



LAB WEEK 6:

Email Relay

NGUYEN CONG LUC

nguyencongluc.82@gmail.com

[Luc Nguyen](#) | [LinkedIn](#)

0329206845

MỤC LỤC

MỤC TIÊU	4
CHUẨN BỊ.....	5
Phần 1. Cài đặt Proxmox Mail Gateway	6
1.1 Tổng quan về Proxmox Mail Gateway	6
1.2 Cài đặt Proxmox Mail Gateway	6
1.3 Thêm SSL cho website PMG	12
1.3.1 Cấu hình DNS cho website PMG	12
1.3.2 Khắc phục lỗi kho lưu trữ Proxmox	13
1.3.3 Cấu hình DNS Record	14
1.3.4 Cài đặt Certbot và chứng chỉ SSL từ Let's Encrypt	14
1.3.5 Áp dụng chứng chỉ SSL vào website PMG.....	15
Phần 2. Cấu hình PMG làm Email Relay cho Zimbra.....	16
2.1 Cấu hình Relay PMG trong Mail Proxy:	16
2.1.1 Cấu hình Relaying:	16
2.1.2 Cấu hình Replay Domains:	17
2.1.3 Cấu hình Port:.....	17
2.1.4 Cấu hình Options:.....	18
2.1.5 Cấu hình Transports:	19
2.1.6 Cấu hình Networks:	20
2.1.7 Cấu hình TLS:.....	21
2.1.8 Cấu hình DKIM:	21
2.1.9 Cấu hình Whitelist:	23
2.2 Cấu hình Zimbra để gửi qua PMG:.....	23
Phần 3. Cấu hình đảm bảo Mail Exchange, SPF, DKIM, DMARC valid.....	25
3.1 Cấu hình MX.....	25
3.2 Cấu hình SPF	25
3.2 Cấu hình DKIM	26
3.3 Cấu hình DMARC	26
3.4 Cấu hình PTR.....	26
3.5 Kiểm tra gửi email	27
3.5.1 Gửi email từ Zimbra qua PMG tới Email Server khác.:	27
3.5.2 Gửi email từ Email Server khác qua PMG đến Zimbra:	29
Phần 4. Tìm hiểu về các chức năng có trên PMG.....	31
4.1 Spam Filtering (Lọc thư rác):.....	31
4.1.1 Kiểm tra và cài đặt cấu hình SpamAssassin trên giao diện.....	31
4.1.2 Huấn luyện dữ liệu cho Bayesian	32
4.1.3 Chỉnh sửa file cấu hình SpamAssassin trong file custom.....	34
4.1.4 Thử nghiệm gửi email spam và email sạch đến zimbra:	36
4.2 Virus Scanning (Quét virus):	38
4.2.1 Cấu hình ClamAV.....	38
4.2.2 Chuẩn bị virus thử nghiệm	39

4.2.3 Chuẩn bị mail client, thêm virus và thử nghiệm gửi đi.....	40
4.2.4 Kiểm tra kết quả	41
4.3 Greylisting (Tạm hoãn email):	42
4.4 Hạn chế Email gửi đến với DNSBL, User Blacklist và Mail Filter-Rules:	43
4.4.1 Chặn email với DNSBL (Danh sách đen DNS)	43
4.4.2 Cách ly email với User Blacklist	44
4.4.3 Chặn email với Mail Filter-Rules	45
4.5 Tracking Center (Theo dõi luồng email):	48
4.6 Quarantine (Cách ly email):	49
4.7 Quét Email Gửi Đi (Outgoing Mail Scanning).....	50
4.8 Thống kê và Báo cáo (Statistics and Reporting)	51

MỤC TIÊU

Week 6: Email Relay

Yêu cầu:

- Request 1 IP WAN từ leader: IP: 45.122.223.89/25 GW: 45.122.223.1
- Download phần mềm Proxmox Mail Gateway (Đã download và mount vào VM sẵn).
 - ISO proxmox-mail-gateway_8.1-1.iso

Memory	2.00 GiB
Processors	1 (1 sockets, 1 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
Cloudinit Drive (ide0)	backup:164/vm-164-cloudinit.qcow2,media=cdrom,size=4M
CD/DVD Drive (ide2)	backup:iso/proxmox-mail-gateway_8.1-1.iso,media=cdrom,size=1309398K
Hard Disk (virtio0)	backup:164/vm-164-disk-0.qcow2,discard=on,size=20684M
Network Device (net0)	virtio=BC:24:11:2C:EE:43,bridge=vbr0,firewall=1,tag=111
Serial Port (serial0)	socket

- Tạo 1 VM và cài đặt Proxmox Mail Gateway (PMG) lên 1 VM này (đã tạo và assign)
- Cấu hình toàn bộ hệ thống email từ server Email Server của tuần 5(45.122.223.81) gửi và nhận email qua hệ thống PMG này.
- Đảm bảo SPF, DKIM, DMARC valid cho email khi gửi ra.
- Tìm hiểu về các chức năng có trên PMG.

CHUẨN BỊ

- Cấu hình Hardware:

Virtual Machine 124 (ns12-w06-lucnc) on node 'intern' No Tags

Component	Value
Memory	4.00 GiB
Processors	4 (2 sockets, 2 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
CloudInit Drive (ide0)	backup:124/vm-124-cloudinit.qcow2,media=cdrom,size=4M
CD/DVD Drive (ide2)	backup:iso/proxmox-mail-gateway_8.1-1.iso,media=cdrom,size=1309398K
Hard Disk (virtio0)	backup:124/vm-124-disk-0.qcow2,discard=on,size=20684M
Network Device (net0)	virtio=BC:24:11:55:9C:25,bridge=vbr0,firewall=1,tag=111
Serial Port (serial0)	socket

- Cấu hình Cloud-Init

Virtual Machine 124 (ns12-w06-lucnc) on node 'intern' No Tags

Component	Value
User	nguyencongluc
Password	*****
DNS domain	vhost.vn
DNS servers	103.232.121.8
SSH public key	none
Upgrade packages	Yes
IP Config (net0)	ip=45.122.223.89/25,gw=45.122.223.1

Phần 1. Cài đặt Proxmox Mail Gateway

1.1 Tổng quan về Proxmox Mail Gateway

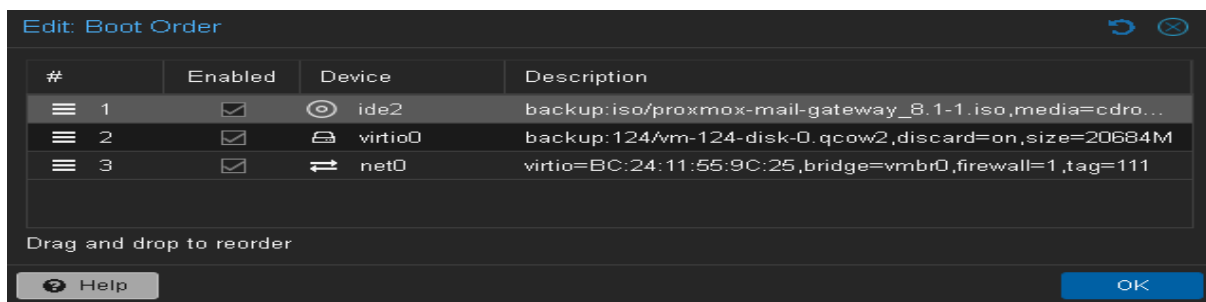
Proxmox Mail Gateway (PMG) là một giải pháp mã nguồn mở dựa trên Debian, được thiết kế để làm máy chủ trung chuyển email (mail relay). PMG cung cấp các tính năng chính như:

- **Lọc spam và virus:** Sử dụng SpamAssassin và ClamAV để bảo vệ hệ thống email.
- **Xác thực email:** Hỗ trợ SPF, DKIM, DMARC để đảm bảo email hợp lệ.
- **Quản lý email:** Theo dõi, cách ly (quarantine) và thống kê lưu lượng email.
- **Dễ triển khai:** Giao diện web thân thiện, tích hợp tốt với các mail server như Zimbra.

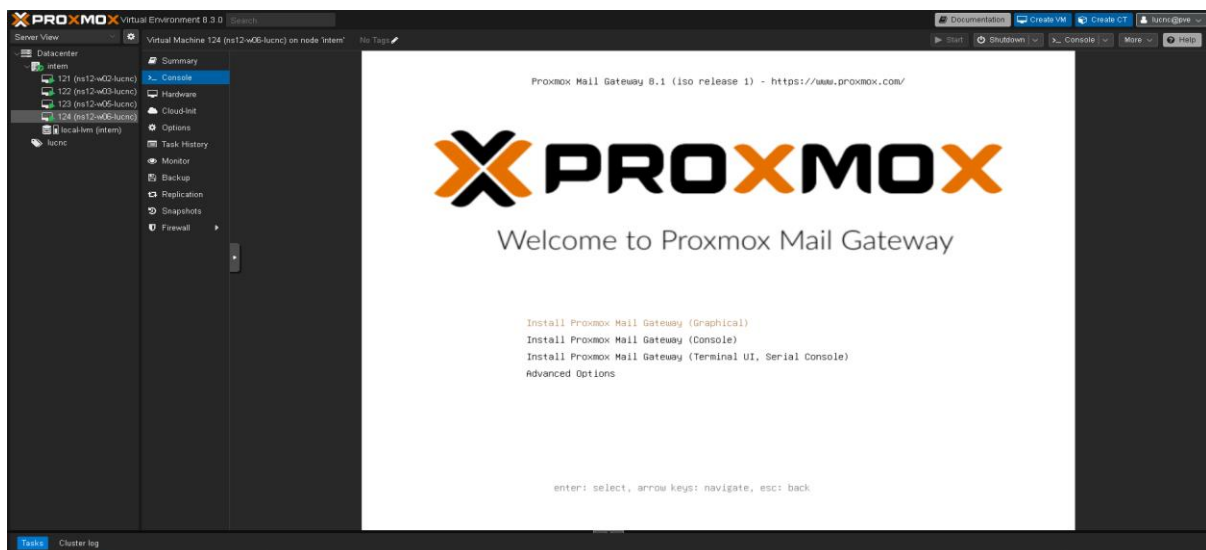
PMG hoạt động như một lớp bảo vệ và trung chuyển giữa mail server nội bộ và Internet, giúp tăng cường bảo mật và hiệu quả quản lý email.

1.2 Cài đặt Proxmox Mail Gateway

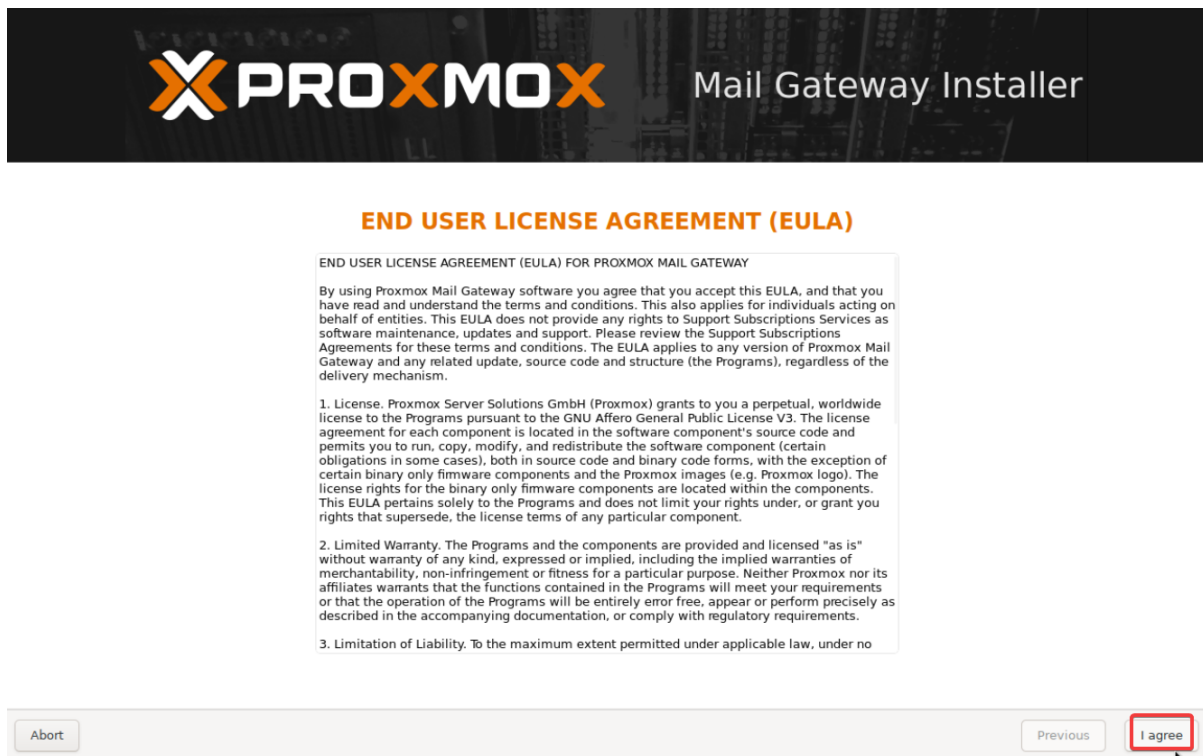
- Trong Proxmox->Options->Boot Orders: đảm bảo đặt thứ tự boot order để file ISO PMG(Proxmox-mail-gateway) lên trước, thế thì khi khởi động mới boot vào được



- Nhấn enter tại giao diện trang chủ



- Nhấn I agree



The screenshot shows the 'END USER LICENSE AGREEMENT (EULA)' screen of the Proxmox Mail Gateway Installer. At the top, the Proxmox logo and 'Mail Gateway Installer' are displayed. The main content area contains the EULA text, which includes a preamble and three numbered sections: 1. License, 2. Limited Warranty, and 3. Limitation of Liability. At the bottom, there are three buttons: 'Abort', 'Previous', and 'I agree'. The 'I agree' button is highlighted with a red rectangle.

END USER LICENSE AGREEMENT (EULA)

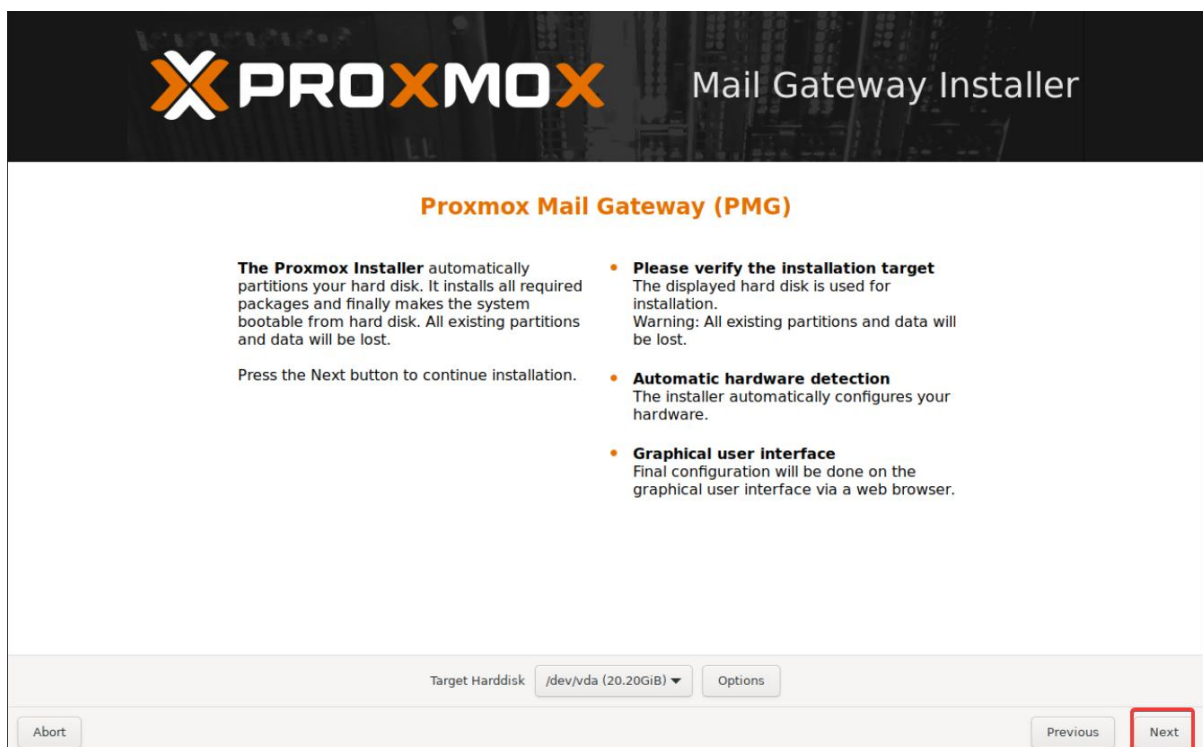
END USER LICENSE AGREEMENT (EULA) FOR PROXMOX MAIL GATEWAY

By using Proxmox Mail Gateway software you agree that you accept this EULA, and that you have read and understand the terms and conditions. This also applies for individuals acting on behalf of entities. This EULA does not provide any rights to Support Subscriptions Services as software maintenance, updates and support. Please review the Support Subscriptions Agreements for these terms and conditions. The EULA applies to any version of Proxmox Mail Gateway and any related update, source code and structure (the Programs), regardless of the delivery mechanism.

1. License. Proxmox Server Solutions GmbH (Proxmox) grants to you a perpetual, worldwide license to the Programs pursuant to the GNU Affero General Public License V3. The license agreement for each component is located in the software component's source code and permits you to run, copy, modify, and redistribute the software component (certain obligations in some cases), both in source code and binary code forms, with the exception of certain binary only firmware components and the Proxmox images (e.g. Proxmox logo). The license rights for the binary only firmware components are located within the components. This EULA pertains solely to the Programs and does not limit your rights under, or grant you rights that supersede, the license terms of any particular component.
2. Limited Warranty. The Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose. Neither Proxmox nor its affiliates warrants that the functions contained in the Programs will meet your requirements or that the operation of the Programs will be entirely error free, appear or perform precisely as described in the accompanying documentation, or comply with regulatory requirements.
3. Limitation of Liability. To the maximum extent permitted under applicable law, under no

Abort Previous **I agree**

- Bấm Next



The screenshot shows the 'Proxmox Mail Gateway (PMG)' screen of the Proxmox Mail Gateway Installer. At the top, the Proxmox logo and 'Mail Gateway Installer' are displayed. The main content area contains information about the Proxmox Installer, including a warning about hard disk partitions and a list of features: Please verify the installation target, Automatic hardware detection, and Graphical user interface. At the bottom, there are three buttons: 'Abort', 'Previous', and 'Next'. The 'Next' button is highlighted with a red rectangle.

Proxmox Mail Gateway (PMG)

The Proxmox Installer automatically partitions your hard disk. It installs all required packages and finally makes the system bootable from hard disk. All existing partitions and data will be lost.

Press the Next button to continue installation.

- **Please verify the installation target**
The displayed hard disk is used for installation.
Warning: All existing partitions and data will be lost.
- **Automatic hardware detection**
The installer automatically configures your hardware.
- **Graphical user interface**
Final configuration will be done on the graphical user interface via a web browser.

Target Harddisk: /dev/vda (20.20GiB) Options

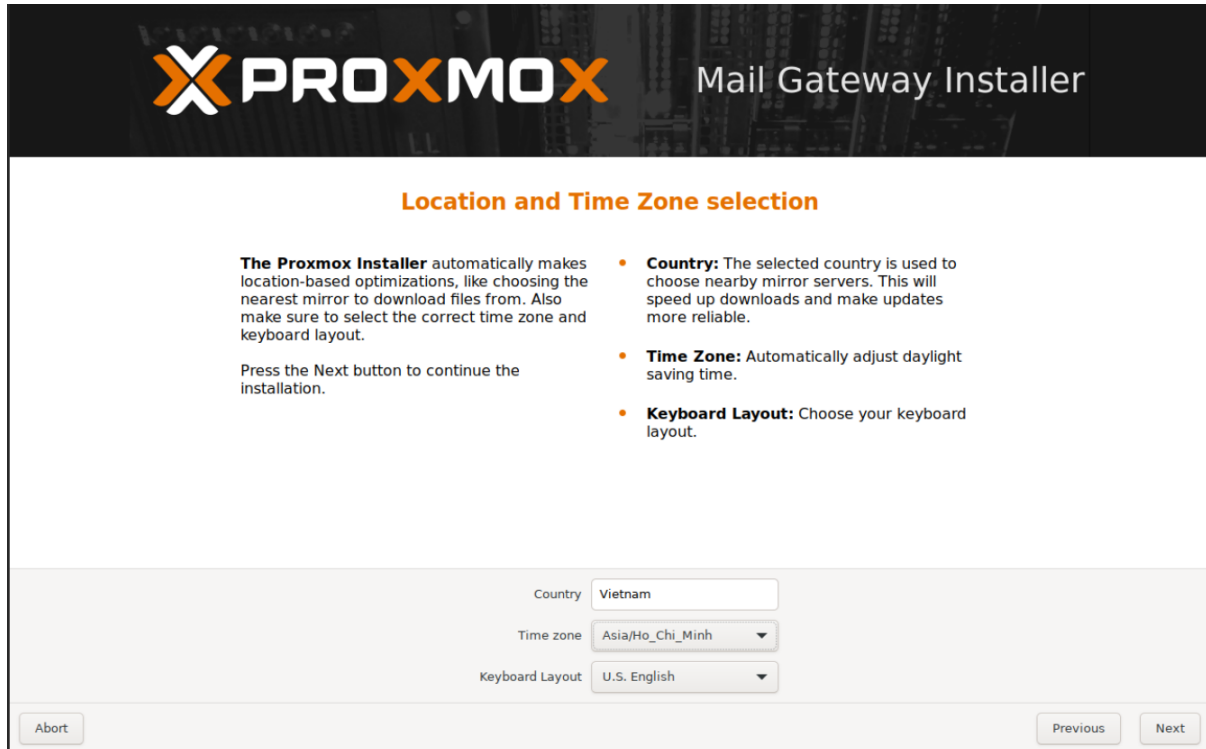
Abort Previous **Next**

- Nhập:

Country: Vietnam,

Time zone: Asia/HoChiMinh,

KeyboardLayout: U.S.English



PROXMOX Mail Gateway Installer

Location and Time Zone selection

The Proxmox Installer automatically makes location-based optimizations, like choosing the nearest mirror to download files from. Also make sure to select the correct time zone and keyboard layout.

Press the Next button to continue the installation.

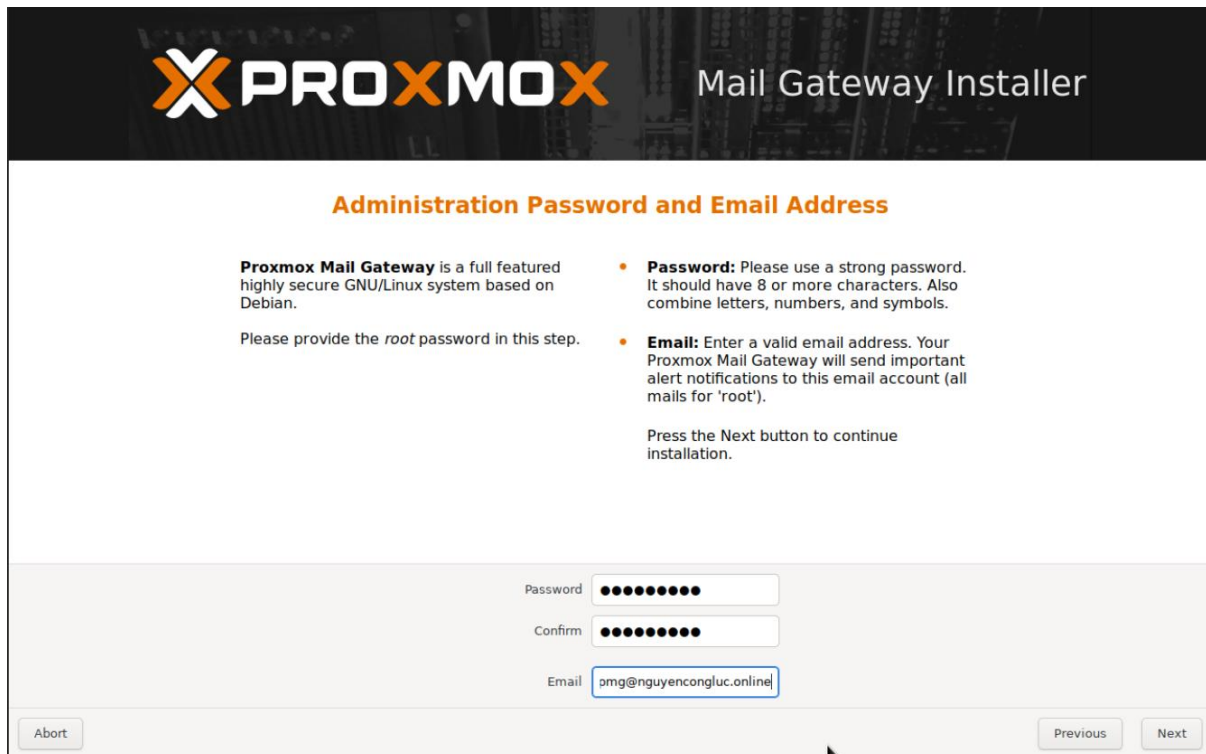
- **Country:** The selected country is used to choose nearby mirror servers. This will speed up downloads and make updates more reliable.
- **Time Zone:** Automatically adjust daylight saving time.
- **Keyboard Layout:** Choose your keyboard layout.

Country:

Time zone:

Keyboard Layout:

- Nhập password và email của server là: pmg@nguyencongluc.online



PROXMOX Mail Gateway Installer

Administration Password and Email 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.
- **Email:** 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:

Email:

- Management interface chọn card mạng đang có

- HostnameFQDN (Fully Qualified Domain Name) phải khớp với cấu hình DNS sau này.

: pmg.nguyencongluc.online

- IP Address (CIDR): 45.122.223.89/24

Gateway: 45.122.223.1

DNS Server: 8.8.8.8(Sử dụng Google DNS (8.8.8.8) làm máy chủ DNS để phân giải tên miền.

Nếu mạng có DNS nội bộ, bạn có thể thay bằng địa chỉ đó.)

PROXMOX Mail Gateway Installer

Management Network Configuration

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

After you have finished, press the Next button. You will be shown a list of the options that you chose during the previous steps.

- IP address (CIDR):** Set the main IP address and netmask for your server in CIDR notation.
- Gateway:** IP address of your gateway or firewall.
- DNS Server:** IP address of your DNS server.

Management Interface: ens18 - bc:24:11:55:9c:25 (virtio_net)

Hostname (FQDN): pmg.nguyencongluc.online

IP Address (CIDR): 45.122.223.89 / 24

Gateway: 45.122.223.1

DNS Server: 8.8.8.8

Abort Previous Next

- Kết quả:

PROXMOX Mail Gateway Installer

Summary

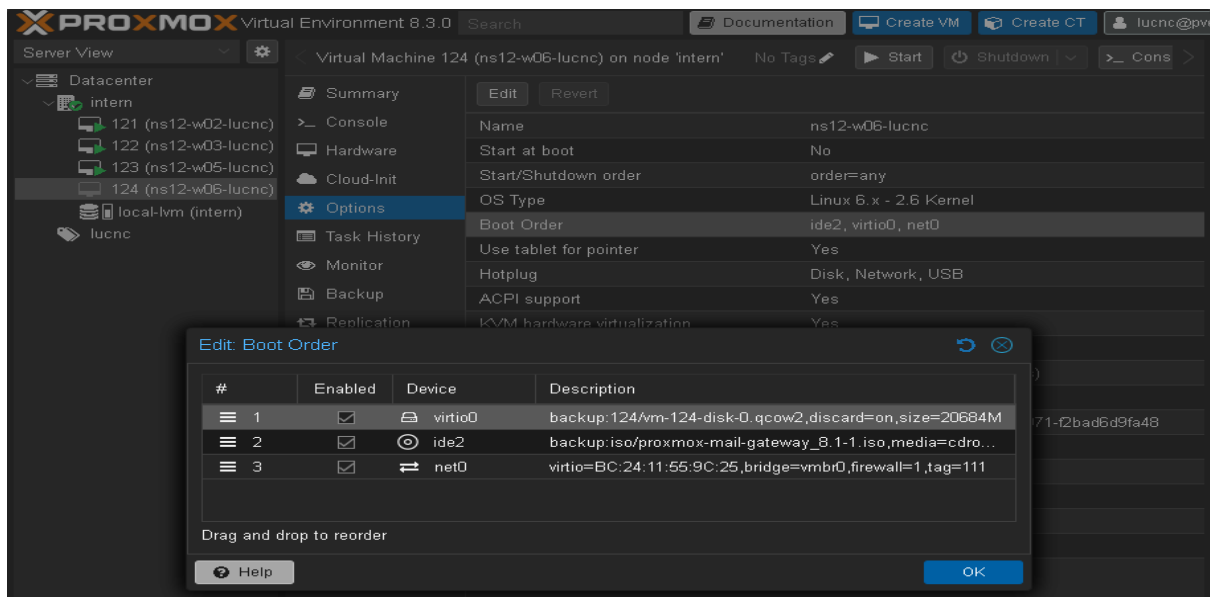
Please confirm the displayed information. Once you press the **Install** button, the installer will begin to partition your drive(s) and extract the required files.

Option	Value
Filesystem:	ext4
Disk(s):	/dev/vda
Country:	Vietnam
Timezone:	Asia/Ho_Chi_Minh
Keymap:	en-us
Email:	pmg@nguyencongluc.online
Management Interface:	ens18
Hostname:	pmg
IP CIDR:	45.122.223.89/24
Gateway:	45.122.223.1
DNS:	8.8.8.8

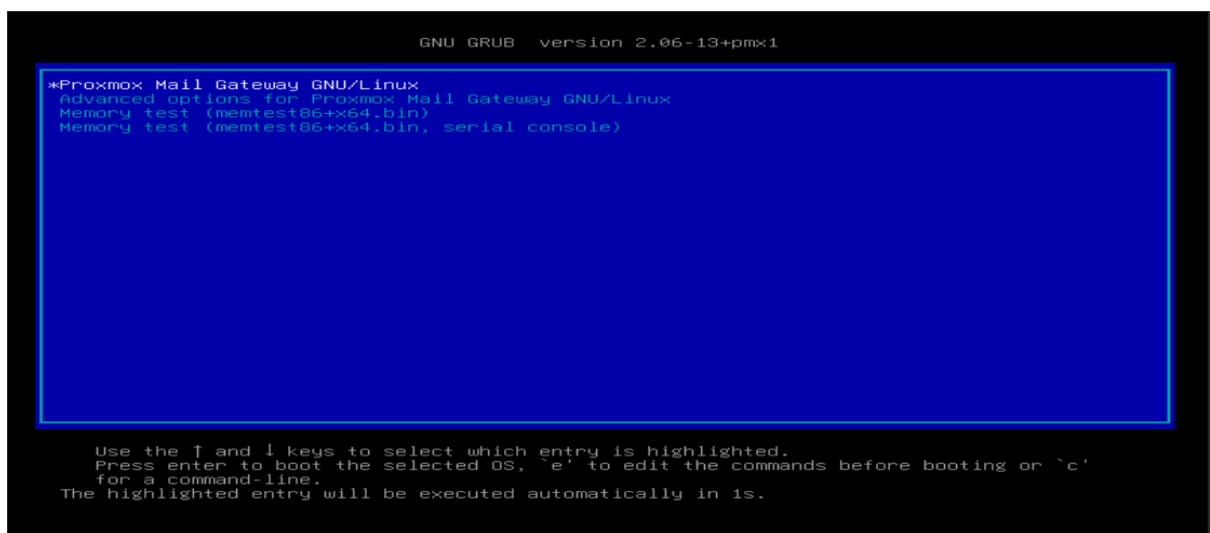
☒ Automatically reboot after successful installation

Abort Previous Install

- PMG sẽ cài đặt khoảng 5', sau đó sẽ restart lại. Lúc này cần stop Promox để cấu hình lại thứ tự boot trong Boot Order, cho disk - virtio0 lên trước ISO



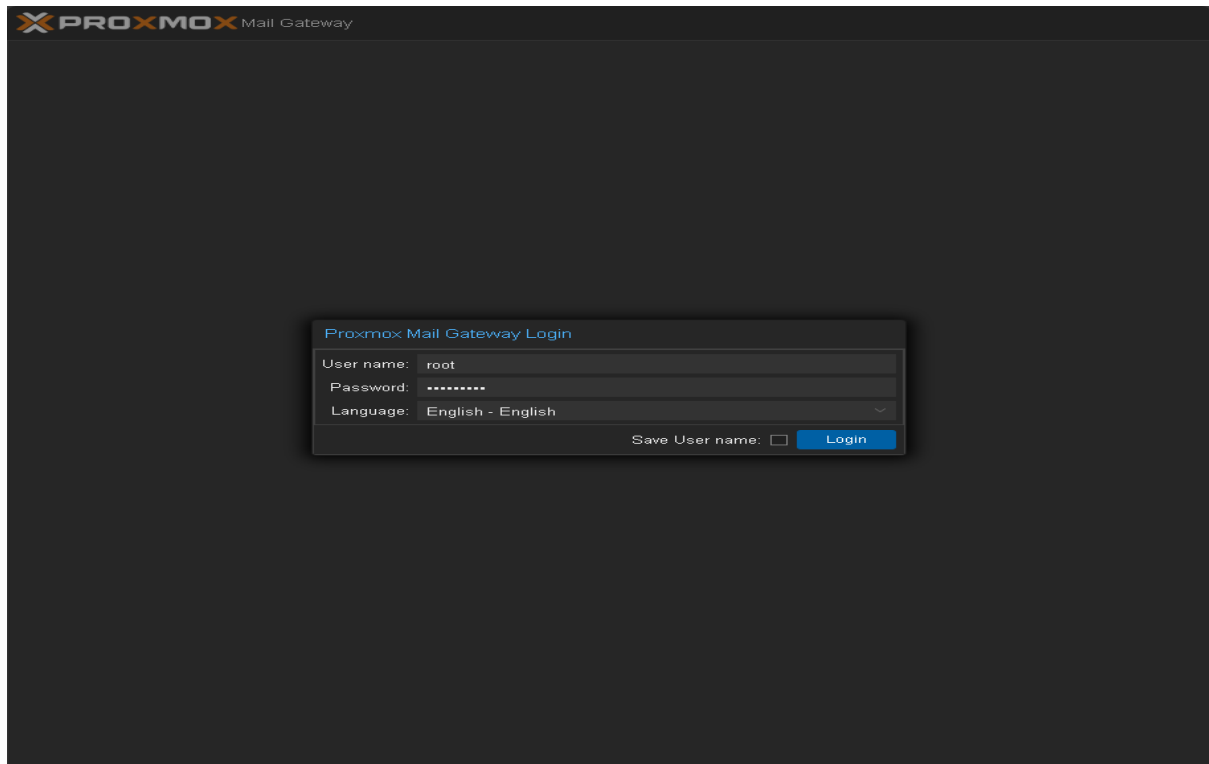
- Màn hình khi khởi động



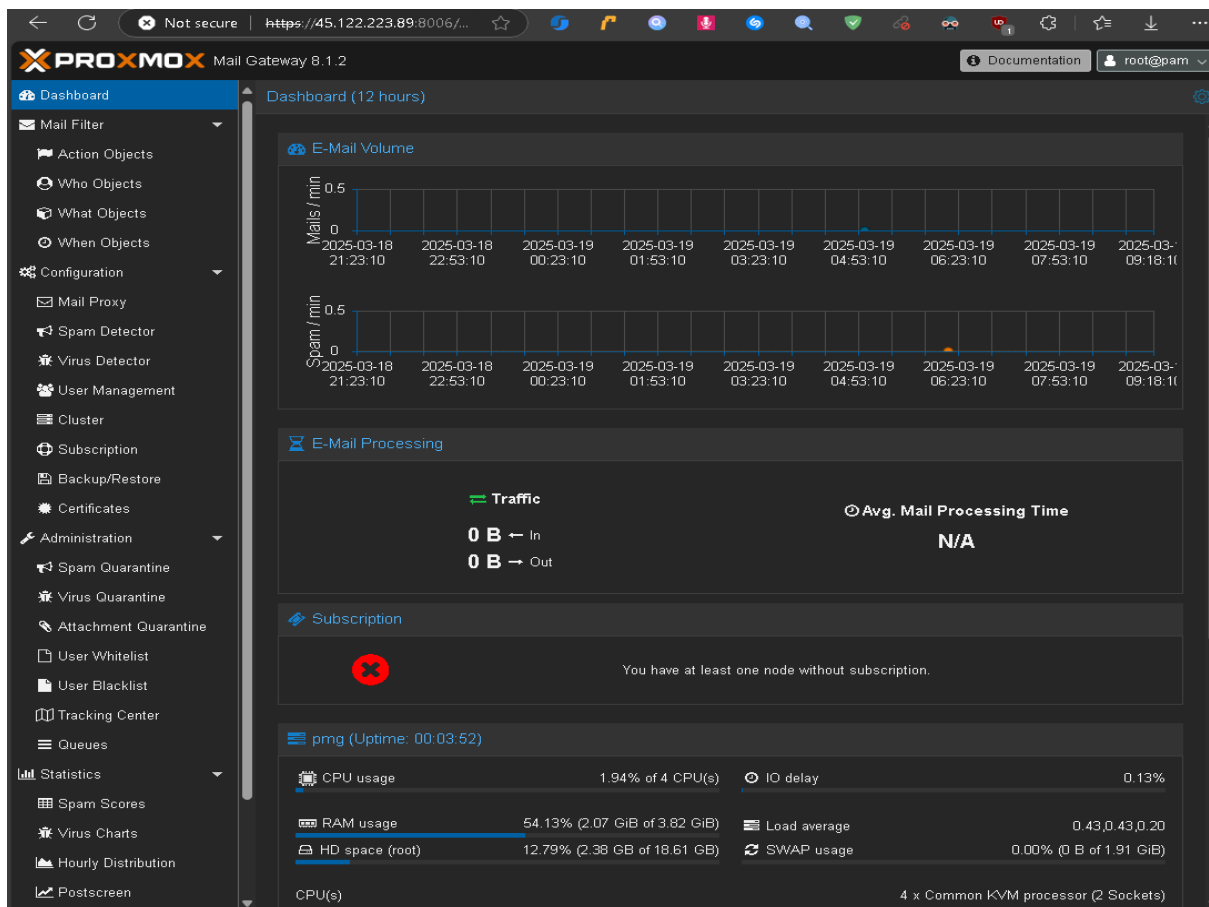
- Giao diện sau khi login thành công: Username: root, password: pass điền lúc setup



- Trên trình duyệt truy cập link để vào khu vực quản trị PMG: <https://45.122.223.89:8006/> với tài khoản trên



- Giao diện chính:



1.3 Thêm SSL cho website PMG

- Yêu cầu cần có SSL để có thể mã hóa các gói tin đi qua website.

1.3.1 Cấu hình DNS cho website PMG

- Thêm 2 DNS Record cho PMG ở nhà cung cấp Domain
- Bản ghi A: Để truy cập domain dưới sẽ chạy đến IP server của PMG

Name: pmg. nguyencongluc.com

Type: A

Value: 45.122.223.89

pmg	A	45.122.223.89	0
-----	---	---------------	---

1.3.2 Khắc phục lỗi kho lưu trữ Proxmox

- Khi chạy lệnh update hoặc tải về thêm file thì sẽ bị lỗi hệ thống không thể truy cập vào kho lưu trữ của Proxmox vì VM đang sử dụng phiên bản Proxmox Mail Gateway yêu cầu giấy phép trả phí, trong khi máy chưa kích hoạt subscription.

```
root@pmg:~# apt update
Hit:1 http://ftp.debian.org/debian bookworm InRelease
Hit:2 http://security.debian.org bookworm-security InRelease
Hit:3 http://ftp.debian.org/debian bookworm-updates InRelease
Err:4 https://enterprise.proxmox.com/debian/pmg bookworm InRelease
 401 Unauthorized [IP: 117.120.5.24 443]
Reading package lists... Done
E: Failed to fetch https://enterprise.proxmox.com/debian/pmg/dists/bookworm/InRelease 401 Unauthorized [IP: 117.120.5.24 443]
E: The repository 'https://enterprise.proxmox.com/debian/pmg bookworm InRelease' is not signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
```

- Cách khắc phục: Nếu không có subscription hoặc chỉ dùng phiên bản miễn phí, cần chuyển sang kho lưu trữ cộng đồng (community repository) hoặc tắt kho enterprise:

+ Cách 1: Vô hiệu hóa repository enterprise:(Nên dùng trước)

Mở file cấu hình PMG: nano /etc/apt/sources.list.d/pmg-enterprise.list

```
root@pmg:~# nano /etc/apt/sources.list.d/pmg-enterprise.list
```

Thêm dấu # để comment dòng: #deb https://enterprise.proxmox.com/debian/pmg bookworm InRelease

```
GNU nano 7.2 /etc/apt/sources.list.d/pmg-enterprise.list *
#deb https://enterprise.proxmox.com/debian/pmg bookworm pmg-enterprise
```

+ Cách 2(Chỉ dùng khi cách 1 không xử lý được): Kiểm tra file cấu hình nguồn APT, mở file: nano /etc/apt/sources.list

```
root@pmg:~# nano /etc/apt/sources.list
```

Và thêm dòng sau để dùng repository cộng đồng:

deb http://download.proxmox.com/debian/pmg bookworm pmg-no-subscription

```
GNU nano 7.2 /etc/apt/sources.list *
deb http://ftp.debian.org/debian bookworm main contrib
deb http://ftp.debian.org/debian bookworm-updates main contrib
# security updates
deb http://security.debian.org bookworm-security main contrib
deb http://download.proxmox.com/debian/pmg bookworm pmg-no-subscription
```

1.3.3 Cấu hình DNS Record

- Thêm Record bảng A trở domain pmg.nguyencongluc.online về IP 45.122.223.89

Tên	Loại	Giá trị	Độ ưu tiên	Thao tác
pmg.nguyencongluc.online	A	45.122.223.89		Lưu Hủy

1.3.4 Cài đặt Certbot và chứng chỉ SSL từ Let's Encrypt

- Lệnh cài đặt Cài đặt Certbot:

apt update && apt install -y certbot

```
root@pmg:~# apt update && apt install -y certbot
Hit:1 http://security.debian.org bookworm-security InRelease
Hit:2 http://ftp.debian.org/debian bookworm InRelease
Hit:3 http://ftp.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
```

- Sử dụng Certbot để tải về và cài đặt chứng chỉ SSL từ Let's Encrypt:

certbot certonly --standalone -d pmg.nguyencongluc.online

```
root@pmg:~# certbot certonly --standalone -d pmg.nguyencongluc.online
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Requesting a certificate for pmg.nguyencongluc.online

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/pmg.nguyencongluc.online/fullchain.pem
Key is saved at: /etc/letsencrypt/live/pmg.nguyencongluc.online/privkey.pem
This certificate expires on 2025-06-19.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

-----
If you like Certbot, please consider supporting our work by:
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
* Donating to EFF: https://eff.org/donate-le
```

- Kiểm tra chứng chỉ:

ls /etc/letsencrypt/live/pmg.nguyencongluc.online

```
root@pmg:~# ls /etc/letsencrypt/live/pmg.nguyencongluc.online
cert.pem chain.pem fullchain.pem privkey.pem README
```

1.3.5 Áp dụng chứng chỉ SSL vào website PMG

- PMG sử dụng file /etc/pmg/pmg-api.pem để lưu trữ SSL cho giao diện web. Và Proxmox yêu cầu file PEM có thứ tự:

1. Private Key
2. Certificate
3. CA Bundle (nếu có)

- Dùng lệnh để kết hợp chứng chỉ gộp lại từ các file gốc của Certbot, đảm bảo thứ tự:

```
cat /etc/letsencrypt/live/pmg.nguyencongluc.online/privkey.pem \
```

```
/etc/letsencrypt/live/pmg.nguyencongluc.online/cert.pem \
```

```
/etc/letsencrypt/live/pmg.nguyencongluc.online/chain.pem > /etc/pmg/pmg-api.pem
```

```
root@pmg:~# cat /etc/letsencrypt/live/pmg.nguyencongluc.online/privkey.pem /etc/letsencrypt/live/pmg.nguyencongluc.online/cert.pem /etc/letsencrypt/live/pmg.nguyencongluc.online/chain.pem > /etc/pmg/pmg-api.pem
```

- Set quyền tối thiểu cho file như sau: `chmod 644 /etc/pmg/pmg-api.pem`

Và kiểm tra: `ls -l /etc/pmg/pmg-api.pem`

```
root@pmg:~# chmod 644 /etc/pmg/pmg-api.pem
root@pmg:~# ls -l /etc/pmg/pmg-api.pem
-rw-r--r-- 1 root root 3166 Mar 21 13:16 /etc/pmg/pmg-api.pem
```

- Khởi động lại dịch vụ pmgproxy: `root@pmg:~# systemctl restart pmgproxy`

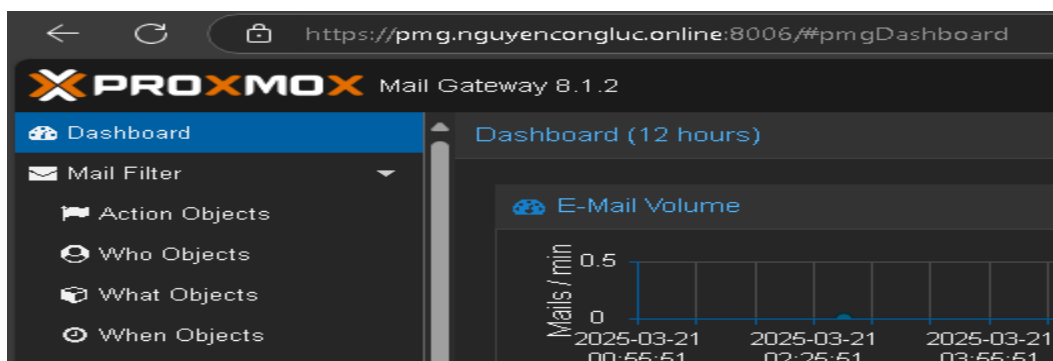
```
root@pmg:~# systemctl restart pmgproxy
```

- Check trạng thái dịch vụ: `root@pmg:~# systemctl status pmgproxy`

```
root@pmg:~# systemctl status pmgproxy
● pmgproxy.service - Proxmox Mail Gateway's unprivileged API and API-proxy daemon
   Loaded: loaded (/lib/systemd/system/pmgproxy.service; enabled; preset: enabled)
   Active: active (running) since Fri 2025-03-21 13:16:44 +07; 2min 50s ago
     Process: 18757 ExecStart=/usr/bin/pmgproxy start (code=exited, status=0/SUCCESS)
    Main PID: 18761 (pmgproxy)
       Tasks: 4 (limit: 4611)
      Memory: 122.0M
         CPU: 2.748s
    CGroup: /system.slice/pmgproxy.service
            └─18761 pmgproxy
              └─18762 "pmgproxy worker"
                └─18763 "pmgproxy worker"
                  └─18764 "pmgproxy worker"

Mar 21 13:16:41 pmg systemd[1]: Starting pmgproxy.service - Proxmox Mail Gateway's unprivileged API and API-proxy daemon..
Mar 21 13:16:44 pmg pmgproxy[18761]: starting server
Mar 21 13:16:44 pmg pmgproxy[18761]: starting 3 worker(s)
Mar 21 13:16:44 pmg pmgproxy[18761]: worker 18762 started
Mar 21 13:16:44 pmg pmgproxy[18761]: worker 18763 started
Mar 21 13:16:44 pmg pmgproxy[18761]: worker 18764 started
Mar 21 13:16:44 pmg systemd[1]: Started pmgproxy.service - Proxmox Mail Gateway's unprivileged API and API-proxy daemon..
```

- Kết quả:



Phần 2. Cấu hình PMG làm Email Relay cho Zimbra

- PMG sẽ hoạt động như một gateway trung gian, xử lý email gửi/nhận trước khi chuyển đến Zimbra (45.122.223.81).

2.1 Cấu hình Relay PMG trong Mail Proxy:

2.1.1 Cấu hình Relaying:

- Truy cập giao diện web PMG: <https://pmg.nguyencongluc.online> hoặc <https://45.122.223.89:8006>.

- Vào Configuration > Mail Proxy > Relaying:

Default Relay: Nhập 45.122.223.81 (IP của Zimbra) hoặc none nếu phần Transports đã cấu hình

Use MX Records: Chọn "No" (vì dùng IP tĩnh của Zimbra).

Lưu cấu hình.

+ Default Relay: Nhập 45.122.223.81 (IP của Zimbra) hoặc none nếu phần Transports đã cấu hình

Quy định địa chỉ IP hoặc tên miền của máy chủ email mà PMG sẽ chuyển tiếp tất cả email đến theo mặc định, trừ khi có quy tắc cụ thể trong Transports.

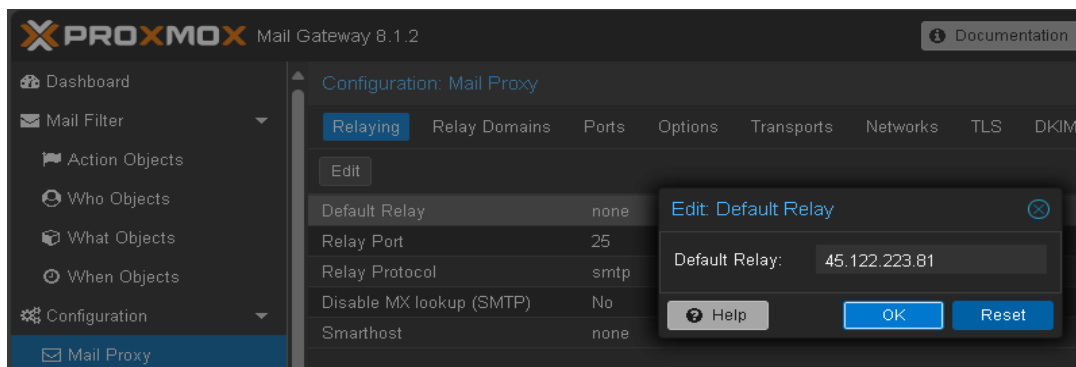
+ Relay Port: 25 (SMTP mặc định).

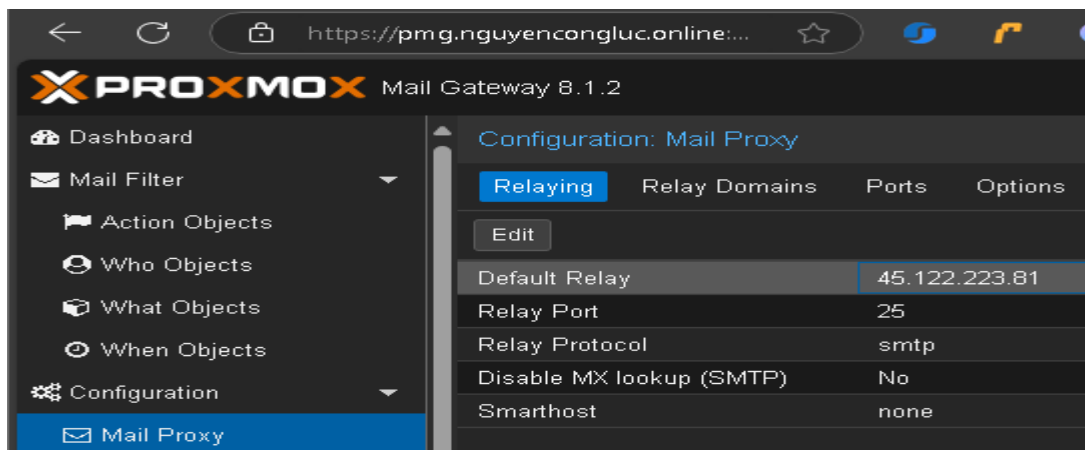
+ Relay Protocol: SMTP (Hoặc STARTTLS nếu Zimbra bật TLS)

Giao thức mà PMG dùng để giao tiếp với máy chủ đích.

+ Smarthost: None.

Một máy chủ trung gian (thường là dịch vụ bên thứ ba) mà PMG gửi tất cả email đi qua thay vì gửi trực tiếp đến đích.

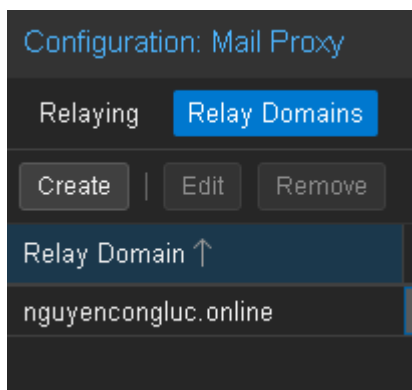




2.1.2 Cấu hình Relay Domains:

Relay Domain: nguyencongluc.online

PMG sẽ chấp nhận tất cả email gửi đến các địa chỉ như user@nguyencongluc.online và chuyển chúng đến đích - máy chủ nội bộ (như Zimbra)



2.1.3 Cấu hình Port:

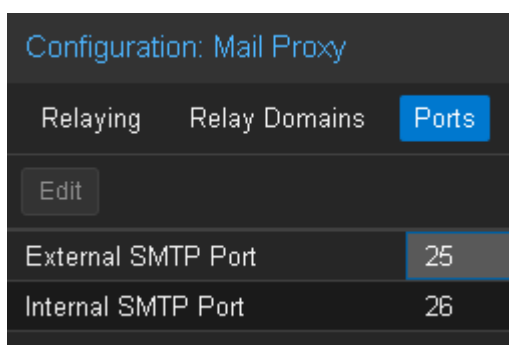
- Để theo mặc định

- External SMTP Port: 25.

Cổng mà PMG lắng nghe để nhận email từ Internet

- Internal SMTP Port: 26.

Cổng mà PMG lắng nghe để nhận email từ các máy chủ nội bộ (như Zimbra) để gửi ra ngoài qua PMG.



2.1.4 Cấu hình Options:

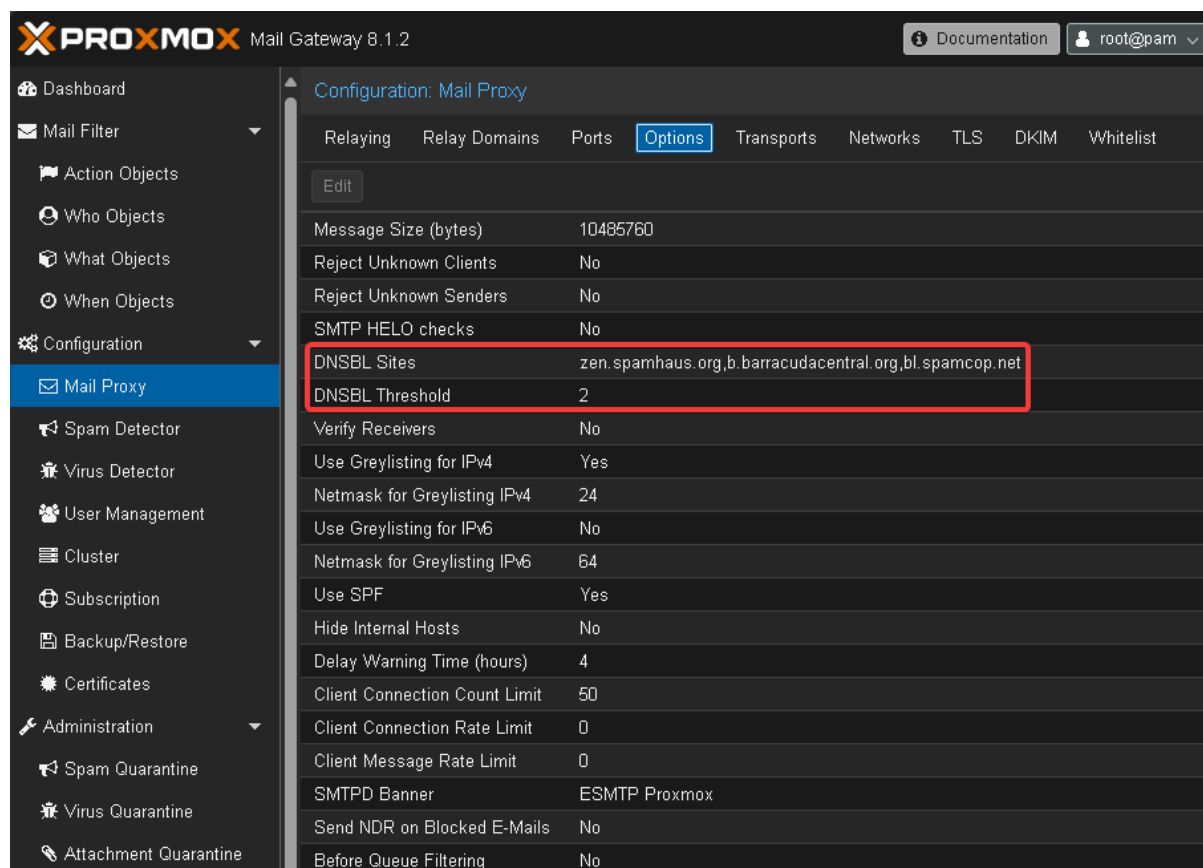
- Đây là các tùy chọn nâng cao giúp kiểm soát hành vi lọc, bảo mật và hiệu suất. Nên để theo mặc định, **tuy nhiên trong lab có cài đặt thêm phần DNSBL (DNS Blacklist) để tăng bảo mật.**

- DNSBL Sites: zen.spamhaus.org,b.barracudacentral.org,bl.spamcop.net

Chặn email từ các địa chỉ IP được liệt kê trong danh sách đen spam nổi tiếng.

- DNSBL Threshold:2

Quy định ngưỡng DNSBL, ở đây là nếu IP gửi email bị liệt kê trong 2 danh sách đen thì email sẽ bị chặn.



The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar contains a navigation menu with 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, and Attachment Quarantine. The main panel is titled 'Configuration: Mail Proxy' and has several tabs: Relaying, Relay Domains, Ports, Options (selected), Transports, Networks, TLS, DKIM, and Whitelist. The 'Options' tab displays a list of configuration items. Two items, 'DNSBL Sites' and 'DNSBL Threshold', are highlighted with a red rectangular box. The 'DNSBL Sites' value is 'zen.spamhaus.org,b.barracudacentral.org,bl.spamcop.net' and the 'DNSBL Threshold' value is '2'.

Configuration Item	Value
Message Size (bytes)	10485760
Reject Unknown Clients	No
Reject Unknown Senders	No
SMTP HELO checks	No
DNSBL Sites	zen.spamhaus.org,b.barracudacentral.org,bl.spamcop.net
DNSBL Threshold	2
Verify Receivers	No
Use Greylisting for IPv4	Yes
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

2.1.5 Cấu hình Transports:

- Xác định nơi PMG gửi email đến cho từng domain cụ thể, thay vì dùng đích mặc định trong Default Relay.

- Vào Configuration > Mail Proxy > Transports:

Thêm mới transport:

+Domain: nguyencongluc.online Chỉ định domain muốn PMG xử lý

+Host: 45.122.223.81. Địa chỉ IP hoặc hostname của máy chủ đích mà email sẽ được gửi đến

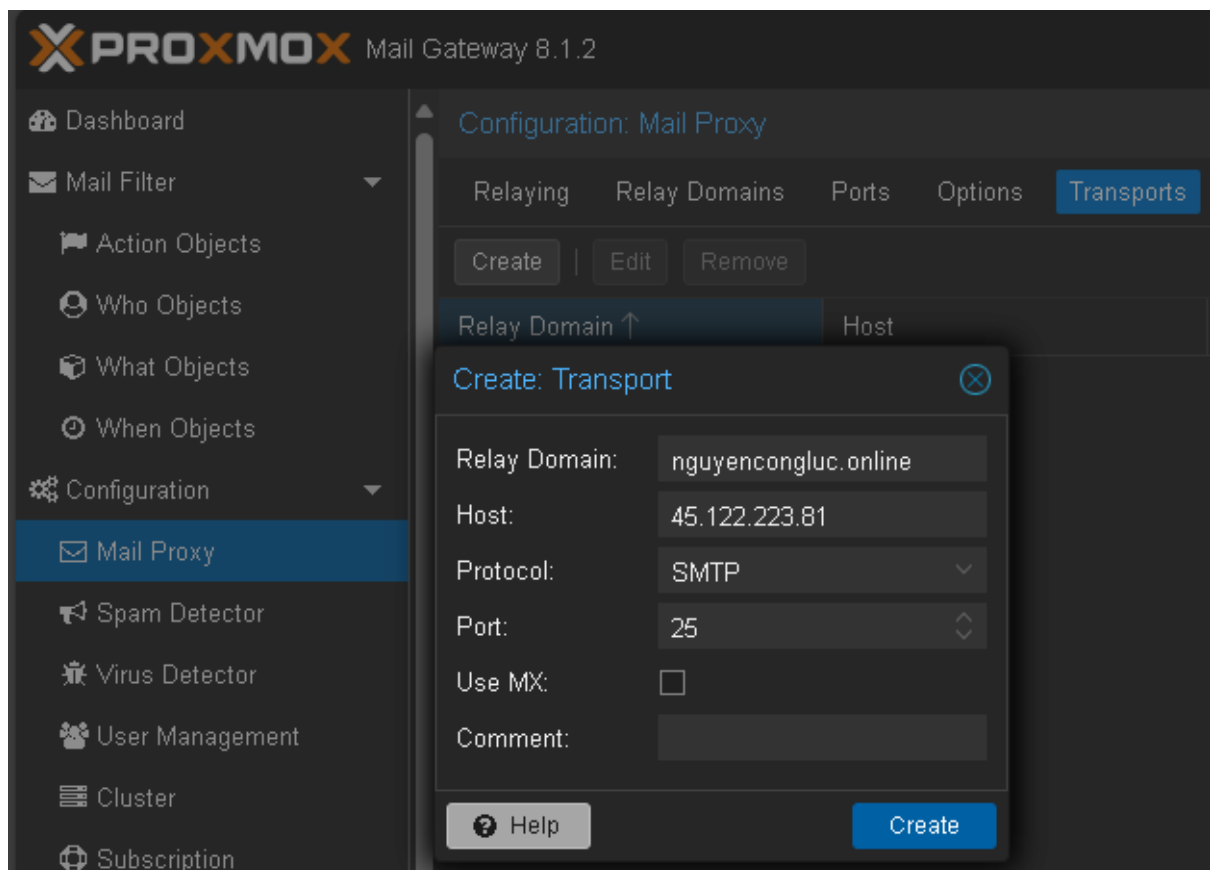
+Protocol: SMTP

+Port: 25. (SMTP mặc định).

+Use MX(Sử dụng MX Lookup): Chọn "No"

Quyết định liệu PMG có tra cứu bản ghi MX của domain để tìm đích gửi email hay không. Tắt nếu muốn gửi trực tiếp đến **Host** đã khai báo (như Zimbra), bật nếu muốn dựa vào DNS MX.

Lưu cấu hình.



Configuration: Mail Proxy						
Relaying	Relay Domains	Ports	Options	Transports	Networks	TLS DKIM Whitelist
Create	Edit	Remove	Filter:			
Relay Domain ↑	Host	Protocol	Port	Use MX	Com...	
nguyencongluc.online	45.122.223.81	smtp	25	No		

2.1.6 Cấu hình Networks:

- Networks: Xác định các mạng/IP mà PMG cho phép gửi email qua mà không áp dụng các kiểm tra bảo mật nghiêm ngặt như SPF, DNSBL, Greylisting hay kiểm tra spam).

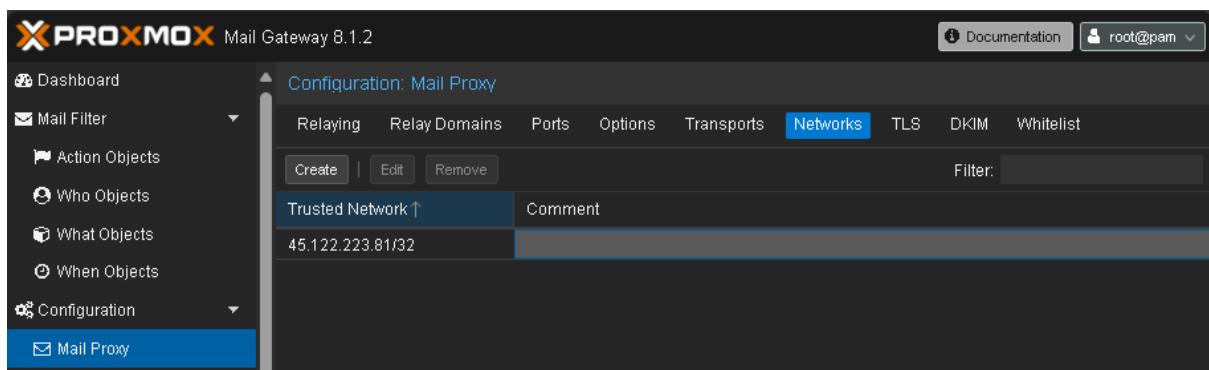
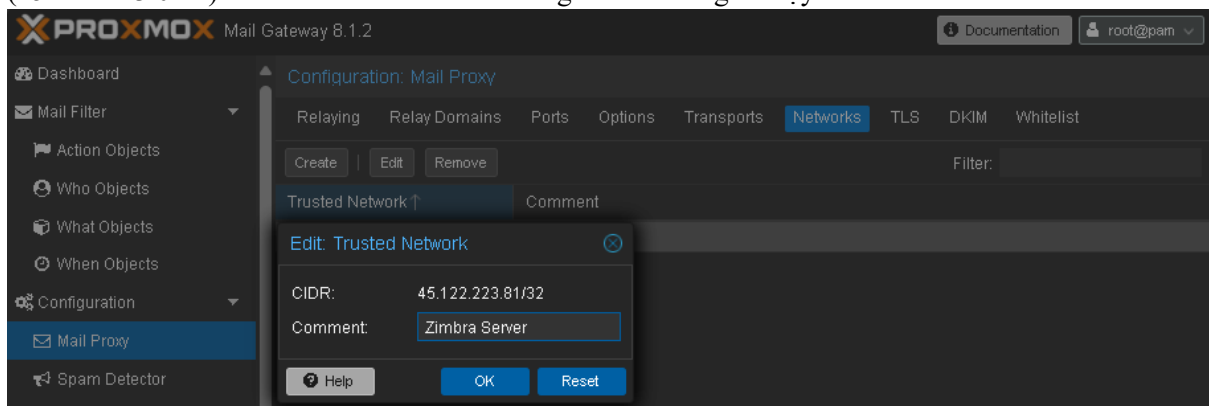
- Vào Configuration > Mail Proxy > Networks:

+ Network: 45.122.223.81/32. Nên dùng dãy mạng đơn trên vì:

Vì /32: Chỉ định một địa chỉ IP duy nhất (ví dụ: 45.122.223.81/32 là chỉ IP 45.122.223.81 của Zimbra).

Còn /24: Chỉ định một dải mạng gồm 256 IP (ví dụ: 45.122.223.0/24 là từ 45.122.223.0 đến 45.122.223.255, tức là bao gồm các IP khác, điều này là không nên vì sẽ trùng các IP không tin cậy đang hoạt động).

Tương lai: Nếu mở rộng mạng với nhiều máy chủ trong dải 45.122.223.x, thì mới chuyển sang /24 (45.122.223.0/24) và đảm bảo các IP khác trong dải đều đáng tin cậy.



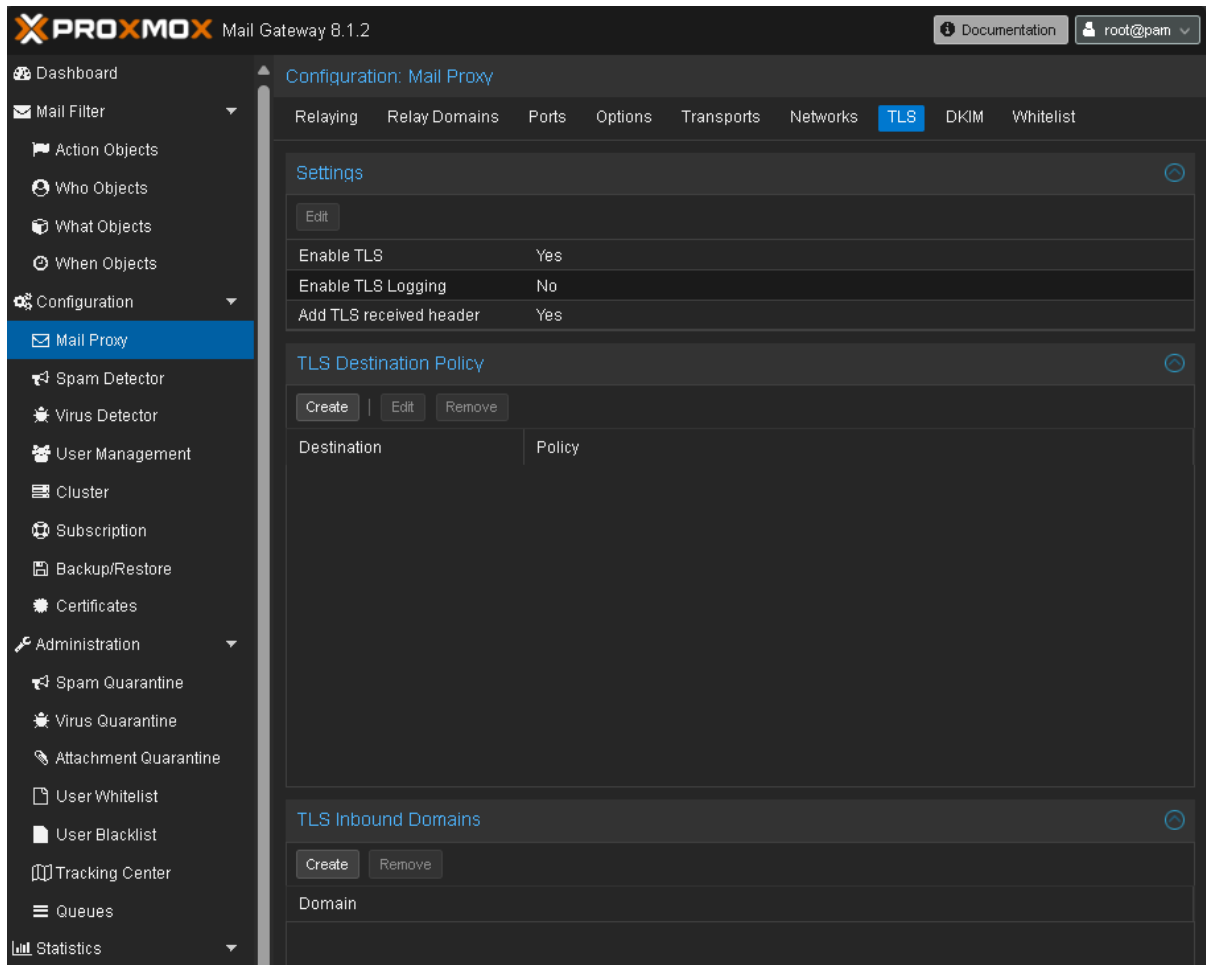
2.1.7 Cấu hình TLS:

- TLS trong Mail Proxy liên quan đến việc kích hoạt và cấu hình mã hóa Transport Layer Security để bảo mật email khi gửi/nhận

+ Enable TLS: Yes

+ Enable TLS Logging: No (Bật log khi cần kiểm tra hoặc gỡ lỗi TLS)

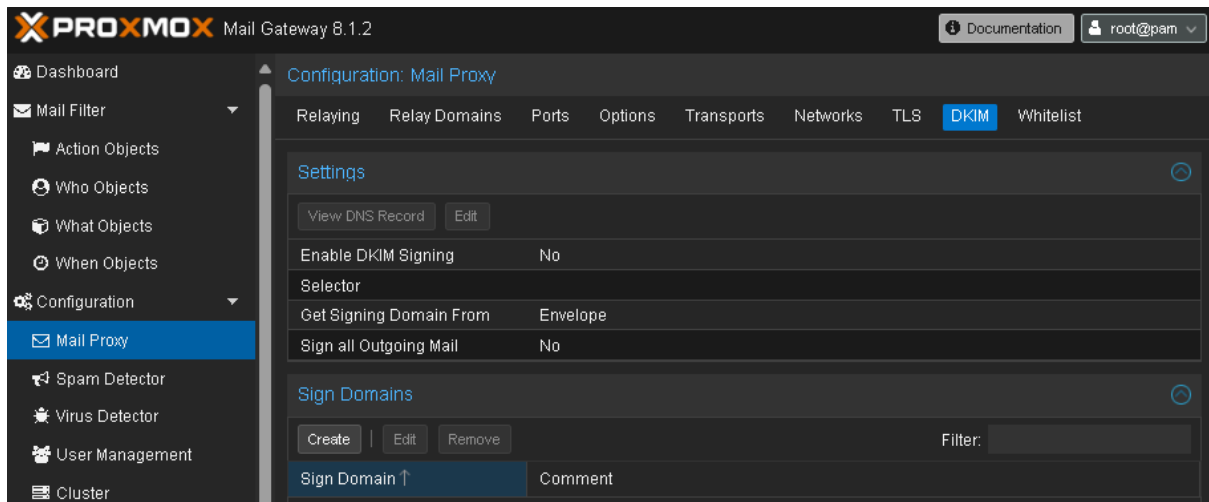
+ Add TLS Received Header: Yes (Thêm header Received: with TLS vào email để ghi lại thông tin mã hóa)



2.1.8 Cấu hình DKIM:

- Là tính năng ký email bằng DomainKeys Identified Mail (DKIM) để xác thực nguồn gốc và tăng độ tin cậy của email. Để chứng minh email thực sự gửi từ domain nguyencongluc.online, giúp tránh bị đánh dấu spam.

- Vì Zimbra đã cấu hình DKIM nên cần bỏ qua việc cấu hình DKIM trên PMG để tránh xung đột, trừ khi muốn chuyển hoàn toàn DKIM sang PMG thì mới tắt DKIM bên Zimbra và bật DKIM trên PMG. Trong email chỉ cần 1 chữ ký số khớp với DNS.



- Xem lại cấu hình trên Zimbra

su - zimbra

zmprov gd nguyencongluc.online | grep -i dkim

```
zimbra@mail:~$ zmprov gd nguyencongluc.online | grep -i dkim
DKIMDomain: nguyencongluc.online
DKIMIdentity: nguyencongluc.online
DKIMKey: -----BEGIN PRIVATE KEY-----
DKIMPublicKey: F11486EA-FF24-11EF-871B-2FB0A8767035._domainkey IN      TXT      ( "v=DKIM1; k=rsa; "
"OJors47LgC/2HMycCsMGp/zu8SLx4XwaMqkfFVvLLA0seCLBQrEofV8K8NSN+VHE04w9Ap/pKrGtEFpa/JVbiPhh3gr0W7JDjfxDg8ZqmjbKV
jP7a8oapJqEi2Hr0W30A+oFDKDQIDAQAB" ) ; ----- DKIM key F11486EA-FF24-11EF-871B-2FB0A8767035 for nguyencongluc.online
DKIMSelector: F11486EA-FF24-11EF-871B-2FB0A8767035
objectClass: DKIM
```

- Kiểm tra DNS:

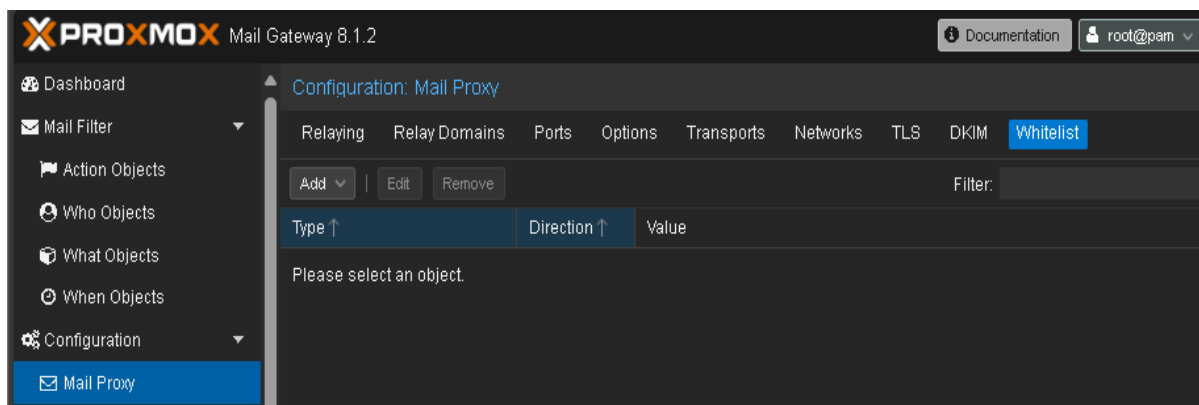
<input type="checkbox"/> F11486EA-FF24-11EF-871B-2FB0A8767035._domainkey	TXT	<pre>v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEA004TniJwQ21 1QPvX9qzLsdTE/09LXfibSUCqcVoqFWijJruu/U 2HVKG2shzS/1VcrEahVGe7Jj606c6WdmoXk ZsGWifa66Dke+98y2keFDv1Arm0bfcvLOXyA UlvZ7ydTvIW4Y9GIMWQW90mz86daXc5+Z 0j3cSKltM8167rJKbkgib/20Mmo5Y7xe5FFKA 3fviYKts9fw7NhTOJors47LgC/2HMycCsMG p/zu8SLx4XwaMqkfFVvLLA0seCLBQrEofV8K 8NSN+VHE04w9Ap/pKrGtEFpa/JVbiPhh3gr0 W7JDjfxDg8ZqmjbKVjP7a8oapJqEi2Hr0W30 A+oFDKDQIDAQAB</pre>	0	Sửa
--	-----	---	---	-----

Chạy lệnh kiểm tra: dig TXT F11486EA-FF24-11EF-871B-2FB0A8767035._domainkey.nguyencongluc.online +short

```
zimbra@mail:~$ dig TXT F11486EA-FF24-11EF-871B-2FB0A8767035._domainkey.nguyencongluc.online +short
"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEA004TniJwQ211QPvX9qzLsdTE/09LXfibSUCqcVoqFWijJruu/U2HVKG2shzS/1VcrEahVGe7Jj606c6WdmoXkZsGWifa66Dke+98y2keFDv1Arm0bfcvLOXyAULvZ7ydTvIW4Y9GIMWQW90mz86daXc5+Z0j3cSKltM8167rJKbkgib/20Mmo5Y7xe5FFKA3f" "viYKts9fw7NhTOJors47LgC/2HMycCsMGp/zu8SLx4XwaMqkfFVvLLA0seCLBQrEofV8K8NSN+VHE04w9Ap/pKrGtEFpa/JVbiPhh3gr0W7JDjfxDg8ZqmjbKVjP7a8oapJqEi2Hr0W30A+oFDKDQIDAQAB"
```

2.1.9 Cấu hình Whitelist:

- Whitelist trong Mail Proxy cho phép bạn định nghĩa các địa chỉ email, domain, hoặc IP được miễn kiểm tra lọc (như spam, virus, SPF, DNSBL)
- Để mặc định không cần thêm gì, vì lab này muốn PMG sẽ áp dụng đầy đủ các quy tắc lọc (SPF, DNSBL, spam, virus) cho email từ Zimbra để đảm bảo không có spam/virus (dù hiếm, nhưng có thể xảy ra nếu Zimbra bị xâm nhập).



2.2 Cấu hình Zimbra để gửi qua PMG:

*Cách 1: Trên giao diện

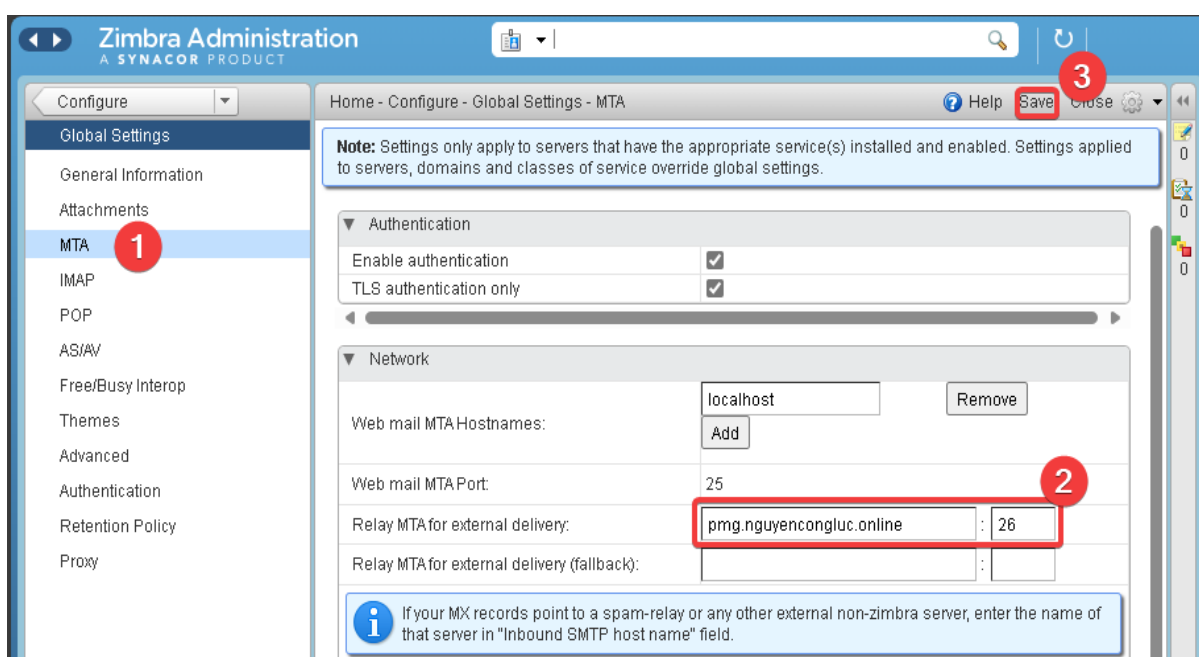
- Truy cập Zimbra Admin Console: <https://mail.nguyencongluc.online:7071> hoặc <https://45.122.223.81:7071>.

- Đăng nhập bằng tài khoản admin

- Vào Configure > Global Settings > MTA:

+Relay MTA for external delivery: Nhập pmg.nguyencongluc.online hoặc 45.122.223.89 (IP của PMG).

+Port: 26 (Để trùng với Internal SrvITP Port của PMG vì đây là port giao tiếp giữa 2 service)



*Cách 2: Trên console:

- Sử dụng lệnh zmprov để thiết lập Relay MTA for external delivery:

```
zmprov modifyServer mail.nguyencongluc.online zimbraMtaRelayHost 45.122.223.89:25
```

- Lưu và khởi động lại dịch vụ MTA:

```
su - zimbra -c "zmmctl restart"
```

```
root@mail:~# su - zimbra -c "zmmctl restart"
Rewriting configuration files...done.
Stopping amavisd... done.
Stopping amavisd-mc... done.
Starting amavisd-mc...done.
Starting amavisd...done.
Stopping saslauthd...done.
Starting saslauthd...done.
/postfix-script: refreshing the Postfix mail system
```


Phần 3. Cấu hình đảm bảo Mail Exchange, SPF, DKIM, DMARC valid

- Vì email giờ được gửi qua PMG, cần cập nhật các bản ghi DNS để xác thực email từ IP của PMG (45.122.223.89).

3.1 Cấu hình MX

- Thêm Bản ghi MX: Để chỉ định “Email server” xử lý cho domain chính

Name: `nguyencongluc.online` Type: MX **Ưu tiên: 10** Value: `pmg.nguyencongluc.com`

Tên	Loại	Giá trị	Độ ưu tiên	Thao tác
<code>nguyencongluc.online</code>	MX	<code>pmg.example.com</code>	10	Lưu Hủy

- Đảm bảo DNS ưu tiên xử lý cho pmg trước thay vì zimbra bằng cách chỉnh Độ ưu tiên PMG cao hơn là 0 để được xếp trước, còn Zimbra là 10. Bản ghi MX của Zimbra vẫn cần để lại để pmg xác thực server zimbra

MX 0 `pmg.nguyencongluc.online` (45.122.223.89)

MX 10 `mail.nguyencongluc.online` (45.122.223.81)

@	MX	<code>mail.nguyencongluc.online</code>	10	Sửa
@	MX	<code>pmg.nguyencongluc.online</code>	0	Sửa

3.2 Cấu hình SPF

- Chỉnh sửa bản ghi TXT trong DNS:

Name: `nguyencongluc.online`

Type: TXT

Value: `v=spf1 ip4:45.122.223.89 ip4:45.122.223.81 ~all`

@	TXT	<code>v=spf1 ip4:45.122.223.89 ip4:45.122.223.81 ~all</code>	0	Sửa
---	-----	--	---	---------------------

- Kiểm tra;

`dig TXT nguyencongluc.online`

```
root@pmg:~# dig TXT nguyencongluc.online

; <<>> DiG 9.18.24-1-Debian <<>> TXT nguyencongluc.online
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48963
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;nguyencongluc.online.      IN      TXT

;; ANSWER SECTION:
nguyencongluc.online.  600     IN      TXT      "v=spf1 ip4:45.122.223.89 ip4:45.122.223.81 ~all"

;; Query time: 88 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Mar 21 14:42:40 +07 2025
;; MSG SIZE rcvd: 109
```

3.2 Cấu hình DKIM

- DKIM đã được tạo trên Zimbra từ Week 5. PMG sẽ sử dụng cùng khóa này(Xem lại trong phần [2.1.8](#))

3.3 Cấu hình DMARC

- Bản ghi DMARC từ Week 5-Zimbra vẫn áp dụng vì rule DMARC 2 lab cần là giống nhau:

Name: _dmarc.example.com

Type: TXT

Value: v=DMARC1; p=quarantine; rua=mailto:admin@nguyencongluc.online;
ruf=mailto:admin@nguyencongluc.online;

- Kiểm tra: dig TXT _dmarc.nguyencongluc.online

```
root@pmg:~# dig TXT _dmarc.nguyencongluc.online

; <<>> DiG 9.18.24-1-Debian <<>> TXT _dmarc.nguyencongluc.online
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21351
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;_dmarc.nguyencongluc.online.  IN      TXT

;; ANSWER SECTION:
_dmarc.nguyencongluc.online. 600 IN      TXT      "v=DMARC1; p=quarantine; rua=mailto:admin@nguyenco
ngluc.online; ruf=mailto:admin@nguyencongluc.online; fo=1;"

;; Query time: 84 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Fri Mar 21 14:45:46 +07 2025
;; MSG SIZE rcvd: 176
```

3.4 Cấu hình PTR

- PTR sẽ dịch ngược IP ra domain làm tăng độ uy tín cho server, **nếu mail gửi đi có warning về việc thiếu PTR ở IP của Proxmox Mail Gateway thì cần cấu hình thêm PTR từ nhà cung cấp IP để trong IP 45.122.223.89 tới domain pmg.nguyencongluc.online**

- Sau khi cấu hình PTR, check với lệnh: nslookup 45.122.223.89

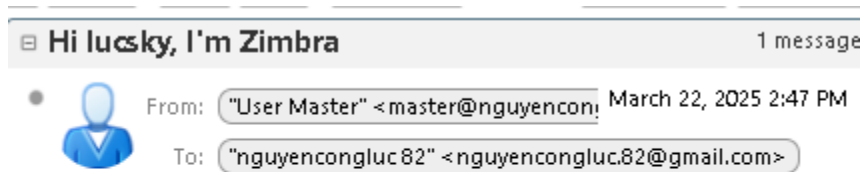
```
C:\Users\Nguyen Cong Luc>nslookup 45.122.223.89
Server:      UnKnown
Address:     fe80::1

Name:       pmg.nguyencongluc.online
Address:    45.122.223.89
```

3.5 Kiểm tra gửi email

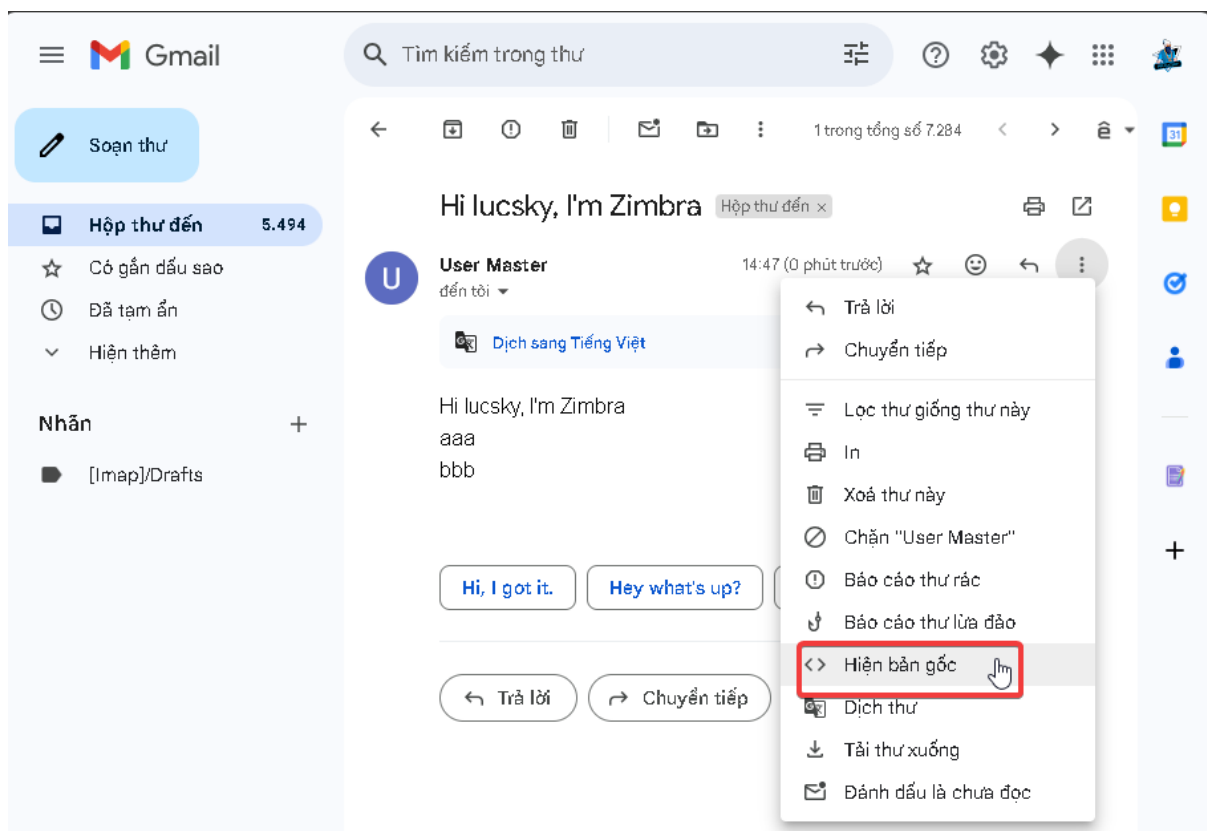
3.5.1 Gửi email từ Zimbra qua PMG tới Email Server khác.:

- Mail gửi đi trên Zimbra:



Hi lucsky, I'm Zimbra
aaa
bbb

- Mail qua PMG và đến Gmail:



- Kiểm tra nội dung thư gốc thấy thư đã đi qua PMG:

```
pmg 1/5 ^ v 🔍 ✕ ) smtp.mailfrom=master@nguyencongluc.online;
p=QUARANTINE dis=NONE)

Return-Path: <master@nguyencongluc.online>
Received: from pmg.nguyencongluc.online (pmg.nguyencongluc.online.
[45.122.223.89])
    by mx.google.com with ESMTPS id 41be03b00d2f7-
af8a2c313195i6514246a12.599.2025.03.22.00.47.53
    for <nguyencongluc.82@gmail.com>
    (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
    Sat, 22 Mar 2025 00:47:53 -0700 (PDT)
Received-SPF: pass (google.com: domain of master@nguyencongluc.online designates
45.122.223.89 as permitted sender) client-ip=45.122.223.89;
Authentication-Results: mx.google.com;
    dkim=pass header.i=@nguyencongluc.online header.s=F11486EA-FF24-11EF-871B-
2FB0A8767035 header.b=04eq2ko5;
    spf=pass (google.com: domain of master@nguyencongluc.online designates
45.122.223.89 as permitted sender) smtp.mailfrom=master@nguyencongluc.online;
    dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE)
header.from=nguyencongluc.online
Received: from pmg.nguyencongluc.online (localhost.localdomain [127.0.0.1]) by
pmg.nguyencongluc.online (Proxmox) with ESMTP id B19A140E66 for
<nguyencongluc.82@gmail.com>; Sat, 22 Mar 2025 14:47:51 +0700 (+07)
Received: from mail.nguyencongluc.online (mail.nguyencongluc.online
[45.122.223.81]) (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
    key-exchange X25519 server-signature RSA-PSS (4096 bits) server-digest
SHA256) (No client certificate requested) by pmg.nguyencongluc.online (Proxmox)
```

- Và các phương thức xác thực SPF, DKIM, DMARC đều đã hoạt động

ID thư	<361456115.32.1742629670180.JavaMail.zimbra@nguyencongluc.online>
Tạo lúc:	lúc 14:47 22 tháng 3, 2025 (Đã gửi sau 3 giây)
Từ:	User Master <master@nguyencongluc.online> Đang dùng Zimbra 8.8.15_GA_4717 (ZimbraWebClient - GC134 (Win)/8.8.15_GA_4717)
Đến:	nguyencongluc.82@gmail.com
Tiêu đề:	Hi lucsky, I'm Zimbra
SPF:	PASS với IP 45.122.223.89 Hãy tìm hiểu thêm
DKIM:	'PASS' với miền nguyencongluc.online Tìm hiểu thêm
DMARC:	'PASS' Tìm hiểu thêm

3.5.2 Gửi email từ Email Server khác qua PMG đến Zimbra:

- Mail gửi từ Gmail:



Lực Công <nguyencongluc.82@gmail.com>

đến User ▼

Hi Zimbra, Im Lucsky

Vào 14:47 Th 7, 22 thg 3, 2025 User Master <master@nguyencongluc.online> đã viết:

...

← Trả lời

→ Chuyển tiếp



- Mail nhận ở Zimbra:

The screenshot shows the Zimbra web interface. At the top, there's a search bar and a user profile for 'User Master'. Below this, the email list shows two messages. The first message is from 'Hi lucsky, I'm Zimbra' with a subject line '2 messages'. The second message is from 'User Master' with the subject 'Hi lucsky, I'm Zimbra aaa bbb'. A context menu is open over the second message, displaying various actions such as Reply, Reply to All, Forward, Delete, Mark as Spam, Tag Message, Move, Print, Mark as Read, Mark as Unread, Flag, Unflag, Redirect, Edit as New, Create Filter, Create Appointment, Create Task, Open in a separate window, Show Original, and Clear Search Highlights. The 'Show Original' option is highlighted.

- Kiểm tra nội dung thư gốc thấy thư đã đi qua PMG và các phương thức xác thực SPF, DKIM, DMARC đều đã hoạt động

```
https://mail.nguyencongluc.online/service/home/~/?auth=co&view=text&id=510
Return-Path: <nguyencongluc.82@gmail.com>
Received: from mail.nguyencongluc.online (LHLO mail.nguyencongluc.online)
(45.122.223.81) by mail.nguyencongluc.online with LMTP; Sat, 22 Mar 2025
07:55:24 +0000 (UTC)
Received: from localhost (localhost [127.0.0.1])
by mail.nguyencongluc.online (Postfix) with ESMTPL id 06C7C8D6F7
for <master@nguyencongluc.online>; Sat, 22 Mar 2025 07:55:24 +0000 (UTC)
X-Spam-Flag: NO
X-Spam-Score: -1.558
X-Spam-Level:
X-Spam-Status: No, score=-1.558 required=6.6 tests=[ALL_TRUSTED=-1,
DKIM_SIGNED=0.1, DKIM_VALID=-0.1, DKIM_VALID_AU=-0.1, DKIM_VALID_EF=-0.1,
DMARC_PASS_NONE=-0.6, FREEMAIL_ENVFROM_END_DIGIT=0.25, FREEMAIL_FROM=0.001,
HTML_MESSAGE=0.001, SPF_HELO_NONE=0.001, SPF_PASS=-0.001,
T_SCC_BODY_TEXT_LINE=-0.01] autolearn=ham autolearn_force=no
Authentication-Results: mail.nguyencongluc.online (amavis);
dkimpass (2048-bit key) header.d=gmail.com
Received: from mail.nguyencongluc.online ([127.0.0.1])
by localhost (mail.nguyencongluc.online [127.0.0.1]) (amavis, port 10032)
with ESMTPL id zyPPr4LudhGL for <master@nguyencongluc.online>;
Sat, 22 Mar 2025 07:55:23 +0000 (UTC)
Received: from localhost (localhost [127.0.0.1])
by mail.nguyencongluc.online (Postfix) with ESMTPL id 5B028BD706
for <master@nguyencongluc.online>; Sat, 22 Mar 2025 07:55:23 +0000 (UTC)
X-Virus-Scanned: amavis at nguyencongluc.online
Received: from mail.nguyencongluc.online ([127.0.0.1])
by localhost (mail.nguyencongluc.online [127.0.0.1]) (amavis, port 10026)
with ESMTPL id vfxXk-ts3jyVZ for <master@nguyencongluc.online>;
Sat, 22 Mar 2025 07:55:23 +0000 (UTC)
Received: from pmg.nguyencongluc.online (pmg.nguyencongluc.online [45.122.223.89])
by mail.nguyencongluc.online (Postfix) with ESMTPL id E9B9F8D6F7
for <master@nguyencongluc.online>; Sat, 22 Mar 2025 07:55:22 +0000 (UTC)
Received: from pmg.nguyencongluc.online (localhost.localdomain [127.0.0.1])
by pmg.nguyencongluc.online (Proxmox) with ESMTPL id 562FC40E66
for <master@nguyencongluc.online>; Sat, 22 Mar 2025 14:55:22 +0700 (+07)
Received-SPF: pass (gmail.com ... spf.google.com: Sender is authorized to use 'nguyencongluc.82@gmail.com' in 'mfrom' identity
(mechanism 'include:netblocks.google.com' matched)) receiver=pmg.nguyencongluc.online; identity=mailfrom; envelope-
from="nguyencongluc.82@gmail.com"; helo=mail-pjl-f42.google.com; client-ip=209.85.216.42
Received: from mail-pjl-f42.google.com (mail-pjl-f42.google.com [209.85.216.42])
(using TLSv1.3 with cipher TLS_AES_128_GCM_SHA256 (128/128 bits)
key-exchange X25519 server-signature RSA-PSS (4096 bits) server-digest SHA256)
(No client certificate requested)
by pmg.nguyencongluc.online (Proxmox) with ESMTPL id D08D840E56
for <master@nguyencongluc.online>; Sat, 22 Mar 2025 14:55:20 +0700 (+07)
Received: by mail-pjl-f42.google.com with SMTP id 98e67ed59e1d1-2ff797f8f1bso4712922a91.3
for <master@nguyencongluc.online>; Sat, 22 Mar 2025 00:55:20 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20230601; t=1742630113; x=1743234913; darn=nguyencongluc.online;
h=to:subject:message-id:date:from:in-reply-to:references:mime-version
:from:to:cc:subject:date:message-id:reply-to;
bh=a/zQ38Lv8hFpBVcmSFw5iMoTozf981jz+OvFQI4bw8=;
b=KAXFpylk8RNU60druSty8DM26oEHCdGYJLYT0UBNZLXmyCO7vRg6YwGVjhmH2k6z10
sEykCuWdaIQ8tfzhfEi6JGqGszgfEuFnbRLrv3BEK23w+F53FqM2BQz/BLOX9voZFbX
uF//h4h4b6n5r8MFf6wNY3HQghjHnNBHeBzms9JUVUek7060D1KSCHIQCvmsN+lyF+
zQ7dNKPv8qzCd/scWimVzmHc52LVZANg0LLJ9UDIJHMYGSDWBH5jCr8TRD1YrgAsHac/
s1OxWK1muFvppny1QIEk8jYN+kZ0L+u1XxwHdp0n2baHcmBpeTMez0yam1Nv1vFVE+
5kva=
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

Phần 4. Tìm hiểu về các chức năng có trên PMG.

Proxmox Mail Gateway (PMG) là một giải pháp bảo mật email mã nguồn mở mạnh mẽ được phát triển bởi Proxmox Server Solutions GmbH. Nó hoạt động như một proxy email, được triển khai giữa tường lửa và máy chủ email nội bộ, giúp bảo vệ hệ thống email khỏi các mối đe dọa như spam, virus, trojan và phishing. Dưới đây là các chức năng chính của Proxmox Mail Gateway cùng với mô tả chi tiết.

4.1 Spam Filtering (Lọc thư rác):

- Ý nghĩa: Sử dụng SpamAssassin để chấm điểm và lọc email dựa trên nội dung, nguồn gửi, và hành vi. Giảm thiểu email rác đến người dùng.

- Công cụ: Bayesian Filter, Razor2, RBL (Realtime Blackhole List).

* Các bước thực hiện:

4.1.1 Kiểm tra và cài đặt cấu hình SpamAssassin trên giao diện

- Vào Configuration > Spam Detector > Options.

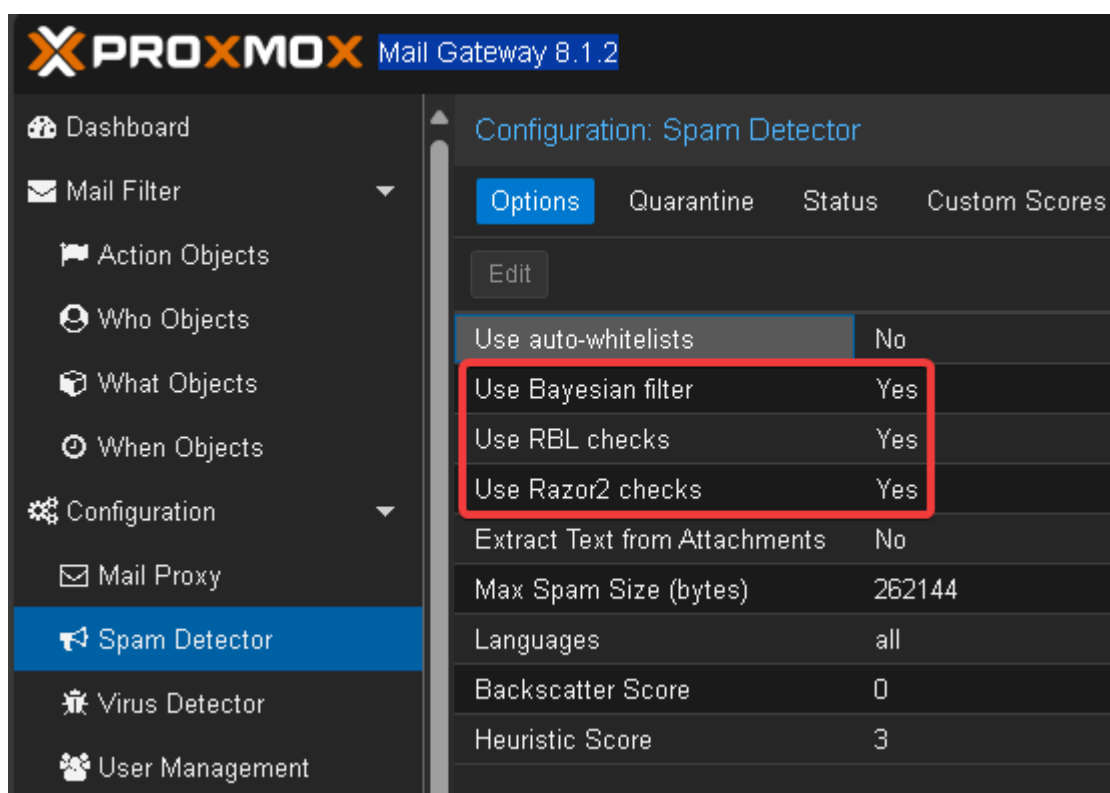
- Đảm bảo:

+Use Bayesian filter: Yes (phân tích xác suất nội dung).

+Use Razor2 checks: Yes (dữ liệu cộng đồng về spam).

+Use RBL checks: Yes (danh sách đen thời gian thực).

- Lý do: Các bộ lọc này kết hợp để tăng độ chính xác trong việc phát hiện spam.



4.1.2 Huấn luyện dữ liệu cho Bayesian

- Bayesian trong SpamAssassin là bộ lọc spam dựa trên xác suất Bayes. Nó học từ email spam và hợp lệ để tính toán xác suất một email là spam, giúp chặn thư rác hiệu quả và thích nghi với spam mới.

- Bayesian Filter cần dữ liệu spam và ham để hoạt động, vì vậy cần tải tập dữ liệu mẫu spam/ham từ nguồn uy tín:

+SpamAssassin Public Corpus: <https://spamassassin.apache.org/old/publiccorpus/>

+Tải file spam.tar.bz2 (spam) và easy_ham.tar.bz2 (ham).



Name	Last modified	Size	Description
Parent Directory	-	-	-
20021010_easy_ham.tar.bz2	2004-06-29 03:26	1.6M	
20021010_hard_ham.tar.bz2	2004-12-16 19:49	1.0M	
20021010_spam.tar.bz2	2004-06-29 03:26	1.1M	
20030228_easy_ham.tar.bz2	2004-06-29 03:26	1.5M	
20030228_easy_ham_2.tar.bz2	2004-06-29 03:26	1.0M	
20030228_hard_ham.tar.bz2	2004-12-16 19:49	1.0M	
20030228_spam.tar.bz2	2004-06-29 03:26	1.1M	
20030228_spam_2.tar.bz2	2004-06-29 03:26	2.0M	
20050311_spam_2.tar.bz2	2005-03-11 23:55	2.0M	
obsolete/	2018-06-04 06:37	-	
readme.html	2006-01-31 20:30	4.5K	

- Chạy các lệnh sau để tạo folder và download file:

```
mkdir -p spamassassin_publiccorpus
```

```
wget https://spamassassin.apache.org/old/publiccorpus/20021010\_easy\_ham.tar.bz2
```

```
wget https://spamassassin.apache.org/old/publiccorpus/20021010\_spam.tar.bz2
```

```
root@pmg:~# mkdir -p spamassassin_publiccorpus
root@pmg:~# curl https://spamassassin.apache.org/old/publiccorpus/20021010_easy_ham.tar.bz2
Warning: Binary output can mess up your terminal. Use "--output -" to tell
Warning: curl to output it to your terminal anyway, or consider "--output
Warning: <FILE>" to save to a file.
root@pmg:~# mkdir -p spamassassin_publiccorpus
root@pmg:~# wget https://spamassassin.apache.org/old/publiccorpus/20021010_easy_ham.tar.bz2
--2025-03-25 17:04:33-- https://spamassassin.apache.org/old/publiccorpus/20021010_easy_ham.tar.bz2
Resolving spamassassin.apache.org (spamassassin.apache.org)... 151.101.2.132, 2a04:4e42::644
Connecting to spamassassin.apache.org (spamassassin.apache.org)|151.101.2.132|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1677144 (1.6M) [application/x-bzip2]
Saving to: '20021010_easy_ham.tar.bz2'

20021010_easy_ham.tar.bz2 100%[=====] 1.60M 5.83MB/s in 0.3s

2025-03-25 17:04:34 (5.83 MB/s) - '20021010_easy_ham.tar.bz2' saved [1677144/1677144]

root@pmg:~# wget https://spamassassin.apache.org/old/publiccorpus/20021010_spam.tar.bz2
--2025-03-25 17:04:50-- https://spamassassin.apache.org/old/publiccorpus/20021010_spam.tar.bz2
Resolving spamassassin.apache.org (spamassassin.apache.org)... 151.101.2.132, 2a04:4e42::644
Connecting to spamassassin.apache.org (spamassassin.apache.org)|151.101.2.132|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1192582 (1.1M) [application/x-bzip2]
Saving to: '20021010_spam.tar.bz2'

20021010_spam.tar.bz2 100%[=====] 1.14M 4.49MB/s in 0.3s

2025-03-25 17:04:51 (4.49 MB/s) - '20021010_spam.tar.bz2' saved [1192582/1192582]
```


- Giải nén:

```
tar -xjf 20021010_spam.tar.bz2
```

```
tar -xjf 20021010_easy_ham.tar.bz2
```

```
root@pmg:~/spamassassin_publiccorpus# tar -xjf 20021010_spam.tar.bz2
```

```
root@pmg:~/spamassassin_publiccorpus# tar -xjf 20021010_easy_ham.tar.bz2
```

- Kết quả

```
root@pmg:~/spamassassin_publiccorpus# ls
20021010_easy_ham.tar.bz2  20021010_spam.tar.bz2  easy_ham  spam
```

- 1 file nội dung trong tập dữ liệu spam:

```
root@pmg:~/spamassassin_publiccorpus/spam# cat 0250.80b7bd444753246734e015af7b6d2d65
From iiu-admin@taint.org Sat Sep 7 22:05:49 2002
Return-Path: <iiu-admin@taint.org>
Delivered-To: zzzz@localhost.jmason.org
Received: from localhost (jalapeno [127.0.0.1])
  by zzzzason.org (Postfix) with ESMTP id 08A4916F22
  for <zzzz@localhost>; Sat, 7 Sep 2002 21:57:45 +0100 (IST)
Received: from jalapeno [127.0.0.1]
  by localhost with IMAP (fetchmail-5.9.0)
  for zzzz@localhost (single-drop); Sat, 07 Sep 2002 21:57:45 +0100 (IST)
Received: from dogma.slashnull.org (localhost [127.0.0.1]) by
  dogma.slashnull.org (8.11.6/8.11.6) with ESMTP id g874l2C06886 for
  <zzzz-list-admin-iiu@jmason.org>; Sat, 7 Sep 2002 05:47:02 +0100
Received: from linux.local ([213.9.248.135]) by dogma.slashnull.org
  (8.11.6/8.11.6) with SMTP id g874ksc06868 for <iiu-admin@taint.org>;
  Sat, 7 Sep 2002 05:46:54 +0100
Message-Id: <200209070446.g874ksc06868@dogma.slashnull.org>
Received: (gmail 11101 invoked from network); 7 Sep 2002 04:47:28 -0000
Received: from unknown (HELO h) (192.168.0.2) by linux.local with SMTP;
  7 Sep 2002 04:47:28 -0000
From: "Sales Department" <smokesdirect@terra.es>
Subject: Half Price Cigarettes and Tobacco
To: iiu-admin@taint.org
Reply-To: smokesdirect@terra.es
Date: Sat, 7 Sep 2002 06:53:25 +0200
X-Priority: 3
X-Library: Indy 8.0.25
Sender: iiu-owner@taint.org
Errors-To: iiu-owner@taint.org
X-BeenThere: iiu@iiu.taint.org
X-Mailman-Version: 2.0.10
Precedence: bulk
List-Unsubscribe: <http://iiu.taint.org/mailman/listinfo/iiu>,
  <mailto:iiu-request@iiu.taint.org?subject=unsubscribe>
List-Id: Irish Internet Users <iiu.iiu.taint.org>
List-Post: <mailto:iiu@iiu.taint.org>
List-Help: <mailto:iiu-request@iiu.taint.org?subject=help>
List-Subscribe: <http://iiu.taint.org/mailman/listinfo/iiu>,
  <mailto:iiu-request@iiu.taint.org?subject=subscribe>
List-Archive: <http://iiu.taint.org/pipermail/iiu/>

Dear Sir or Madam

In the past you have requested information on discounted products. We hope that you find this of interest. If you are not a smoker, and find this email offensive, we sincerely apologise! We will be only too happy to take you off our mailing list.

If you are a smoker, however, and are fed up with paying high prices for your cigarettes and tobacco, take a look at what we have to offer by clicking on this link.
http://www.smokersunited.co.uk/?S=15&ID=2

We can send you, legally, by registered air mail, direct to your door, 4 cartons of cigarettes or 40 pouches of rolling tobacco (all brands are available) from only 170 Euros - about 105 pounds - fully inclusive of postage and packing. Why pay more?

To remove yourself from our mailing list, please click below
mailto:smokersclub@terra.es

Yours faithfully.
Smokers United
http://www.smokersunited.co.uk/?S=15&ID=2
```

- Trong folder làm việc chứa easy_ham và spam, thực hiện huấn luyện Bayesian:

+ Huấn luyện spam: sa-learn --spam spam/*

```
root@pmg:~/spamassassin_publiccorpus# sa-learn --spam spam/*
Learned tokens from 486 message(s) (501 message(s) examined)
```

+ Huấn luyện ham: sa-learn --ham easy_ham/*

```
root@pmg:~/spamassassin_publiccorpus# sa-learn --ham easy_ham/*
Learned tokens from 2456 message(s) (2551 message(s) examined)
```

- Kiểm tra tiến trình học: `sa-learn --dump magic`

+ Trước:

```
root@pmg:~# sa-learn --dump magic
0.000      0      3      0 non-token data: bayes db version
0.000      0      0      0 non-token data: nspam
0.000      0      0      0 non-token data: nham
0.000      0      0      0 non-token data: ntokens
0.000      0      0      0 non-token data: oldest atime
0.000      0      0      0 non-token data: newest atime
0.000      0      0      0 non-token data: last journal sync atime
0.000      0      0      0 non-token data: last expiry atime
0.000      0      0      0 non-token data: last expire atime delta
0.000      0      0      0 non-token data: last expire reduction count
```

+ Sau:

```
root@pmg:~/spamassassin_publiccorpus# sa-learn --dump magic
0.000      0      3      0 non-token data: bayes db version
0.000      0      486      0 non-token data: nspam
0.000      0      2456      0 non-token data: nham
0.000      0      143664      0 non-token data: ntokens
0.000      0      1012542533      0 non-token data: oldest atime
0.000      0      1742897821      0 non-token data: newest atime
0.000      0      0      0 non-token data: last journal sync atime
0.000      0      0      0 non-token data: last expiry atime
0.000      0      0      0 non-token data: last expire atime delta
0.000      0      0      0 non-token data: last expire reduction count
```

4.1.3 Chỉnh sửa file cấu hình SpamAssassin trong file custom

- Thực hiện `cat /etc/pmg/spamassassin/custom.cf`

```
root@pmg:~# cat /etc/pmg/spamassassin/custom.cf
cat: /etc/pmg/spamassassin/custom.cf: No such file or directory
```

- Nếu file `/etc/pmg/spamassassin/custom.cf` không tồn tại trên hệ thống của bạn (No such file or directory). Điều này có nghĩa là Proxmox Mail Gateway (PMG) đang sử dụng cấu hình mặc định của SpamAssassin, bao gồm ngưỡng điểm spam (`required_score`) mặc định là 5.0, và các tùy chọn như `bayes_auto_learn` chưa được bật. Đây có thể là lý do chính khiến email spam không bị lọc, ngay cả khi Bayesian đã được huấn luyện với dữ liệu (`nspam`: 486, `nham`: 2456).

- Vì vậy bước tiếp theo là tạo và cấu hình file `custom.cf` để tối ưu hóa **Spam Filtering**, đảm bảo email spam như FREE MONEY bị chặn hoặc cách ly, và không đến Zimbra (master@nguyencongluc.online)

```
root@pmg:~# mkdir -p /etc/pmg/spamassassin
```

```
root@pmg:~# nano /etc/pmg/spamassassin/custom.cf
```

```
root@pmg:~# mkdir -p /etc/pmg/spamassassin
root@pmg:~# nano /etc/pmg/spamassassin/custom.cf
```

- Thêm cấu hình tối ưu

```
GNU nano 7.2 /etc/pmg/spamassassin/custom.cf *
# Ngưỡng điểm spam
required_score 3.0

# Bật auto-learning cho Bayesian
bayes_auto_learn 1
bayes_auto_learn_threshold_nonspam 0.1
bayes_auto_learn_threshold_spam 6.0

# Tắt whitelist nếu cần
use_auto_whitelist 0
```

required_score 3.0: Giảm ngưỡng từ 5.0 xuống 3.0 để dễ lọc spam hơn.

bayes_auto_learn 1: Bật tự học cho Bayesian.

bayes_auto_learn_threshold_nonspam 0.1: Email < 0.1 điểm là ham.

bayes_auto_learn_threshold_spam 6.0: Email > 6.0 điểm là spam.

use_auto_whitelist 0: Tắt whitelist tự động để không bỏ qua Gmail.

- Cách tính điểm và xử lý ngưỡng trong SpamAssassin:

+Tính điểm: Tổng điểm spam tính từ quy tắc (Bayesian, Razor2, RBL, nội dung). Ví dụ: "FREE MONEY" (+1.0), Bayesian (+3.5) = 4.5.

+required_score 3.0: Điểm $\geq 3.0 \rightarrow$ spam, bị lọc, mail có thể là spam hoặc chỉ là nhầm lẫn.

+bayes_auto_learn 1: Bật tự học Bayesian.

+bayes_auto_learn_threshold_nonspam 0.1: Điểm < 0.1 \rightarrow học là ham vì mail uy tín.

+bayes_auto_learn_threshold_spam 6.0: Điểm > 6.0 \rightarrow học là spam vì mail lúc này quá nguy hiểm.

+use_auto_whitelist 0: Tắt whitelist, không bỏ qua Gmail.

- Sau khi thêm cấu hình tối ưu, tiến hành đồng bộ trên PMG: pmgconfig sync --restart 1

```
root@pmg:~/spamassassin_publiccorpus# pmgconfig sync --restart 1
```

4.1.4 Thử nghiệm gửi email spam và email sạch đến zimbra:

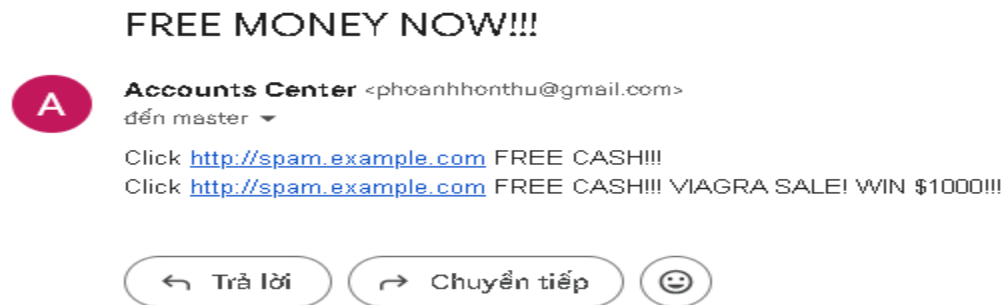
- Gửi Email Spam với nội dung như sau từ user gmail: phoanhhonthu@gmail.com đến master@nguyencongluc.online

Subject: FREE MONEY NOW!!!

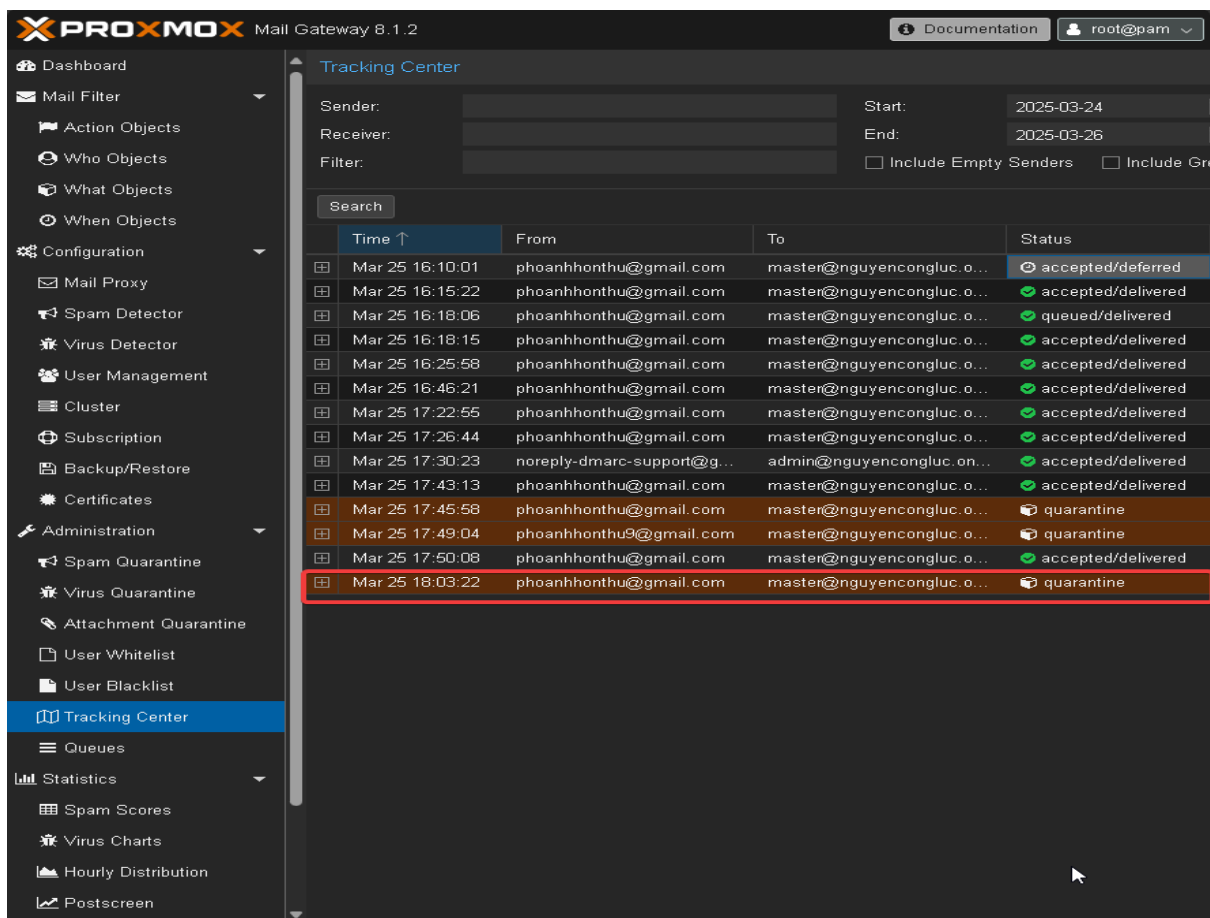
Body: Click <http://spam.example.com> FREE CASH!!!

Click <http://spam.example.com> FREE CASH!!!

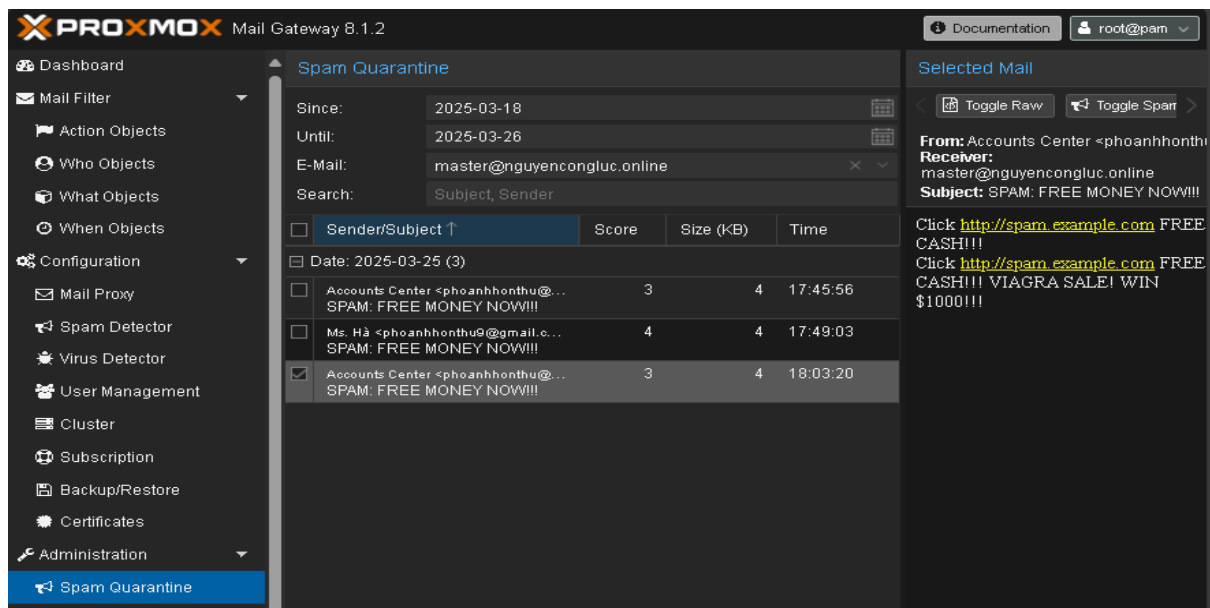
VIAGRA SALE! WIN \$1000!!!



- Trong Administration->Tracking Center: Tìm thấy email vừa gửi đã bị quarantine(cách ly)



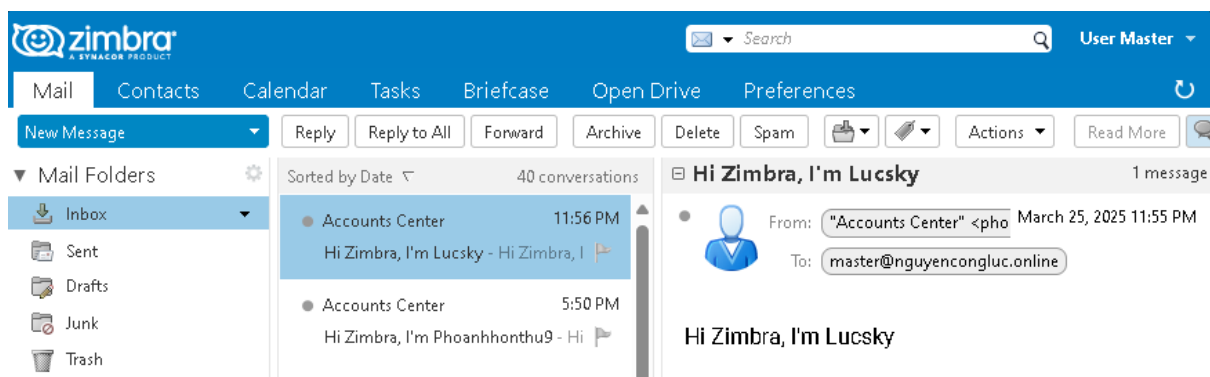
- Trong Administration->Spam Quarantine: Cũng tìm thấy nội dung email vừa gửi đã bị quarantine(cách ly)



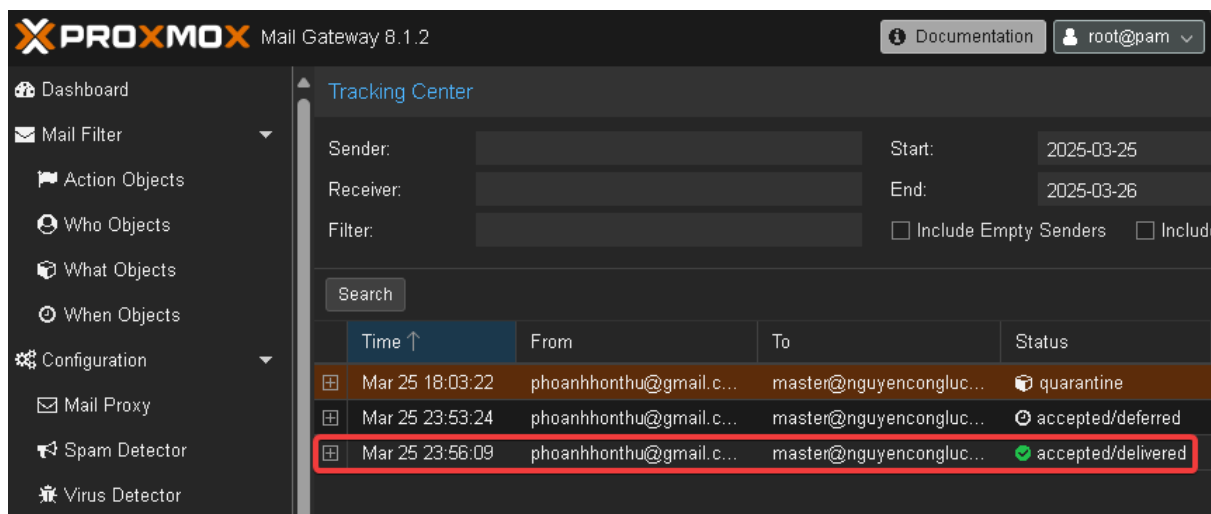
- Trường hợp gửi 1 “ham email” -email sạch:



- Zimbra nhận được mail ngay lập tức



- Trong Administration->Tracking Center tìm thấy thông tin Email đã được vận chuyển



4.2 Virus Scanning (Quét virus):

- Ý nghĩa: Tích hợp ClamAV để phát hiện và chặn email chứa virus, mã độc, bảo vệ hệ thống khỏi các mối đe dọa.

- Công cụ: Cơ sở dữ liệu virus ClamAV.

* Các bước thực hiện:

4.2.1 Cấu hình ClamAV

- Vào Configuration > Virus Detector:

+ Giữ nguyên cấu hình ban đầu

+ Đảm bảo Enable Virus Scanning: Yes.

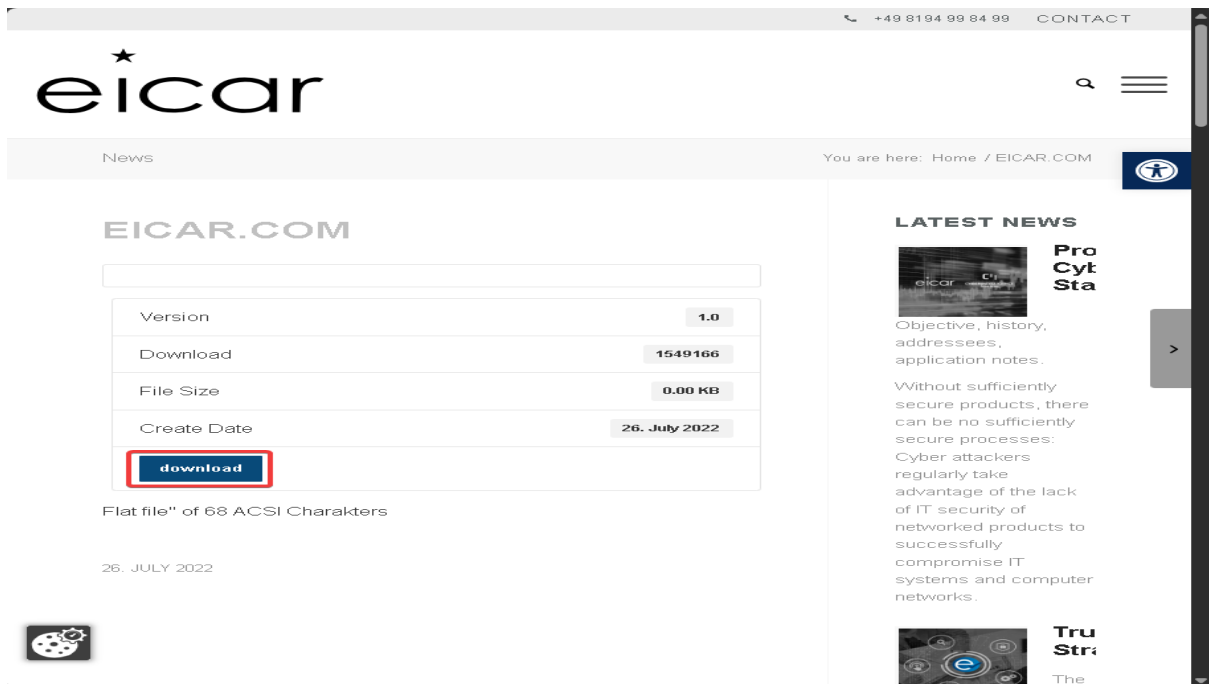
- Cập nhật database - Đảm bảo ClamAV sẵn sàng phát hiện virus mới nhất:

freshclam

```
root@pmg:~# freshclam
ClamAV update process started at Wed Mar 26 15:51:00 2025
Pruning unwanted or deprecated database file safebrowsing.cvd.
daily database available for update (local version: 27199, remote version: 27588)
Current database is 389 versions behind.
Downloading database patch # 27200...
WARNING: downloadFile: file not found: https://database.clamav.net/daily-27200.cdiff
WARNING: downloadPatch: Can't download daily-27200.cdiff from https://database.clamav.net/daily-27200.cdiff
Downloading database patch # 27200...
WARNING: downloadFile: file not found: https://database.clamav.net/daily-27200.cdiff
WARNING: downloadPatch: Can't download daily-27200.cdiff from https://database.clamav.net/daily-27200.cdiff
Downloading database patch # 27200...
WARNING: downloadFile: file not found: https://database.clamav.net/daily-27200.cdiff
WARNING: downloadPatch: Can't download daily-27200.cdiff from https://database.clamav.net/daily-27200.cdiff
Downloading database patch # 27200...
WARNING: downloadFile: file not found: https://database.clamav.net/daily-27200.cdiff
WARNING: downloadPatch: Can't download daily-27200.cdiff from https://database.clamav.net/daily-27200.cdiff
Downloading database patch # 27200...
WARNING: downloadFile: file not found: https://database.clamav.net/daily-27200.cdiff
WARNING: downloadPatch: Can't download daily-27200.cdiff from https://database.clamav.net/daily-27200.cdiff
WARNING: Incremental update failed, trying to download daily.cvd
Time: 5.05s, ETA: 0.05s [=====] 61.62MiB/61.62MiB
Testing database: '/var/lib/clamav//tmp.ff048ea41b/clamav-cfe644cd8334d3035bf84b9df1e3c593.tmp-daily.cvd' ...
Database test passed.
daily.cvd updated (version: 27588, sigs: 2074268, f-level: 90, builder: raynman)
main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
bytecode database available for update (local version: 335, remote version: 336)
Current database is 1 version behind.
Downloading database patch # 336...
Time: 0.25s, ETA: 0.05s [=====] 842B/842B
Testing database: '/var/lib/clamav//tmp.ff048ea41b/clamav-dd1f3072f79349ae5b2bc139ff644.tmp-bytecode.cld' ...
Database test passed.
bytecode.cld updated (version: 336, sigs: 83, f-level: 90, builder: nrandolp)
ClamAV successfully notified about the update.
```

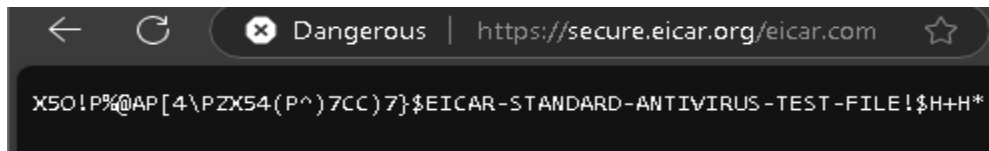
4.2.2 Chuẩn bị virus thử nghiệm

- Tải file EICAR từ <https://www.eicar.org/download/eicar-com/>.

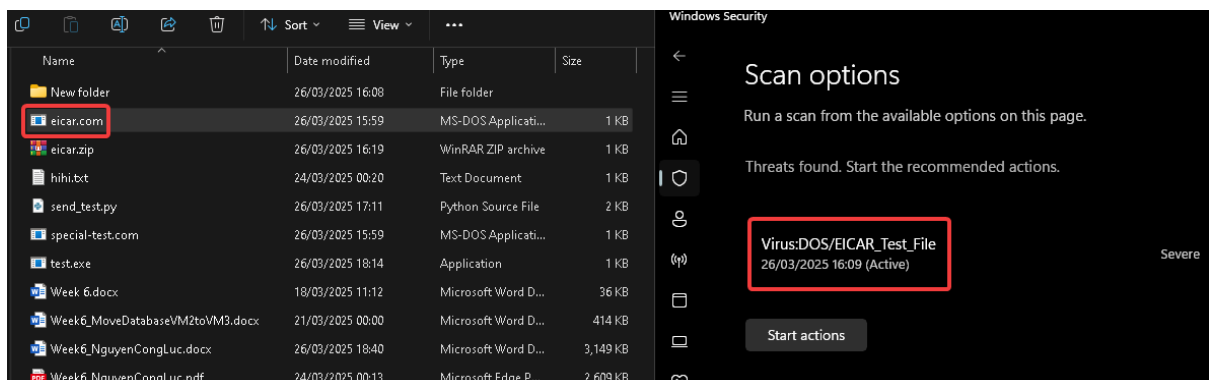


- Sau khi click vào download sẽ dẫn đến link: <https://secure.eicar.org/eicar.com> chứa mã độc: X5O!P%#@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

Thực hiện download về



- Đây là EICAR Test File, một tệp kiểm tra chuẩn dành cho phần mềm diệt virus. Nó không phải là virus thực sự, mà chỉ là một chuỗi ký tự đặc biệt do European Institute for Computer Antivirus Research (EICAR) tạo ra để kiểm tra xem phần mềm diệt virus có hoạt động đúng không. Và phần mềm virus sẽ scan được nó là virus.



4.2.3 Chuẩn bị mail client, thêm virus và thử nghiệm gửi đi

- Đa số các mail server sẽ filter virus, loại bỏ virus trong thư user trước khi gửi đi nên phải tự cài đặt một email client thuần túy, tập trung vào việc gửi và nhận email, không có chức năng quét hoặc lọc virus, spam.

Mutt là một chương trình đáp ứng các yêu cầu trên. Mutt chỉ thực hiện gửi và nhận email dòng lệnh (command-line email client) trên các hệ điều hành như Linux/Unix. Nó nhẹ, mạnh mẽ, hỗ trợ đính kèm file, quản lý hộp thư và tùy chỉnh cao, thường được dùng để gửi email tự động hoặc thủ công từ server.

- Cài đặt mutt trên server Ubuntu: apt install mutt

```
root@ns12-w03-lucnc:~/sendtest# apt install mutt
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

- Tạo thư mục làm việc và file chứa virus trên 1 server linux (khác server pmg và zimbra):

```
root@ns12-w03-lucnc:~# mkdir -p special_test
```

```
root@ns12-w03-lucnc:~# cd special_test/
```

```
root@ns12-w03-lucnc:~/special_test# echo 'X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*' > special-test.com
```

```
root@ns12-w03-lucnc:~/special_test# cat special-test.com
```

```
root@ns12-w03-lucnc:~# mkdir -p special_test
root@ns12-w03-lucnc:~# cd special_test/
root@ns12-w03-lucnc:~/special_test# echo 'X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*' > special-test.com
root@ns12-w03-lucnc:~/special_test# cat special-test.com
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

- Tiến hành gửi email với mutt:

```
echo "This email contains a test file to verify the system." | mutt -s "Special Feature Test" -a special-test.com -- master@nguyencongluc.online
```

-s: Tiêu đề email.

-a: Đính kèm file (phải đặt trước -- và địa chỉ email).

--: Phân tách tùy chọn và địa chỉ nhận.

```
root@ns12-w03-lucnc:~/special_test# echo "This email contains a test file to verify the system." | mutt -s "Special Feature Test" -a special-test.com -- master@nguyencongluc.online
```


4.2.4 Kiểm tra kết quả

- Kiểm tra Tracking Center: Vào Administration->Tracking Center: Mail đã bị cách ly(quarantine) và không gửi đến được user master zimbra.

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar contains a navigation menu with 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, and Tracking Center (highlighted). The main panel is titled 'Tracking Center' and displays a table of email tracking records. The table has columns for Time, From, To, and Status. The records show emails from various sources, including 'phoanhonthu@gmail.com' and 'root@ns12-w03-lucnc.vhost.vn', all sent to 'master@nguyencongluc.online'. The status of these emails is 'accepted/delivered', 'quarantine', or 'queued/delivered'.

Time ↑	From	To	Status
Mar 26 18:13:27	phoanhonthu@gmail.com	master@nguyencongluc.online	accepted/delivered
Mar 26 18:15:59	root@ns12-w03-lucnc.vhost.vn	master@nguyencongluc.online	quarantine
Mar 26 18:16:00	postmaster@pmg.nguyencongluc.online	pmg@nguyencongluc.online	queued/delivered
Mar 26 18:16:46	root@ns12-w03-lucnc.vhost.vn	master@nguyencongluc.online	quarantine
Mar 26 18:16:47	postmaster@pmg.nguyencongluc.online	pmg@nguyencongluc.online	queued/delivered
Mar 26 20:06:33	root@ns12-w03-lucnc.vhost.vn	master@nguyencongluc.online	quarantine
Mar 26 20:06:34	postmaster@pmg.nguyencongluc.online	pmg@nguyencongluc.online	queued/delivered

- Kiểm tra Virus Quarantine, thấy nội dung của 3 email bị cách ly.

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar is the same as the previous screenshot, with 'Virus Quarantine' highlighted. The main panel is titled 'Virus Quarantine' and displays a table of quarantined emails. The table has columns for Date, Sender/Receiver/Subject, Virus, Size (K-B), and Time. The records show emails from 'root@ns12-w03-lucnc.vhost.vn' to 'master@nguyencongluc.online' with the subject 'Special Feature Test'. The virus detected is 'Eicar...'. The status of these emails is 'quarantine'.

Date	Sender/Receiver/Subject	Virus	Size (K-B)	Time ↓
2025-03-26 (3)				
	root@ns12-w03-lucnc.vhost.vn To: master@nguyencongluc.online Special Feature Test	Eicar...	1	20:06:30
	root@ns12-w03-lucnc.vhost.vn To: master@nguyencongluc.online Special Feature Test	Eicar...	1	18:16:45
	root@ns12-w03-lucnc.vhost.vn To: master@nguyencongluc.online Special Feature Test	Eicar...	1	18:15:56

- User Master từ zimbra đã được bảo vệ khỏi virus email.

The screenshot shows the Zimbra User Master interface. The top bar contains the Zimbra logo, a search bar, and the user name 'User Master'. The main panel is titled 'Mail' and displays a list of mail folders: Mail, Contacts, Calendar, Tasks, Briefcase, Open Drive, and Preferences. Below the folders, there is a 'New Message' button and a 'Sorted by Date' dropdown. The list shows 47 conversations. The first conversation is from 'Accounts Center' at 12:03 AM, with the subject 'Hi Zimbra, I'm Lucsky - Hi Ziml'. The interface also includes buttons for 'Reply', 'Reply to All', 'Forward', 'Archive', 'Delete', 'Spam', and 'Actions'.

4.3 Greylisting (Tạm hoãn email):

- Ý nghĩa: Từ chối tạm thời email từ nguồn không xác định, buộc máy chủ gửi lại sau một khoảng thời gian. Giảm spam từ các nguồn không tuân thủ RFC.

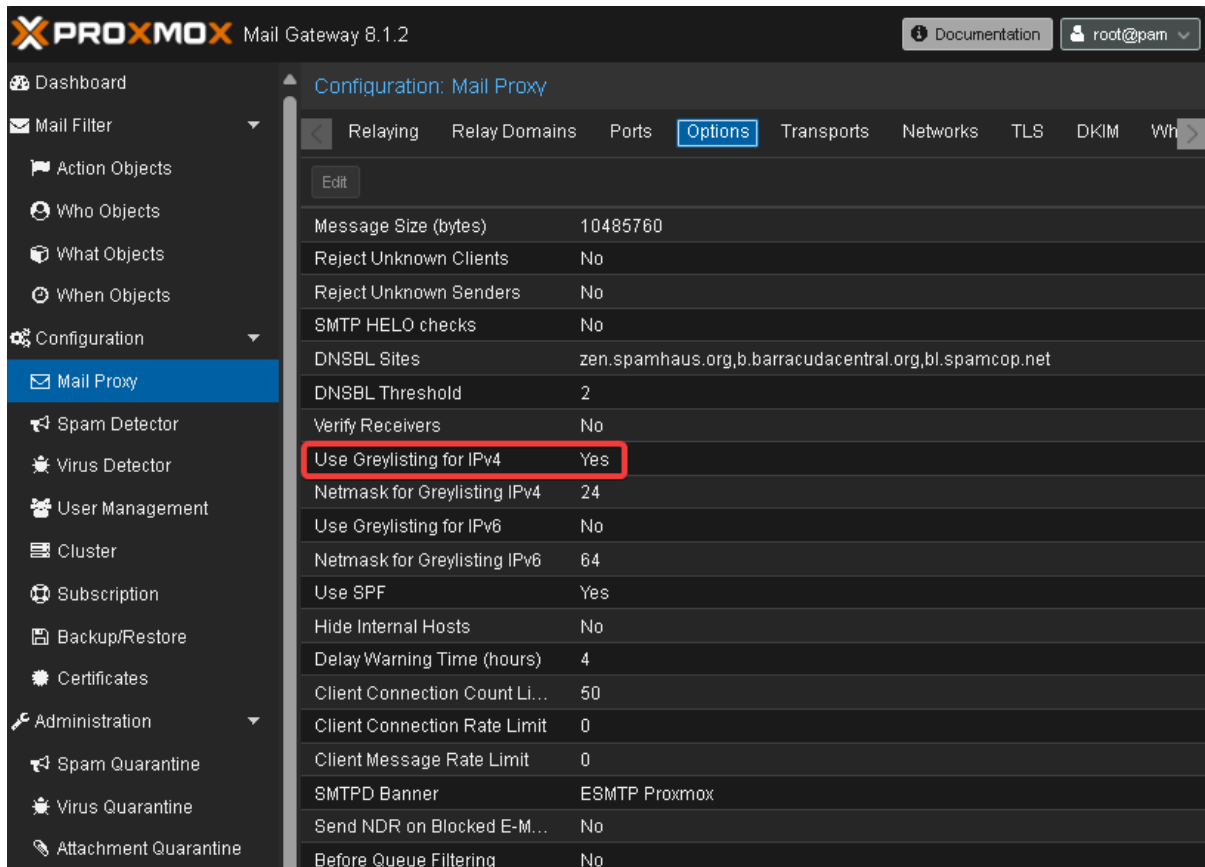
- Cách cấu hình:

Vào Configuration > Mail Proxy > Options.

Tích Use Greylisting IPV4: Yes (thời gian mặc định: 5 phút).

Lưu cấu hình.

Lý do: Kích hoạt cơ chế trì hoãn để kiểm tra hành vi gửi lại của máy chủ gửi.



The screenshot shows the Proxmox Mail Gateway 8.1.2 configuration interface. The left sidebar contains a navigation menu with categories like Mail Filter, Configuration, and Administration. The 'Mail Proxy' option under Configuration is selected. The main panel displays the 'Configuration: Mail Proxy' settings, with the 'Options' tab active. A table lists various configuration options, with 'Use Greylisting for IPv4' highlighted by a red rectangle and set to 'Yes'.

Option	Value
Message Size (bytes)	10485760
Reject Unknown Clients	No
Reject Unknown Senders	No
SMTP HELO checks	No
DNSBL Sites	zen.spamhaus.org,b.barracudacentral.org,bl.spamcop.net
DNSBL Threshold	2
Verify Receivers	No
Use Greylisting for IPv4	Yes
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-Mail	No
Before Queue Filtering	No

4.4 Hạn chế Email gửi đến với DNSBL, User Blacklist và Mail Filter-Rules:

4.4.1 Chặn email với DNSBL (Danh sách đen DNS)

- Ý nghĩa: Chặn email từ các địa chỉ IP nằm trong danh sách đen (DNSBL), như zen.spamhaus.org.

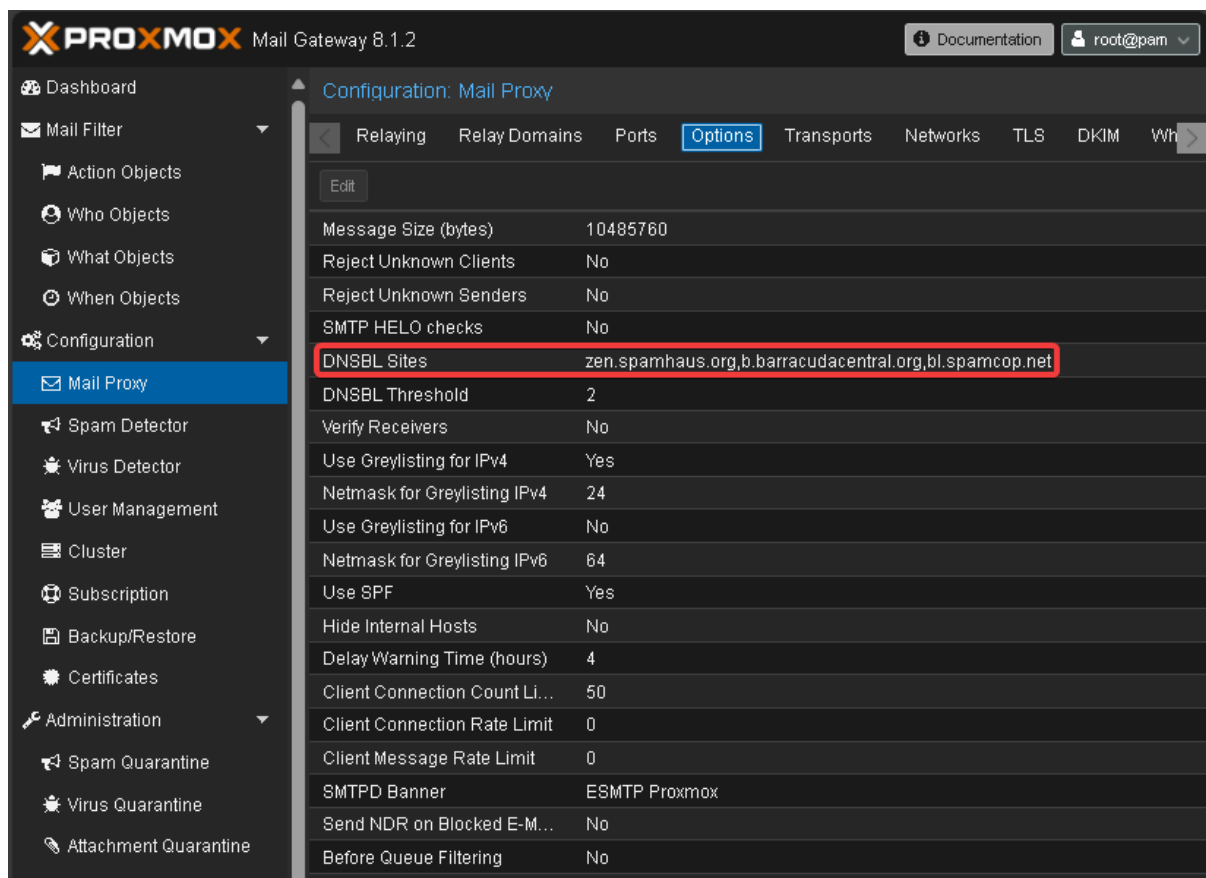
- Cách cấu hình:

Vào Configuration > Mail Proxy > Options.

Trong DNSBL Sites, thêm zen.spamhaus.org, b.barracudacentral.org, bl.spamcop.net

Lưu cấu hình.

Lý do: Sử dụng danh sách đen uy tín để chặn nguồn spam.



4.4.2 Cách ly email với User Blacklist

- Ý nghĩa: Với tính năng này, có thể đánh dấu thủ công các email từ một số tên miền hoặc địa chỉ nhất định là thư rác.

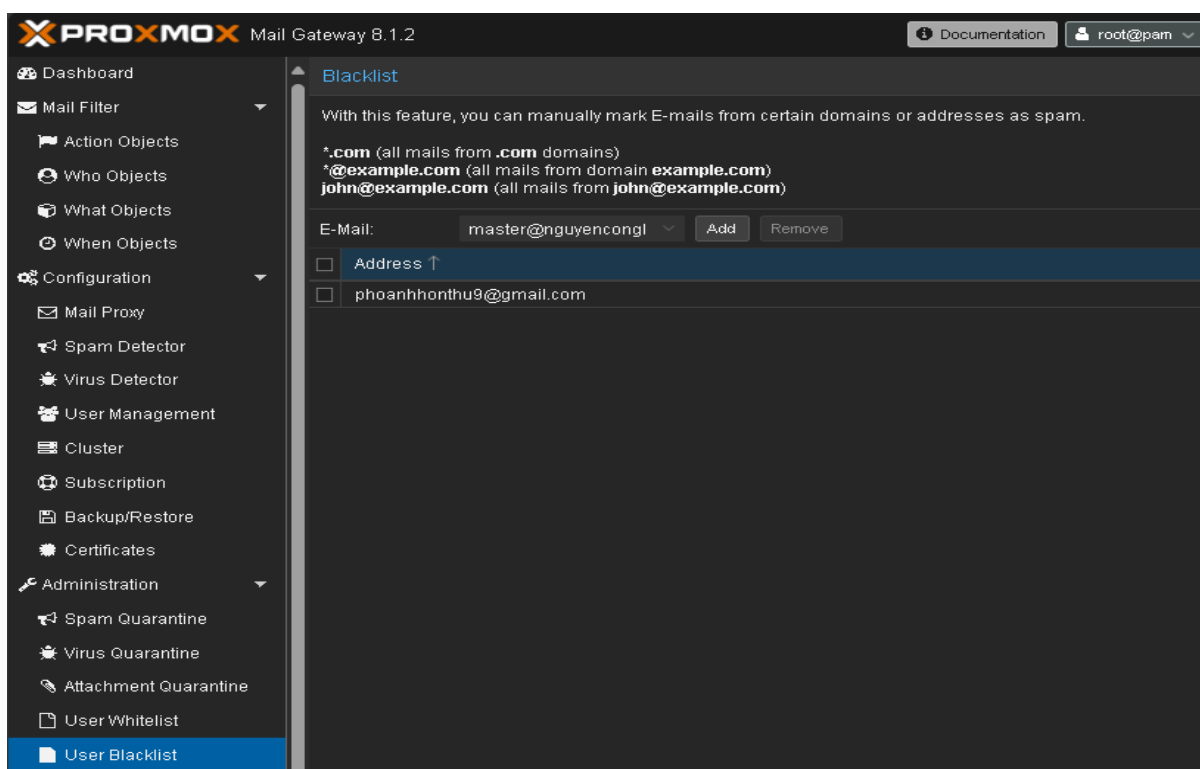
- Cách cấu hình:

Vào Administration > User Blacklist

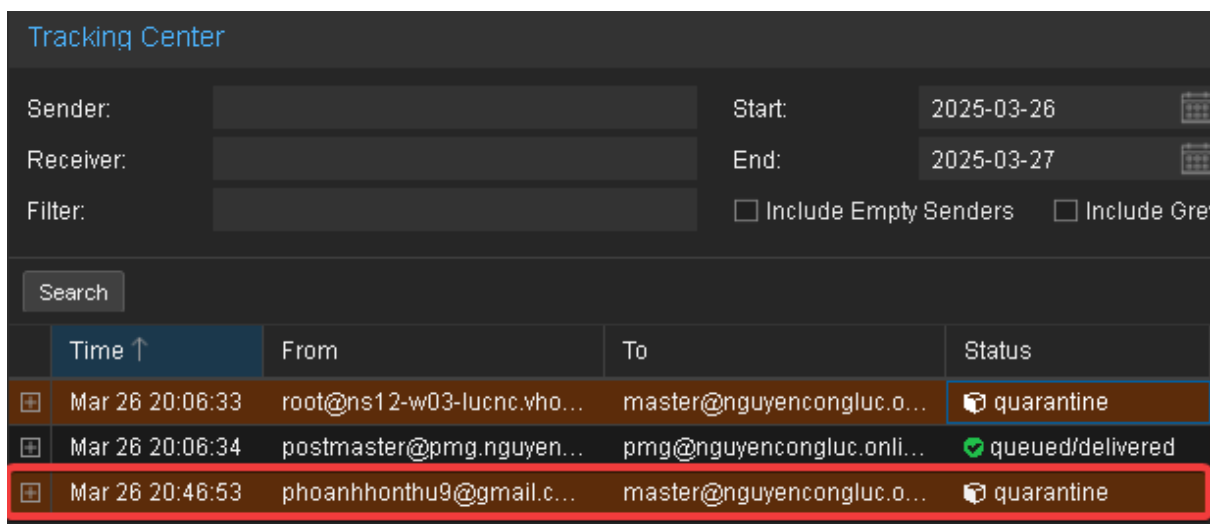
Trong mục E-Mail, chọn phoanhonthu9@gmail.com từ danh sách thả xuống (nếu không có, nhập thủ công).

Nhấn Add, sau đó nhập yourtest@gmail.com vào trường Address.

Nhấn OK để lưu.



- Kết quả đã cách ly spam thành công:

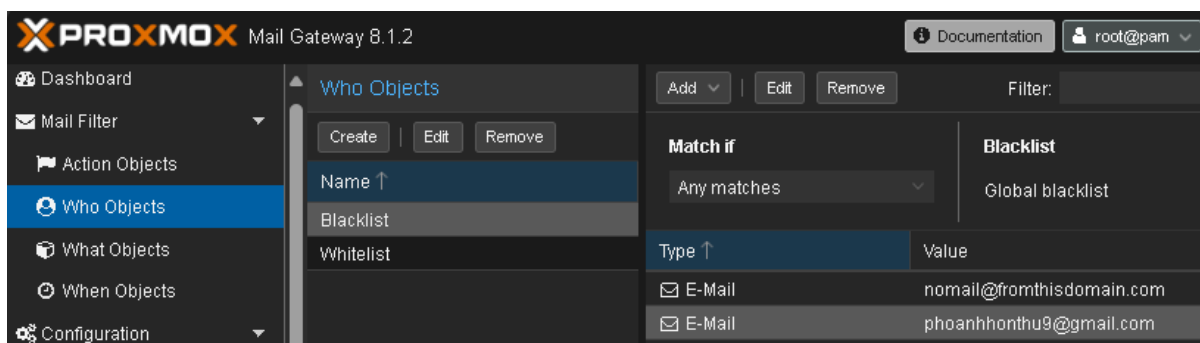


4.4.3 Chặn email với Mail Filter-Rules

- Vào Configuration > Mail Filter > Rules.

Đây là nơi bạn định nghĩa các quy tắc lọc email dựa trên tiêu chí như người gửi, người nhận, nội dung, v.v.

- Thêm user phoanhthonu9@gmail.com vào Blacklist trong Who Object:



* Tạo một quy tắc mới:

-Vào Mail Filter > Nhấn nút Add để tạo quy tắc mới.

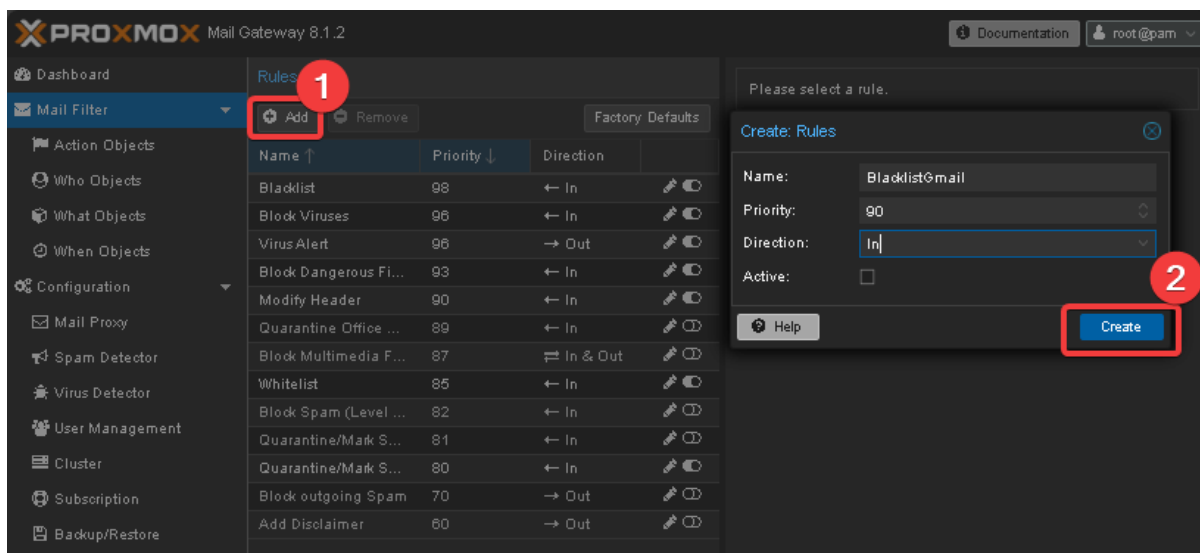
-Cấu hình quy tắc:

Name: Đặt tên để nhận biết, ví dụ: Block_phoanhthonu9.

Priority: Đặt giá trị cao (ví dụ: 90) để ưu tiên thực thi trước các quy tắc khác.

Direction: Chọn In (chỉ áp dụng cho email đến).

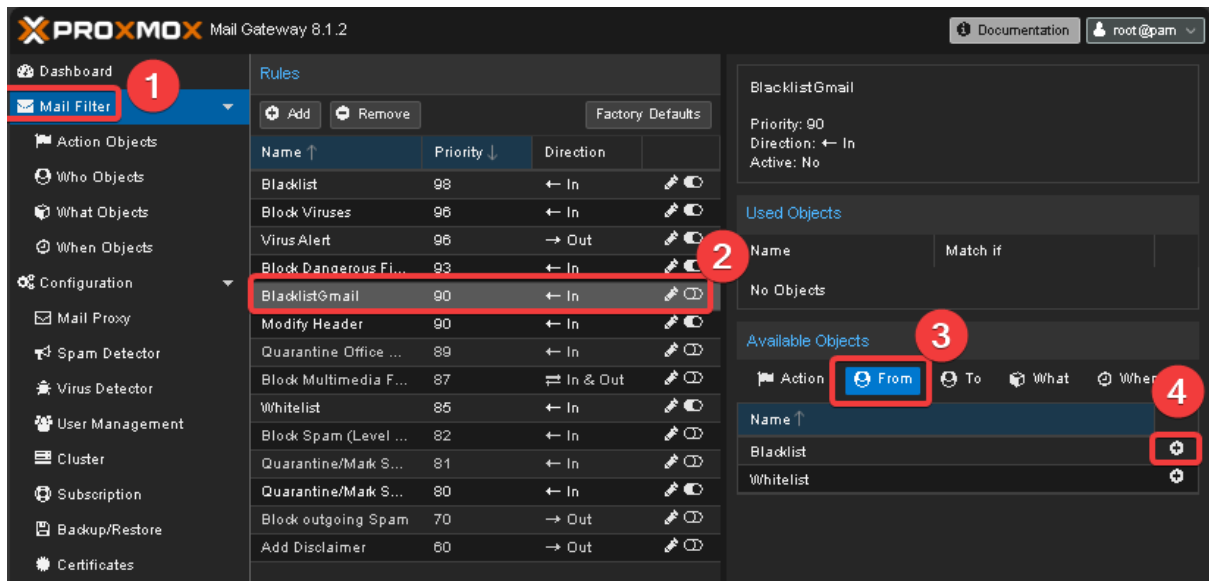
Action: Để trống tạm thời, sẽ thêm sau.



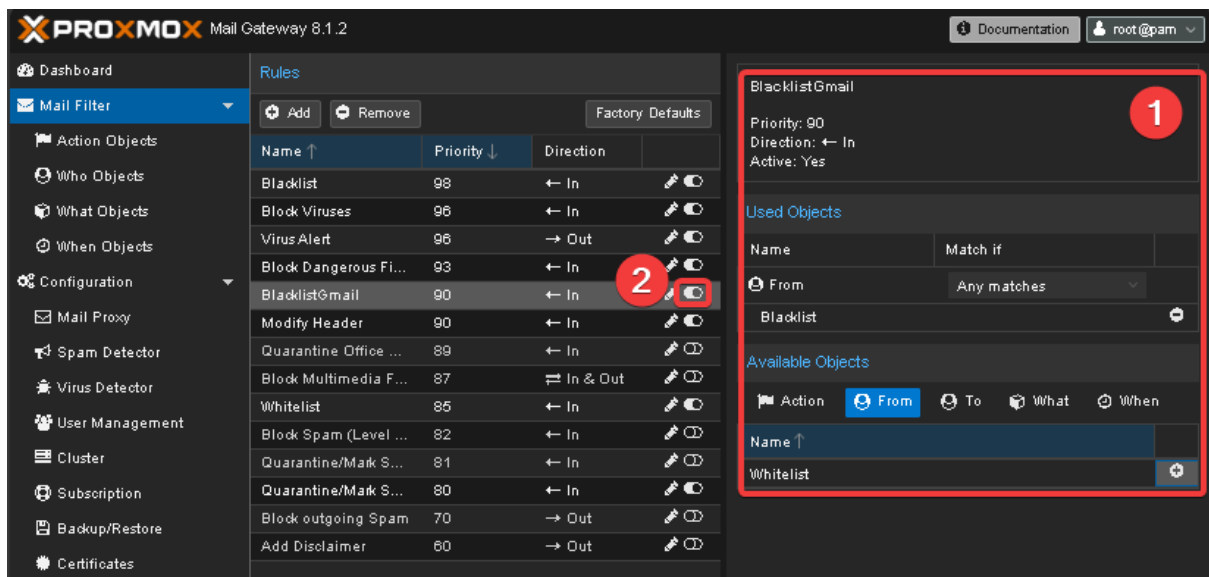
* Thêm hành động chặn

- Vẫn trong rules, trong Name > Click vào BlacklistGmail

Trong Available Objects > From > Chọn Thêm Blacklist để vào ds người gửi cần chặn

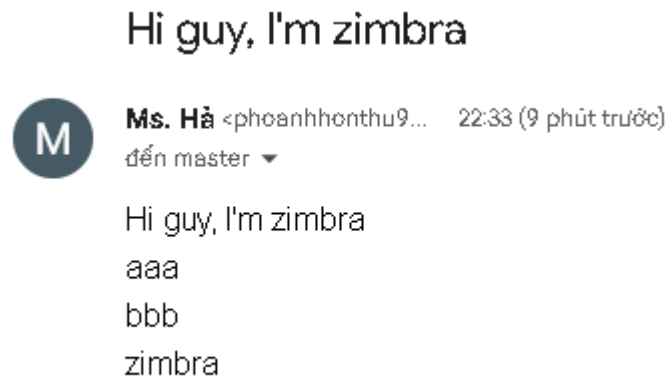


- Kiểm tra và bật lên Rules:



* Gửi mail để kiểm tra quy tắc hoạt động:

- Mail gửi từ Gmail:



- Mail bị chặn ở PMG:

PROXMOX Mail Gateway 8.1.2

Tracking Center

Sender: [] Start: 2025-03-26 19:39

Receiver: [] End: 2025-03-27 00:00

Filter: [] ☐ Include Empty Senders ☐ Include Greylist

Search []

Time ↑	From	To	Status
Mar 26 20:06...	root@ns12-w03-lucnc.vhost.vn	master@nguyencongluc.online	quarantine
Mar 26 20:06...	postmaster@pmg.nguyencongluc.online	pmg@nguyencongluc.online	queued/delivered
Mar 26 20:46...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 21:52...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 22:05...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 22:06...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 22:08...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 22:09...	phoanhonthu9@gmail.com	master@nguyencongluc.online	accepted/delivered
Mar 26 22:16...	phoanhonthu9@gmail.com	master@nguyencongluc.online	blocked
Mar 26 22:33...	phoanhonthu9@gmail.com	master@nguyencongluc.online	blocked

4.5 Tracking Center (Theo dõi luồng email):

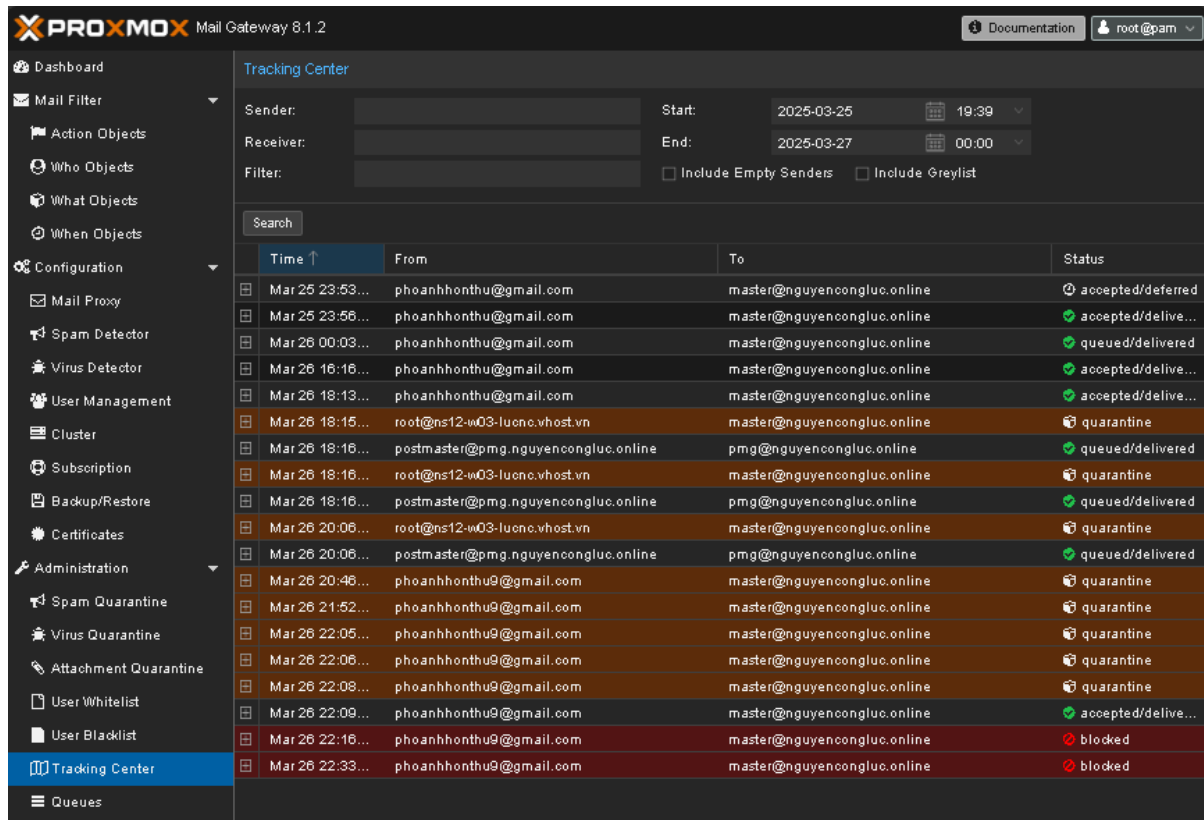
- Ý nghĩa: Cung cấp giao diện theo dõi toàn bộ email đi qua PMG, giúp quản trị viên phân tích trạng thái (chấp nhận, chặn, cách ly).

- Có 3 trạng thái email:

1: Accepted → Đã đến Zimbra.

2: Quarantine → Bị giữ vì spam.

3: Blocked → Bị chặn vì virus.



PROXMOX Mail Gateway 8.1.2

Documentation root@pmg

Tracking Center

Sender: [] Start: 2025-03-25 19:39
Receiver: [] End: 2025-03-27 00:00
Filter: [] ☐ Include Empty Senders ☐ Include Greylist

Search []

Time ↑	From	To	Status
Mar 25 23:53...	phoanhonthu@gmail.com	master@nguyencongluc.online	accepted/deferred
Mar 25 23:56...	phoanhonthu@gmail.com	master@nguyencongluc.online	accepted/delive...
Mar 26 00:03...	phoanhonthu@gmail.com	master@nguyencongluc.online	queued/delivered
Mar 26 16:16...	phoanhonthu@gmail.com	master@nguyencongluc.online	accepted/delive...
Mar 26 18:13...	phoanhonthu@gmail.com	master@nguyencongluc.online	accepted/delive...
Mar 26 18:16...	root@ns12-w03-lucnc.vhost.vn	master@nguyencongluc.online	quarantine
Mar 26 18:16...	postmaster@pmg.nguyencongluc.online	pmg@nguyencongluc.online	queued/delivered
Mar 26 18:16...	root@ns12-w03-lucnc.vhost.vn	master@nguyencongluc.online	quarantine
Mar 26 18:16...	postmaster@pmg.nguyencongluc.online	pmg@nguyencongluc.online	queued/delivered
Mar 26 20:06...	root@ns12-w03-lucnc.vhost.vn	master@nguyencongluc.online	quarantine
Mar 26 20:06...	postmaster@pmg.nguyencongluc.online	pmg@nguyencongluc.online	queued/delivered
Mar 26 20:46...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 21:52...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 22:05...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 22:06...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 22:08...	phoanhonthu9@gmail.com	master@nguyencongluc.online	quarantine
Mar 26 22:09...	phoanhonthu9@gmail.com	master@nguyencongluc.online	accepted/delive...
Mar 26 22:16...	phoanhonthu9@gmail.com	master@nguyencongluc.online	blocked
Mar 26 22:33...	phoanhonthu9@gmail.com	master@nguyencongluc.online	blocked

4.6 Quarantine (Cách ly email):

Ý nghĩa: Lưu trữ email spam hoặc virus để kiểm tra thủ công, cho phép khôi phục hoặc xóa tùy nhu cầu.

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar contains a navigation menu with 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 (selected), Virus Quarantine, and Attachment Quarantine. The main panel is titled 'Spam Quarantine' and displays a list of quarantined emails. The list is filtered by date (2025-03-26) and shows 5 items. Each item includes a checkbox, sender information, score, size (KB), and time. The right sidebar shows 'Selected Mail' with a 'Toggle Raw' button.

<input type="checkbox"/>	Sender/Subject	Score	Size (KB)	Time ↓
Date: 2025-03-26 (5)				
<input type="checkbox"/>	Ms. Hà <phoanhonthu9@gmail.com> SPAM: Hi Zimbra	100	4	22:08:09
<input type="checkbox"/>	Ms. Hà <phoanhonthu9@gmail.com> SPAM: Hi Zimbra	100	4	22:06:38
<input type="checkbox"/>	Ms. Hà <phoanhonthu9@gmail.com> SPAM: Hi	100	4	22:04:59
<input type="checkbox"/>	Ms. Hà <phoanhonthu9@gmail.com> SPAM: Hi	100	4	21:52:33
<input type="checkbox"/>	Ms. Hà <phoanhonthu9@gmail.com> SPAM: Hi Zimbra	100	4	20:46:46
Date: 2025-03-25 (3)				
<input type="checkbox"/>	Accounts Center <phoanhonthu@g...> SPAM: FREE MONEY NOW!!!	3	4	18:03:20
<input type="checkbox"/>	Ms. Hà <phoanhonthu9@gmail.com> SPAM: FREE MONEY NOW!!!	4	4	17:49:03
<input type="checkbox"/>	Accounts Center <phoanhonthu@g...> SPAM: FREE MONEY NOW!!!	3	4	17:45:56

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar is the same as the previous screenshot, but 'Virus Quarantine' is selected. The main panel is titled 'Virus Quarantine' and displays a list of quarantined emails. The list is filtered by date (2025-03-26) and shows 3 items. Each item includes a checkbox, sender/receiver/subject information, virus name, size (KB), and time. The right sidebar shows 'Selected Mail' with a 'Toggle Raw' button.

<input type="checkbox"/>	Sender/Receiver/Subject	Virus	Size (KB)	Time ↓
Date: 2025-03-26 (3)				
<input type="checkbox"/>	root <root@ns12-w03-lucnc.vhost.vn> To: master@nguyencongluc.online Special Feature Test	Eicar...	1	20:06:30
<input type="checkbox"/>	root <root@ns12-w03-lucnc.vhost.vn> To: master@nguyencongluc.online Special Feature Test	Eicar...	1	18:16:45
<input type="checkbox"/>	root <root@ns12-w03-lucnc.vhost.vn> To: master@nguyencongluc.online Special Feature Test	Eicar...	1	18:15:56

4.7 Quét Email Gửi Đi (Outgoing Mail Scanning)

- Chức năng: Không giống nhiều giải pháp chỉ quét email đến, PMG quét cả email gửi đi để phát hiện virus từ máy chủ nội bộ và thu thập thông kê.

- Đặc điểm nổi bật:

+Bảo vệ danh tiếng doanh nghiệp.

+Ngăn gửi virus ra ngoài (hữu ích ở các quốc gia có luật nghiêm ngặt).

- Một email chứa virus từ user Zimbra đã bị Zimbra server chặn khi gửi đi và thông báo về Admin user

Hi

From: "User Master" <master@nguyencongluc.online>
To: "phoanhthonthu" <phoanhthonthu@gmail.com>

eicar.com (67 B) [Download](#) | [Briefcase](#) | [Remove](#)

Hi

admin@nguyen...uc.online

Read More View

VIRUS (Win.Test.EICAR_HDB-1) in mail FROM LOCAL [45.122.223.81]:60634 <master@nguyencongluc.on 1 message

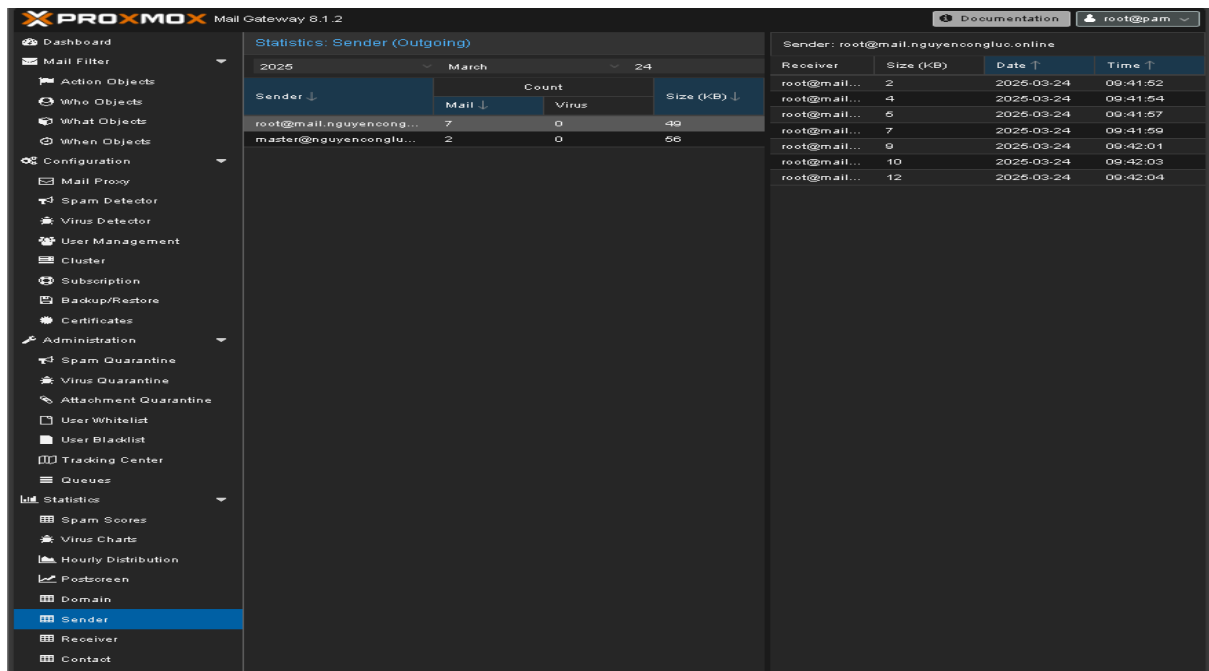
From: "Content-filter at mail.nguyencongluc.online" <admin@nguyencongluc.online>
To: admin@nguyencongluc.online

March 26, 2025 10:57 PM

header.hdr (783 B) [Download](#) | [Briefcase](#) | [Remove](#)

A virus was found: Win.Test.EICAR_HDB-1
Scanner detecting a virus: ClamAV-clamd
Content type: Virus
Internal reference code for the message is 608570-04/PxVA3smjH01Z
First upstream SMTP client IP address: [45.122.223.81]:60634
mail.nguyencongluc.online
Received trace: ESMTP://[45.122.223.81]:60634
Return-Path: <master@nguyencongluc.online>
From: User Master <master@nguyencongluc.online>
Message-ID: <1712756762.202.1743004626446.JavaMail.zimbra@nguyencongluc.online>
Subject: Hi
The message has been quarantined as: virus-quarantine.zvw2skqpez@nguyencongluc.online
The message WAS NOT relayed to:
<phoanhthonthu@gmail.com>:
250 2.7.0 ok, discarded, id=608570-04 - infected: win.test.eicar_hdb-1
Virus scanner output:
p003: Win.Test.EICAR_HDB-1 FOUND
p006: Win.Test.EICAR_HDB-1 FOUND
Return-Path: <master@nguyencongluc.online>
Received: from mail.nguyencongluc.online (mail.nguyencongluc.online [45.122.223.81])
by mail.nguyencongluc.online (Postfix) with ESMTP id BA422BD342
for <phoanhthonthu@gmail.com>; Wed, 26 Mar 2025 15:57:06 +0000 (UTC)
Date: Wed, 26 Mar 2025 15:57:06 +0000 (UTC)
From: User Master <master@nguyencongluc.online>
To: phoanhthonthu <phoanhthonthu@gmail.com>
Message-ID: <1712756762.202.1743004626446.JavaMail.zimbra@nguyencongluc.online>
Subject: Hi

- Trong "Statistics" > "Sender", sẽ thấy dữ liệu email gửi đi.



4.8 Thống kê và Báo cáo (Statistics and Reporting)

- Chức năng: PMG cung cấp báo cáo chi tiết về lưu lượng email, bao gồm số lượng spam, virus, email gửi/nhận.

- Đặc điểm nổi bật:

+Biểu đồ trực quan.

+Báo cáo tùy chỉnh qua email (HTML và plain-text).

-Hình ảnh gợi ý: Xem mục "Statistics" trong giao diện PMG, với các biểu đồ như "Mail Flow" hoặc "Spam Score Distribution".

