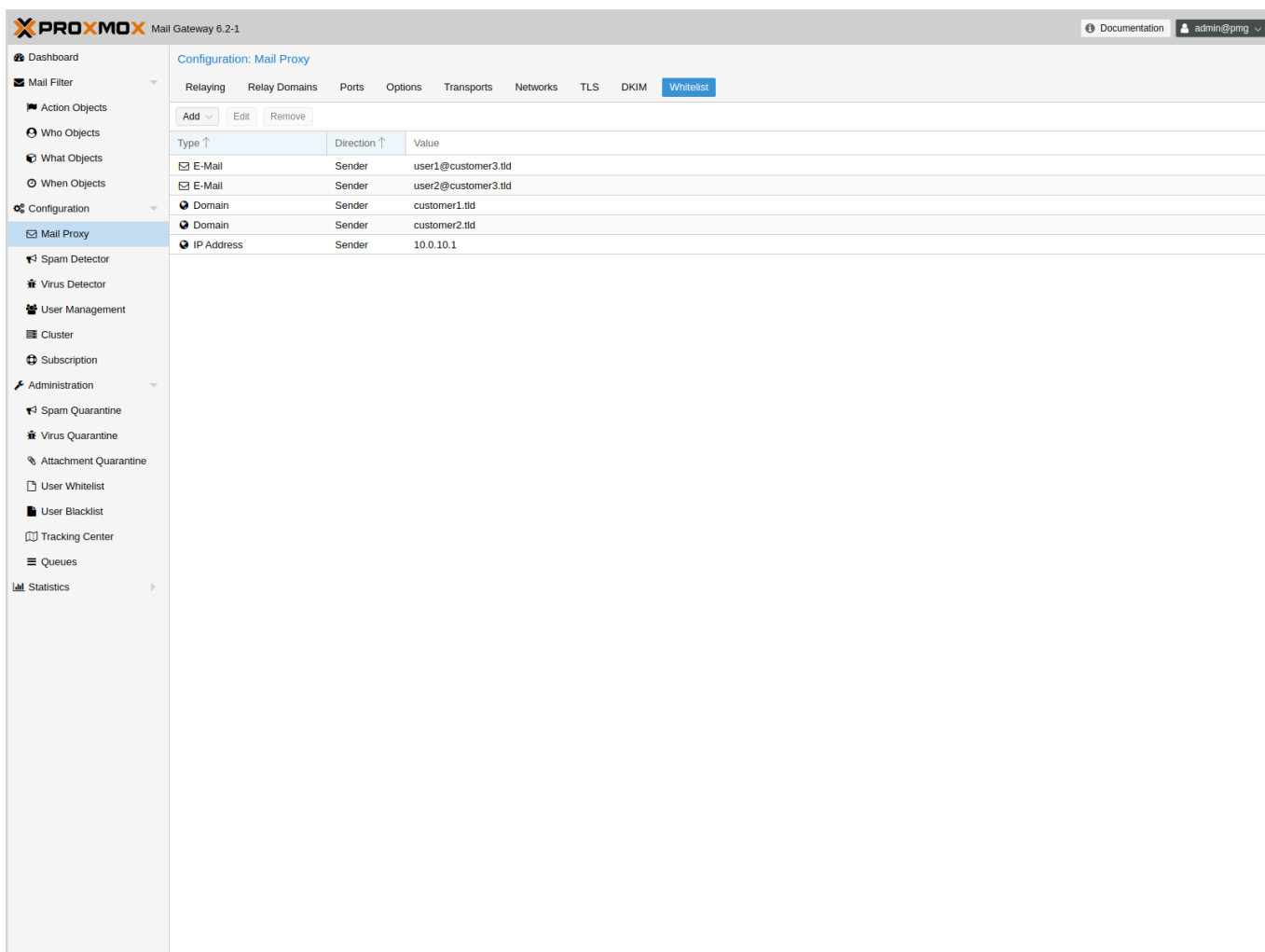
`dkim_sign: <boolean> (default = 0)`

DKIM sign outbound mails with the configured Selector.

`dkim_sign_all_mail: <boolean> (default = 0)`

DKIM sign all outgoing mails irrespective of the Envelope From domain.

4.7.11 Whitelist



Type ↑	Direction ↑	Value
E-Mail	Sender	user1@customer3.tld
E-Mail	Sender	user2@customer3.tld
Domain	Sender	customer1.tld
Domain	Sender	customer2.tld
IP Address	Sender	10.0.10.1

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

DNSBL checks are done by `postscreen`, which works on IP addresses and networks. This means it can only make use of the `IP Address` and `IP Network` entries.

Note

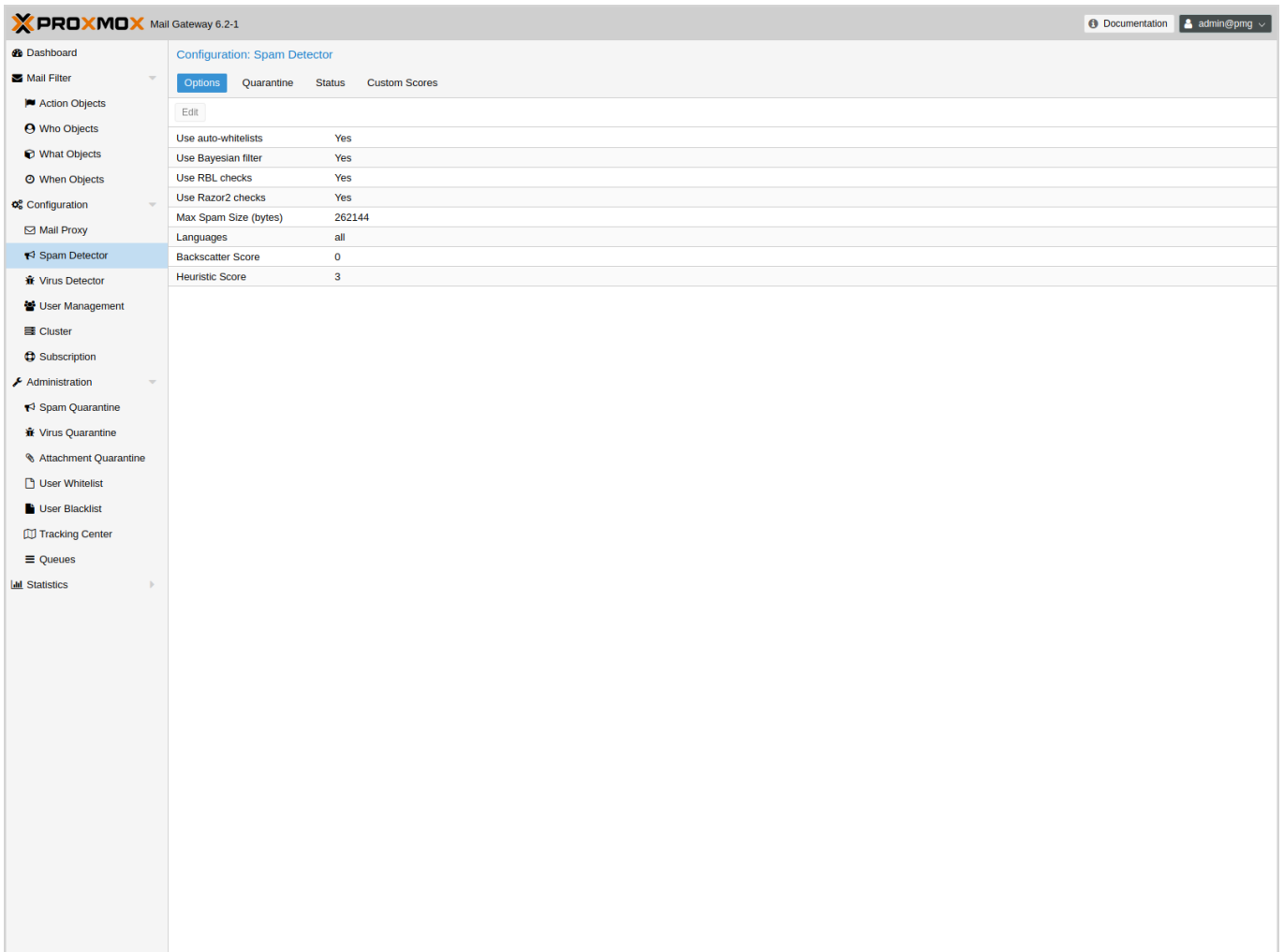
If you use a backup MX server (for example, your ISP offers this service for you) you should always add those servers here.

Note

To disable DNSBL checks entirely, remove any `DNSBL Sites` entries in [Mail Proxy Options](#) Section [4.7.4](#).

4.8 Spam Detector Configuration

4.8.1 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 email will be analyzed and have 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 ClamAV heuristics (Encrypted Archives/Documents, 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.

4.8.2 Quarantine

Configuration: Spam Detector	
Options Quarantine Status Custom Scores	
Edit	
Lifetime (days)	7
Authentication mode	Ticket
User Spamreport Style	Verbose
Quarantine Host	none
Quarantine port	Default
Email "From:"	none
View images	Yes
Allow HREFs	Yes

Proxmox Mail Gateway analyses all incoming email messages and decides for each email if it is ham or spam (or virus). Good emails are delivered to the inbox and spam messages are moved into the spam quarantine. The system can be configured to send daily reports to inform users about personal spam messages received in the last day. The report is only sent if there are new messages in the quarantine.

Some options are only available in the config file `/etc/pmg/pmg.conf`, and not in the web interface.

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. Useful 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.

port: <integer> (1 - 65535) (*default = 8006*)

Quarantine Port. Useful if you have a reverse proxy or port forwarding for the webinterface. Only used for the generated Spam report.

protocol: <http | https> (*default = https*)

Quarantine Webinterface Protocol. Useful if you have a reverse proxy for the webinterface. Only used for the generated Spam report.

quarantinelink: <boolean> (*default = 0*)

Enables user self-service for Quarantine Links. Caution: this is accessible without authentication

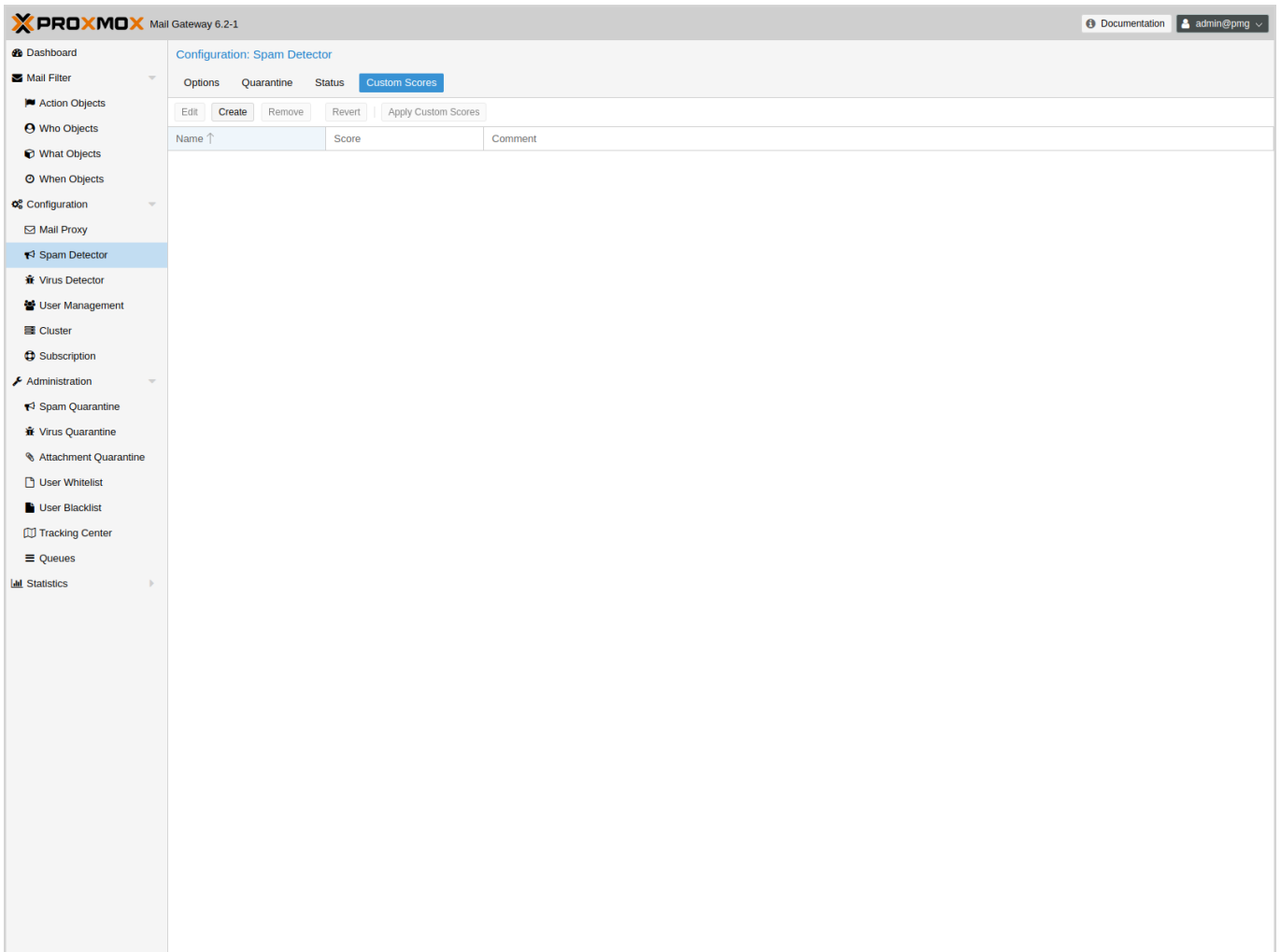
reportstyle: <custom | none | short | verbose> (*default = verbose*)

Spam report style.

viewimages: <boolean> (*default = 1*)

Allow to view images.

4.8.3 Customization of Rulescores



While the default scoring of **SpamAssassin™**'s ruleset provides very good detection rates, sometimes your particular environment can benefit from slightly adjusting the score of a particular rule. Two examples:

- Your system receives spam mails which are scored at 4.9 and you have a rule which puts all mails above 5 in the quarantine. The one thing the spam mails have in common is that they all hit *URIBL_BLACK*. By increasing the score of this rule by 0.2 points the spam mails would all be quarantined instead of being sent to your users
- Your system tags many legitimate mails from a partner organization as spam, because the organization has a policy that each mail has to start with *Dear madam or sir* (generating 1.9 points through the rule *DEAR_SOMETHING*). By setting the score of this rule to 0, you can disable it completely.

The system logs all the rules which a particular mail hits. Analyzing the logs can lead to finding such a pattern in your environment.

You can adjust the score of a rule by creating a new *Custom Rule Score* entry in the GUI and entering a **SpamAssassin™** rule as the name.

Note

In general, it is strongly recommended not to make large changes to the default scores.

4.9 Virus Detector Configuration

4.9.1 Options

Setting	Value
Block encrypted archives and documents	No
Max recursion	5
Max files	1000
Max file size	25000000
Max scan size	100000000
Max credit card numbers	0

All mails are automatically passed to the included virus detector (**ClamAV®**). The default settings 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)

Whether to mark encrypted archives and documents as heuristic virus match. A match does not necessarily result in an immediate block, it just raises the Spam Score by `clamav_heuristic_score`.

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 (in bytes) 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)

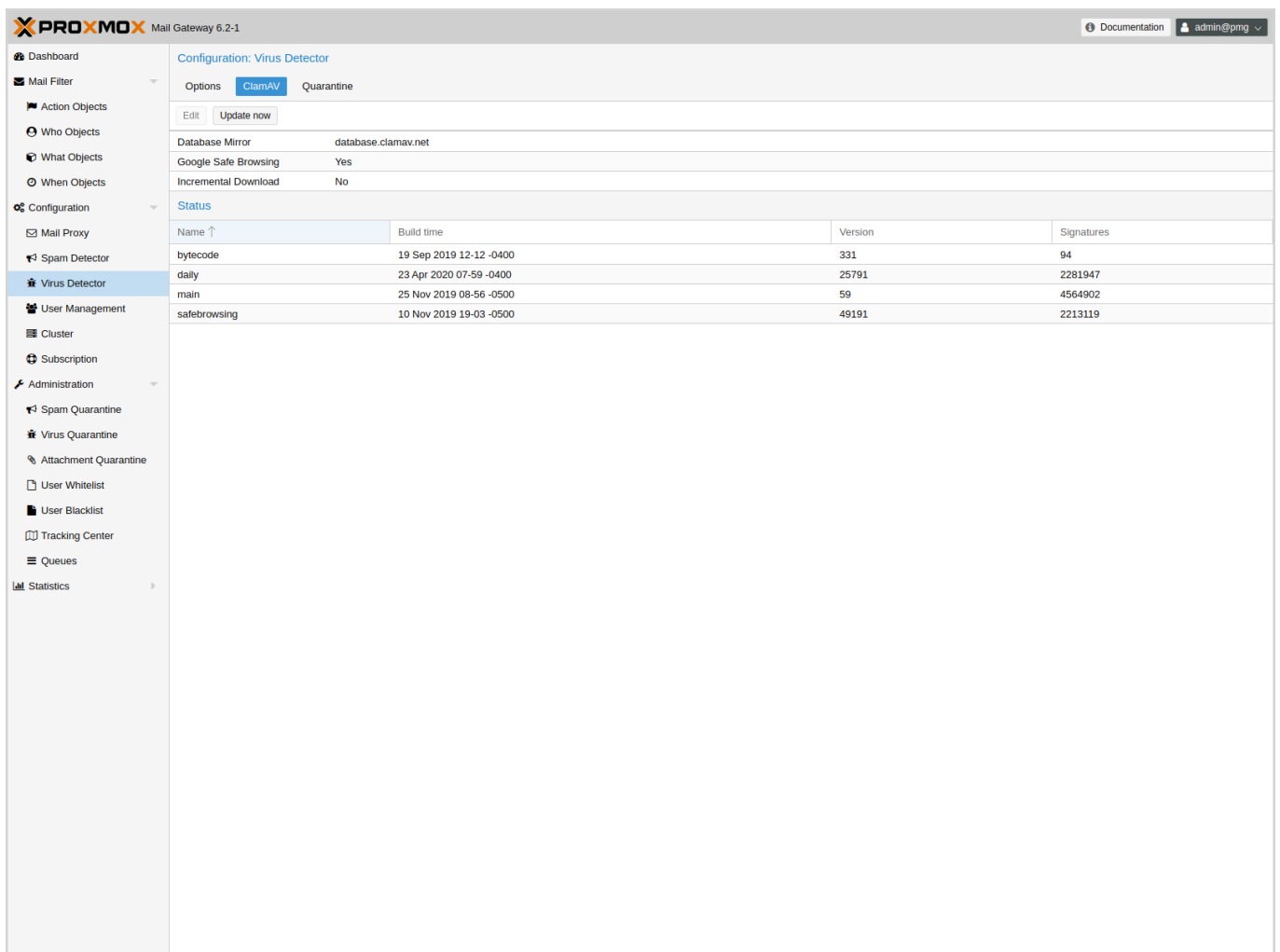
Sets the maximum amount of data (in bytes) to be scanned for each input file.

safebrowsing: <boolean> (default = 0)

Enables support for Google Safe Browsing. (deprecated option, will be ignored)

scriptedupdates: <boolean> (default = 1)

Enables ScriptedUpdates (incremental download of signatures)

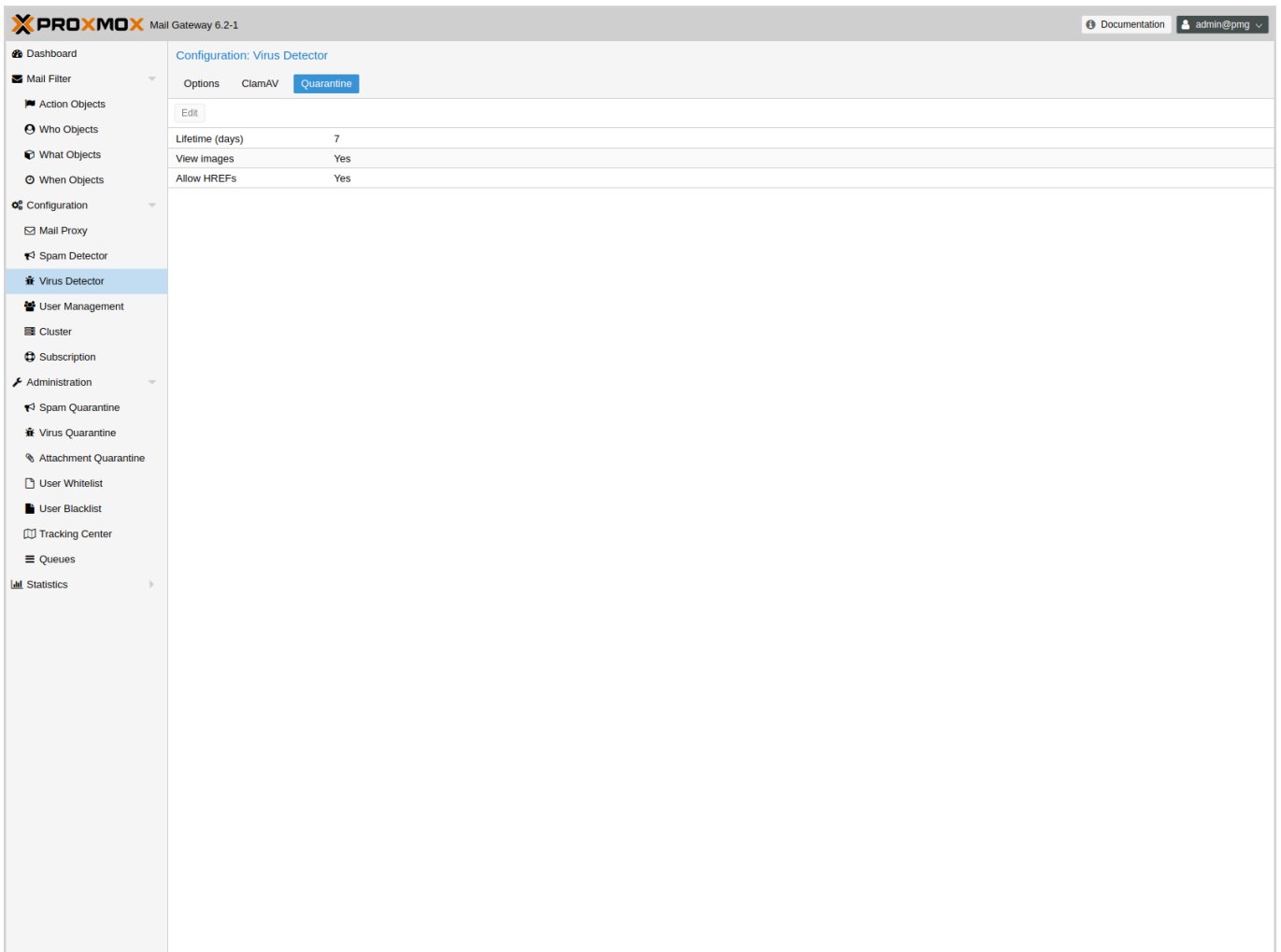


The screenshot shows the Proxmox Mail Gateway 6.2-1 GUI. The left sidebar contains navigation menus for Dashboard, Mail Filter, Configuration, and Administration. The main content area is titled 'Configuration: Virus Detector' and has tabs for 'Options' and 'Quarantine'. Under the 'Options' tab, there are three configuration items: 'Database Mirror' set to 'database.clamav.net', 'Google Safe Browsing' set to 'Yes', and 'Incremental Download' set to 'No'. Below these is a 'Status' section with a table showing the status of various signature databases.

Name ↑	Build time	Version	Signatures
bytecode	19 Sep 2019 12:12 -0400	331	94
daily	23 Apr 2020 07:59 -0400	25791	2281947
main	25 Nov 2019 08:56 -0500	59	4564902
safebrowsing	10 Nov 2019 19:03 -0500	49191	2213119

Please note that the virus signature database is automatically updated. You can see the database status in the GUI, and also trigger manual updates from there.

4.9.2 Quarantine



Identified virus mails are automatically moved to the virus quarantine. The administrator can view these mails from the GUI, and choose to 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.

4.10 Custom SpamAssassin configuration

This is only for advanced users. SpamAssassin™'s rules and their associated scores get updated regularly and are trained on a huge corpus, which gets classified by experts. In most cases, adding a rule for matching

a particular keyword is the wrong approach, leading to many false positives. Usually bad detection rates are better addressed by properly setting up DNS than by adding a custom rule - watch out for matches to `URIBL_BLOCKED` in the logs or spam-headers - see the [SpamAssassin DNSBL documentation](#).

To add or change the Proxmox **SpamAssassin™** configuration, log in to the console via SSH and change to the `/etc/mail/spamassassin/` directory. In this directory there are several files (`init.pre`, `local.cf`, ...) - do not change them, as `init.pre`, `v310.pre`, `v320.pre`, `local.cf` will be overwritten by the [template engine](#) Section 4.3, while the others can get updated by any **SpamAssassin™** package upgrade.

To add your custom configuration, you have to create a new file named `custom.cf` (in `/etc/mail/spamassassin/`) then add your configuration there. Make sure to use the correct **SpamAssassin rule syntax** and test it with:

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

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

To adjust the score assigned to a particular rule, you can also use the [Custom Rule Score](#) Section 4.8.3 settings in the GUI.

4.11 Custom Check Interface

For use-cases which are not handled by the Proxmox Mail Gateway Virus Detector and **SpamAssassin™** configuration, advanced users can create a custom check executable which, if enabled will be called before the Virus Detector and before passing an email through the Rule System. The custom check API is kept as simple as possible, while still providing a great deal of control over the treatment of an email. Its input is passed via two CLI arguments:

- the *api-version* (currently `v1`) - for potential future change of the invocation
- the *queue-file-name* - a filename, which contains the complete email as `rfc822/eml` file

The expected output needs to be printed to STDOUT and consists of two lines:

- the *api-version* (currently `v1`) - see above
- one of the following 3 results:
 - *OK* - email is OK
 - *VIRUS: <virusdescription>* - email is treated as if it contained a virus (the virus description is logged and added to the email's headers)
 - *SCORE: <number>* - `<number>` is added (negative numbers are also possible) to the email's spamscore

The check is run with a 5 minute timeout - if this is exceeded, the check executable is killed and the email is treated as OK.

All output written to STDERR by the check is written with priority `err` to the journal/mail.log.

Below is a simple sample script following the API (and yielding a random result) for reference:

```
#!/bin/sh

echo "called with $*" 1>&2

if [ "$#" -ne 2 ]; then
    echo "usage: $0 APIVERSION QUEUEFILENAME" 1>&2
    exit 1
fi

apiver="$1"
shift

if [ "$apiver" != "v1" ]; then
    echo "wrong APIVERSION: $apiver" 1>&2
    exit 2
fi

queue_file="$1"

echo "v1"

choice=$(shuf -i 0-3 -n1)

case "$choice" in
    0)
        echo OK
        ;;
    1)
        echo SCORE: 4
        ;;
    2)
        echo VIRUS: Random Virus
        ;;
    3) #timeout-test
        for i in $(seq 1 7); do
            echo "custom checking mail: $queue_file - minute $i" 1>&2
            sleep 60
        done
        ;;
esac

exit 0
```

The custom check needs to be enabled in the admin section of `/etc/pmg/pmg.conf`

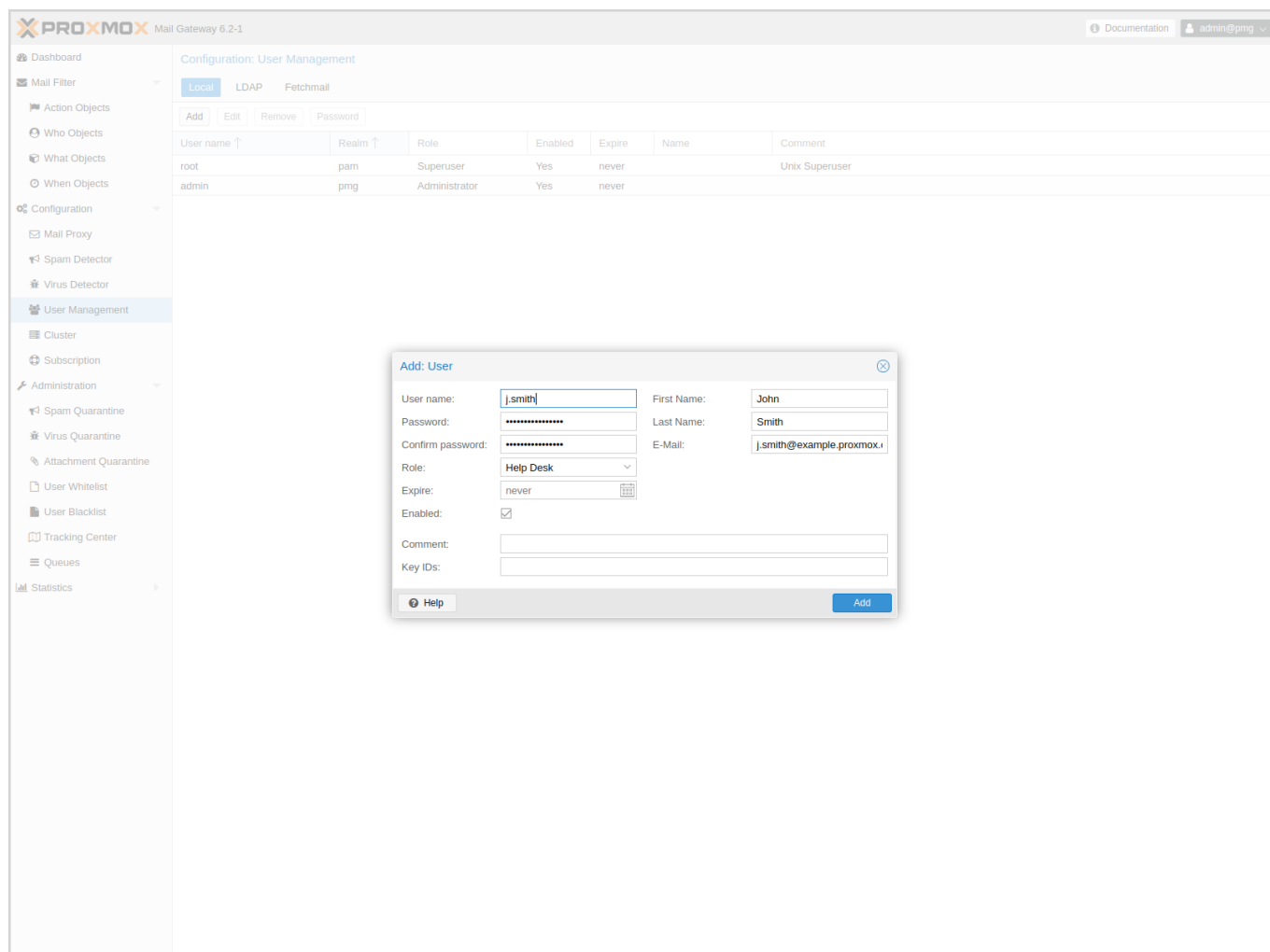
```
section: admin
    custom_check 1
```

The location of the custom check executable can also be set there with the key `custom_check_path` and defaults to `/usr/local/bin/pmg-custom-check`.

4.12 User Management

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

4.12.1 Local Users



The screenshot shows the Proxmox Mail Gateway administration interface. The main content area is titled 'Configuration: User Management' and has tabs for 'Local', 'LDAP', and 'Fetchmail'. Below the tabs is a table of users:

User name	Realm	Role	Enabled	Expire	Name	Comment
root	pam	Superuser	Yes	never		Unix Superuser
admin	pmg	Administrator	Yes	never		

An 'Add: User' dialog box is open, showing the following fields:

- User name: j.smith
- Password: [masked]
- Confirm password: [masked]
- Role: Help Desk
- Expire: never
- Enabled:
- Comment: [empty]
- Key IDs: [empty]
- First Name: John
- Last Name: Smith
- E-Mail: j.smith@example.proxmox.

Local users can manage and audit Proxmox Mail Gateway. They can login on the management web interface.

There are four roles:

Administrator

Is allowed to manage settings of Proxmox Mail Gateway, excluding 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.

Helpdesk

Combines permissions of the *Auditor* and the *Quarantine Manager* role.

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

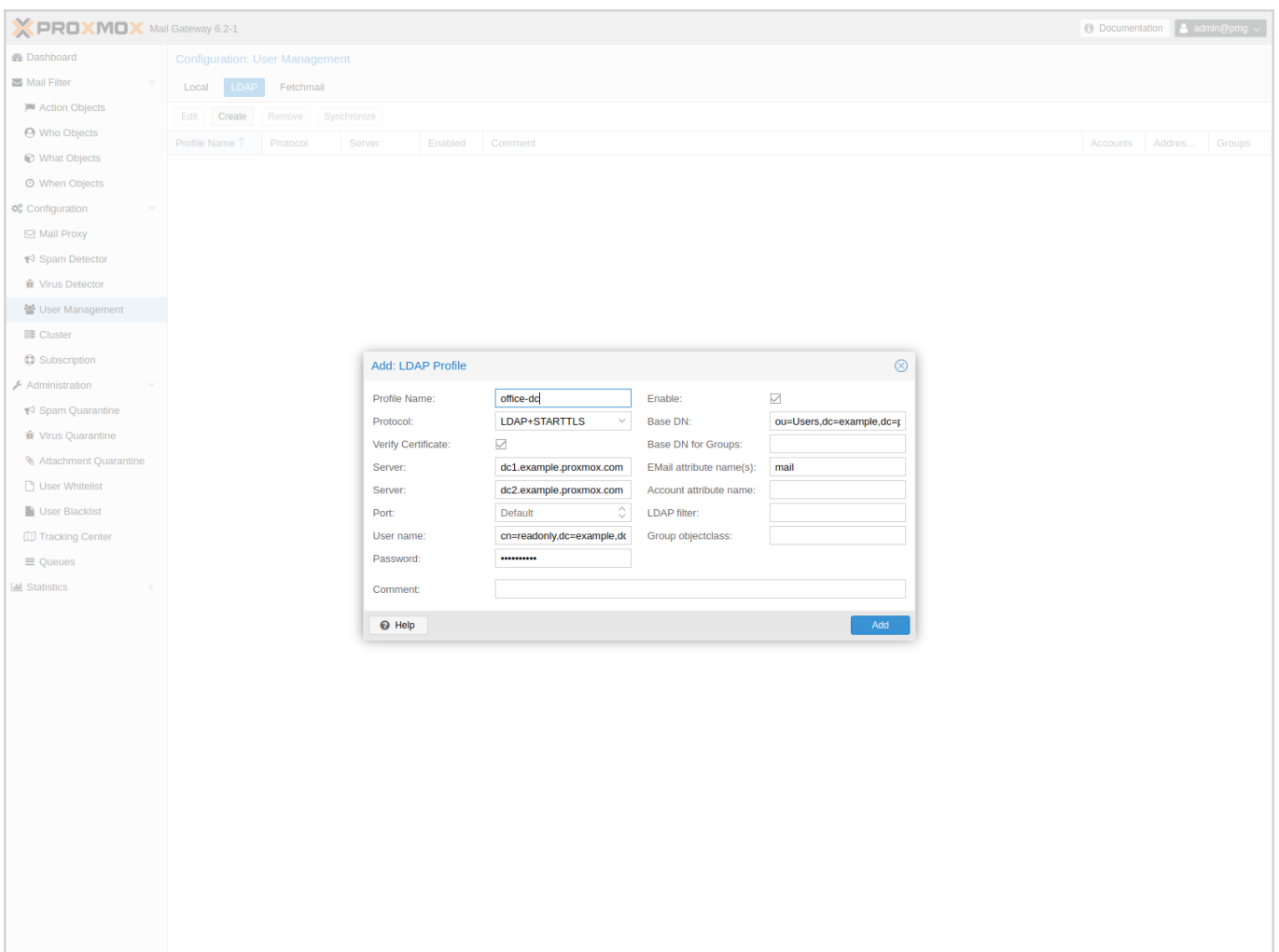
Note

Only PAM users are able to log in via the web interface and ssh, while the users created through 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 on the fields, see [user.conf](#) Section D.3

4.12.2 LDAP/Active Directory



The screenshot displays the Proxmox Mail Gateway 6.2-1 web interface. The main content area is titled 'Configuration: User Management' and shows a table with columns for Profile Name, Protocol, Server, Enabled, Comment, Accounts, Address..., and Groups. A modal dialog box titled 'Add: LDAP Profile' is open in the foreground. The dialog contains the following fields:

- Profile Name: office-did
- Protocol: LDAP+STARTTLS
- Verify Certificate:
- Server: dc1.example.proxmox.com
- Server: dc2.example.proxmox.com
- Port: Default
- User name: cn=readonly,dc=example,dc=
- Password: [masked]
- Comment: [empty]
- Enable:
- Base DN: ou=Users,dc=example,dc=
- Base DN for Groups: [empty]
- EMail attribute name(s): mail
- Account attribute name: [empty]
- LDAP filter: [empty]
- Group objectclass: [empty]

With Proxmox Mail Gateway, users can use LDAP and Active directory as authentication methods to access their individual [Spam Quarantine](#) Section 6.2.1. Additionally, if users have extra email aliases defined in the LDAP directory, they will have a single spam quarantine for all of these.

Note

Authentication via LDAP must first be enabled using the `Authentication mode (authmode)` parameter in the [Spam Detector's Quarantine configuration settings](#) Section 4.8.2.

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

Creating a profile requires (at least) the following:

- `Profile Name`: The name assigned to the LDAP profile.
- `Protocol`: LDAP, LDAPS, or LDAP+STARTTLS (LDAP+STARTTLS is recommended).
- `Server`: The domain name/IP address of the LDAP server. A fallback can also be configured using the second field.
- `User name`: The Bind DN for authentication on the LDAP server. This is required if your server does not support anonymous binds.
- `Password`: Password for the Bind DN user.
- `Base DN`: The directory which users are searched under.

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 about the options can be found here: [ldap.conf](#) Section D.4

Bind user

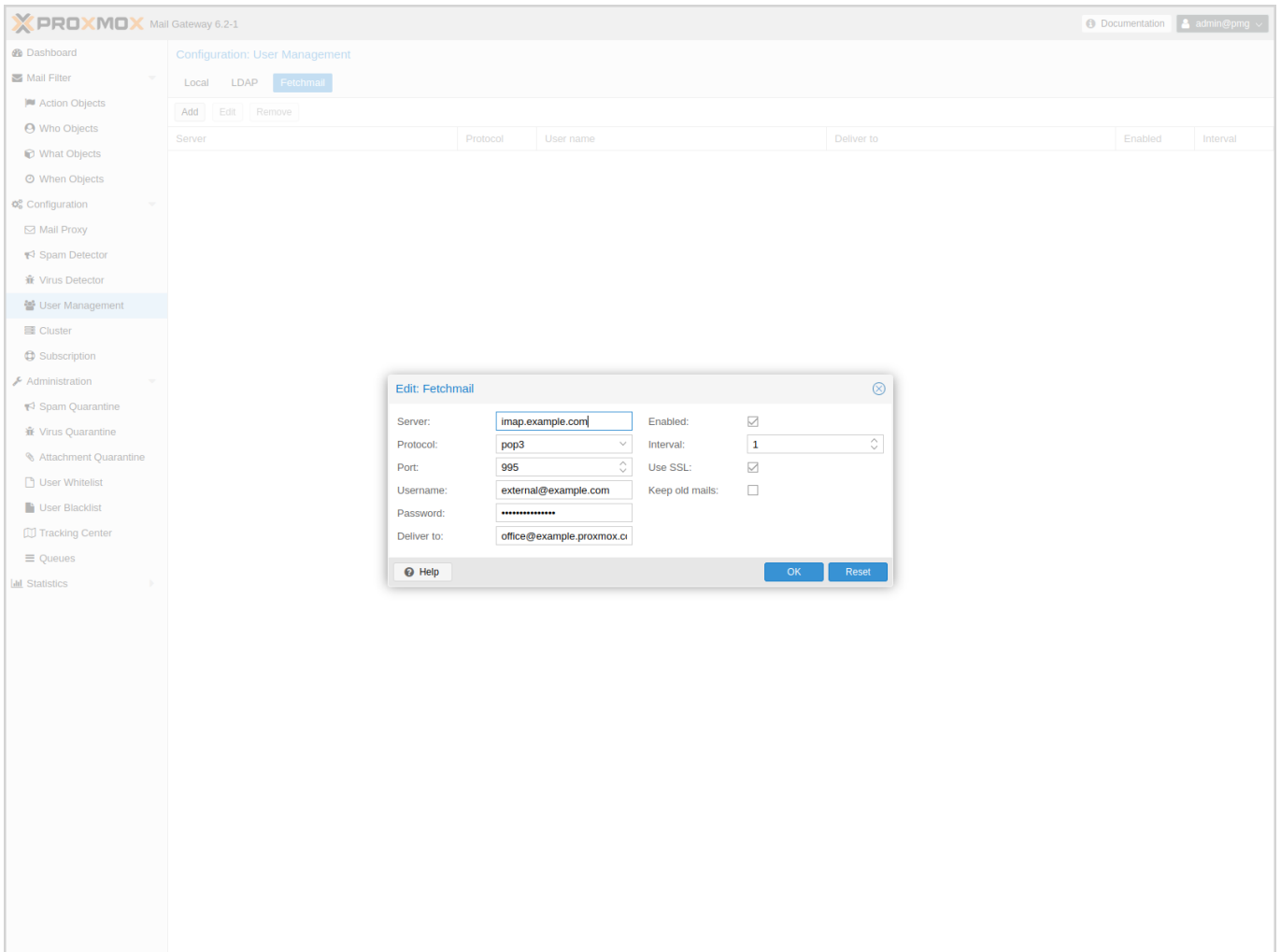
It is highly recommended that the user which you use for connecting to the LDAP server only has permission to query the server. For LDAP servers (for example OpenLDAP or FreeIPA), the username has to be of a format like `uid=username,cn=users,cn=accounts,dc=domain`, where the specific fields depend on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

Sync

Proxmox Mail Gateway synchronizes the relevant user and group information periodically, so that the information is quickly available, even when the LDAP/AD server is temporarily inaccessible.

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

4.12.3 Fetchmail



Fetchmail is a utility for polling and forwarding emails. You can define email accounts, which will then be fetched and forwarded to the email address you defined.

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

The API and web interface offer the 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

4.13 Two-Factor Authentication

Users of the admin interface can configure two-factor authentication to increase protection of their accounts.

Note

Joining a cluster with two-factor authentication enabled for the `root` user is not supported. Remove the second factor when joining the cluster.

4.13.1 Available Second Factors

You can set up multiple second factors, in order to avoid a situation in which losing your smartphone or security key locks you out of your account permanently.

The following two-factor authentication methods are available:

- User configured TOTP (**Time-based One-Time Password**). A short code derived from a shared secret and the current time, it changes every 30 seconds.
 - WebAuthn (**Web Authentication**). A general standard for authentication. It is implemented by various security devices, like hardware keys or trusted platform modules (TPM) from a computer or smart phone.
 - Single use Recovery Keys. A list of keys which should either be printed out and locked in a secure place or saved digitally in an electronic vault. Each key can be used only once. These are perfect for ensuring that you are not locked out, even if all of your other second factors are lost or corrupt.
-

4.13.2 Configuration of Two-Factor

Users can choose to enable *TOTP* or *WebAuthn* as a second factor on login, via the *TFA* button in the user list.

Users can always add and use one time *Recovery Keys*.

4.13.3 TOTP

There is no server setup required. Simply install a TOTP app on your smartphone (for example, [andOTP](#)) and use the Proxmox Backup Server web-interface to add a TOTP factor.

After opening the *TOTP* window, the user is presented with a dialog to set up *TOTP* authentication. The *Secret* field contains the key, which can be randomly generated via the *Randomize* button. An optional *Issuer Name* can be added to provide information to the *TOTP* app about what the key belongs to. Most *TOTP* apps will show the issuer name together with the corresponding *OTP* values. The username is also included in the QR code for the *TOTP* app.

After generating a key, a QR code will be displayed, which can be used with most OTP apps such as FreeOTP. The user then needs to verify the current user password (unless logged in as *root*), as well as the ability to correctly use the *TOTP* key, by typing the current *OTP* value into the *Verification Code* field and pressing the *Apply* button.

4.13.4 WebAuthn

For WebAuthn to work, you need to have two things:

- A trusted HTTPS certificate (for example, by using [Let's Encrypt](#) Section 4.6.3). While it probably works with an untrusted certificate, some browsers may warn or refuse WebAuthn operations if it is not trusted.
- Setup the WebAuthn configuration (see **User Management** → **Two Factor** → **WebAuthn** in the Proxmox Mail Gateway web interface). This can be auto-filled in most setups.

Once you have fulfilled both of these requirements, you can add a WebAuthn configuration in the **Two Factor** panel under **Datacenter** → **Permissions** → **Two Factor**.

4.13.5 Recovery Keys

Recovery key codes do not need any preparation; you can simply create a set of recovery keys in the **Two Factor** panel under **Datacenter** → **Permissions** → **Two Factor**.

Note

There can only be one set of single-use recovery keys per user at any time.

4.13.6 WebAuthn Configuration

To allow users to use *WebAuthn* authentication, it is necessary to use a valid domain with a valid SSL certificate, otherwise some browsers may warn or refuse to authenticate altogether.

Note

Changing the *WebAuthn* configuration may render all existing *WebAuthn* registrations unusable!

You can configure WebAuthn directly in the *Two Factor* panel, there's an auto-fill button that will set the correct values for most setups.

Chapter 5

Rule-Based Mail Filter

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

The screenshot shows the Proxmox Mail Gateway administration interface. The main content area displays a table of rules:

Name ↑	Priority ↓	Direction	
Blacklist	98	← In	
Block Viruses	96	← In	
Virus Alert	96	→ Out	
Block Dangerous Files	93	← In	
Modify Header	90	← In	
Quarantine Office Files	89	← In	
Block Multimedia Files	87	↔ In & Out	
Whitelist	85	← In	
Block Spam (Level 10)	82	← In	
Quarantine/Mark Spam (Level 5)	81	← In	
Quarantine/Mark Spam (Level 3)	80	← In	
Block outgoing Spam	70	→ Out	
Add Disclaimer	60	→ Out	

The right-hand panel shows the configuration for the selected 'Blacklist' rule:

- Blacklist**
- Priority: 98
- Direction: ← In
- Active: Yes

Below this, there are sections for 'Used Objects' and 'Available Objects'. The 'Available Objects' section lists various actions and filters that can be applied to the rule, such as 'Accept', 'Attachment Quarantine (remove all)', 'Attachment Quarantine (remove matching)', 'Disclaimer', 'Modify Spam Level', 'Modify Spam Subject', 'Notify Admin', 'Notify Sender', 'Quarantine', 'Remove all attachments', and 'Remove attachments'.

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 recipient of the email? Those objects can be used for the *TO* and/or *FROM* category.

Example: EMail-object - Who is the sender or recipient of the email?

What - objects

What is in the email?

Example: Does the email contain spam?

When - objects

When is the email received by Proxmox Mail Gateway?

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

Action - objects

Defines the final actions.

Example: Mark email 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 to all incoming emails

Out

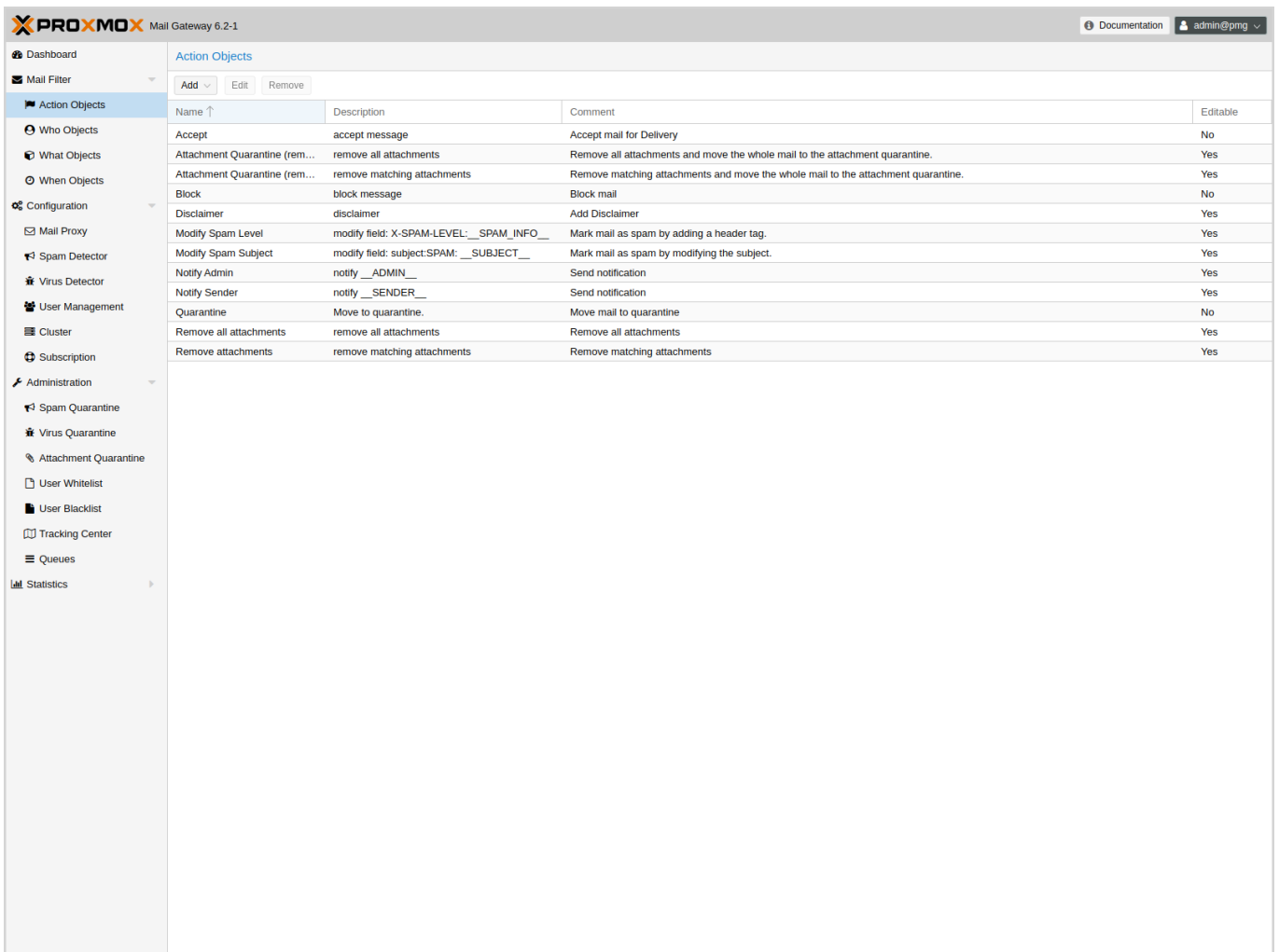
Rule applies to all outgoing emails

In & Out

Rule applies to both directions

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

5.1 Action - objects



Name ↑	Description	Comment	Editable
Accept	accept message	Accept mail for Delivery	No
Attachment Quarantine (rem...	remove all attachments	Remove all attachments and move the whole mail to the attachment quarantine.	Yes
Attachment Quarantine (rem...	remove matching attachments	Remove matching attachments and move the whole mail to the attachment quarantine.	Yes
Block	block message	Block mail	No
Disclaimer	disclaimer	Add Disclaimer	Yes
Modify Spam Level	modify field: X-SPAM-LEVEL: __SPAM_INFO__	Mark mail as spam by adding a header tag.	Yes
Modify Spam Subject	modify field: subject-SPAM: __SUBJECT__	Mark mail as spam by modifying the subject.	Yes
Notify Admin	notify __ADMIN__	Send notification	Yes
Notify Sender	notify __SENDER__	Send notification	Yes
Quarantine	Move to quarantine.	Move mail to quarantine	No
Remove all attachments	remove all attachments	Remove all attachments	Yes
Remove attachments	remove matching attachments	Remove matching attachments	Yes

Please note that some actions stop further rule processing. 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 C](#), 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, for instance, when a previous rule removed attachments.

5.1.6 Header Attributes

This object is able to add or modify mail header attributes. As with Notifications above, you can use [macros Appendix C](#), making this a very powerful object. For example, the *Modify Spam Level* actions add detailed information 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 rule's *What* - object. You can also specify the replacement text, if you want.

You can optionally move these mails into the attachment quarantine, where the original mail with all attachments will be stored. The mail with the attachments removed will continue through the rule system.

Note

The Attachment Quarantine lifetime is the same as for the Spam Quarantine.

5.1.8 Disclaimer

Add a Disclaimer.

The disclaimer can contain HTML markup. It will be added to the first `text/html` and `text/plain` part of an email. A disclaimer only gets added if its text can be encoded in the mail's character encoding.

5.2 Who objects

The screenshot displays the Proxmox Mail Gateway 6.2-1 web interface. The top navigation bar includes the Proxmox logo, the version number 'Mail Gateway 6.2-1', and a user profile for 'admin@pmg'. The left sidebar contains a navigation menu with categories: Dashboard, Mail Filter (Action Objects, Who Objects, What Objects, When Objects), Configuration (Mail Proxy, Spam Detector, Virus Detector, User Management, Cluster, Subscription), Administration (Spam Quarantine, Virus Quarantine, Attachment Quarantine, User Whitelist, User Blacklist, Tracking Center, Queues, Statistics), and a Statistics section. The main content area is titled 'Who Objects' and features a table with columns for 'Name' and 'Value'. A dropdown menu is open over the 'Add' button, listing options: Regular Expression, E-Mail, Domain, IP Address, IP Network, LDAP Group, and LDAP User. The table contains one entry with 'Blacklist' in the Name column and 'nomail@fromthisdomain.com' in the Value column. The table also has 'Whitelist' listed under the Name column.

These types of objects can be used for the *TO* and/or *FROM* category, and match the sender or recipient of the email. A single object can combine multiple items, and the following item types are available:

E-Mail

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 belongs to a specific LDAP user or group.

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

5.3 What objects

Filter Type	Value
Content Type Filter	content-type=application/javascript
Content Type Filter	content-type=application/x-executable
Content Type Filter	content-type=application/x-java
Content Type Filter	content-type=application/x-ms-dos-executable
Content Type Filter	content-type=application/x-ms-dos-executable
Content Type Filter	content-type=message/partial
Match Filename	filename=.*(vbs pif lnk shs shb)
Match Filename	filename=.*\.{+}

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

Spam Filter

Matches if the detected spam level is greater than or equal to the configured value.

Virus Filter

Matches on infected mails.

Match Field

Match specified mail header fields (for example, `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. This also matches the content-types of all regular (non-archived) attachments.

Match Archive Filename

Uses regular expressions to match attachment filenames inside archives. This also matches the filenames for all regular (non-archived) attachments.

5.4 When objects

The screenshot shows the Proxmox Mail Gateway 6.2-1 administration interface. The left sidebar contains a navigation menu with categories like Dashboard, Mail Filter, Action Objects, Who Objects, What Objects, When Objects, Configuration, and Administration. The main content area is titled 'When Objects' and features a table with columns 'Name' and 'Value'. A table row is visible with 'Office Hours' in the Name column and 'Usual office hours' in the Value column. Below this, there is a table with columns 'Type' and 'Value', containing one entry: 'TimeFrame' with the value '08:00-16:00'. At the top right of the main area, there are buttons for 'Add', 'Edit', and 'Remove'.

When objects are used to activate rules at specific times of the day. You can compose them from 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 represents a list of text patterns which you would like to match. The following is a short introduction to the syntax of regular expressions used by some objects. If you are familiar with Perl, you will 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 "e2mail" but not "e-some-mail" or "email".

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

Another metacharacter is the asterisk (`*`). This indicates that the character immediately preceding it may be repeated any number of times, including zero. `e*mail` would match "email", "mail", and "eeemail".

The plus (`+`) metacharacter indicates that the character immediately preceding it appears one or more times. So `e+mail` does not match "mail".

Metacharacters can also be combined. A common combination includes the period and asterisk metacharacters (`.*`), with the asterisk 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.

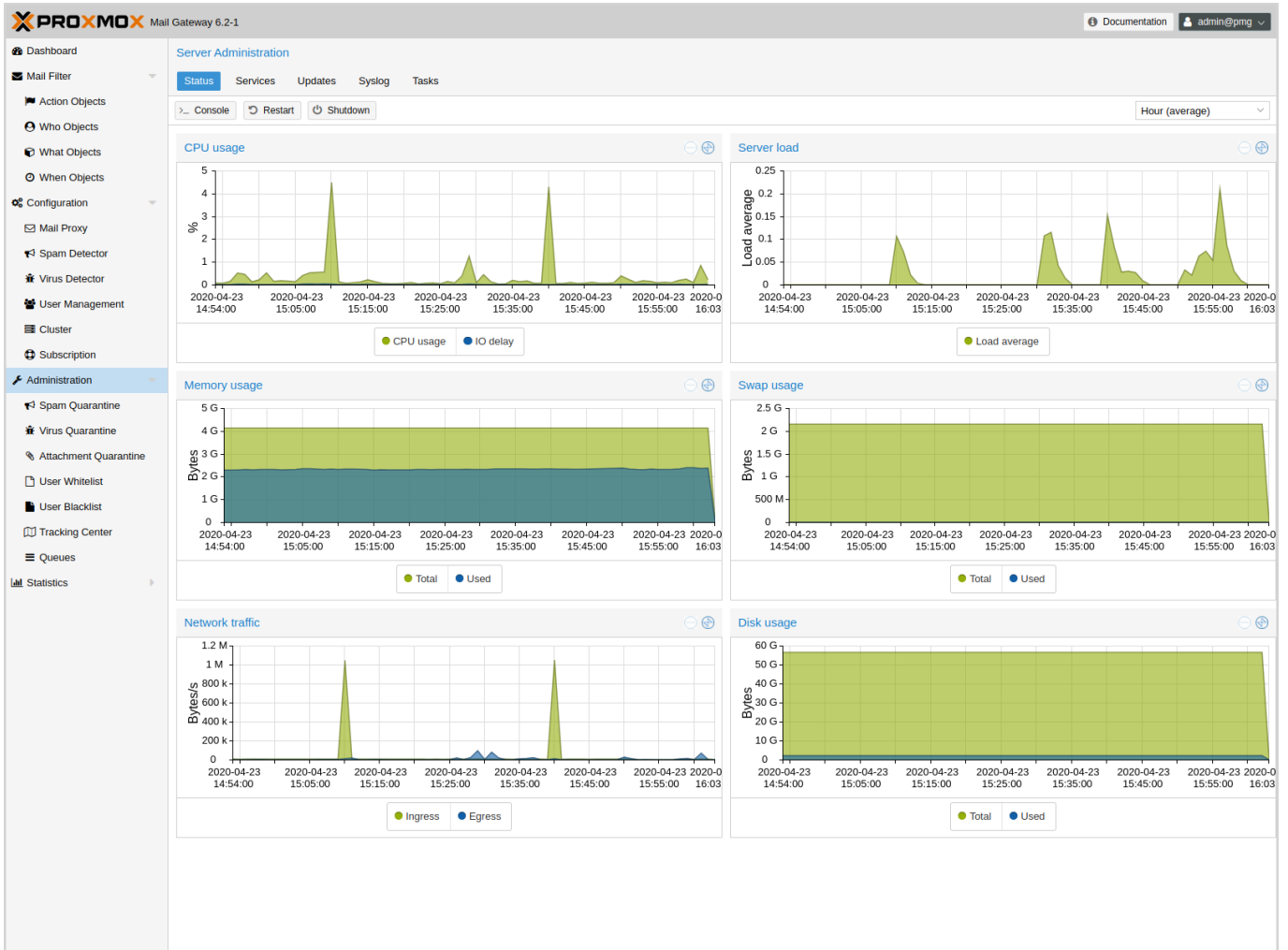
Chapter 6

Administration

The Administration GUI allows you to carry out common tasks such as updating software packages, managing quarantines, viewing the status of services, and managing mail queues. It also provides server statistics, in order to verify server health.

6.1 Server Administration

6.1.1 Status



This page shows statistics about server CPU, memory, disk and network usage. You can select the displayed time span from the upper right.

Administrators can open a terminal window using the *Console* button. It is also possible to trigger a server *Restart* or *Shutdown*.

6.1.2 Services

The screenshot shows the Proxmox Mail Gateway Administration interface. The top bar indicates 'Mail Gateway 6.2-1' and 'admin@pmg'. The left sidebar contains navigation menus for Dashboard, Mail Filter, Action Objects, Who Objects, What Objects, When Objects, Configuration, Mail Proxy, Spam Detector, Virus Detector, User Management, Cluster, Subscription, Administration, Spam Quarantine, Virus Quarantine, Attachment Quarantine, User Whitelist, User Blacklist, Tracking Center, Queues, and Statistics. The main content area is titled 'Server Administration' and has tabs for Status, Services (selected), Updates, Syslog, and Tasks. Below the tabs are buttons for Start, Stop, Restart, and Syslog. A table lists the following services:

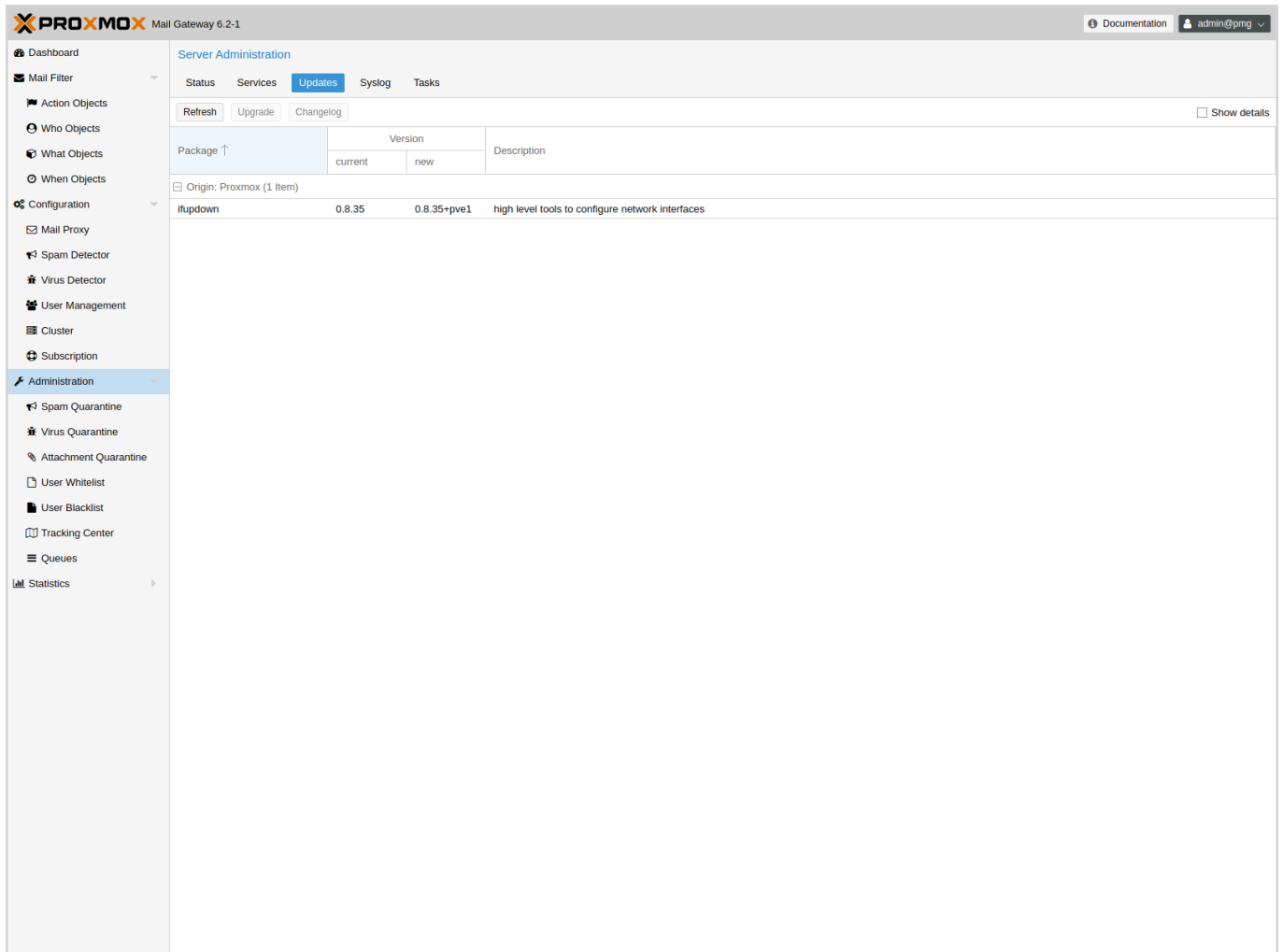
Name ↑	Status	Description
clamav-daemon	running	Clam AntiVirus userspace daemon
clamav-freshclam	running	ClamAV virus database updater
fetchmail	exited	LSB: init-Script for system wide fetchmail daemon
pmg-daily	success	Daily Proxmox Mail Gateway activities
pmg-hourly	success	Hourly Proxmox Mail Gateway activities
pmg-smtp-filter	running	Proxmox SMTP Filter Daemon
pmgdaemon	running	Proxmox Mail Gateway API Daemon
pmgmirror	dead	Proxmox Mail Gateway Database Mirror Daemon
pmgpolicy	running	Proxmox Mail Gateway Policy Daemon
pmgproxy	running	Proxmox Mail Gateway API
pmgreport	success	Send Daily System Report Mail
pmgspamreport	success	Send Daily Spam Report Mails
pmgtunnel	dead	Proxmox Mail Gateway Cluster Tunnel Daemon
postfix	running	Postfix Mail Transport Agent (instance -)
postgres	running	PostgreSQL Cluster 11-main
rsyslog	running	System Logging Service
ssh	running	OpenBSD Secure Shell server
systemd-timesyncd	running	Network Time Synchronization

This panel lists all the major services used for mail processing and cluster synchronization. If necessary, you can start, stop or restart them. The *Syslog* button shows the system log, filtered for the selected service.

Please note that Proxmox Mail Gateway uses **systemd** to manage services, so you can also use the standard `systemctl` command line tool to manage or view service status, for example:

```
systemctl status postfix
```


6.1.3 Updates



The screenshot displays the Proxmox Mail Gateway Administration interface. The top navigation bar includes the Proxmox logo, the text "Mail Gateway 6.2-1", and a user profile for "admin@pmg". The left sidebar contains a navigation menu with categories like "Mail Filter", "Configuration", "Administration", and "Statistics". The main content area is titled "Server Administration" and has tabs for "Status", "Services", "Updates", "Syslog", and "Tasks". The "Updates" tab is active, showing a table of available updates. The table has columns for "Package", "Version", and "Description". A "Refresh" button and an "Upgrade" button are visible at the top of the table. The table lists one update for the "iftupdown" package, showing the current version "0.8.35" and the new version "0.8.35+pve1".

Package ↑	Version		Description
	current	new	
Origin: Proxmox (1 Item)			
iftupdown	0.8.35	0.8.35+pve1	high level tools to configure network interfaces

We release software updates on a regular basis, and it is recommended to always run the latest available version. This page shows the available updates, and administrators can run an upgrade by pressing the *Upgrade* button.

See section [Package Repositories](#) Section 3.5 for details about the available package repositories.

6.1.4 Syslog and Tasks

The screenshot shows the Proxmox Mail Gateway Administration interface. The top navigation bar includes the Proxmox logo, the title 'Mail Gateway 6.2-1', and a user profile 'admin@pmg'. The left sidebar contains a navigation menu with categories: Dashboard, Mail Filter, Action Objects, Who Objects, What Objects, When Objects, Configuration (Mail Proxy, Spam Detector, Virus Detector), User Management, Cluster, Subscription, Administration (Spam Quarantine, Virus Quarantine, Attachment Quarantine, User Whitelist, User Blacklist, Tracking Center, Queues), and Statistics. The main content area is titled 'Server Administration' and has tabs for Status, Services, Updates, Syslog, and Tasks. The 'Syslog' tab is selected, showing a list of log entries. The log entries include timestamps, service names, and detailed messages. For example, one entry shows a connection from [192.168.30.128]:57990 to [192.168.30.128]:25. Another entry shows a message received from a client with details like 'message-id', 'size', and 'rcpt'. The interface also includes controls for 'Live Mode', 'Select Timespan', and filters for 'Since' and 'Until' dates.

The Syslog page gives you a quick real-time log view. You can use the [Tracking Center Section 6.3](#) to search the logs.

The Tasks page provides a history of the administration tasks that you carried out on the server, such as upgrading the system. Each task entry provides status information about the task, as well as the output.

6.2 Quarantine

6.2.1 Spam

The screenshot displays the Proxmox Mail Gateway 6.2-1 interface for the Spam Quarantine section. On the left, a navigation menu includes options like Mail Filter, Action Objects, Who Objects, What Objects, When Objects, Configuration, Mail Proxy, Spam Detector, Virus Detector, User Management, Cluster, Subscription, and Administration. The main area is divided into two panes. The left pane shows a list of quarantined emails with columns for Sender/Subject, Score, Size (KB), and Time. The right pane shows the selected email's details, including the sender, subject, and body text.

Sender/Subject	Score	Size (KB)	Time
<input type="checkbox"/> noreply1587650637@nowhere.tld SPAM: Proxmox Test Message ...	1002	1	16:03:57
<input type="checkbox"/> noreply1587650284@nowhere.tld SPAM: Proxmox Test Message ...	1002	1	15:58:04
<input type="checkbox"/> noreply1587649815@nowhere.tld SPAM: Proxmox Test Message ...	1002	1	15:50:15
<input type="checkbox"/> noreply1587638648@nowhere.tld SPAM: Proxmox Test Message ...	1002	1	12:44:08
<input type="checkbox"/> noreply1587630430@nowhere.tld SPAM: Proxmox Test Message ...	1002	1	10:27:10
<input type="checkbox"/> noreply1587629786@nowhere.tld SPAM: Proxmox Test Message ...	1002	1	10:16:26

The selected email details are as follows:

From: noreply1587650637@nowhere.tld
Subject: SPAM: Proxmox Test Message from noreply1587650637@nowhere.tld

This is just a small SPAM test message
XJS+C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

This panel lets you inspect the mail quarantine. Emails can be safely previewed and if desired, delivered to the original user.

The email preview on the web interface is very secure, as malicious code (attacking your operating system or email client) is removed by Proxmox Mail Gateway.

Users can access their personalized quarantine via the daily spam report or by navigating to the URL configured for the quarantine (defaults to `https://<pmg-host>:8006/quarantine`) and logging in with their LDAP credentials (email address and password).

You can additionally enable user self-service for sending an access link from the Quarantine Login page. To enable this on the Quarantine Login page, edit `/etc/pmg/pmg.conf`. See section [Spam Detector Configuration - Quarantine](#) Section 4.8.2 for more details about the available settings.

6.2.2 Virus

Allows administrators to inspect quarantined virus mails.

6.2.3 Attachment

Allows administrators to inspect quarantined mails and download their attachments or deliver/delete them.

Note

Use the options of the *Remove attachment* action to control the Attachment Quarantine.

6.2.4 User White- and Blacklist

This is mostly useful to debug or verify white- and blacklist user settings. The administrator should not change these values because users can manage this themselves.

6.3 Tracking Center

The screenshot shows the Proxmox Mail Gateway 6.2-1 Tracking Center interface. The top navigation bar includes 'Dashboard', 'Mail Filter', 'Action Objects', 'Who Objects', 'What Objects', 'When Objects', 'Configuration', 'Mail Proxy', 'Spam Detector', 'Virus Detector', 'User Management', 'Cluster', 'Subscription', 'Administration', 'Spam Quarantine', 'Virus Quarantine', 'Attachment Quarantine', 'User Whitelist', 'User Blacklist', and 'Tracking Center'. The 'Tracking Center' section is active, showing a search filter for Sender, Receiver, and Filter, with options to include empty senders and greytiles. A table displays email tracking records with columns for Time, From, To, and Status. A detailed log view is also visible, showing SMTP and cleanup actions.

Time	From	To	Status
Apr 23 15:04:01	mailtestsender.good@proxtest.com	d.musterman@example.proxmox.com	accepted/delivered
Apr 23 15:04:01	mailtestsender.good@proxtest.com	ceo@example.proxmox.com	accepted/delivered
Apr 23 15:04:16	mailtestsender.good@proxtest.com	ferdi@example.proxmox.com	accepted/delivered
Apr 23 15:04:21	mailtestsender.good@proxtest.com	d.musterman@example.proxmox.com	accepted/delivered
Apr 23 15:04:23	mailtestsender.good@proxtest.com	ferdi@example.proxmox.com	accepted/delivered

```

Apr 23 15:04:23 pmg-demo postfix/smtpd[5249]: connect from pmg-demo.proxmox.com[192.168.30.128]
Apr 23 15:04:23 pmg-demo postfix/smtpd[5249]: 6ECB63210E3: client=pmg-demo.proxmox.com[192.168.30.128]
Apr 23 15:04:23 pmg-demo postfix/cleanup[5650]: 6ECB63210E3: message-id=<20200423130423.6ECB63210E3@pmg-demo.proxmox.com>
Apr 23 15:04:23 pmg-demo postfix/qmgr[2161]: 6ECB63210E3: from=<mailtestsender.good@proxtest.com>, size=943, nrcpt=1 (queue active)
Apr 23 15:04:23 pmg-demo postfix/smtpd[5249]: disconnect from pmg-demo.proxmox.com[192.168.30.128] ehlo=1 mail=1 rcpt=1 data=1 commands=4
Apr 23 15:04:23 pmg-demo pmg-smtp-filter[5764]: 3210E55EA192576F911: new mail message-id=<20200423130423.6ECB63210E3@pmg-demo.proxmox.com>#012
Apr 23 15:04:23 pmg-demo postfix/smtpd[5772]: connect from localhost.localdomain[127.0.0.1]
Apr 23 15:04:23 pmg-demo postfix/smtpd[5772]: 7223C321220: client=localhost.localdomain[127.0.0.1], orig_client=pmg-demo.proxmox.com[192.168.30.128]
Apr 23 15:04:23 pmg-demo postfix/cleanup[5650]: 7223C321220: message-id=<20200423130423.6ECB63210E3@pmg-demo.proxmox.com>
Apr 23 15:04:23 pmg-demo postfix/qmgr[2161]: 7223C321220: from=<mailtestsender.good@proxtest.com>, size=1154, nrcpt=1 (queue active)
Apr 23 15:04:23 pmg-demo pmg-smtp-filter[5764]: 3210E55EA192576F911: accept mail to <ferdi@example.proxmox.com> (7223C321220) (rule: default-accept)
Apr 23 15:04:23 pmg-demo postfix/smtpd[5772]: disconnect from localhost.localdomain[127.0.0.1] ehlo=1 xforward=1 mail=1 rcpt=1 data=1 commands=5
Apr 23 15:04:23 pmg-demo pmg-smtp-filter[5764]: 3210E55EA192576F911: processing time: 0.013 seconds (0, 0.007, 0)
Apr 23 15:04:23 pmg-demo postfix/lmtp[5803]: 6ECB63210E3: to=<ferdi@example.proxmox.com>, relay=127.0.0.1[127.0.0.1]:10023, delay=0.02, delays=0/0/0/0.01, dsn=2.5.0, sta
Apr 23 15:04:23 pmg-demo postfix/qmgr[2161]: 6ECB63210E3: removed
Apr 23 15:04:23 pmg-demo postfix/smtp[5773]: 7223C321220: to=<ferdi@example.proxmox.com>, relay=192.168.30.48[192.168.30.48]:25, delay=0.01, delays=0/0/0/0.01, dsn=2.0.0
Apr 23 15:04:23 pmg-demo postfix/qmgr[2161]: 7223C321220: removed

```

Email processing is a complex task and involves several service daemons. Each daemon logs information to the syslog service. The problem is that a server analyzes many emails in parallel, so it is usually very hard to find all logs corresponding to a specific mail.

The Tracking Center simplifies the search for emails dramatically. We use highly optimized and safe Rust¹ code to search the available syslog data. This is very fast and powerful, and works for sites processing

¹A language empowering everyone to build reliable and efficient software. <https://www.rust-lang.org/>

several million emails per day.

The result is a list of received mails, including the following data:

Time	Timestamp of first syslog entry found
From	Envelope <i>From</i> address (the sender)
To	The email receiver address
Status	Delivery status
Syslog	The corresponding syslog entries are shown if you double click such an entry or if you press the + button on the left

To narrow the search down further, you can specify filters and set a *Start* and *End* time. By default, the start time is set to the last hour. If you still get too many entries, you can try to restrict the search to a specific sender or receiver address, or search for a specific text string in the logs (*Filter* entry).

Note

Search is faster if you use a shorter time interval.

The *Status* field summarizes what happened with an email. Proxmox Mail Gateway is a mail proxy, meaning that the proxy receives mails from outside, processes them and finally sends the result to the receiver.

The first phase is receiving the mail. The proxy may reject the mail early or accept the mail and feed it into the filter. The filter rules can then block or accept the mail.

In the second phase, accepted mails need to be delivered to the receiver. This action may also fail or succeed. *Status* combines the results from the first and second phase.

Status	Phase	Description
rejected	1	Email rejected (for example, the sender IP is listed on an IP blacklist)
greylisted	1	Email temporarily rejected by greylisting
queued/deferred	1	Internal email was queued, still trying to deliver
queued/bounced	1	Internal email was queued but not accepted by the target email server (for example, user unknown)
queued/delivered	1	Internal email was queued and delivered
quarantine	1	Email was moved to quarantine
blocked	1	Email was blocked by filter rules
accepted/deferred	2	Email accepted, still trying to deliver
accepted/bounced	2	Email accepted, but not accepted by the target email server (for example, user unknown)
accepted/delivered	2	Email accepted and delivered

6.4 Postfix Queue Administration

PROXMOX Mail Gateway 6.2-4

Queue Administration

Summary Deferred Mail

Flush Queue Delete all Messages Discard address verification database

Domain	Total	5m	10m	20m	40m	80m	160m	320m	640m	1280m	1280m+
TOTAL	442	5	8	11	88	135	195	0	0	0	0
fake.proxmox.com	442	5	8	11	88	135	195	0	0	0	0

Mail-queues are one of the central concepts of the SMTP protocol. Once a mail server accepts a mail for further processing it saves it to a queue. After the mail is either relayed to another system, stored locally or discarded, it is deleted from the local mail-queue.

If immediate processing is not possible, for example because a downstream mail server is not reachable, the mail remains on the queue for later processing.

The *Queue Administration* panel provides a summary about the current state of the postfix mail-queue, similar to the *qshape (1)* command-line utility. It shows domains for which mails were not delivered, and how long they have been queued.

The three Action Buttons on top provide the most common queue operations:

Flush Queue

Attempt to deliver all currently queued mail, for example if a downstream server has become available again.

Delete All Messages

Delete all currently queued mail, for example if the queue contains only spam.

Discard address verification database

Clear the recipient verification cache.

A sudden increase in queued mails should be closely inspected. This increase can indicate issues connecting to downstream servers or that one of the servers for which you relay emails sends spam itself.

6.4.1 Deferred Mail

The screenshot shows the 'Queue Administration' interface in Proxmox Mail Gateway 6.2-4. The 'Deferred Mail' tab is active, displaying a table of deferred emails. The table has columns for Time, Size, Sender, Receiver, and Reason. The Reason column contains various error messages such as 'No route to host' and 'delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host'.

Time	Size	Sender	Receiver	Reason
2020-06-04 09:10:05	2.61 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 07:58:11	1.71 KIB	mailtestsender.good@pro...	ceo@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:29:33	2.59 KIB	mailtestsender.good@pro...	ceo@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 09:21:46	2.92 KIB	mailtestsender.good@pro...	d.musterman@fake.prox...	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:30:15	2.88 KIB	mailtestsender.good@pro...	ceo@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:43:28	2.30 KIB	mailtestsender.good@pro...	ceo@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:31:19	2.92 KIB	mailtestsender.good@pro...	d.musterman@fake.prox...	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 07:58:41	2.30 KIB	mailtestsender.good@pro...	ceo@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 09:20:45	2.92 KIB	mailtestsender.good@pro...	d.musterman@fake.prox...	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 09:49:21	2.61 KIB	mailtestsender.good@pro...	j.smith@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:01:47	2.02 KIB	mailtestsender.good@pro...	ferdt@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:09:38	2.91 KIB	mailtestsender.good@pro...	d.musterman@fake.prox...	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 09:19:28	2.90 KIB	mailtestsender.good@pro...	j.smith@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:35:23	2.33 KIB	mailtestsender.good@pro...	d.musterman@fake.prox...	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:04:34	2.90 KIB	mailtestsender.good@pro...	j.smith@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:39:13	2.02 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:35:56	1.73 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 07:59:46	1.73 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:29:18	2.31 KIB	mailtestsender.good@pro...	j.smith@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:15:08	2.90 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 09:19:15	2.02 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:13:43	2.31 KIB	mailtestsender.good@pro...	j.smith@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:44:13	2.61 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:29:29	2.62 KIB	mailtestsender.good@pro...	d.musterman@fake.prox...	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:19:50	2.61 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:50:48	2.90 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 09:27:16	2.90 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 09:22:09	2.61 KIB	mailtestsender.good@pro...	office@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 09:22:49	1.73 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:30:44	2.90 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:35:43	1.72 KIB	mailtestsender.good@pro...	ferdt@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:51:12	2.60 KIB	mailtestsender.good@pro...	ferdt@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:39:01	2.90 KIB	mailtestsender.good@pro...	office@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:43:59	2.31 KIB	mailtestsender.good@pro...	ferdt@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:35:17	2.02 KIB	mailtestsender.good@pro...	t.last@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 09:19:24	1.74 KIB	mailtestsender.good@pro...	d.musterman@fake.prox...	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:36:12	2.31 KIB	mailtestsender.good@pro...	ferdt@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:09:22	1.73 KIB	mailtestsender.good@pro...	office@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 07:59:40	2.60 KIB	mailtestsender.good@pro...	ferdt@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:29:27	1.73 KIB	mailtestsender.good@pro...	j.smith@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host
2020-06-04 08:14:58	2.00 KIB	mailtestsender.good@pro...	ceo@fake.proxmox.com	delivery temporarily suspended: connect to 192.168.30.129[192.168.30.129]:25: No route to host

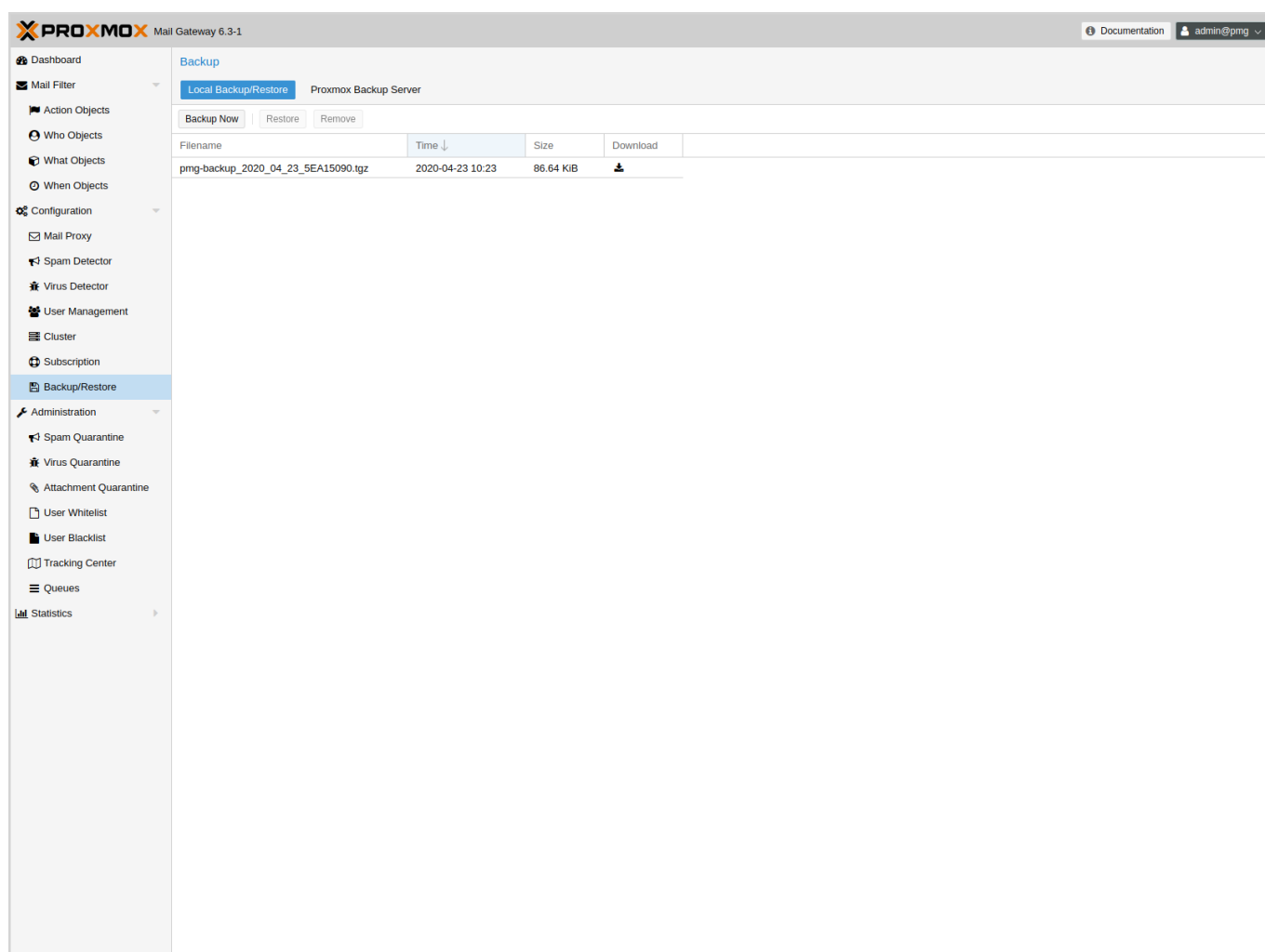
In the *Deferred Mail* tab, you can examine each deferred email separately. In addition to providing contact information about the sender and receiver, you can also check the reason for which an email remains queued.

You can view the complete headers and filter by sender or receiver of queued emails.

Here, you can also flush or delete each deferred email independently.

Chapter 7

Backup and Restore



Proxmox Mail Gateway includes the ability to back up 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, nor does it contain mail data from the postfix queue or the spam and virus quarantines.

Backups can be created locally or stored on a [Proxmox Backup Server](#) instance.

7.1 Local Backups

You can create a backup by simply pressing the *Backup* button in the *Local Backup/Restore* tab 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
```

Local 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 which 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 example, 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
```

7.2 Proxmox Backup Server

In order to back up your Proxmox Mail Gateway configuration on a Proxmox Backup Server, you first need to configure the instance as a backup *remote*. You can then directly create and restore backups, as well as create a scheduled *backup job* to run regular backups.

7.2.1 Remotes

A Proxmox Backup Server remote can be configured using the *Proxmox Backup Server* panel in the *Backup/Restore* menu of the GUI, or by using the `remote` subcommand of `pmgbackup`.

Note

You can use API Tokens in place of a username/password combination.

Example addition of a Proxmox Backup Server remote with id archive.

```
# pmgbackup proxmox-backup remote add archive --datastore big --server ↵
  backup.proxmox.com --user 'pmgbackup@pbs!token' --password --fingerprint ↵
  09:54:ef:...snip...:88:af:47:fe:4c:3b:cf:8b:26:88:0b:4e:3c:b2
Enter new password: *****
Retype new password: *****
```

The fingerprint is optional, if the certificate of the Proxmox Backup Server remote is signed by a CA trusted by Proxmox Mail Gateway.

Additionally, you can configure `prune-settings` for each remote, giving you flexible control over how many backups should be stored on the Proxmox Backup Server over a specific period of time.

Setting the prune options for the Proxmox Backup Server remote with id archive.

```
# pmgbackup remote set archive --keep-last 3 --keep-daily 14 --keep-weekly ↵
  8 --keep-monthly 12 --keep-yearly 7
```

If prune settings are configured, the backup-group of Proxmox Mail Gateway is pruned automatically after each successful backup.

The `notify` and `include-statistics` settings of a remote define the defaults for notifications and whether to include the statistic database in backups. They are also used for [scheduled backups](#) Section 7.2.2.

The public settings are stored in `/etc/pmg/pbs/pbs.conf`. Sensitive settings, like passwords are stored in individual files named after the remote inside `/etc/pmg/pbs/`:

Configuration Example (`/etc/pmg/pbs/pbs.conf`)

```
pbs: archive
    datastore big
    server backup.proxmox.com
    fingerprint 09:54:ef:..snip...:88:af:47:fe:4c:3b:cf:8b:26:88:0b:4e:3 ←
        c:b2
    keep-daily 30
    keep-last 5
    keep-monthly 3
    keep-yearly 5
    username pmgbackup@pbs!token
```

7.2.2 Backup Jobs

The screenshot displays the Proxmox Mail Gateway 6.3-1 interface for configuring backup jobs. The main content area is titled 'Backup' and includes sections for 'Local Backup/Restore', 'Remote', 'Schedule on 'demo'', and 'Backup snapshots on 'demo''.

Remote Configuration:

Remote ↑	Server	Datastore	User ID	Enabled
demo	192.168.30.68	test	root@pam/demo	Yes

Schedule on 'demo':

schedule	daily
delay	15 minutes
next-run	Thu 2020-11-19 00:00:00 CET

Backup snapshots on 'demo':

Group ID	Time ↓	Size
pmg-demo	2020-11-18T17:24:47Z	79.25 KiB

With a configured remote, you can create backups using the GUI or the `proxmox-backup backup` subcommand of the `pmgbackup` CLI tool.

Creating a new backup on the Proxmox Backup Server remote with id archive.

```
# pmgbackup proxmox-backup backup archive
starting update of current backup state
Starting backup: host/pmg/2020-11-16T16:38:39Z
```


Scheduled Backups

You can create a `Schedule` for each remote, to periodically create backups of your Proxmox Mail Gateway - for example to run a daily backup at 03:50:00 with a randomized delay of 15 minutes each day:

```
# pmgbackup proxmox-backup job create archive --schedule '*-*-* 03:50:00' ←  
  --delay '15 minutes'
```

The randomized delay can help to prevent load-peaks on the backup server, if you have multiple backups which should all start around the same time.

The schedules are `systemd.timer` units. See the `systemd.time(7)` man page for details on the time specification used.

Chapter 8

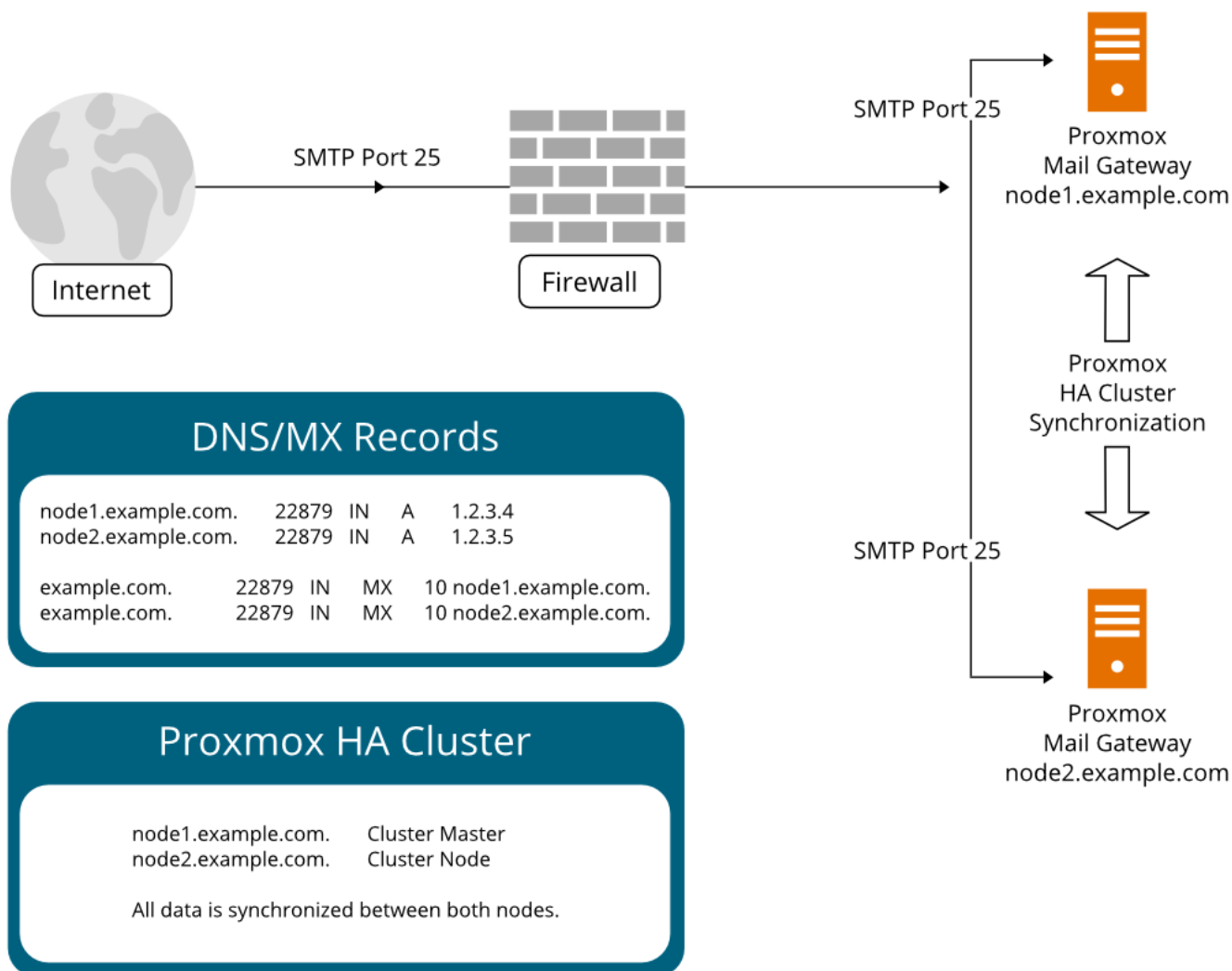
Cluster Management

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

The Proxmox Mail Gateway HA Cluster consists of a master node and several slave nodes (minimum one slave node). Configuration is done on the master, and data is synchronized to all cluster nodes via 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 were taken to make management as easy as possible. A complete cluster setup is done within minutes, and nodes automatically reintegrate after temporary failures, without any operator interaction.



8.1 Hardware Requirements

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

The HA Cluster can also run in virtualized environments.

8.2 Subscriptions

Each node 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.

8.3 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 can then be used as a quarantine host, that 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. An 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, each of which can have different priorities. For example, our MX record looks like this:

```
# 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
```

Notice that there is a single MX record for the domain `proxmox.com`, pointing to `mail.proxmox.com`. The `dig` command automatically outputs 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).

8.3.1 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 a fallback. This can be done by adding an additional MX record with a lower priority (higher number). Continuing from the example above, this would look like:

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

In such a setup, your provider must accept mails for your domain and forward them to you. Please note that this is not advisable, because spam detection needs to be done by the backup MX server as well, and external servers provided by ISPs usually don't do this.

However, 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 reasonable mail server retries mail delivery if the target server is not available. Proxmox Mail Gateway stores mail and retries delivery for up to one week. Thus, you will not lose emails if your mail server is down, even if you run a single server setup.

8.3.2 Load balancing with MX records

Using your ISP's 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.

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. The rest of this section will provide a complete example.

First, you need to have at least two working Proxmox Mail Gateway servers (`mail1.example.com` and `mail2.example.com`) configured as a cluster (see section [Cluster Administration](#) Section 8.4 below), with each having its own IP address. Let us assume the following DNS address records:

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

It is always a good idea to add reverse lookup entries (PTR records) for those hosts, as 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. Following this, you will receive mail on both hosts, load-balanced using round-robin scheduling. If one host fails, the other one is used.

8.3.3 Other ways

Multiple address records

Using several DNS MX records can be tedious, 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.

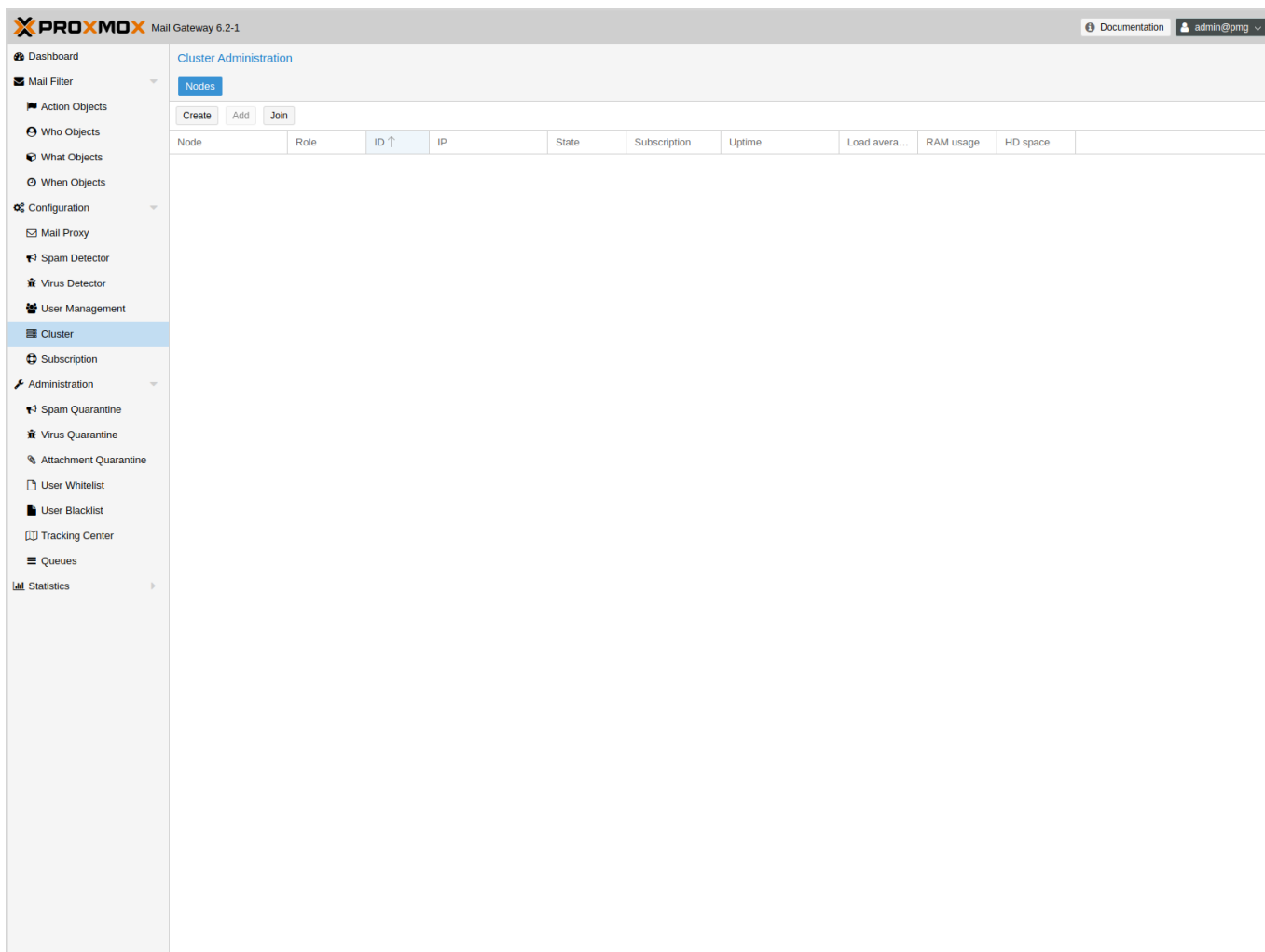
8.4 Cluster Administration

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

Note

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

8.4.1 Creating a Cluster



You can create a cluster from any existing Proxmox Mail Gateway 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

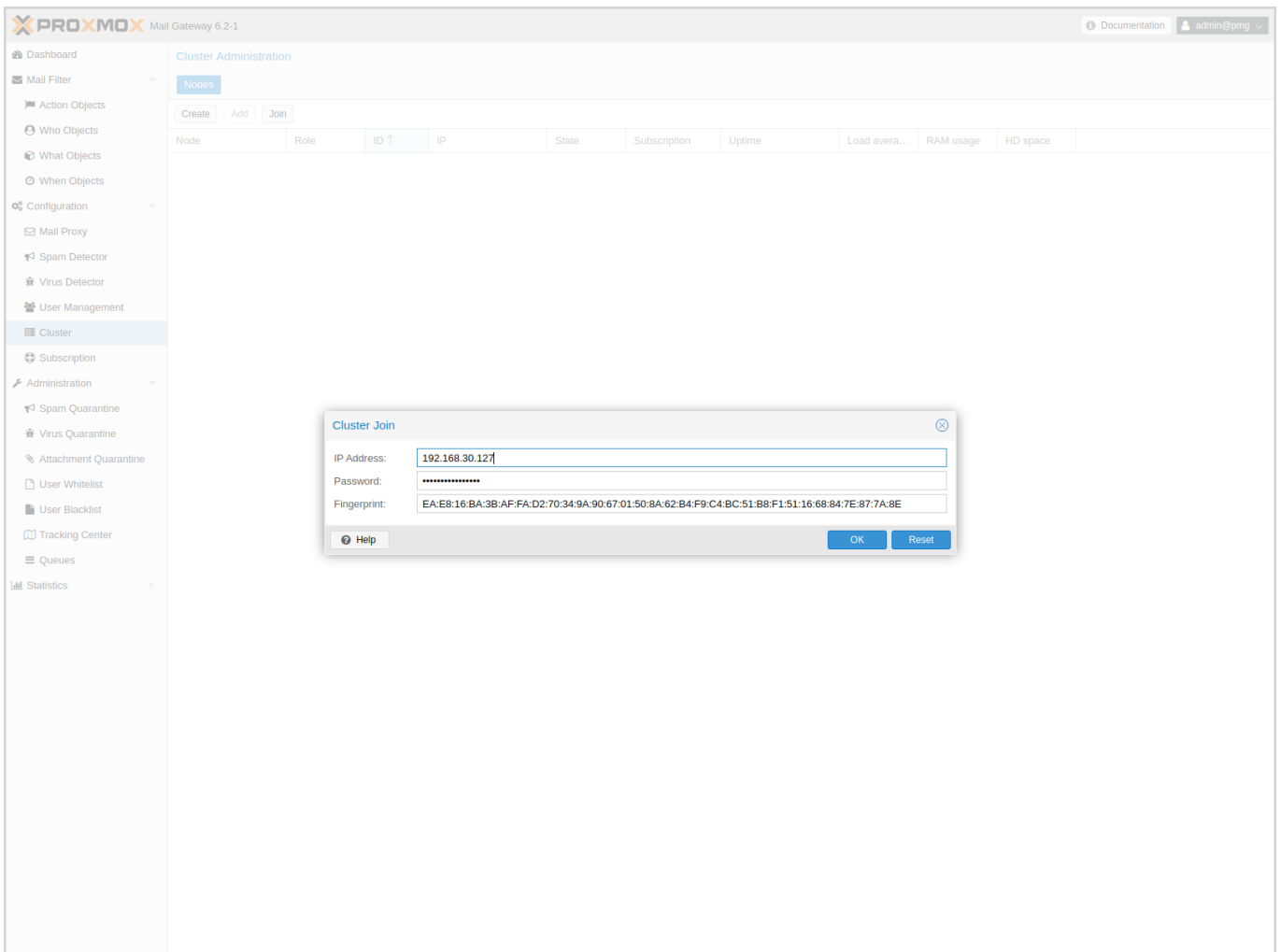
The node where you run the cluster create command will be the *master* node.

8.4.2 Show Cluster Status

The GUI shows the status of all cluster nodes. You can also view this using 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%
```

8.4.3 Adding Cluster Nodes



When you add a new node to a cluster (using `join`), all data on that node is destroyed. The whole database is initialized with the 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 can get this information by pressing the `Add` button on the master node.

Note

Joining a cluster with two-factor authentication enabled for the `root` user is not supported. Remove the second factor when joining the cluster.



Caution

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

Also note that 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.

8.4.4 Deleting Nodes

Please detach nodes from the cluster network, before removing them from the cluster configuration. Only then you should run the following command on the master node:

```
pmgcm delete <cid>
```

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

8.4.5 Disaster Recovery

It is highly recommended to use redundant disks on all cluster nodes (RAID). So in almost any circumstance, 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 lose 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 9

Important Service Daemons

9.1 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 the outside. The `pmgproxy` daemon exposes the API to the outside world.

9.2 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. Operations requiring more permissions are forwarded to the local `pmgdaemon`.

Requests targeted at 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.

9.2.1 Alternative HTTPS certificate

By default, `pmgproxy` uses the certificate `/etc/pmg/pmg-api.pem` for HTTPS connections. This certificate is self signed, and therefore not trusted by browsers and operating systems by default. You can simply replace this certificate with your own (include the key inside the `.pem` file) or obtain one from an ACME enabled CA (configurable in the GUI).

9.2.2 Host based Access Control

It is possible to configure “apache2”-like access control lists. Values are read from file `/etc/default/pmgproxy`. For example:

```
ALLOW_FROM="10.0.0.1-10.0.0.5,192.168.0.0/22"
DENY_FROM="all"
POLICY="allow"
```

IP addresses can be specified using any syntax understood by `Net::IP`. The name `all` is an alias for `0/0` and `::/0` (meaning all IPv4 and IPv6 addresses).

The default policy is `allow`.

Match	POLICY=deny	POLICY=allow
Match Allow only	allow	allow
Match Deny only	deny	deny
No match	deny	allow
Match Both Allow & Deny	deny	allow

9.2.3 Listening IP

By default the `pmgproxy` daemon listens on the wildcard address and accepts connections from both IPv4 and IPv6 clients.

By setting `LISTEN_IP` in `/etc/default/pmgproxy`, you can control which IP address the `pmgproxy` daemon binds to. The IP-address needs to be configured on the system.

Setting the `sysctl net.ipv6.bindv6only` to the non-default `1` will cause the daemons to only accept connections from IPv6 clients, while usually also causing lots of other issues. If you set this configuration, we recommend either removing the `sysctl` setting, or setting the `LISTEN_IP` to `0.0.0.0` (which will allow only IPv4 clients).

`LISTEN_IP` can be used to restrict the socket to an internal interface, thus leaving less exposure to the public internet, for example:

```
LISTEN_IP="192.0.2.1"
```

Similarly, you can also set an IPv6 address:

```
LISTEN_IP="2001:db8:85a3::1"
```

Note that if you want to specify a link-local IPv6 address, you need to provide the interface name itself. For example:

```
LISTEN_IP="fe80::c463:8cff:feb9:6a4e%vmbro"
```



Warning

The nodes in a cluster need access to `pmgproxy` for communication, possibly across different subnets. It is **not recommended** to set `LISTEN_IP` on clustered systems.

To apply the change you need to either reboot your node or fully restart the `pmgproxy` service:

```
systemctl restart pmgproxy.service
```

Note

Unlike `reload`, a `restart` of the `pmgproxy` service can interrupt some long-running worker processes, for example, a running console. Therefore, you should set a maintenance window to bring this change into effect.

9.2.4 SSL Cipher Suite

You can define the cipher list in `/etc/default/pmgproxy`, via the `CIPHERS (TLS <= 1.2)` and `CIPHERSUITE (TLS >= 1.3)` keys.

For example:

```
CIPHERS="ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:↵  
    ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-↵  
    ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-↵  
    AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:↵  
    ECDHE-RSA-AES128-SHA256"
```

The above is the default. See the `ciphers(1)` man page from the `openssl` package for a list of all available options.

The first of these ciphers that is available to both the client and `pmgproxy` will be used.

Additionally, you can allow the client to choose the cipher from the list above, by disabling the `HONOR_CIPHER_ORDER` option in `/etc/default/pmgproxy`:

```
HONOR_CIPHER_ORDER=0
```

9.2.5 Supported TLS versions

The insecure SSL versions 2 and 3 are unconditionally disabled for `pmgproxy`. TLS versions below 1.1 are disabled by default on recent OpenSSL versions, which is honored by `pmgproxy` (see `/etc/ssl/openssl.c`).

To disable TLS version 1.2, set the following in `/etc/default/pmgproxy`:

```
DISABLE_TLS_1_2=1
```

or, respectively, to disable TLS version 1.3:

```
DISABLE_TLS_1_3=1
```

Note

Unless there is a specific reason to do so, it is not recommended to manually adjust the supported TLS versions.

9.2.6 Diffie-Hellman Parameters

You can define the used Diffie-Hellman parameters in `/etc/default/pmgproxy` by setting `DHPARAMS` to the path of a file containing DH parameters in PEM format, for example:

```
DHPARAMS="/path/to/dhparams.pem"
```

If this option is not set, the built-in `skip2048` parameters will be used.

Note

DH parameters are only used if a cipher suite utilizing the DH key exchange algorithm is negotiated.

9.2.7 COMPRESSION

By default `pmgproxy` uses gzip HTTP-level compression for compressible content, if the client supports it. This can be disabled in `/etc/default/pmgproxy`

```
COMPRESSION=0
```

9.3 pmg-smtp-filter - Proxmox SMTP Filter Daemon

The Proxmox SMTP Filter Daemon does the actual spam filtering, using [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 the 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 resent to Postfix at `127.0.0.1:10025`.

9.4 pmgpolicy - Proxmox Mail Gateway Policy Daemon

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

9.5 pmgtunnel - Cluster Tunnel Daemon

This daemon creates an ssh tunnel to the Postgres databases on other cluster nodes (port 5432). The tunnel is used to synchronize the database, using an application-specific, asynchronous replication algorithm.

9.6 pmgmirror - Database Mirror Daemon

Proxmox Mail Gateway uses an application-specific, asynchronous replication algorithm 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 10

Useful Command Line Tools

10.1 pmgdb - Database Management Toolkit

The `pmgdb` toolkit is used to simplify common database management tasks. It is primarily used internally to create and initialize the default database. You can also use it to reset the filter rules to factory defaults:

```
pmgdb reset
```

Or you can dump a human-readable copy of the filter rules:

```
pmgdb dump
```

10.2 pmgsh - API Shell

The `pmgsh` tool can be used to access the Proxmox Mail Gateway API via the command line.

Examples

List entries:

```
# pmgsh ls /
```

Call the *GET* method on a 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
```

10.3 pmgversion - Version Info

`pmgversion` prints detailed version information for Proxmox Mail Gateway packages.

Examples

Print Proxmox Mail Gateway version:

```
# pmgversion
```

List version details for important packages:

```
# pmgversion -v
```

Please use the Debian package manager for details about other packages:

```
# dpkg -l
```

10.4 pmgsubscription - Subscription Management

Proxmox Mail Gateway is free and open-source software. The company that develops it (Proxmox Server Solutions GmbH) offers **support** in many ways, with different support channels, levels, and pricing.

The tool `pmgsubscription` is used to handle Proxmox Mail Gateway subscriptions. Please use the GUI or the `set` command to upload a new key:

```
# pmgsubscription set <key>
```

Note

Subscription keys are bound to specific servers (*Server ID*), so you can use them for exactly one server. Each server needs its own key.

The `get` command is used to view the current subscription status:

```
# pmgsubscription get
key: pmgc-xxxxxxxxxx
level: c
productname: Proxmox Mail Gateway Trial Subscription 1 year
regdate: 2017-12-15 00:00:00
serverid: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
status: Active
url: https://www.proxmox.com/en/proxmox-mail-gateway/pricing
```

10.5 pmgperf - Proxmox Simple Performance Benchmark

The command line tool `pmgperf` gathers some general performance data. This is mostly useful for debugging and identifying 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	hard disk 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 <i>write-back</i> 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 of the 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)
```

10.6 pmgqm - Quarantine Management Toolkit

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

The possible timespans are `week`, `yesterday`, and `today`. The default `pmgspamreport.service` is run at 00:05 every day and calls the `pmgqm` command with the `--timespan yesterday` parameter. This will send a spam report if at least one new spam mail was moved to the quarantine since the beginning of the previous day.

The service can be edited, for example, to change the timespan to `today` or `week`, with the following command:

```
systemctl edit pmgspamreport.service
```

The timer can be edited with the command below:

```
systemctl edit pmgspamreport.timer
```

10.7 pmgreport - Send daily system report email

Generates and sends the daily system report email.

10.8 pmgupgrade - Upgrade Proxmox Mail Gateway

This is a small wrapper around `apt full-upgrade`. We use this to print additional information, like when a node reboot is required, due to a kernel update. Additionally, it can run an interactive shell after the update. This is used when starting an upgrade using the web GUI.

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

```
# apt update
# apt full-upgrade
```

10.9 pmg-log-tracker - Backend for the Tracking Center

`pmg-log-tracker` is the backend for the Tracking Center. It parses the syslog files in `/var/log/` for mail information. You can specify a different file to parse, for example the mail log `/var/log/mail.log`, using the `-i` option.

As an example, parsing the `mail.log` file for everything between the 1st and 15th of July would be possible with the following command:

```
pmg-log-tracker -i /var/log/mail.log -s "2021-07-01 00:00:00" -e ↵
"2021-07-15 23:59:59"
```

Start time `-s` and end time `-e` are optional. By default the end time will be the current time and the start time will be 0:00 of the current day.

With the `--verbose` option, additional info will be printed, such as the complete log for every mail.

It is also possible to filter the log entries based on hostname, from address, to address, and other parameters. For a complete overview of all available options, see `pmg-log-tracker --help`.

As a side effect of parsing the syslog, which doesn't contain information about the year of the entries, the year passed to the `-s` and `-e` options has to be the current one, rather than the one in which the logs were actually created.

10.10 nmap - Port Scans

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

Test Razor port (tcp port 2703):

```
# nmap -Pn -sS -p 2703 c301.cloudmark.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-14 12:20 CEST
Nmap scan report for c301.cloudmark.com (208.83.137.114)
Host is up (0.13s latency).

PORT      STATE SERVICE
2703/tcp  open  sms-chat

Nmap done: 1 IP address (1 host up) scanned in 6.83 seconds
```

For more information about `nmap` usage, see the [Nmap Reference Guide](#), also available as a manual page (`man nmap`).

Chapter 11

Frequently Asked Questions

Note

New FAQs are appended to the bottom of this section.

1. *What distribution is Proxmox Mail Gateway based on?*

Proxmox Mail Gateway is based on [Debian GNU/Linux](#)

2. *What license does the Proxmox Mail Gateway project use?*

Proxmox Mail Gateway code is licensed under the GNU Affero General Public License, version 3 (as of the 5.0 release).

3. *Will Proxmox Mail Gateway run on a 32bit processor?*

Proxmox Mail Gateway works only on 64-bit CPUs (AMD or Intel). There is no plan for 32-bit platform support.

4. *How long will my Proxmox Mail Gateway version be supported?*

Proxmox Mail Gateway versions are supported at least as long as the corresponding Debian Version is [oldstable](#). Proxmox Mail Gateway uses a rolling release model, and using the latest stable version is always recommended.

Proxmox Mail Gateway Version	Debian Version	First Release	Debian EOL	Proxmox EOL
Proxmox Mail Gateway 7.x	Debian 11 (Bullseye)	2021-07	tba	tba
Proxmox Mail Gateway 6.x	Debian 10 (Buster)	2019-08	2022-07	2022-07
Proxmox Mail Gateway 5.x	Debian 9 (Stretch)	2018-01	2020-07	2020-07

Note

Proxmox Mail Gateway releases before 5.0 are not listed here. As they are all EOL (End Of Life), it's highly recommended to upgrade to a newer version, if still in use.

How can I upgrade Proxmox Mail Gateway to the next release?

Minor version upgrades, for example, upgrading from Proxmox Mail Gateway version 5.1 to 5.2, can be done just like any normal update, either through the *Node* → *Updates* panel or through the command line with:

```
apt update
apt full-upgrade
```

Note

Always ensure that you correctly set up the [package repositories](#) Section 3.5, and only continue with the actual upgrade if `apt update` did not hit any errors.

Major version upgrades, for example, going from Proxmox Mail Gateway 5.4 to 6.0, are also supported. They must be carefully planned and tested, and should **never** be started without having an up-to-date backup ready. Although the specific upgrade steps depend on your respective setup, we provide general instructions and advice on how an upgrade should be performed:

- [Upgrade from Proxmox Mail Gateway 6.x to 7.0](#)
- [Upgrade from Proxmox Mail Gateway 5.x to 6.0](#)

Chapter 12

Bibliography

12.1 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

12.2 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
-

12.3 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

Command Line Interface

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

pmgbackup <COMMAND> [ARGS] [OPTIONS]

pmgbackup backup [OPTIONS]

Backup the system configuration.

--notify <always | error | never> (*default = never*)

Specify when to notify via e-mail

--statistic <boolean> (*default = 1*)

Backup statistic databases.

pmgbackup help [OPTIONS]

Get help about specified command.

--extra-args <array>

Shows help for a specific command

--verbose <boolean>

Verbose output format.

pmgbackup list

pmgbackup proxmox-backup backup <remote> [OPTIONS]

Create a new backup and prune the backup group afterwards, if configured.

<remote>: <string>

Proxmox Backup Server ID.

--notify <always | error | never> (*default = never*)

Specify when to notify via e-mail

--statistic <boolean> (default = 1)

Backup statistic databases.

pmgbackup proxmox-backup forget <remote> <backup-id> <backup-time>

Forget a snapshot

<remote>: <string>

Proxmox Backup Server ID.

<backup-id>: <string>

ID (hostname) of backup snapshot

<backup-time>: <string>

Backup time in RFC 3339 format

pmgbackup proxmox-backup job create <remote> [OPTIONS]

Create backup schedule

<remote>: <string>

Proxmox Backup Server ID.

--delay [0-9a-zA-Z.]+ (default = 5min)

Randomized delay to add to the starttime (RandomizedDelaySec setting of the systemd.timer)

--schedule [0-9a-zA-Z*.:,\- /]+ (default = daily)

Schedule for the backup (OnCalendar setting of the systemd.timer)

pmgbackup proxmox-backup job delete <remote>

Delete backup schedule

<remote>: <string>

Proxmox Backup Server ID.

pmgbackup proxmox-backup job show <remote> [FORMAT_OPTIONS]

Get timer specification

<remote>: <string>

Proxmox Backup Server ID.

pmgbackup proxmox-backup list <remote> [FORMAT_OPTIONS]

Get snapshots stored on remote.

<remote>: <string>

Proxmox Backup Server ID.

pmgbackup proxmox-backup remote add <remote> --datastore <string> --server <string> [OPTIONS]

Add Proxmox Backup Server remote instance.

<remote>: <string>

Proxmox Backup Server ID.

--datastore (?: [A-Za-z0-9_] [A-Za-z0-9._\-*])

Proxmox Backup Server datastore name.

--disable <boolean>

Flag to disable (deactivate) the entry.

--fingerprint ([A-Fa-f0-9]{2}:){31}[A-Fa-f0-9]{2}

Certificate SHA 256 fingerprint.

--include-statistics <boolean>

Include statistics in scheduled backups

--keep-daily <N>

Keep backups for the last <N> different days. If there is more than one backup for a single day, only the latest one is kept.

--keep-hourly <N>

Keep backups for the last <N> different hours. If there is more than one backup for a single hour, only the latest one is kept.

--keep-last <N>

Keep the last <N> backups.

--keep-monthly <N>

Keep backups for the last <N> different months. If there is more than one backup for a single month, only the latest one is kept.

--keep-weekly <N>

Keep backups for the last <N> different weeks. If there is more than one backup for a single week, only the latest one is kept.

--keep-yearly <N>

Keep backups for the last <N> different years. If there is more than one backup for a single year, only the latest one is kept.

--namespace

(?: (?: [A-Za-z0-9_] [A-Za-z0-9._\-*]) /) {0,7} (?: (?: [A-Za-z0-9_] [A-Za-z0-9._\-*])

Proxmox Backup Server namespace in the datastore, defaults to the root NS.

--notify <always | error | never>

Specify when to notify via e-mail

--password <password>

Password or API token secret for the user on the Proxmox Backup Server.

--server <string>

Proxmox Backup Server address.

--username (? : [^\s\\@]+\@[^\s\\/\\@]+)

Username or API token ID on the Proxmox Backup Server

pmgbackup proxmox-backup remote list [FORMAT_OPTIONS]

List all configured Proxmox Backup Server instances.

pmgbackup proxmox-backup remote remove <remote>

Delete an PBS remote

<remote>: <string>

Profile ID.

pmgbackup proxmox-backup remote set <remote> [OPTIONS]

Update PBS remote settings.

<remote>: <string>

Proxmox Backup Server ID.

--datastore (? : [A-Za-z0-9_] [A-Za-z0-9._\ -] *)

Proxmox Backup Server datastore name.

--delete <string>

A list of settings you want to delete.

--digest <string>

Prevent changes if current configuration file has different SHA1 digest. This can be used to prevent concurrent modifications.

--disable <boolean>

Flag to disable (deactivate) the entry.

--fingerprint ([A-Fa-f0-9]{2}:){31} [A-Fa-f0-9]{2}

Certificate SHA 256 fingerprint.

--include-statistics <boolean>

Include statistics in scheduled backups

--keep-daily <N>

Keep backups for the last <N> different days. If there is more than one backup for a single day, only the latest one is kept.

--keep-hourly <N>

Keep backups for the last <N> different hours. If there is more than one backup for a single hour, only the latest one is kept.

--keep-last <N>

Keep the last <N> backups.

--keep-monthly <N>

Keep backups for the last <N> different months. If there is more than one backup for a single month, only the latest one is kept.

--keep-weekly <N>

Keep backups for the last <N> different weeks. If there is more than one backup for a single week, only the latest one is kept.

--keep-yearly <N>

Keep backups for the last <N> different years. If there is more than one backup for a single year, only the latest one is kept.

--namespace

(?: (?: [A-Za-z0-9_] [A-Za-z0-9._\ -] *) /) {0,7} (?: (?: [A-Za-z0-9_] [A-Za-z0-9._\ -]

Proxmox Backup Server namespace in the datastore, defaults to the root NS.

--notify <always | error | never>

Specify when to notify via e-mail

--password <password>

Password or API token secret for the user on the Proxmox Backup Server.

--server <string>

Proxmox Backup Server address.

--username (?: [^\s\@]+\@[^\s\/\@]+)

Username or API token ID on the Proxmox Backup Server

pmgbackup proxmox-backup restore <remote> <backup-id> <backup-time> [OPTIONS]

Restore the system configuration.

<remote>: <string>

Proxmox Backup Server ID.

<backup-id>: <string>

backup-id (hostname) of backup snapshot

<backup-time>: <string>

backup-time to restore

--config <boolean> (default = 0)

Restore system configuration.

--database <boolean> (default = 1)

Restore the rule database. This is the default.

--statistic <boolean> (default = 0)

Restore statistic databases. Only considered when you restore the *database*.

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*.

A.2 pmgcm - Proxmox Mail Gateway Cluster Management Toolkit

pmgcm <COMMAND> [ARGS] [OPTIONS]

pmgcm create

Create initial cluster config with current node as master.

pmgcm delete <cid>

Remove a node from the cluster.

<cid>: <integer> (1 - N)

Cluster Node ID.

pmgcm help [OPTIONS]

Get help about specified command.

--extra-args <array>
Shows help for a specific command

--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 join_cmd

An alias for *pmgcm join-cmd*.

pmgcm promote

Promote current node to become the new master.

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.

pmgcm update-fingerprints

Notify master to refresh all certificate fingerprints

A.3 pmgsh - API Shell

Interactive session:

pmgsh

Directly call API functions:

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

A.4 pmgperf - Proxmox Simple Performance Benchmark

pmgperf help

pmgperf [<path>]

Proxmox benchmark.

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

A.5 pmgconfig - Configuration Management Toolkit

pmgconfig <COMMAND> [ARGS] [OPTIONS]

pmgconfig acme account deactivate [<name>] [OPTIONS]

Deactivate existing ACME account at CA.

<name>: <name> (default = default)
ACME account config file name.

--force <boolean> (default = 0)
Delete account data even if the server refuses to deactivate the account.

pmgconfig acme account info [<name>] [FORMAT_OPTIONS]

Return existing ACME account information.

<name>: <name> (default = default)
ACME account config file name.

pmgconfig acme account list

ACME account index.

pmgconfig acme account register [<name>] {<contact>} [OPTIONS]

Register a new ACME account with a compatible CA.

<name>: <name> (default = default)
ACME account config file name.

<contact>: <string>
Contact email addresses.

--directory ^https?://.*
URL of ACME CA directory endpoint.

pmgconfig acme account update [`<name>`] [OPTIONS]

Update existing ACME account information with CA. Note: not specifying any new account information triggers a refresh.

<name>: `<name>` (**default = default**)

ACME account config file name.

--contact `<string>`

Contact email addresses.

pmgconfig acme cert order `<type>` [OPTIONS]

Order a new certificate from ACME-compatible CA.

<type>: `<api | smtp>`

The TLS certificate type (API or SMTP certificate).

--force `<boolean>` (**default = 0**)

Overwrite existing custom certificate.

pmgconfig acme cert renew `<type>` [OPTIONS]

Renew existing certificate from CA.

<type>: `<api | smtp>`

The TLS certificate type (API or SMTP certificate).

--force `<boolean>` (**default = 0**)

Force renewal even if expiry is more than 30 days away.

pmgconfig acme cert revoke `<type>`

Revoke existing certificate from CA.

<type>: `<api | smtp>`

The TLS certificate type (API or SMTP certificate).

pmgconfig acme plugin add `<type>` `<id>` [OPTIONS]

Add ACME plugin configuration.

<type>: `<dns | standalone>`

ACME challenge type.

<id>: `<string>`

ACME Plugin ID name

```
--api <1984hosting | acmedns | acmeproxy | active24 | ad | ali |
anx | arvan | aurora | autodns | aws | azion | azure | cf |
clouddns | cloudns | cn | conoha | constellix | cx | cyon | da |
ddns | desec | df | dgon | dnsimple | do | doapi | domeshop | dp
| dpi | dreamhost | duckdns | durabledns | dyn | dynu | dynv6 |
easydns | edgedns | euserv | exoscale | freedns | gandi_livedns |
gcloud | gd | gdnsdk | he | hetzner | hexonet | hostingde |
huaweicloud | infoblox | infomaniak | internetbs | inwx | ionos |
ispconfig | jd | joker | kappernet | kas | kinghost | knot |
leaseweb | lexicon | linode | linode_v4 | loopia | lua | maradns |
me | miab | misaka | myapi | mydevil | mydnsjp | namecheap |
namecom | namesilo | nederhost | neodigit | netcup | netlify | nic
| njalla | nm | nsd | nsone | nsupdate | nw | oci | one | online |
openprovider | openstack | opnsense | ovh | pdns | pleskxml |
pointhq | porkbun | rackcorp | rackspace | rcode0 | regru |
scaleway | schlundtech | selectel | servercow | simply | tele3 |
transip | ultra | unoeuro | variomedia | veesp | vscale | vultr |
websupport | world4you | yandex | zilore | zone | zonomi>
```

API plugin name

--data File with one key-value pair per line, will be base64url encode for storage in plugin config.

DNS plugin data. (base64 encoded)

--disable <boolean>

Flag to disable the config.

--nodes <string>

List of cluster node names.

--validation-delay <integer> (0 - 172800) (default = 30)

Extra delay in seconds to wait before requesting validation. Allows to cope with a long TTL of DNS records.

pmgconfig acme plugin config <id> [FORMAT_OPTIONS]

Get ACME plugin configuration.

<id>: <string>

Unique identifier for ACME plugin instance.

pmgconfig acme plugin list [OPTIONS] [FORMAT_OPTIONS]

ACME plugin index.

--type <dns | standalone>

Only list ACME plugins of a specific type

pmgconfig acme plugin remove <id>

Delete ACME plugin configuration.

<id>: <string>

Unique identifier for ACME plugin instance.

pmgconfig acme plugin set <id> [OPTIONS]

Update ACME plugin configuration.

<id>: <string>

ACME Plugin ID name

```
--api <1984hosting | acmedns | acmeproxy | active24 | ad | ali |
anx | arvan | aurora | autodns | aws | azion | azure | cf |
clouddns | cloudns | cn | conoha | constellix | cx | cyon | da |
ddnss | desec | df | dgon | dnsimple | do | doapi | domeshop | dp
| dpi | dreamhost | duckdns | durabledns | dyn | dynu | dynv6 |
easydns | edgedns | euserv | exoscale | freedns | gandi_livedns |
gcloud | gd | gdnsdk | he | hetzner | hexonet | hostingde |
huaweicloud | infoblox | infomaniak | internetbs | inwx | ionos |
ispconfig | jd | joker | kapper.net | kas | kinghost | knot |
leaseweb | lexicon | linode | linode_v4 | loopia | lua | maradns |
me | miab | misaka | myapi | mydevil | mydnsjp | namecheap |
namecom | namesilo | nederhost | neodigit | netcup | netlify | nic
| njalla | nm | nsd | nsone | nsupdate | nw | oci | one | online |
openprovider | openstack | opnsense | ovh | pdns | pleskxml |
pointhq | porkbun | rackcorp | rackspace | rcode0 | regru |
scaleway | schlundtech | selectel | servercow | simply | tele3 |
transip | ultra | unoeuro | variomedia | veesp | vscale | vultr |
websupport | world4you | yandex | zilore | zone | zonomi>
```

API plugin name

```
--data File with one key-value pair per line, will be base64url
encode for storage in plugin config.
```

DNS plugin data. (base64 encoded)

```
--delete <string>
```

A list of settings you want to delete.

```
--digest <string>
```

Prevent changes if current configuration file has different SHA1 digest. This can be used to prevent concurrent modifications.

```
--disable <boolean>
```

Flag to disable the config.

--nodes <string>

List of cluster node names.

--validation-delay <integer> (0 - 172800) (default = 30)

Extra delay in seconds to wait before requesting validation. Allows to cope with a long TTL of DNS records.

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 cert delete <type> [<restart>]

DELETE custom certificate chain and key.

<type>: <api | smtp>

The TLS certificate type (API or SMTP certificate).

<restart>: <boolean> (default = 0)

Restart pmgproxy.

pmgconfig cert info [FORMAT_OPTIONS]

Get information about the node's certificates.

pmgconfig cert set <type> <certificates> <key> [OPTIONS] [FORMAT_OPTIONS]

Upload or update custom certificate chain and key.

<type>: <api | smtp>

The TLS certificate type (API or SMTP certificate).

<certificates>: <string>

PEM encoded certificate (chain).

<key>: <string>

PEM encoded private key.

--force <boolean> (default = 0)

Overwrite existing custom or ACME certificate files.

--restart <boolean> (default = 0)

Restart services.

pmgconfig dkim_record

Get the public key for the configured selector, prepared as DKIM TXT record

pmgconfig dkim_set --keysize <integer> --selector <string> [OPTIONS]

Generate a new private key for selector. All future mail will be signed with the new key!

--force <boolean>
Overwrite existing key

--keysize <integer> (1024 - N)
Number of bits for the RSA-Key

--selector <string>
DKIM Selector

pmgconfig dump

Print configuration setting which can be used in templates.

pmgconfig help [OPTIONS]

Get help about specified command.

--extra-args <array>
Shows help for a specific command

--verbose <boolean>
Verbose output format.

pmgconfig init

Generate required files in /etc/pmg/

pmgconfig ldapsync

Synchronize the LDAP database.

pmgconfig sync [OPTIONS]

Synchronize 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.

A.6 pmgdb - Database Management Toolkit

pmgdb <COMMAND> [ARGS] [OPTIONS]

pmgdb delete

Delete PMG rule database.

pmgdb dump

Print the PMG rule database.

pmgdb help [OPTIONS]

Get help about specified command.

--extra-args <array>

Shows help for a specific command

--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 B

Service Daemons

B.1 pmgdaemon - Proxmox Mail Gateway API Daemon

pmgdaemon <COMMAND> [ARGS] [OPTIONS]

pmgdaemon help [OPTIONS]

Get help about specified command.

--extra-args <array>

Shows help for a specific command

--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.

B.2 pmgproxy - Proxmox Mail Gateway API Proxy Daemon

pmgproxy <COMMAND> [ARGS] [OPTIONS]

pmgproxy help [OPTIONS]

Get help about specified command.

--extra-args <array>
Shows help for a specific command

--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.

B.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

B.4 pmgpolicy - Proxmox Mail Gateway Policy Daemon

Please use systemd tools to manage this service.

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

B.5 pmgtunnel - Cluster Tunnel Daemon

pmgtunnel <COMMAND> [ARGS] [OPTIONS]

pmgtunnel help [OPTIONS]

Get help about specified command.

--extra-args <array>
Shows help for a specific command

--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

B.6 pmgmirror - Database Mirror Daemon

pmgmirror <COMMAND> [ARGS] [OPTIONS]

pmgmirror help [OPTIONS]

Get help about specified command.

--extra-args <array>
Shows help for a specific command

--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 C

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 (<i>SPAMLEVEL</i>) point

Appendix D

Configuration Files

D.1 Proxmox Mail Gateway Main Configuration

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

D.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.

D.1.2 Options

SECTION *admin*

advfilter: `<boolean>` (*default = 1*)

Use advanced filters for statistic.

avast: `<boolean>` (*default = 0*)

Use Avast Virus Scanner (`/usr/bin/scan`). You need to buy and install *Avast Core Security* before you can enable this feature.

clamav: `<boolean>` (*default = 1*)

Use ClamAV Virus Scanner. This is the default virus scanner and is enabled by default.

custom_check: `<boolean>` (*default = 0*)

Use Custom Check Script. The script has to take the defined arguments and can return Virus findings or a Spamscore.

custom_check_path: `^/([^\0]+\w/)+[^\0]+$` (**default = /usr/local/bin/pmg-custom-check**)
Absolute Path to the Custom Check Script

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

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

dkim_selector: `<string>`
Default DKIM selector

dkim_sign: `<boolean>` (**default = 0**)
DKIM sign outbound mails with the configured Selector.

dkim_sign_all_mail: `<boolean>` (**default = 0**)
DKIM sign all outgoing mails irrespective of the Envelope From domain.

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**)
Whether to mark encrypted archives and documents as heuristic virus match. A match does not necessarily result in an immediate block, it just raises the Spam Score by `clamav_heuristic_score`.

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 (in bytes) 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 (in bytes) to be scanned for each input file.

safebrowsing: <boolean> (*default = 0*)

Enables support for Google Safe Browsing. (deprecated option, will be ignored)

scriptedupdates: <boolean> (*default = 1*)

Enables ScriptedUpdates (incremental download of signatures)

SECTION *mail*

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

ESMTP banner.

before_queue_filtering: <boolean> (*default = 0*)

Enable before queue filtering by pmg-smtp-filter

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).

dnsbl_threshold: <integer> (0 - N) (*default = 1*)

The inclusive lower bound for blocking a remote SMTP client, based on its combined DNSBL score (see `postscreen_dnsbl_threshold` parameter).

dwarning: <integer> (0 - N) (*default = 4*)

SMTP delay warning time (in hours).

ext_port: <integer> (1 - 65535) (*default = 25*)

SMTP port number for incoming mail (untrusted). This must be a different number than *int_port*.

greylist: <boolean> (*default = 1*)

Use Greylisting for IPv4.

greylist6: <boolean> (*default = 0*)

Use Greylisting for IPv6.

greylistmask4: <integer> (0 - 32) (*default = 24*)

Netmask to apply for greylisting IPv4 hosts

greylistmask6: <integer> (0 - 128) (*default = 64*)

Netmask to apply for greylisting IPv6 hosts

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 = 26*)

SMTP port number for outgoing mail (trusted).

max_filters: <integer> (3 - 40) (*default = 38*)

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 = 100*)

Maximum number of SMTP daemon processes (in).

max_smtpd_out: <integer> (3 - 100) (*default = 100*)

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.

ndr_on_block: <boolean> (*default = 0*)

Send out NDR when mail gets blocked

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 (SMTP only, ignored for LMTP).

relayport: <integer> (1 - 65535) (*default = 25*)

SMTP/LMTP port number for relay host.

relayprotocol: <lmtpl | smtp> (*default = smtp*)

Transport protocol for relay host.

smarthost: <string>

When set, all outgoing mails are delivered to the specified smarthost.

smarthostport: <integer> (1 - 65535) (*default = 25*)

SMTP port number for 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 specifies 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 ClamAV heuristics (Encrypted Archives/Documents, 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. Useful 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.

port: <integer> (1 - 65535) (default = 8006)

Quarantine Port. Useful if you have a reverse proxy or port forwarding for the webinterface. Only used for the generated Spam report.

protocol: <http | https> (default = https)

Quarantine Webinterface Protocol. Useful if you have a reverse proxy for the webinterface. Only used for the generated Spam report.

quarantinelink: <boolean> (*default = 0*)

Enables user self-service for Quarantine Links. Caution: this is accessible without authentication

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.

D.2 Cluster Configuration

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

D.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.

D.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.

D.3 User Configuration

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

D.3.1 File Format

The file has the following format for each user:

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

D.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 | helpdesk | qmanager | root>

User role. Role *root* is reserved for the Unix Superuser.

userid: <string>

User ID

D.4 LDAP Configuration

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

D.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.

D.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.

cafile: <string>

Path to CA file. Only useful with option *verify*

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 | ldap+starttls | ldaps> (*default = ldap*)

LDAP protocol mode (*ldap, ldaps or ldap+starttls*).

port: <integer> (1 - 65535)

Specify the port to connect to.

profile: <string>

Profile ID.

server1: <string>

Server address.

server2: <string>

Fallback server address. Used when the first server is not available.

verify: <boolean> (*default = 0*)

Verify server certificate. Only useful with *ldaps* or *ldap+starttls*.

Appendix E

GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc. <https://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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. Secondly, 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 <https://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.