BÁO CÁO LAB 7

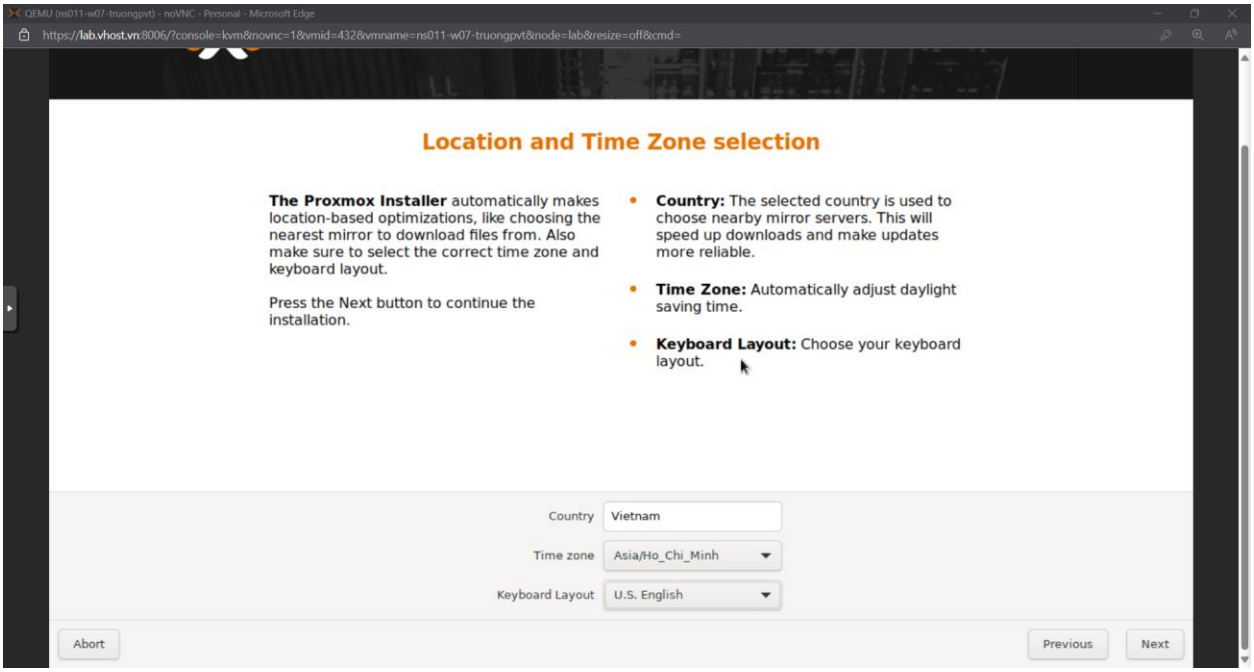
Sinh viên thực hiện	**Sinh viên 1** MSSV: Họ tên: Phan Võ Thiên Trường **Sinh viên 2** MSSV: Họ tên
Lớp	**NS011**
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc *(nếu là nhóm)*	**[Sinh viên 1]**: **[Sinh viên 2]**:
Link Video thực hiện *(nếu có yêu cầu)*	
Ý kiến *(nếu có)* *+ Khó khăn gặp phải* *+ Đề xuất, góp ý…*	
Điểm tự đánh giá *(bắt buộc)*	? /**10**

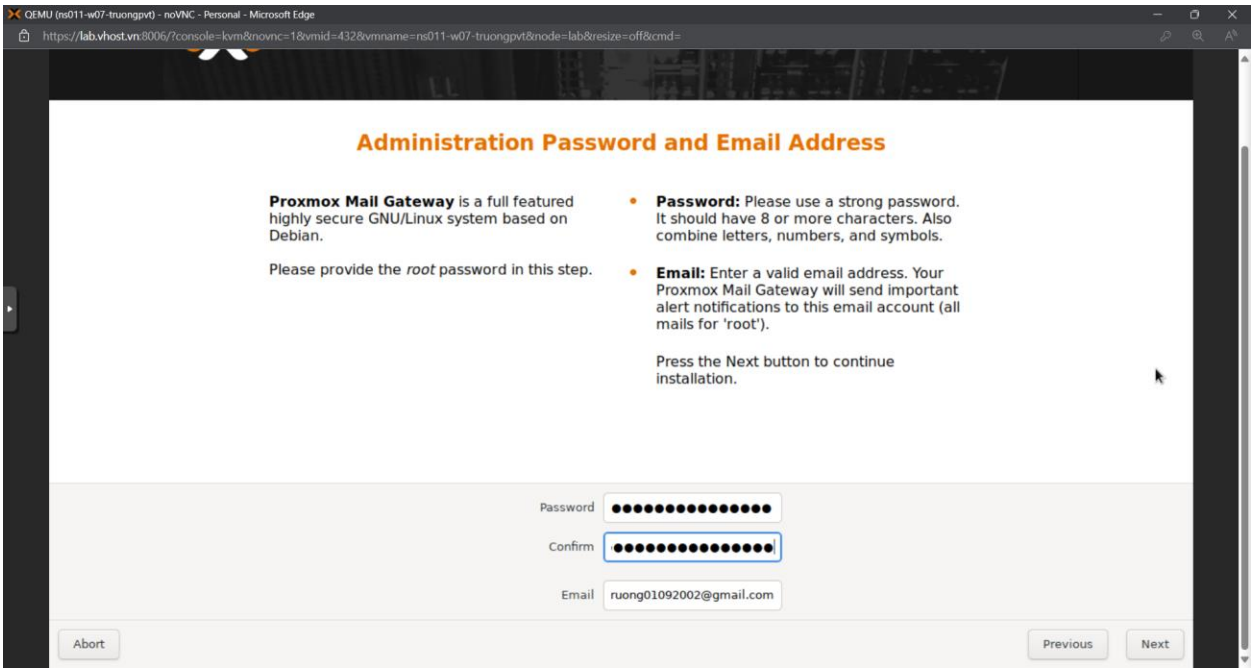
[Nội dung báo cáo chi tiết – Trình bày tùy sinh viên, Xuất file .PDF khi nộp]

- Request IP WAN từ leader.

Trung: 103.223.123.161
Giang: 103.232.123.166
Trường: 103.232.123.167
Kha: 103.232.123.168

Cài đặt Proxmox Mail Gateway lên VM tuần 7.

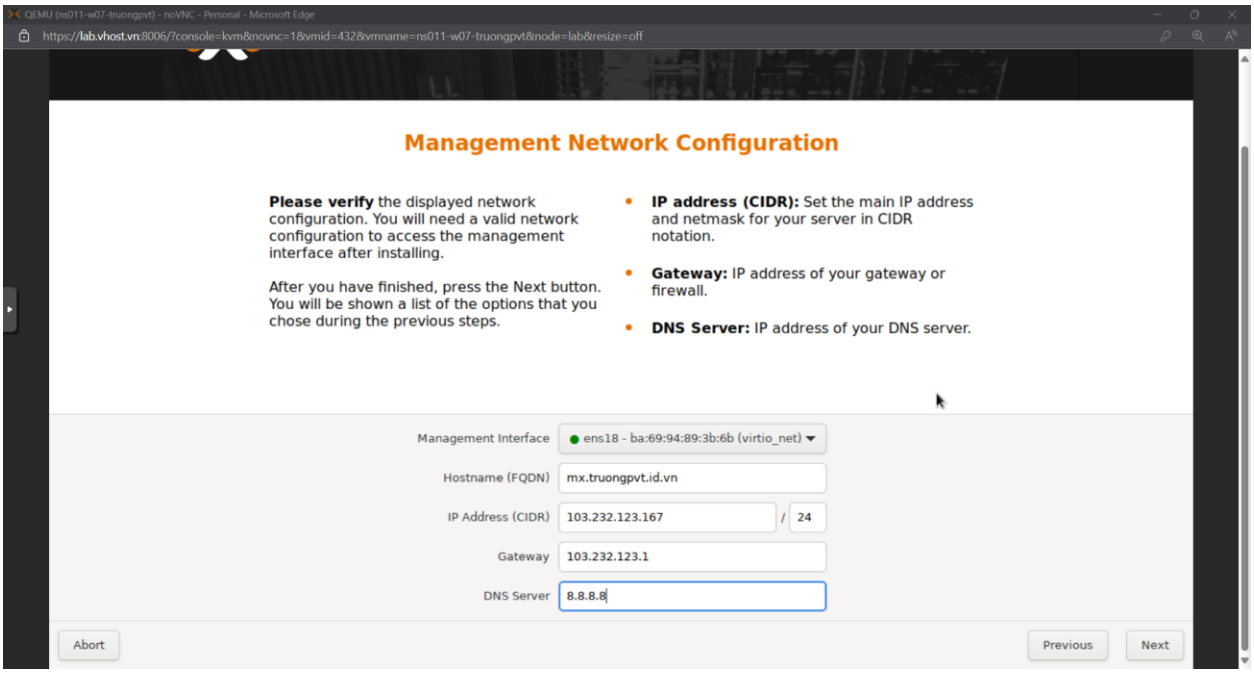


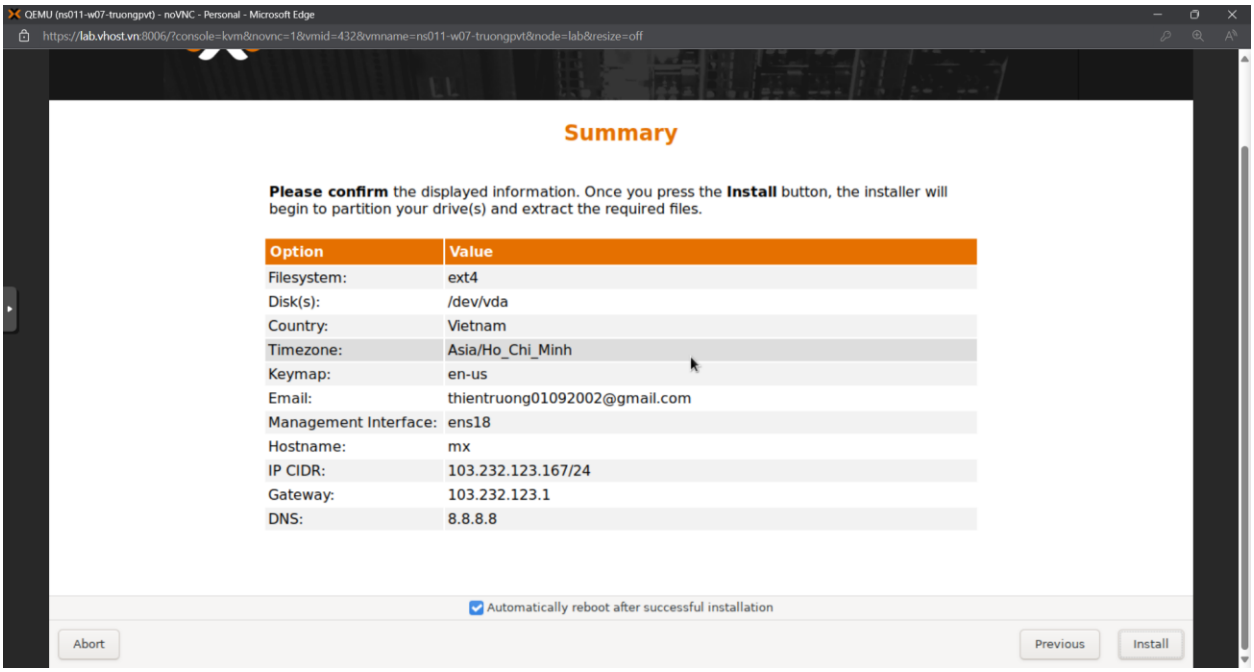


Password: LionEl'Johnson_!

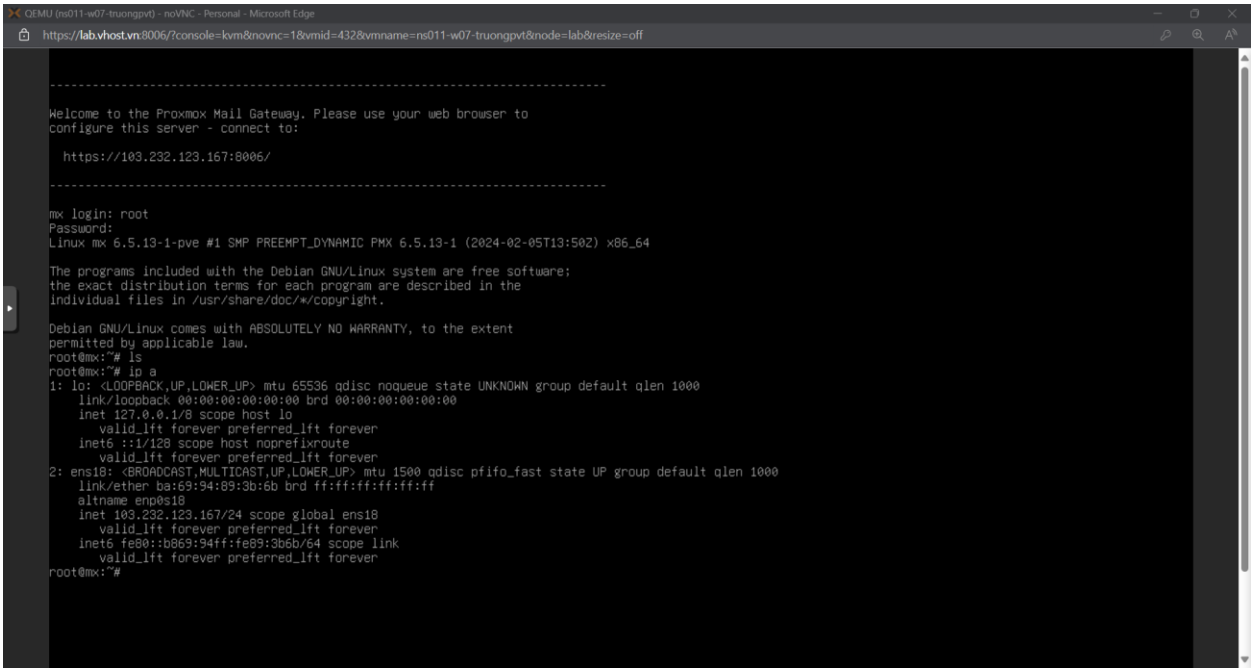
Thiết lập hostname là mx.domain và request mở port, PTR.

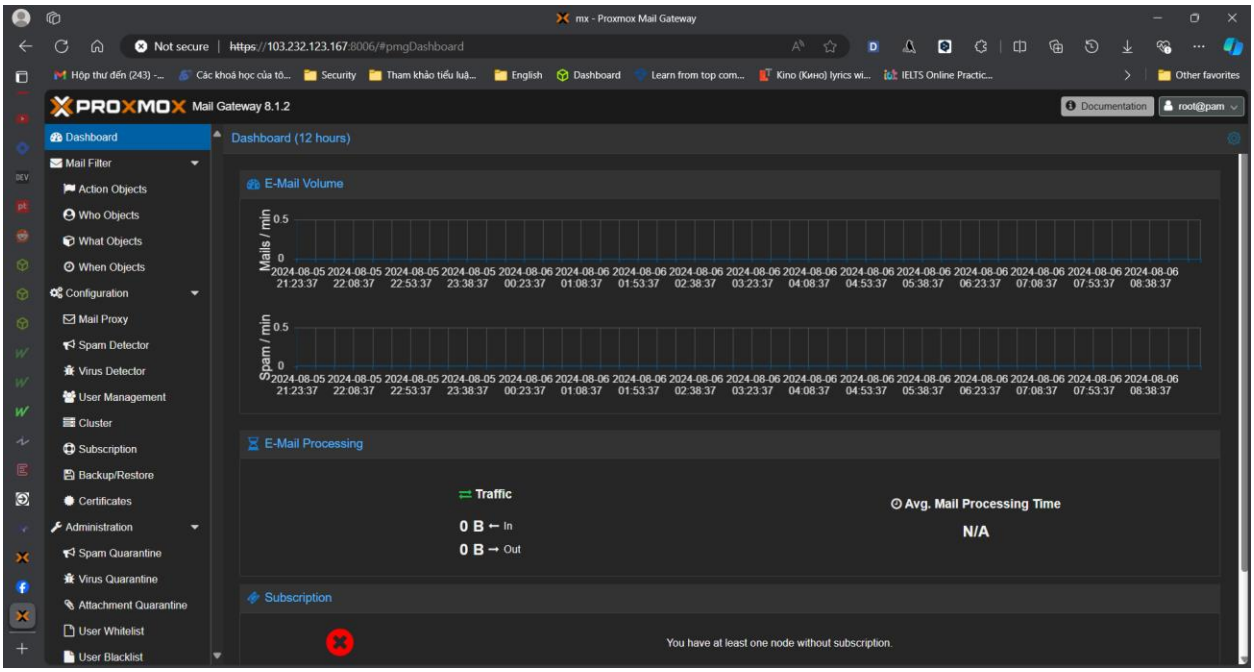
Hostname: mx.truongpvt.id.vn



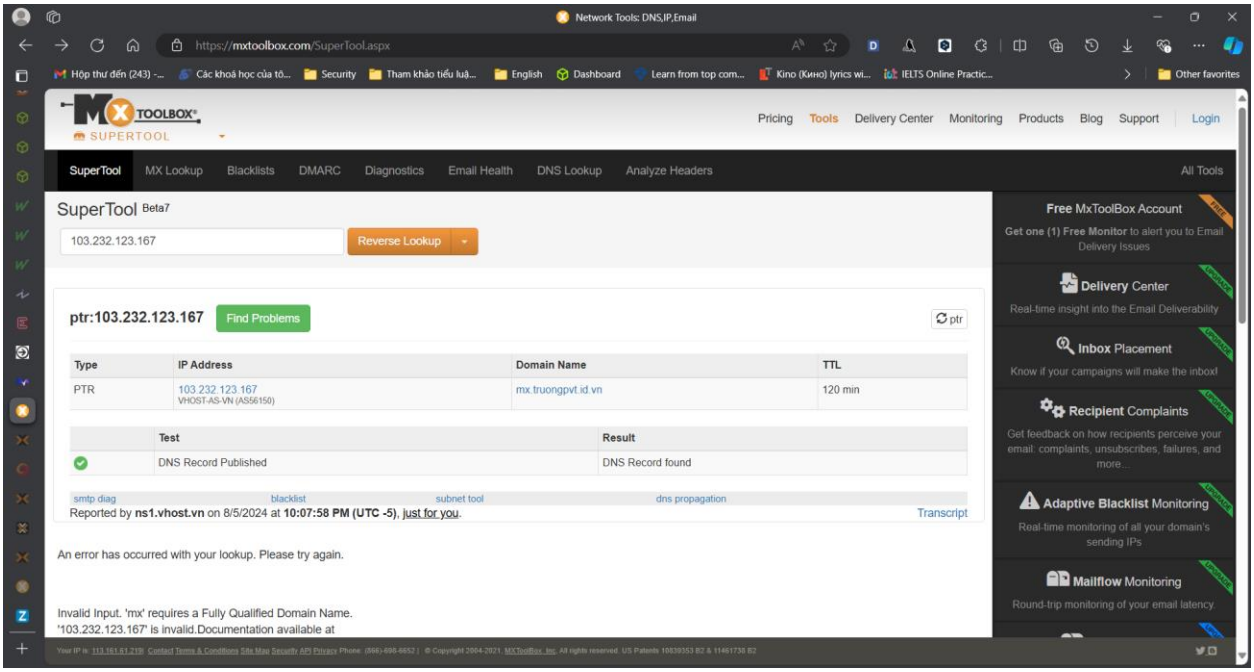


Cài đặt xong đăng nhập bằng user root và password đã tạo




mx - Proxmox Mail Gateway
Not secure | https://103.232.123.167:8006/#pmgDashboard
PROXMOX Mail Gateway 8.1.2
Documentation
root@pam
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
Dashboard (12 hours)
E-Mail Volume
Mails / min
Spam / min
E-Mail Processing
Traffic
0 B ← In
0 B → Out
Avg. Mail Processing Time
N/A
Subscription
You have at least one node without subscription.

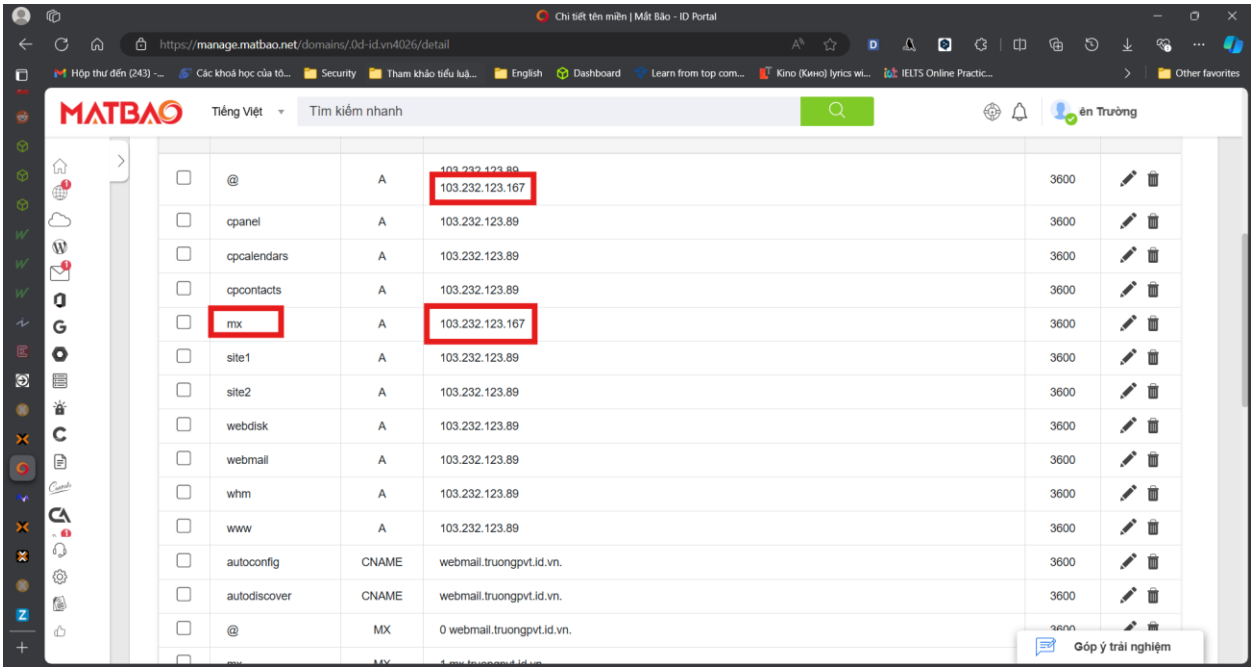
Request PTR

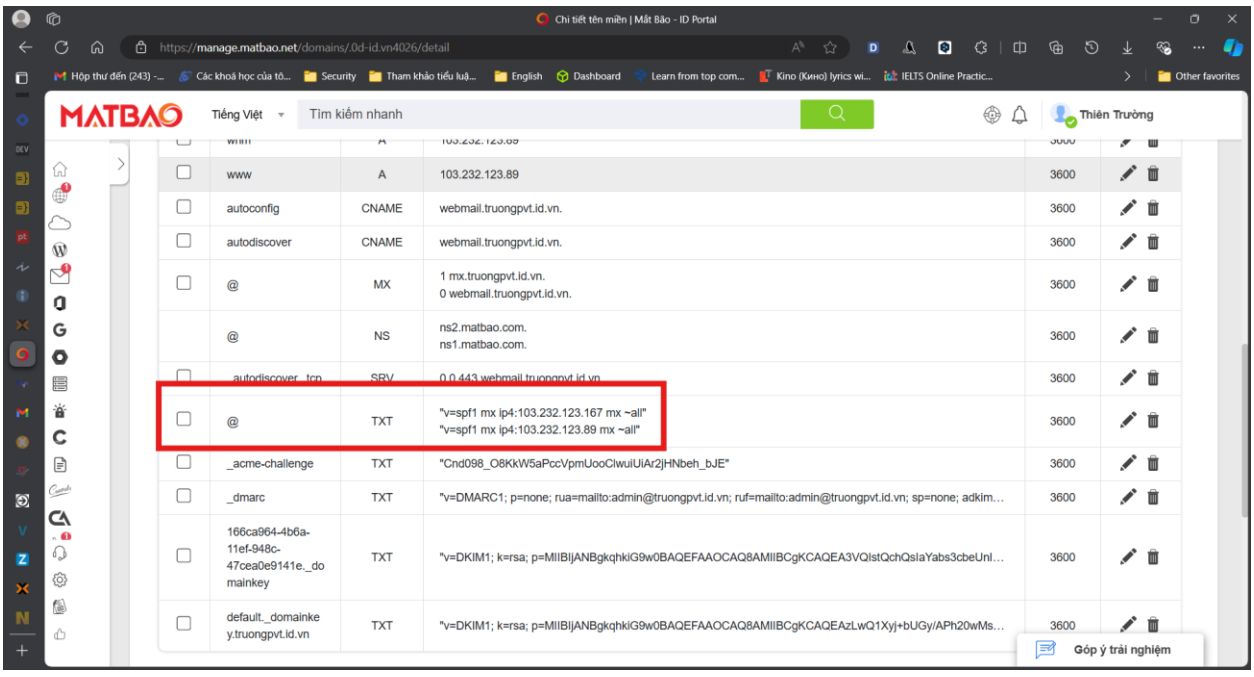

Network Tools: DNS,IP,Email
https://mxtoolbox.com/SuperTool.aspx
MX TOOLBOX SUPERTOOL
Pricing
Tools
Delivery Center
Monitoring
Products
Blog
Support
Login
SuperTool
MX Lookup
Blacklists
DMARC
Diagnostics
Email Health
DNS Lookup
Analyze Headers
All Tools
SuperTool Beta7
103.232.123.167
Reverse Lookup
ptr:103.232.123.167
Find Problems
Type
IP Address
Domain Name
TTL
PTR
103.232.123.167
VHOST-AS-VN (AS56150)
mx.truongpvt.id.vn
120 min
Test
Result
DNS Record Published
DNS Record found
smtp diag
blacklist
subnet tool
dns propagation
Reported by ns1.vhost.vn on 8/5/2024 at 10:07:58 PM (UTC -5), just for you.
Transcript
An error has occurred with your lookup. Please try again.
Invalid Input. 'mx' requires a Fully Qualified Domain Name.
'103.232.123.167' is invalid.Documentation available at
Free MxToolBox Account
Get one (1) Free Monitor to alert you to Email Delivery Issues
Delivery Center
Real-time insight into the Email Deliverability
Inbox Placement
Know if your campaigns will make the inbox!
Recipient Complaints
Get feedback on how recipients perceive your email: complaints, unsubscribes, failures, and more...
Adaptive Blacklist Monitoring
Real-time monitoring of all your domain's sending IPs
Mailflow Monitoring
Round-trip monitoring of your email latency

Cấu hình toàn bộ hệ thống email từ server Email Server của tuần 5 gửi và nhận email qua hệ thống PMG này.

Đầu tiên em cấu hình thêm vào bản ghi DNS trên domain:

- MX A 103.232.123.167
- @ A 103.232.123.167
- MX MX mx.truongpvt.id.vn

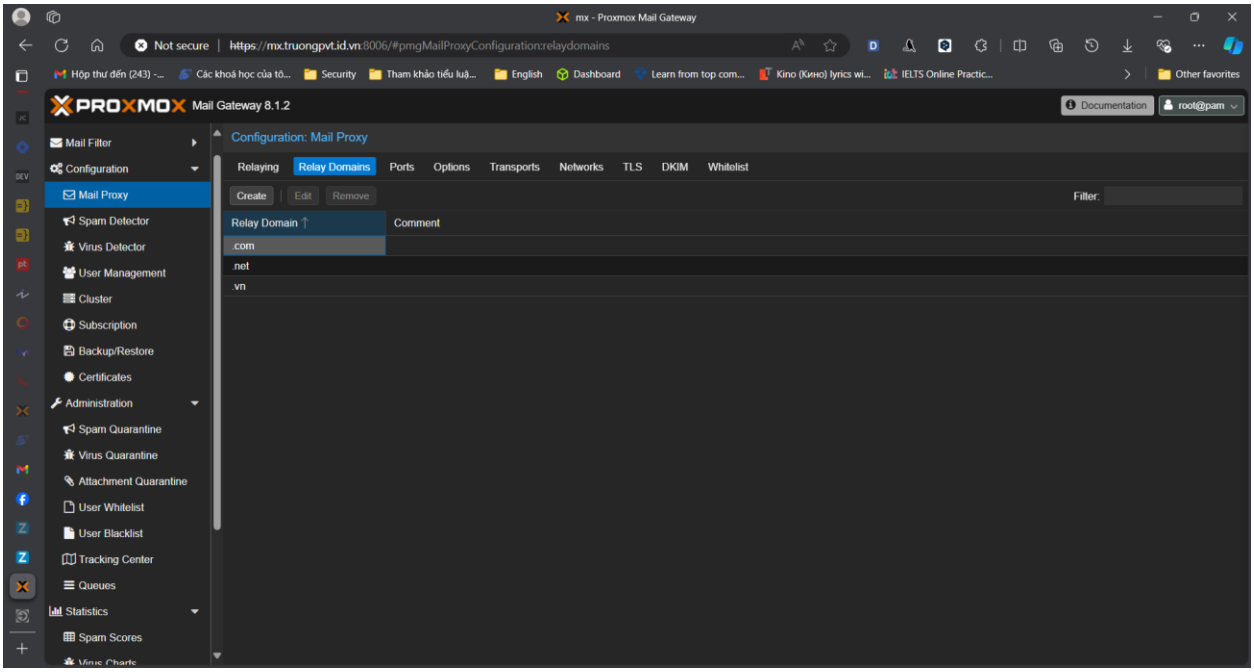


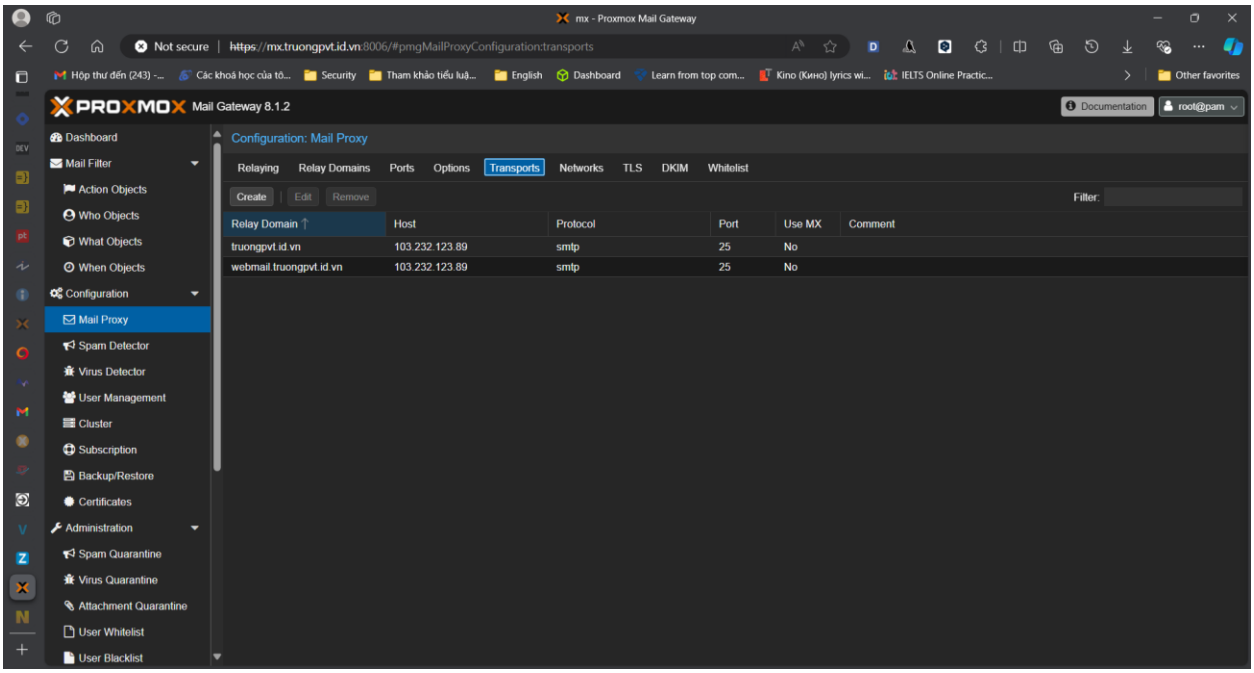


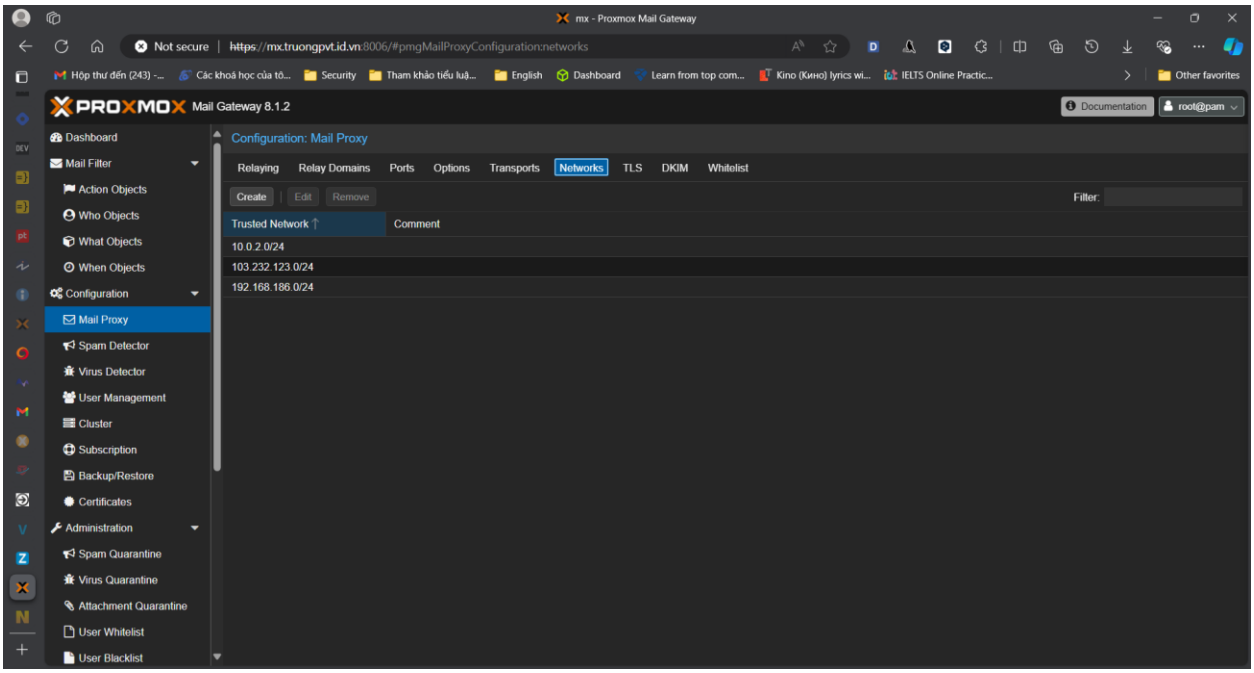
Tiếp đến em cấu hình trên PMG thêm vào relay domain và transport

Relay domain dùng để xét mail từ bên ngoài vào

Transports ngược lại từ trong ra.



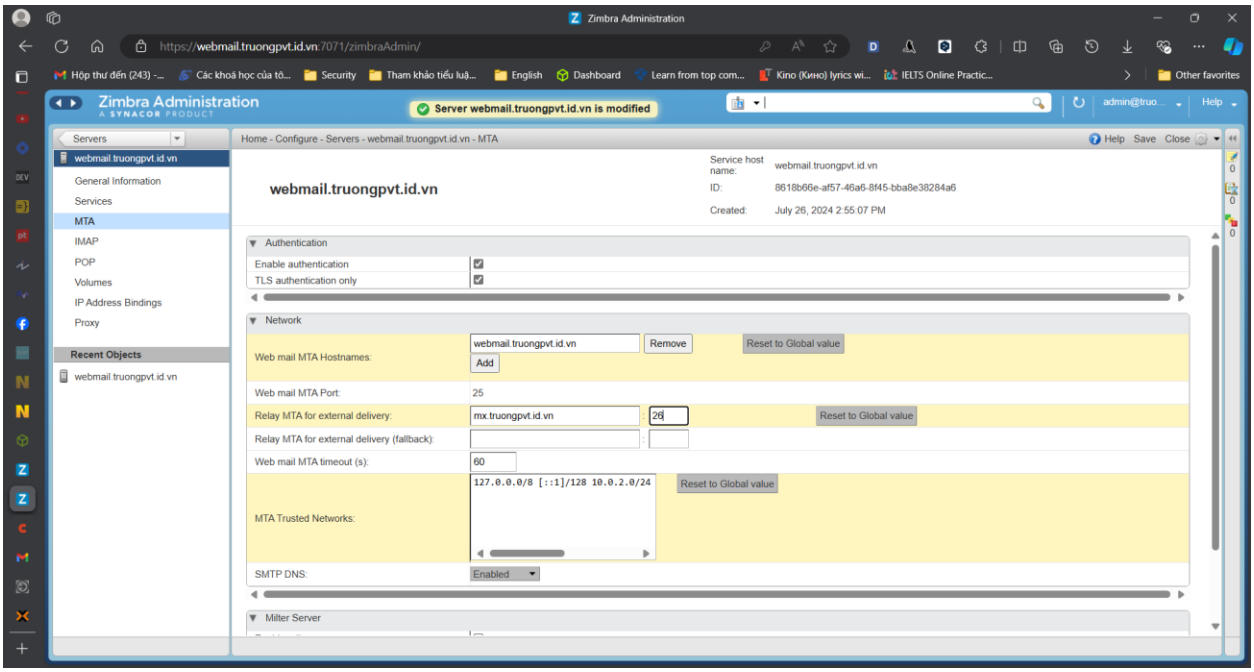


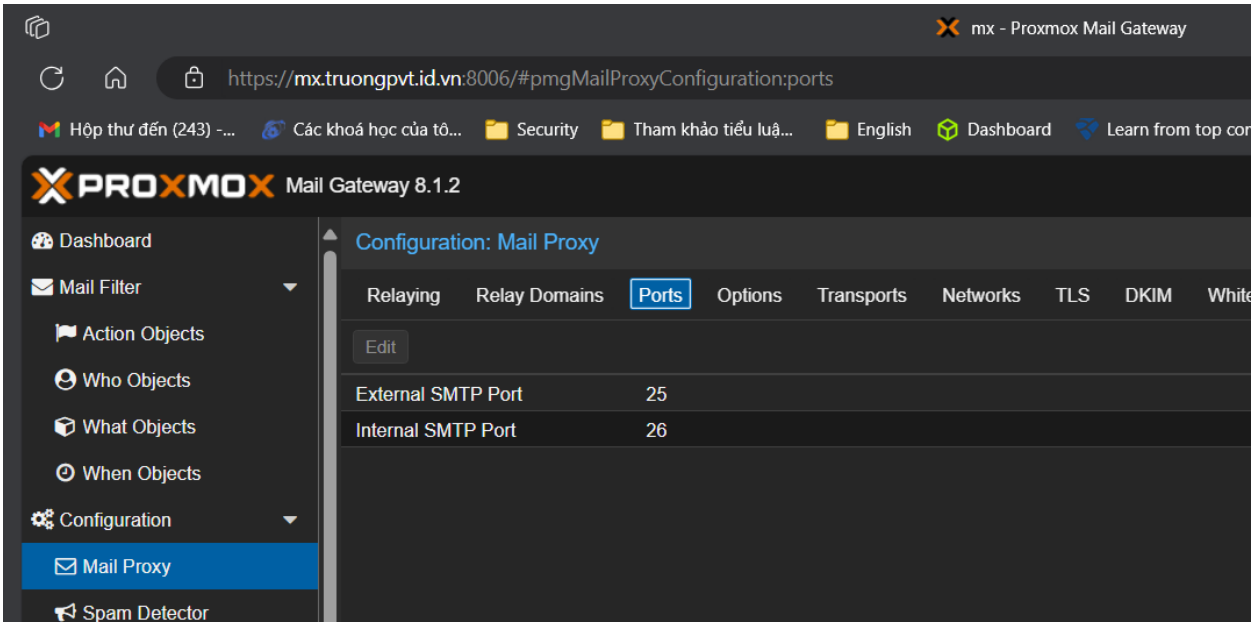


Tiếp theo em cấu hình cho zimbra để nó nhận relay PMG của proxmox theo link: [Hướng dẫn cấu hình Relay Email với Zimbra Mail Server các phiên bản sau 8.0 (vhost.vn)]

```
zmprov ms webmail.truongpvt.id.vn zimbraMtaRelayHost mx.truongpvt.id.vn:25
echo mx. truongpvt.id.vn “truongpvt:LionEl’Johnson_!” >/opt/zimbra/conf/relay_password
postmap /opt/zimbra/conf/relay_password
postmap -q mx.truongpvt.id.vn /opt/zimbra/conf/relay_password
zmprov ms webmail.truongpvt.id.vn zimbraMtaSmtpSaslPasswordMaps
lmdb:/opt/zimbra/conf/relay_password
zmprov ms webmail.truongpvt.id.vn zimbraMtaSmtpSaslAuthEnable yes
zmprov ms webmail.truongpvt.id.vn zimbraMtaSmtpCnameOverridesServername no
zmprov ms webmail.truongpvt.id.vn zimbraMtaSmtpTlsSecurityLevel may
zmprov ms webmail.truongpvt.id.vn zimbraMtaSmtpSaslSecurityOptions noanonymous
```

Vì trong promox có cấu hình để port External SMTP là 25 còn Internal SMTP là 26 nên em sẽ cấu hình MTA của zimbra là port 26



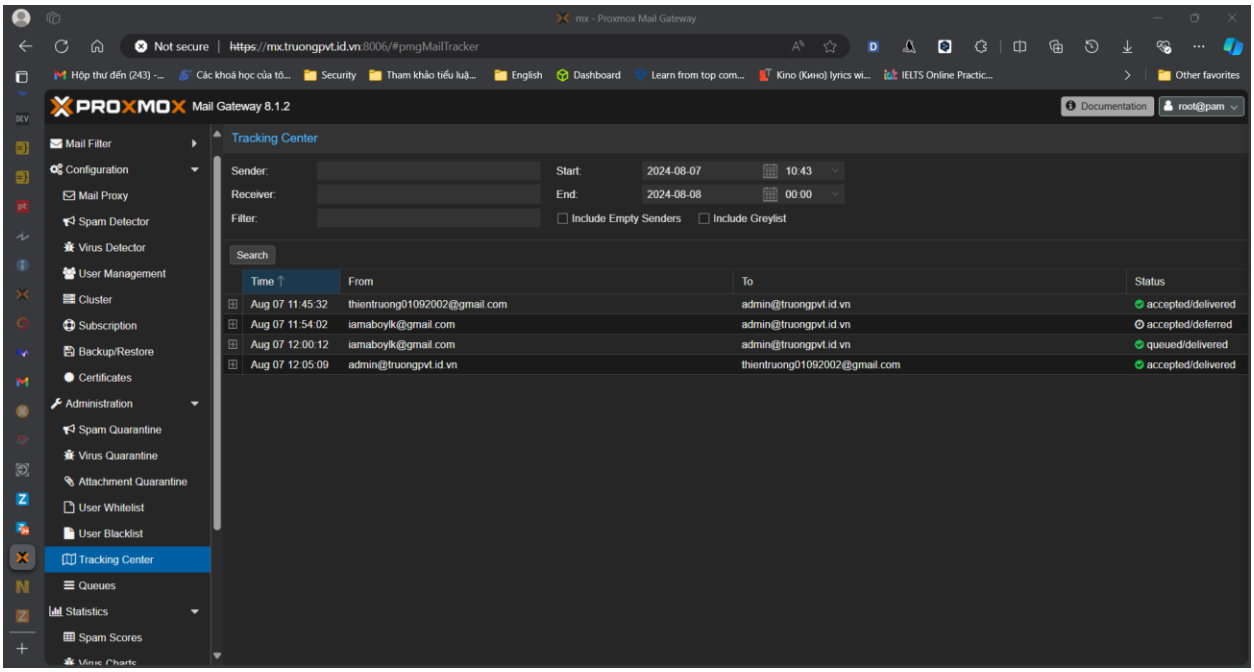


Xong khởi động lại service của zimbra:

```
zmcontrol restart
```

Cuối cùng

- Test gửi mail từ ngoài vào zimbra và ngoài vào trong. Sau đó kiểm tra trên tracking center kiểm tra kết nối



Cấu hình SSL cho PMG và port mail.

Cách 1:

Theo link dưới0

[HOW TO INSTALL SSL LETSENCRYPT IN PROXMOX MAIL GATEWAY 7.3.1 (origrata.com)]

Vì ở đây em sẽ ký trên hệ thống thông qua certbot thay vì Certificates function trên proxmox nên em cần cài nginx

```
apt install nginx -y
```

sau đó tạo file pmg và thêm vào đoạn script

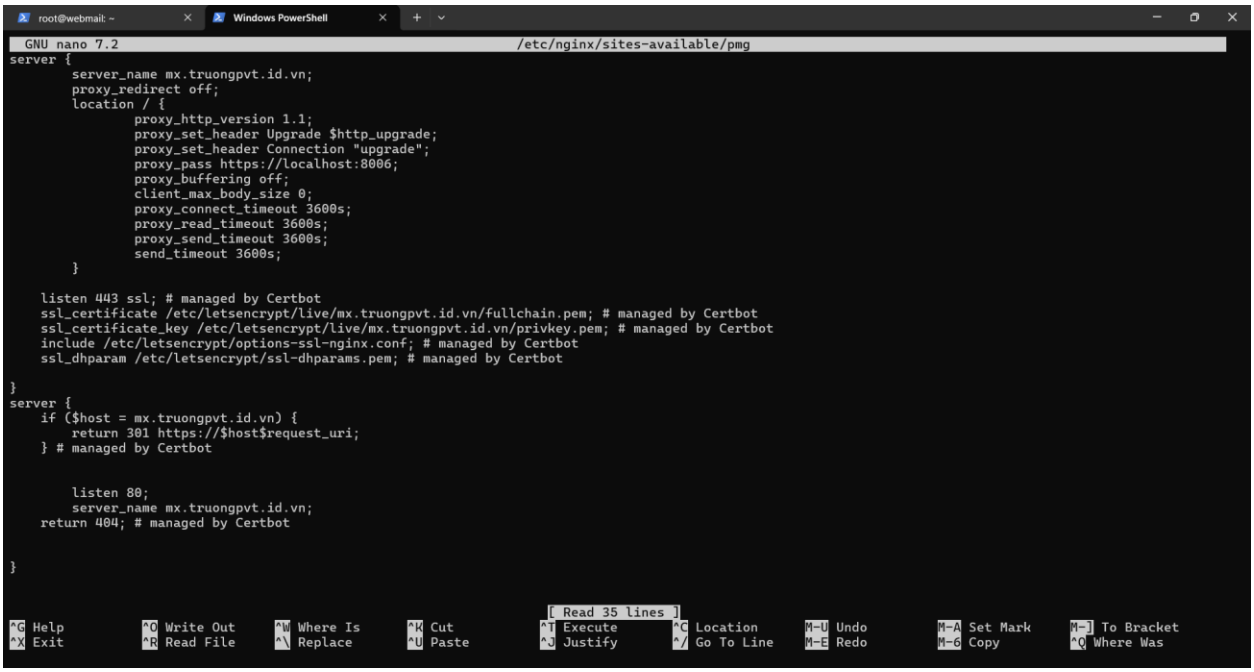
```
server {
        listen 80;
        server_name mx.truongpvt.id.vn;
        proxy_redirect off;
        location / {
                proxy_http_version 1.1;
```

```
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_pass https://localhost:8006;
        proxy_buffering off;
        client_max_body_size 0;
        proxy_connect_timeout 3600s;
        proxy_read_timeout 3600s;
        proxy_send_timeout 3600s;
        send_timeout 3600s;
    }
}
```

Sau đó chạy dòng lệnh dưới để link giữa /etc/nginx/site-availabe/pmg và /etc/nginx/site-enabled/pmg. Sau đó restart lại nginx

```
ln -s /etc/nginx/sites-available/pmg   /etc/nginx/sites-enabled/pmg
systemctl reload nginx
```

1. **ln**: Đây là lệnh để tạo liên kết (link) trong Linux.
2. **-s**: Đây là một option cho lệnh **ln**, nó chỉ định rằng chúng ta muốn tạo một symbolic link (symlink) thay vì hard link.

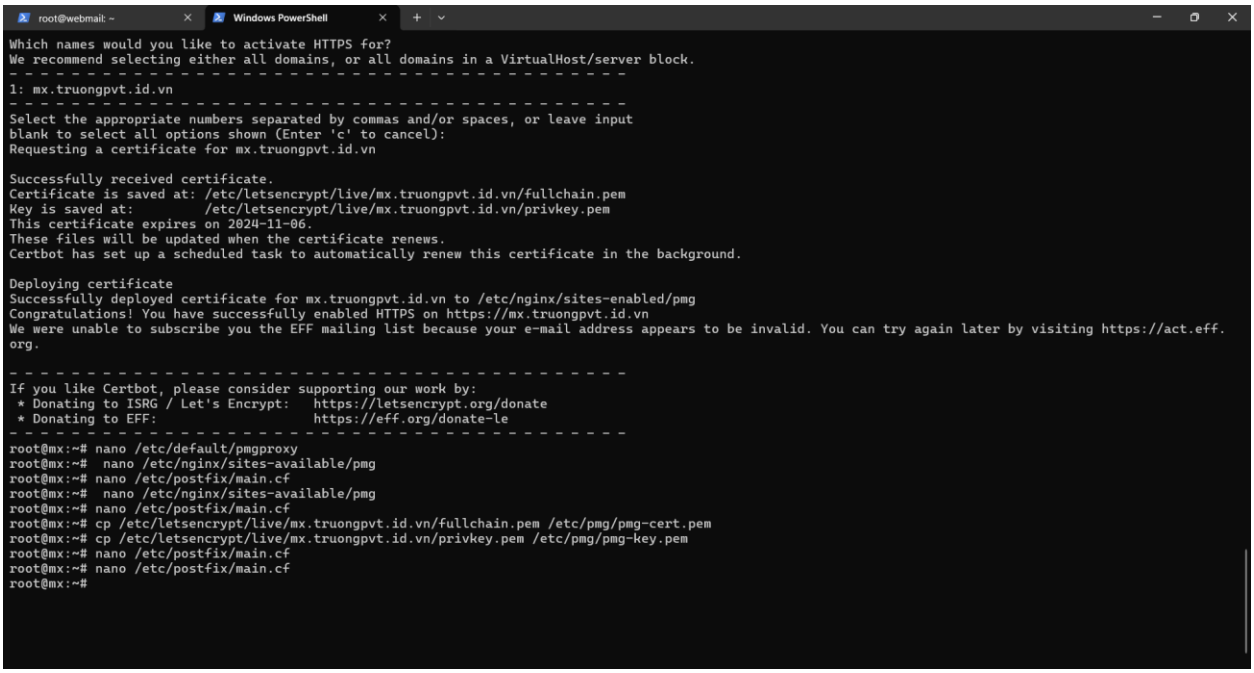


Chỉnh thêm file pmgproxy “LISTEN_IP=127.0.0.1” và restart nó

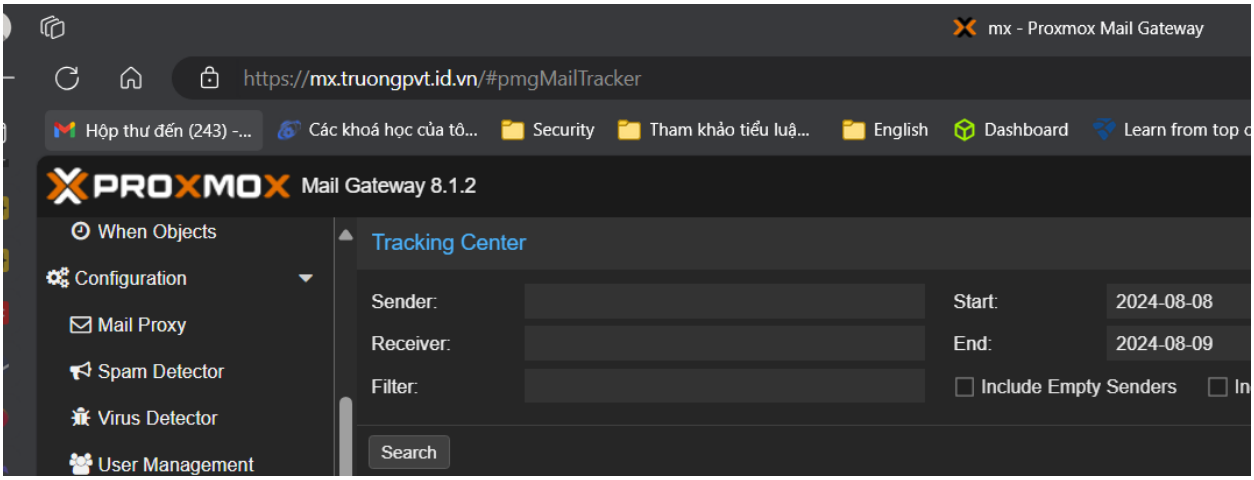
```
nano /etc/default/pmgproxy

sudo systemctl restart
```

Tiếp tới tiến hành ký SSL,

```
apt install -y certbot python3-certbot-nginx
```

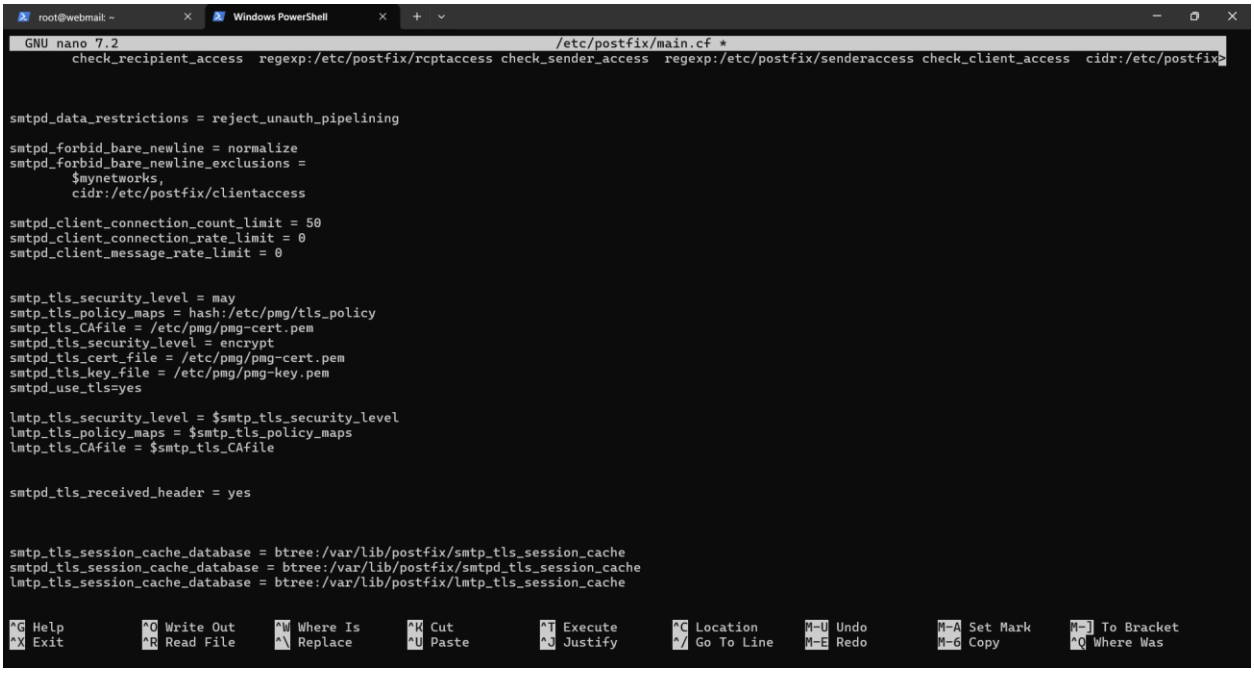


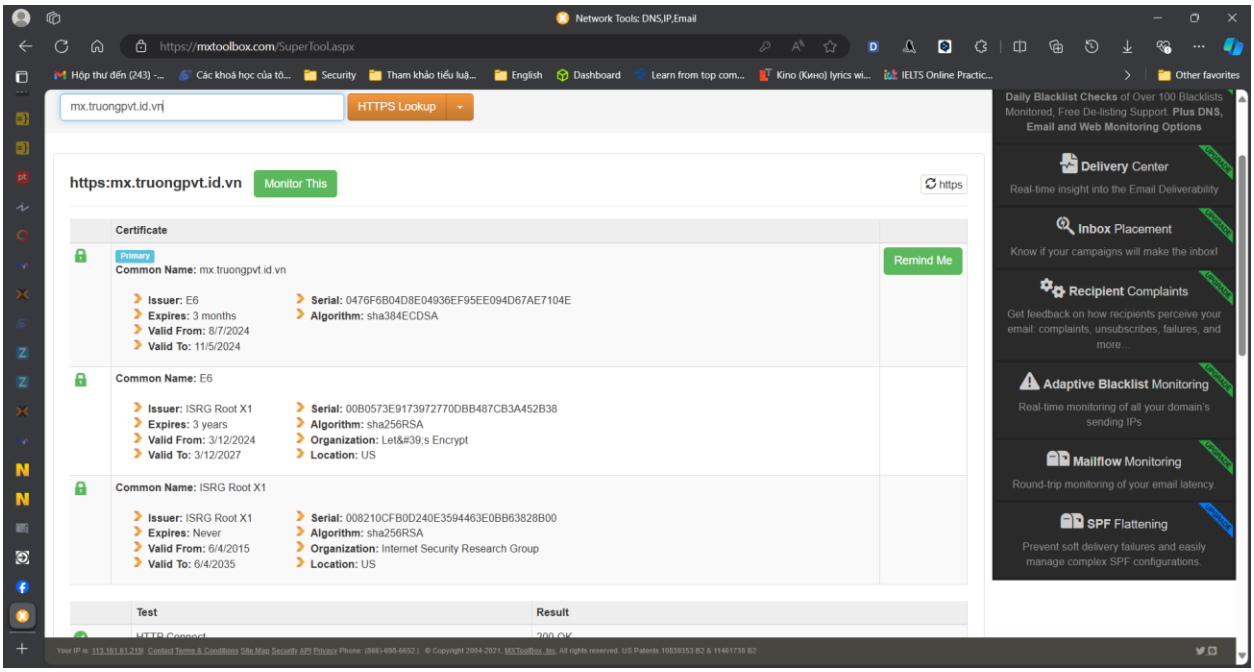
Sau khi ký xong có thể vào URL mx.truongpvt.id.vn mà không cần nhập port và có SSL



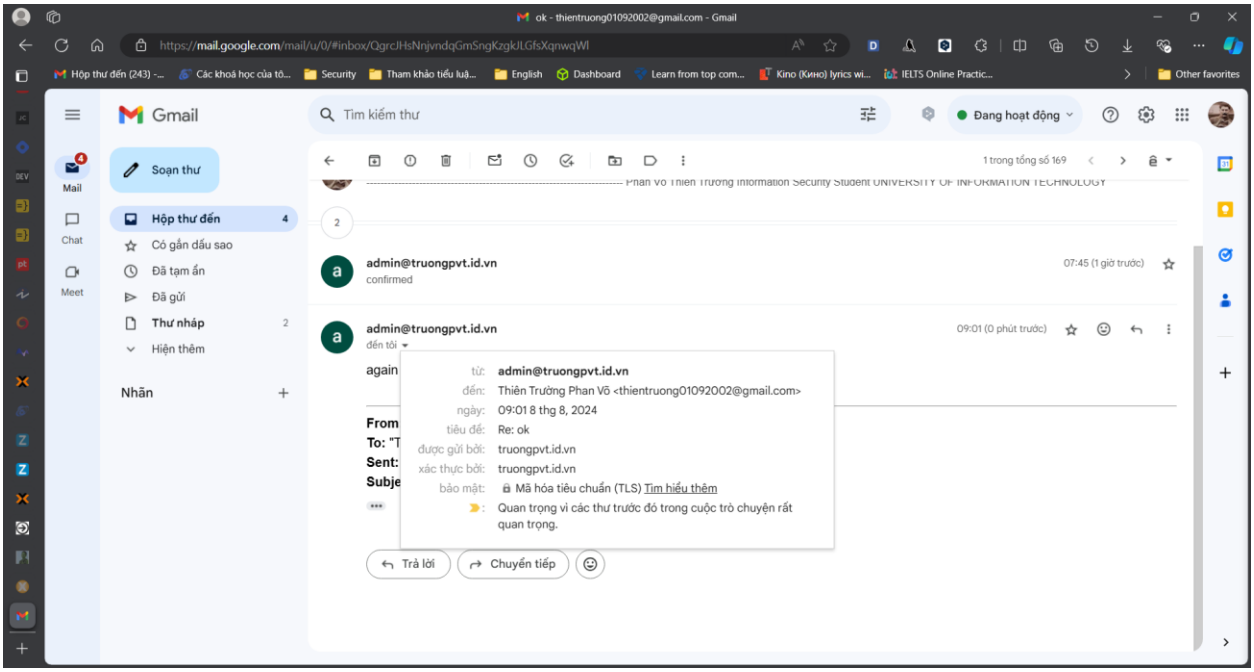
Để tls email khi gửi, em copy key và cert vừa tạo được vào pmg, bật tính năng TLS trên giao diện PMG, đồng thời chỉnh sửa file /etc/postfix/main.cf để trỏ đến key và cert mới. Sau đó restart lại postfix

```
systemctl restart postfix
```



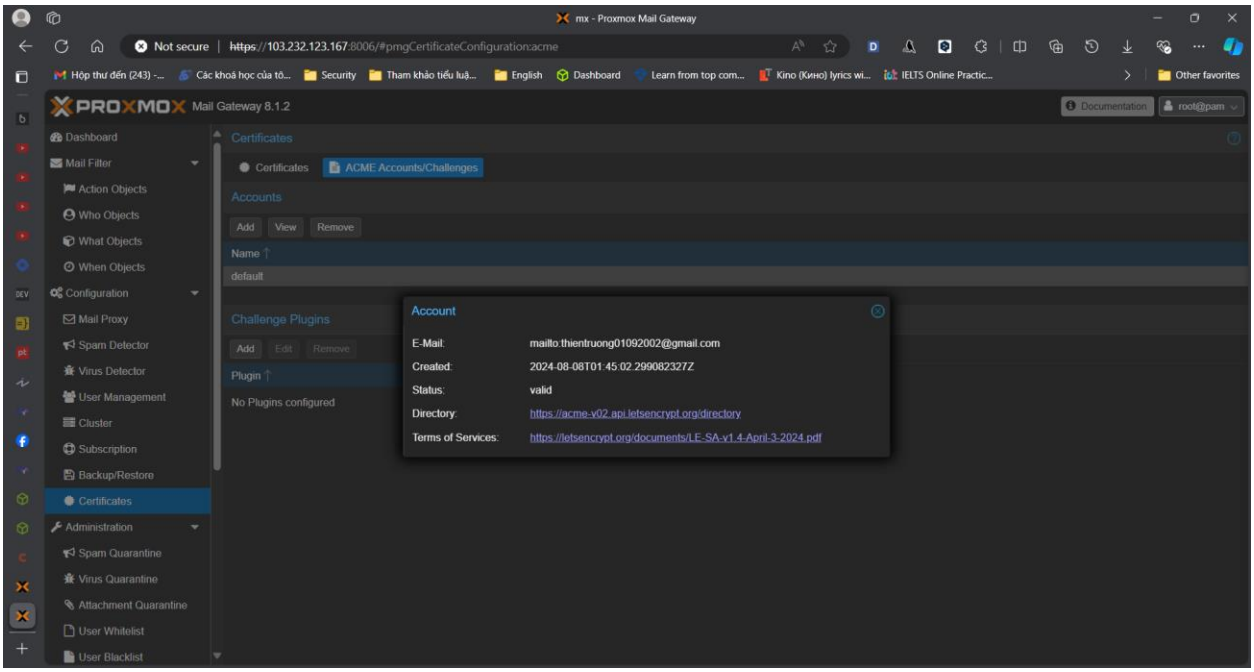


Kiểm tra kết quả thông qua việc gửi lại mail từ zimbra

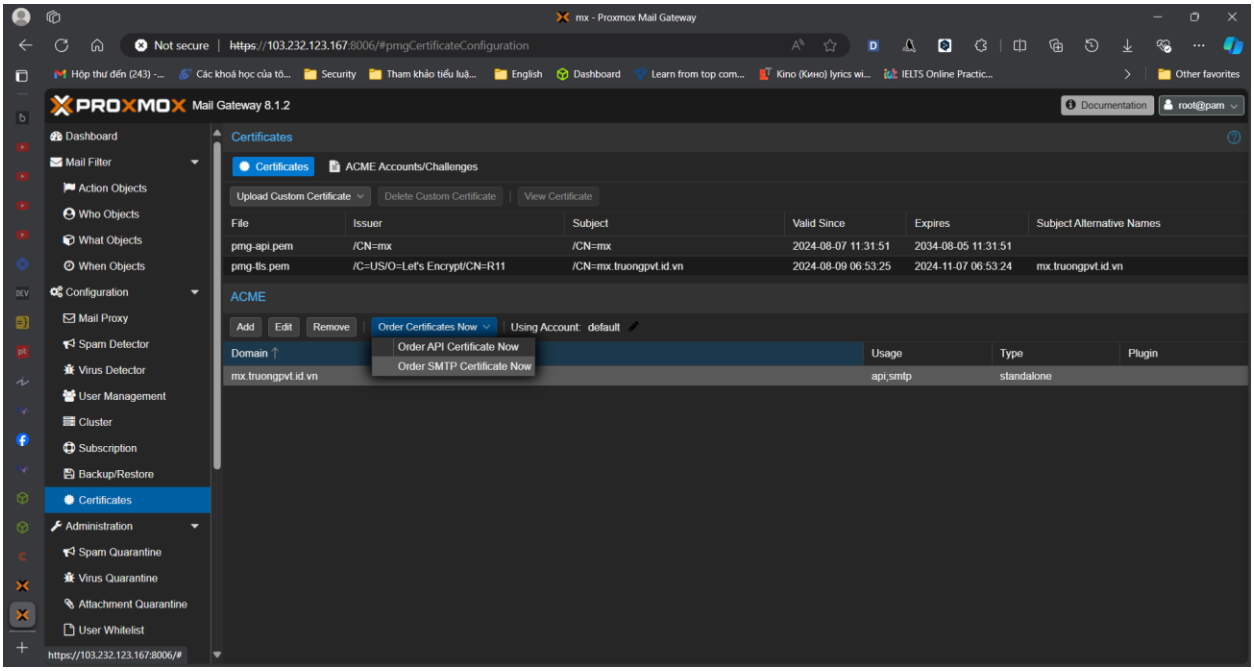


Có cách thứ 2

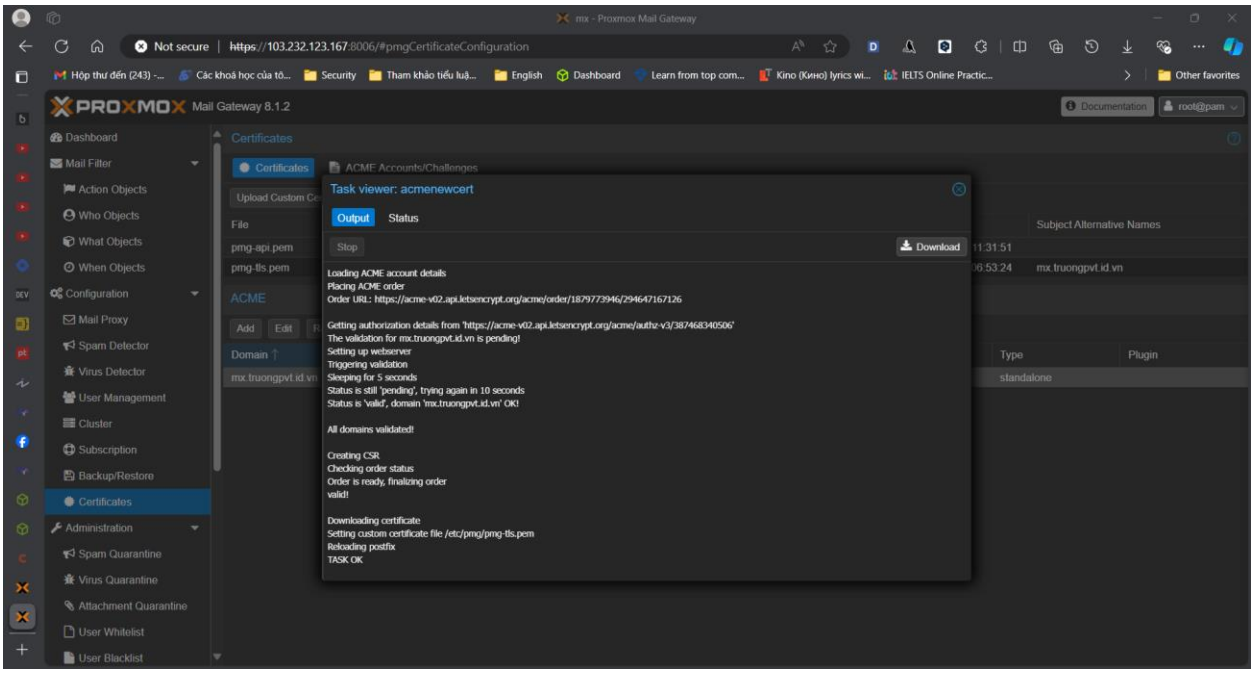
Thay vì cài SSL trên máy có thể xử dụng Certificate function trên proxmox. Đầu tiên cần tạo account ACME.



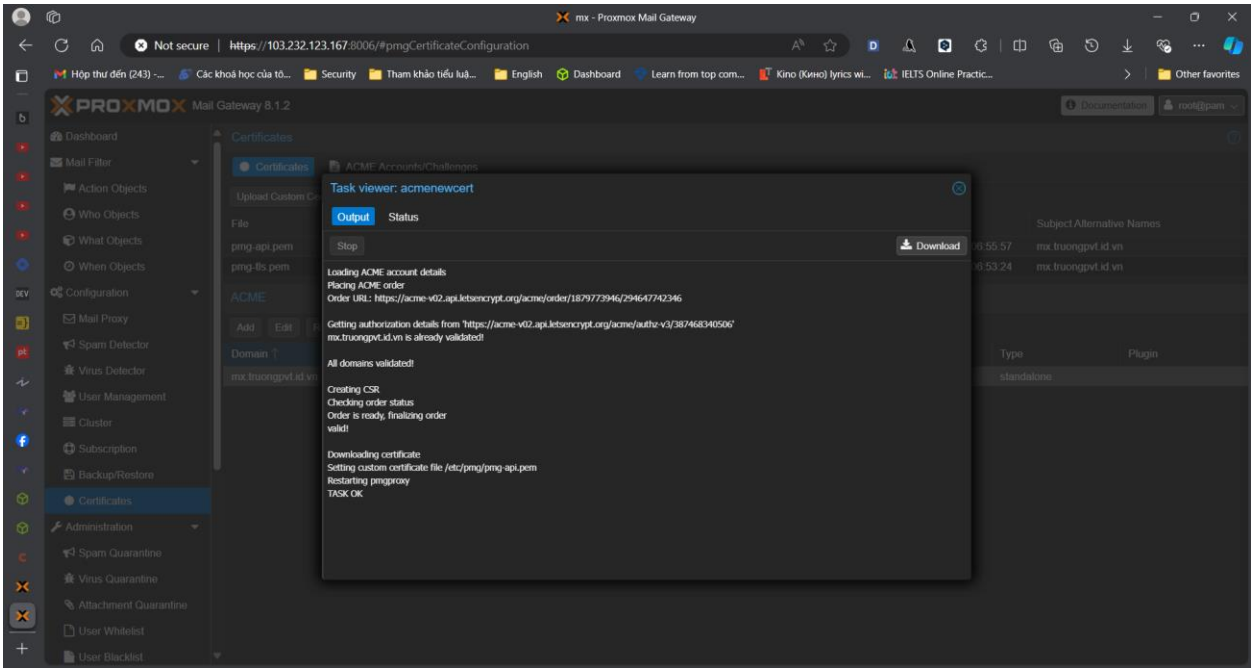
Tiếp theo em thêm vào tên miền mx.truongpvt.id.vn trong tab Certificates kế bên và tiến hành Order Certificates ở cả API và SMTP



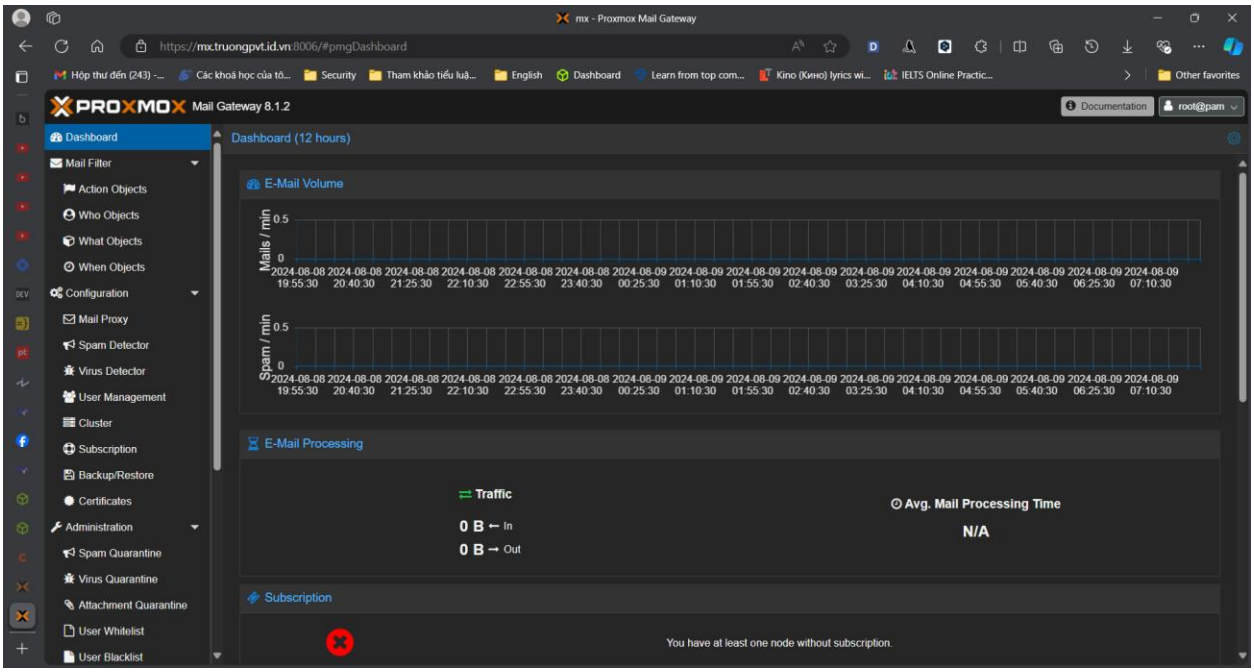
SMTP



API

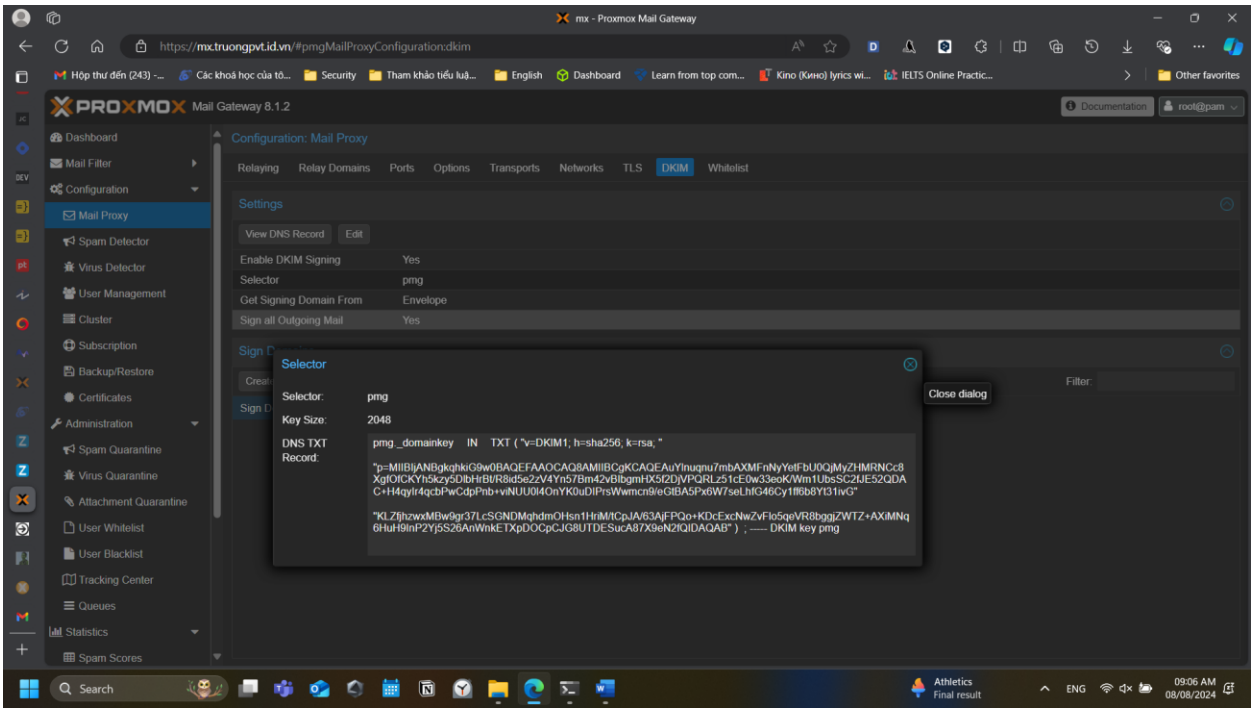


Kết quả hoàn thành nhưng ở đây cần có thêm port 8006

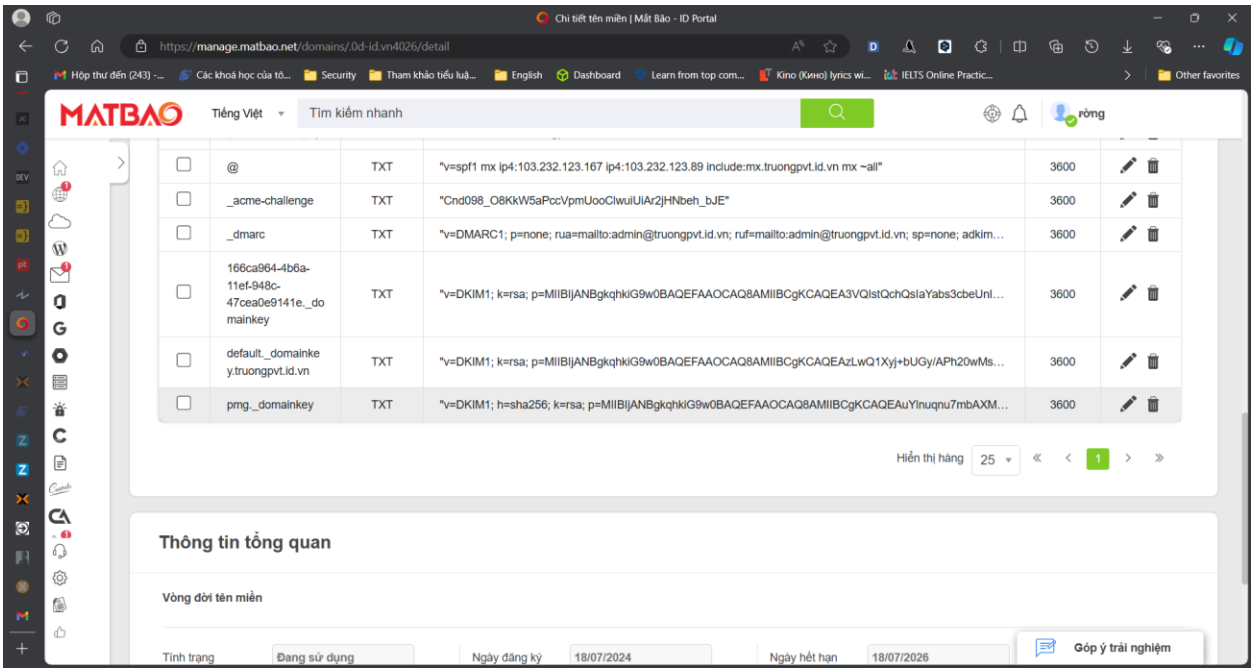


Đảm bảo SPF, DKIM, DMARC valid cho email khi gửi ra.

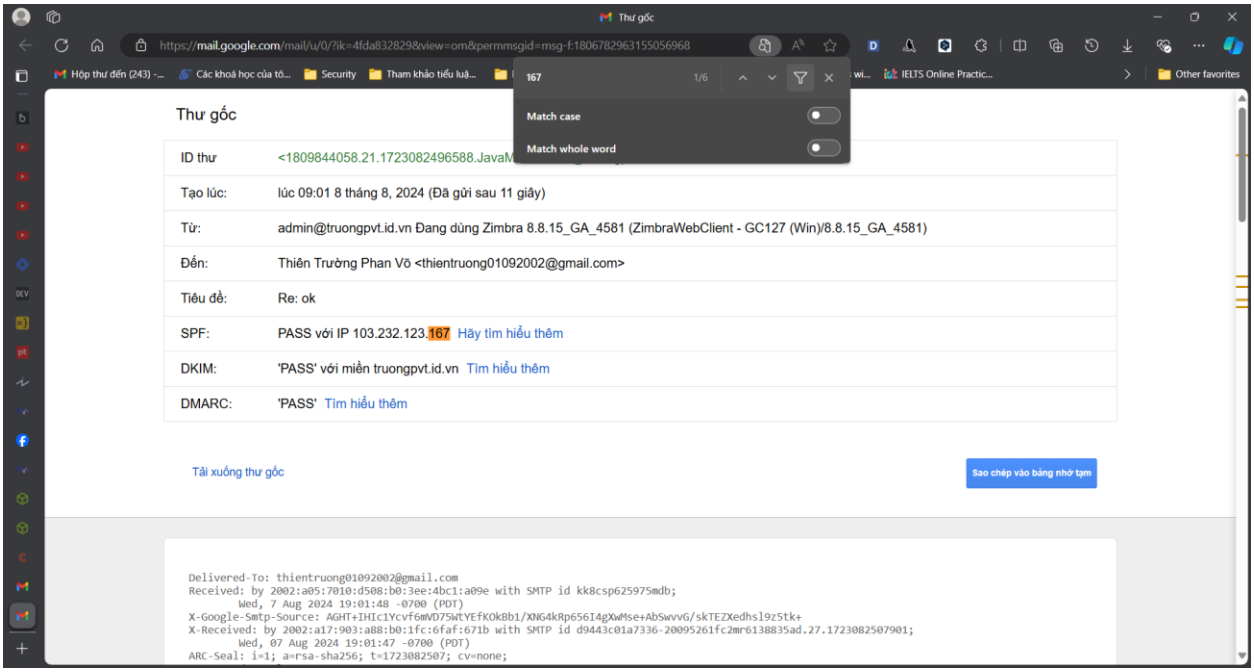
DKIM

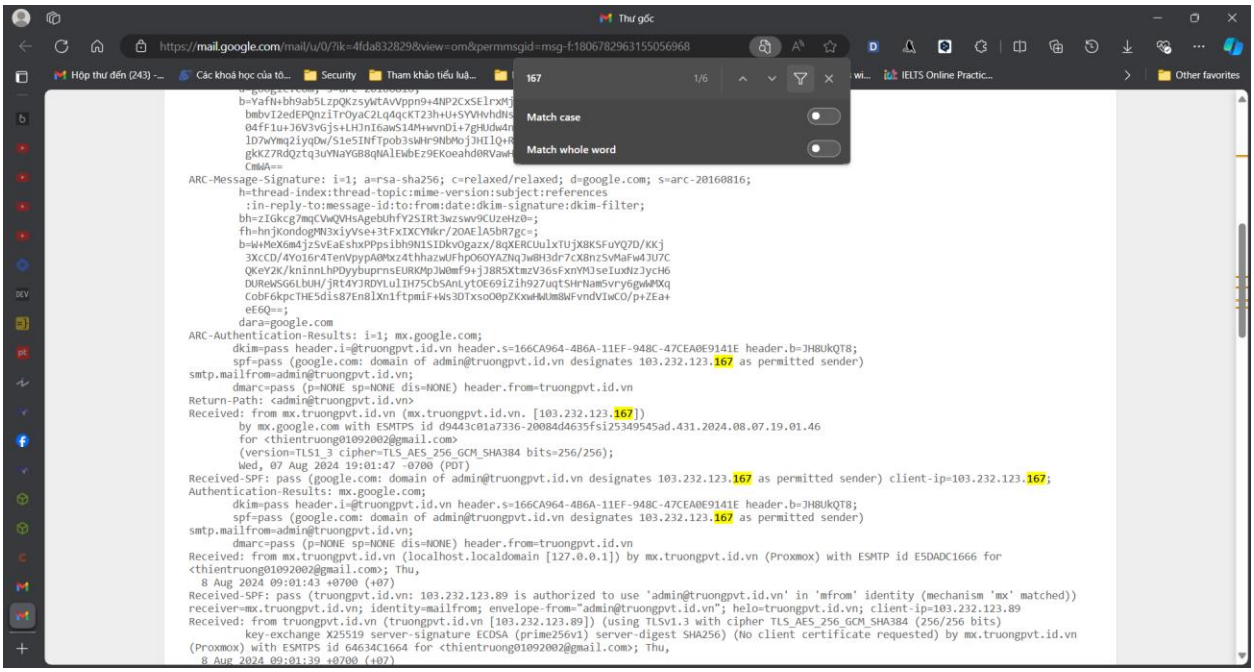


Thêm vào bản ghi DNS của domain



Kiểm tra file gửi từ zimbra đi qua proxmox



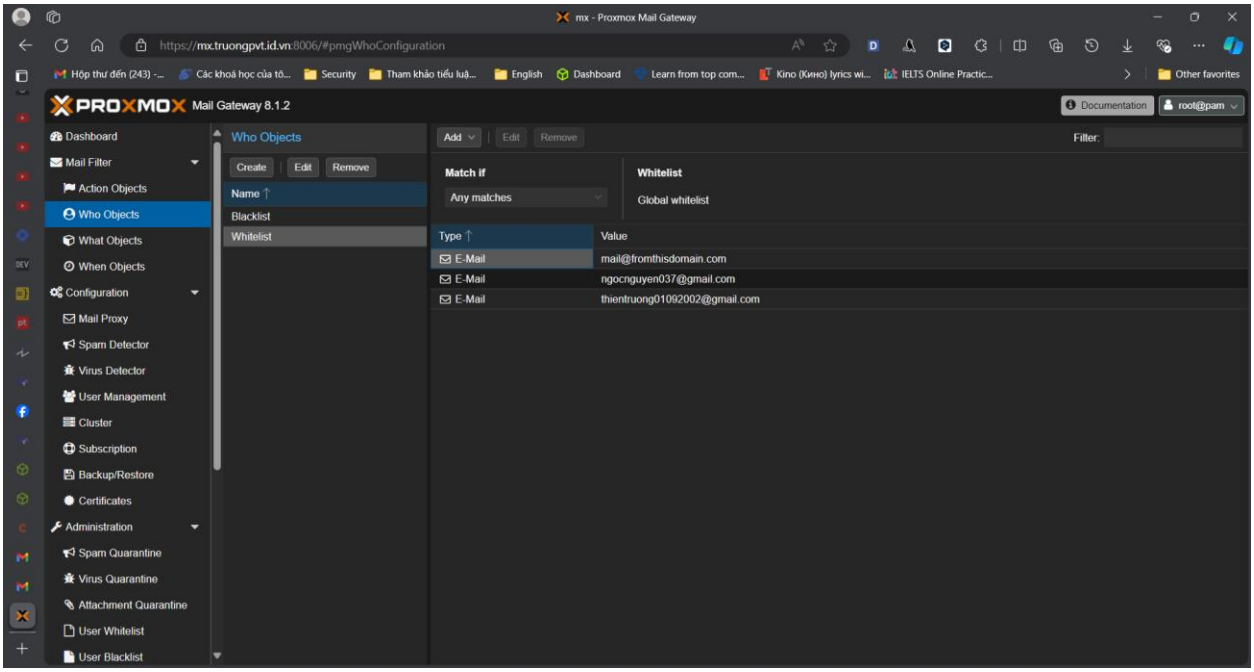


Cấu hình whitelist và blacklist, đảm bảo cho user dưới đây gửi vào (whitelist), block (blacklist) được hệ thống:

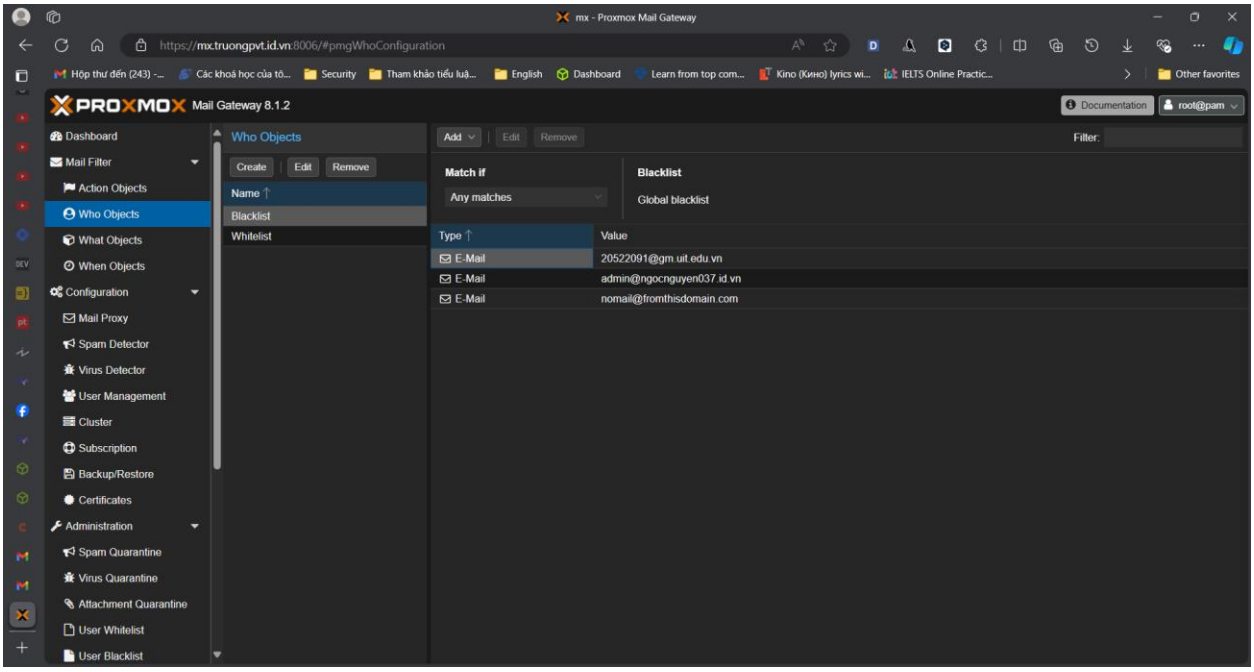
Whitelist: ngocnguyen037@gmail.com

Blacklist: admin@ngocnguyen037.id.vn

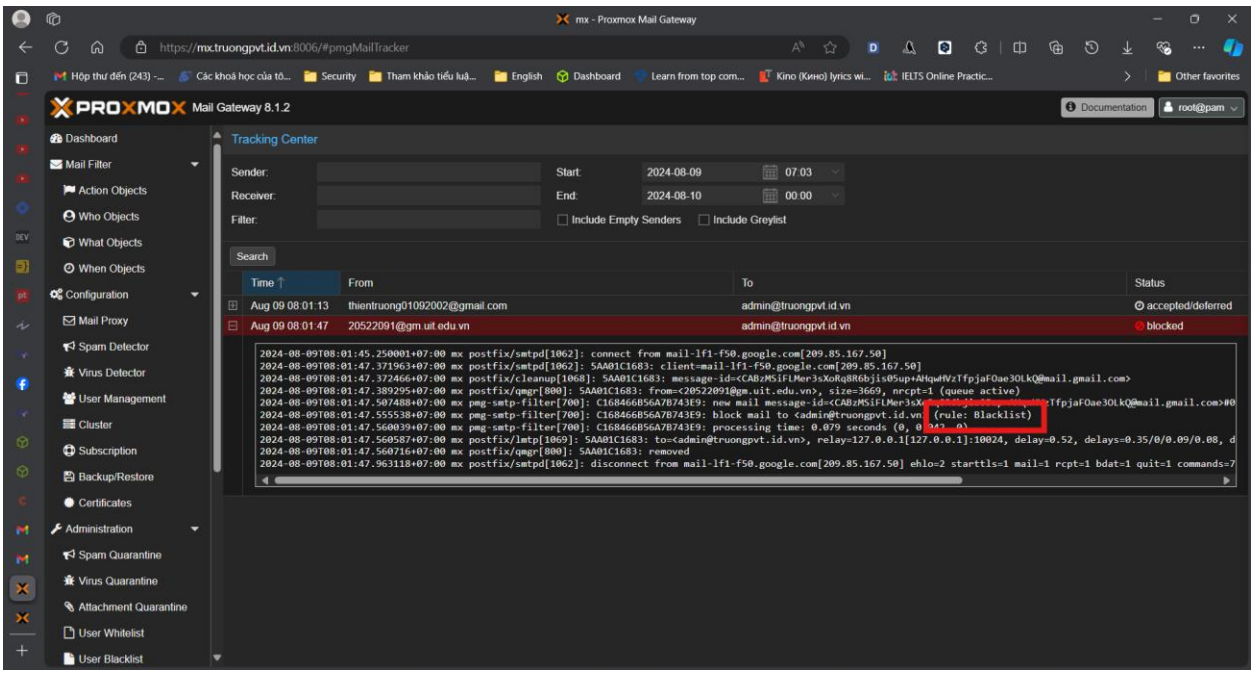
Whitelist

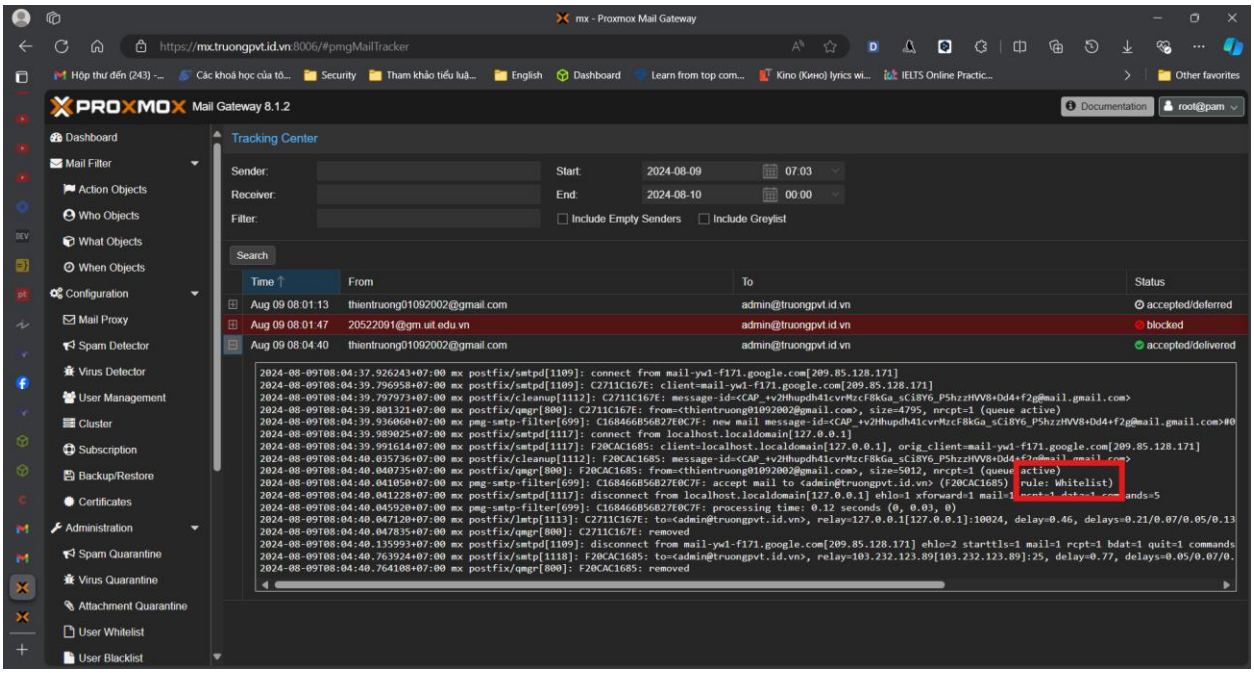


Blacklist



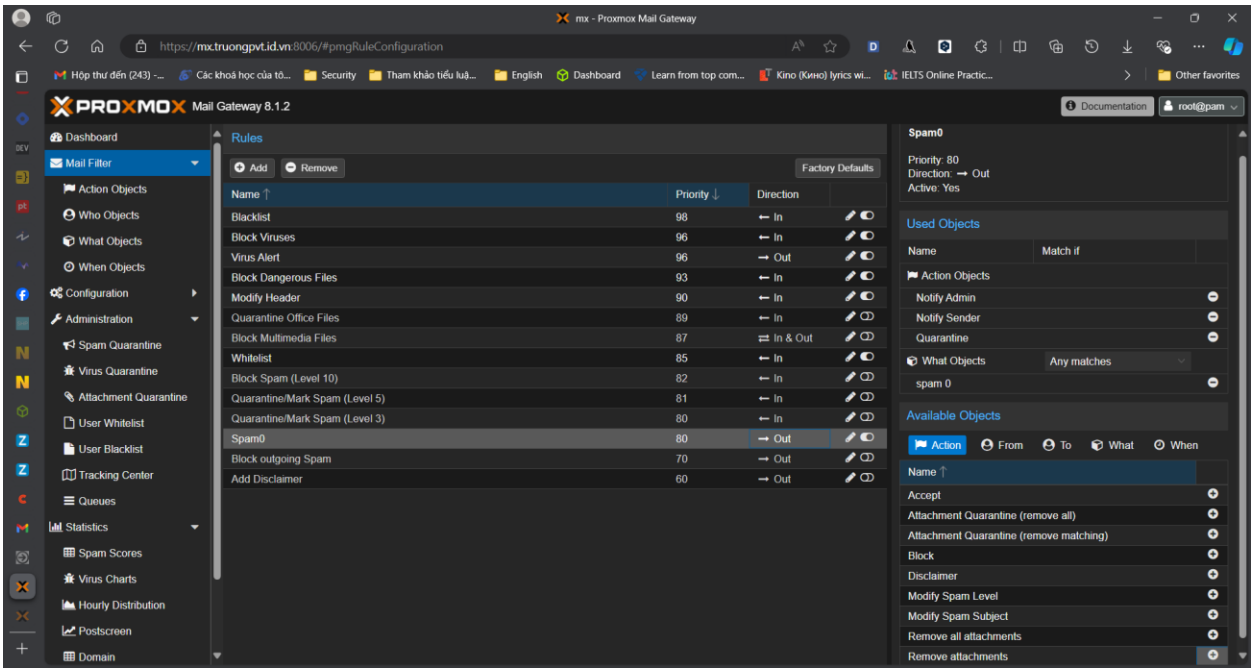
Để check rule hoạt động em tiến hành gửi mail từ 2 gmail 20522091@gm.uit.edu.vn và thientruong01092002@gmail.com



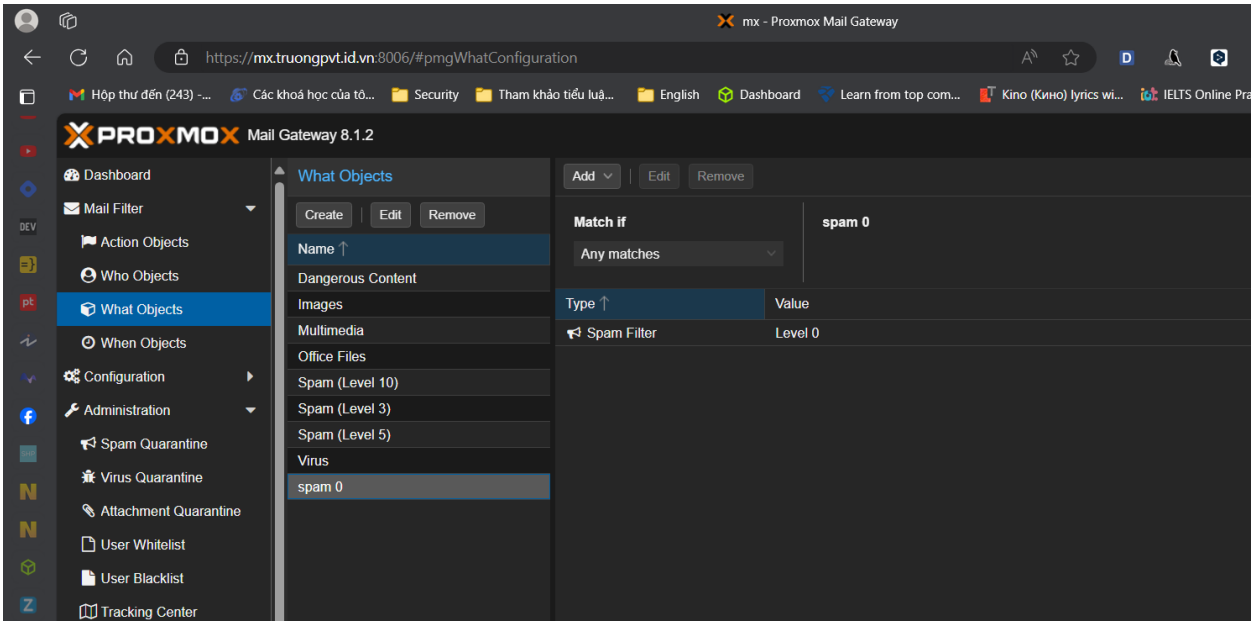


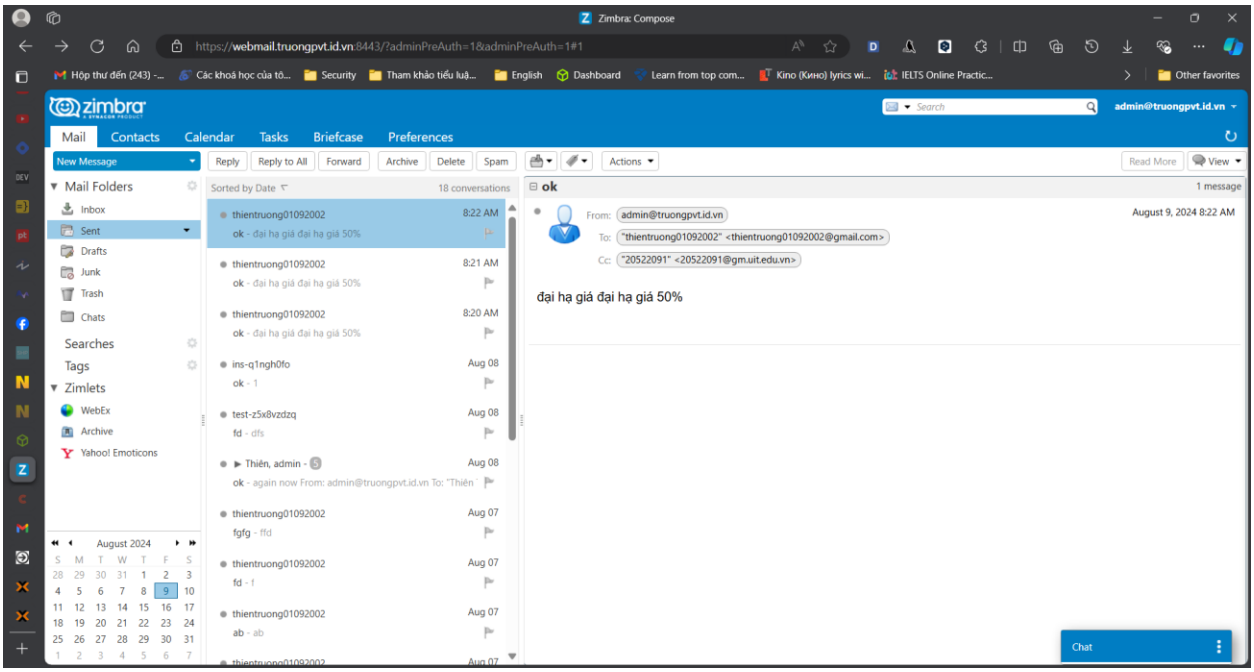
Cấu hình rule Quarantine chiều gửi nếu email đạt điểm spam từ 3 điểm trở lên

Để có thể quarantine email từ zimbra đi ra ngoài nếu đạt điểm spam là 3 thì em sẽ đặt chiều gửi ở đây là out. Nhưng vì điều kiện kích hoạt là điểm spam phải từ 3 nên em sẽ tự tạo rule với điểm spam là 0 để check function của rule spam. Kèm theo là báo lại admin và sender nếu email bị quarantined.


mx - Proxmox Mail Gateway
https://mx.truongpvt.id.vn:8006/#pmgRuleConfiguration
PROXMOX Mail Gateway 8.1.2
Documentation
root@pam
Dashboard
Mail Filter
Action Objects
Who Objects
What Objects
When Objects
Configuration
Administration
Spam Quarantine
Virus Quarantine
Attachment Quarantine
User Whitelist
User Blacklist
Tracking Center
Queues
Statistics
Spam Scores
Virus Charts
Hourly Distribution
Postscreen
Domain
Rules
Add
Remove
Factory Defaults
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
Spam0 80 Out
Block outgoing Spam 70 Out
Add Disclaimer 60 Out
Spam0
Priority: 80
Direction: Out
Active: Yes
Used Objects
Name
Match if
Action Objects
Notify Admin
Notify Sender
Quarantine
What Objects
Any matches
spam 0
Available Objects
Action
From
To
What
When
Name
Accept
Attachment Quarantine (remove all)
Attachment Quarantine (remove matching)
Block
Disclaimer
Modify Spam Level
Modify Spam Subject
Remove all attachments
Remove attachments

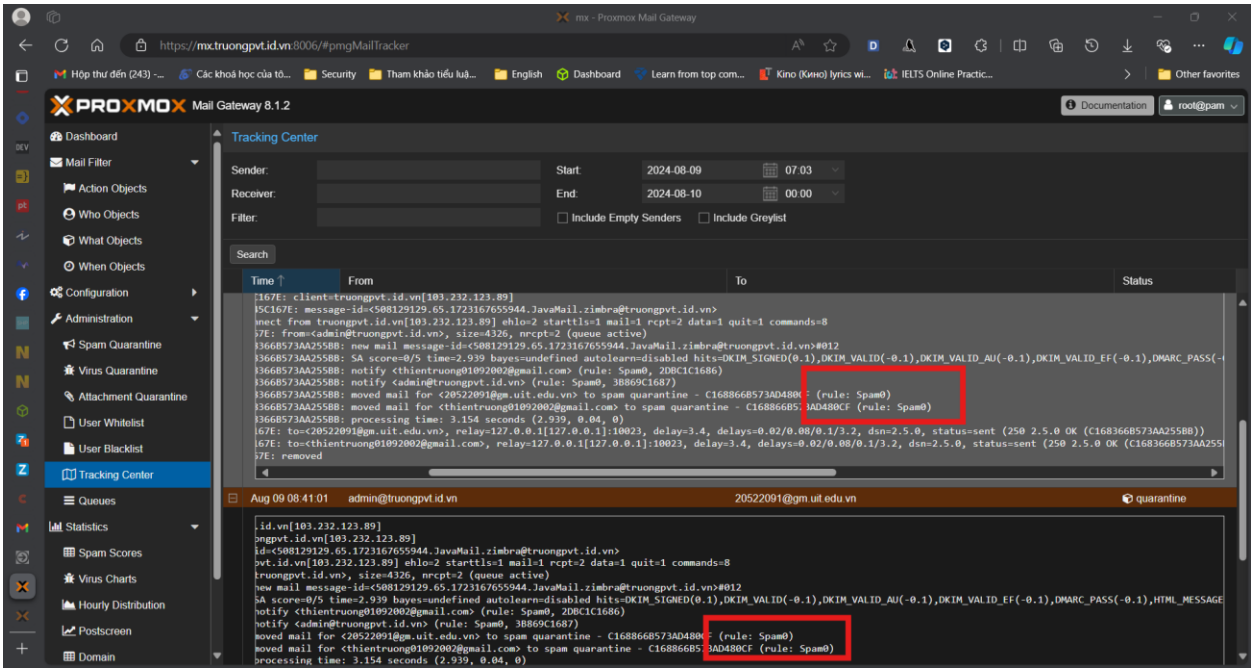
Rule


mx - Proxmox Mail Gateway
https://mx.truongpvt.id.vn:8006/#pmgWhatConfiguration
PROXMOX Mail Gateway 8.1.2
Dashboard
Mail Filter
Action Objects
Who Objects
What Objects
When Objects
Configuration
Administration
Spam Quarantine
Virus Quarantine
Attachment Quarantine
User Whitelist
User Blacklist
Tracking Center
What Objects
Create
Edit
Remove
Name
Dangerous Content
Images
Multimedia
Office Files
Spam (Level 10)
Spam (Level 3)
Spam (Level 5)
Virus
spam 0
Add
Edit
Remove
Match if
Any matches
spam 0
Type
Value
Spam Filter
Level 0

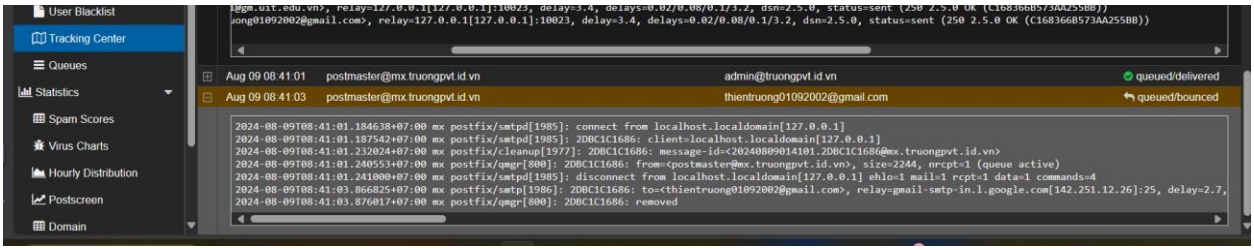


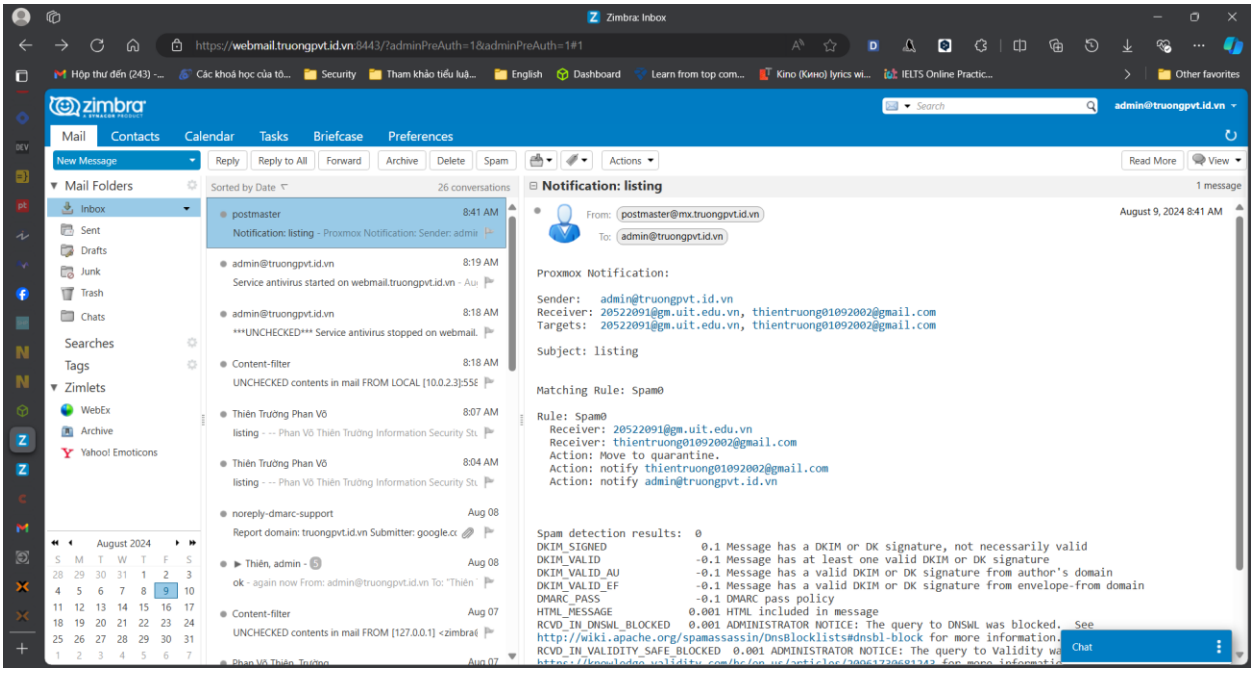
Kết quả

Quarantine



Notify


User Blacklist
Tracking Center
Queues
Statistics
Spam Scores
Virus Charts
Hourly Distribution
Postscreen
Domain
Aug 09 08:41:01 postmaster@mx.truongpvt.id.vn admin@truongpvt.id.vn queued/delivered
Aug 09 08:41:03 postmaster@mx.truongpvt.id.vn thientruong01092002@gmail.com queued/bounced
2024-08-09T08:41:01.184638+07:00 mx postfix/smtpd[1985]: connect from localhost.localdomain[127.0.0.1]
2024-08-09T08:41:01.187542+07:00 mx postfix/smtpd[1985]: 2DBC1C1686: client=localhost.localdomain[127.0.0.1]
2024-08-09T08:41:01.232024+07:00 mx postfix/cleanup[1977]: 2DBC1C1686: message-id=<20240809014101.2DBC1C1686@mx.truongpvt.id.vn>
2024-08-09T08:41:01.240553+07:00 mx postfix/qmgr[800]: 2DBC1C1686: from=<postmaster@mx.truongpvt.id.vn>, size=2244, nrcpt=1 (queue active)
2024-08-09T08:41:01.241000+07:00 mx postfix/smtpd[1985]: disconnect from localhost.localdomain[127.0.0.1] ehlo=1 mail=1 rcpt=1 data=1 commands=4
2024-08-09T08:41:03.866825+07:00 mx postfix/smtp[1986]: 2DBC1C1686: to=<thientruong01092002@gmail.com>, relay=gmail-smtp-in.l.google.com[142.251.12.26]:25, delay=2.7,
2024-08-09T08:41:03.876017+07:00 mx postfix/qmgr[800]: 2DBC1C1686: removed


Zimbra: Inbox
https://webmail.truongpvt.id.vn:8443/?adminPreAuth=1&adminPreAuth=1#1
zimbra
admin@truongpvt.id.vn
Mail Contacts Calendar Tasks Briefcase Preferences
New Message Reply Reply to All Forward Archive Delete Spam Actions Read More View
Mail Folders
Inbox Sent Drafts Junk Trash Chats
Searches Tags
Zimlets
WebEx Archive Yahoo! Emoticons
Sorted by Date 26 conversations
postmaster 8:41 AM Notification: listing - Proxmox Notification: Sender: admi
admin@truongpvt.id.vn 8:19 AM Service antivirus started on webmail.truongpvt.id.vn
admin@truongpvt.id.vn 8:18 AM ***UNCHECKED*** Service antivirus stopped on webmail.
Content-filter 8:18 AM UNCHECKED contents in mail FROM LOCAL [10.0.2.3]:55
Thiên Trường Phan Võ 8:07 AM listing - -- Phan Võ Thiên Trường Information Security St
Thiên Trường Phan Võ 8:04 AM listing - -- Phan Võ Thiên Trường Information Security St
noreply-dmarc-support Aug 08 Report domain: truongpvt.id.vn Submitter: google.c
Thiên, admin - 5 Aug 08 ok - again now From: admin@truongpvt.id.vn To: "Thiên
Content-filter Aug 07 UNCHECKED contents in mail FROM [127.0.0.1] <zimbra
Notification: listing
1 message
From: postmaster@mx.truongpvt.id.vn
To: admin@truongpvt.id.vn
August 9, 2024 8:41 AM
Proxmox Notification:
Sender: admin@truongpvt.id.vn
Receiver: 20522091@gm.uit.edu.vn, thientruong01092002@gmail.com
Targets: 20522091@gm.uit.edu.vn, thientruong01092002@gmail.com
Subject: listing
Matching Rule: Spam0
Rule: Spam0
Receiver: 20522091@gm.uit.edu.vn
Receiver: thientruong01092002@gmail.com
Action: Move to quarantine.
Action: notify thientruong01092002@gmail.com
Action: notify admin@truongpvt.id.vn
Spam detection results: 0
DKIM_SIGNED 0.1 Message has a DKIM or DK signature, not necessarily valid
DKIM_VALID -0.1 Message has at least one valid DKIM or DK signature
DKIM_VALID_AU -0.1 Message has a valid DKIM or DK signature from author's domain
DKIM_VALID_EF -0.1 Message has a valid DKIM or DK signature from envelope-from domain
DMARC_PASS -0.1 DMARC pass policy
HTML_MESSAGE 0.001 HTML included in message
RCVD_IN_DNSWL_BLOCKED 0.001 ADMINISTRATOR NOTICE: The query to DNSWL was blocked. See
http://wiki.apache.org/spamassassin/DnsBlocklists#dnsbl-block for more information.
RCVD_IN_VALIDITY_SAFE_BLOCKED 0.001 ADMINISTRATOR NOTICE: The query to Validity wa
Chat