



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.

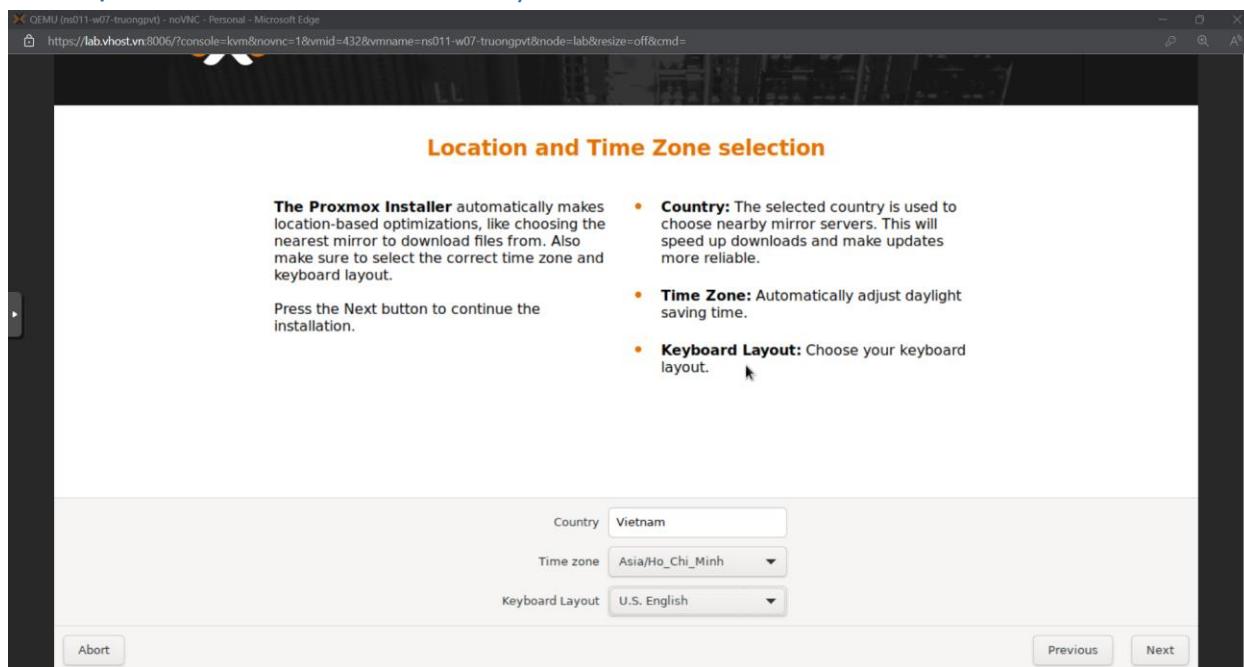
Trung: 103.223.123.161

Giang: 103.232.123.166

Trường: 103.232.123.167

Kha: 103.232.123.168

Cài đặt Proxmox Mail Gateway lên VM tuần 7.





The screenshot shows the "Administration Password and Email Address" step of the Proxmox Mail Gateway setup. It includes instructions for setting a strong password and providing an email address for alerts. The interface shows fields for "Password" (filled with dots), "Confirm" (also filled with dots), and "Email" (set to "ruong01092002@gmail.com"). Buttons for "Abort", "Previous", and "Next" are at the bottom.

Password: LionEl'Johnson_!

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

Hostname: mx.truongpvt.id.vn

The screenshot shows the "Management Network Configuration" step. It instructs users to verify the displayed network configuration and provides options for IP address (CIDR), Gateway, and DNS Server. The configuration fields include "Management Interface" (set to "ens18 - ba:69:94:89:3b:6b (virtio_net)"), "Hostname (FQDN)" (set to "mx.truongpvt.id.vn"), "IP Address (CIDR)" (set to "103.232.123.167 / 24"), "Gateway" (set to "103.232.123.1"), and "DNS Server" (set to "8.8.8.8"). Buttons for "Abort", "Previous", and "Next" are at the bottom.



QEMU (ns011-w07-truongpt) - noVNC - Personal - Microsoft Edge
https://lab.vhost.vn:8006/?console=kvm&novnc=1&vmid=432&vmname=ns011-w07-truongpt&node=lab&resize=off

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:	thientruong01092002@gmail.com
Management Interface:	ens18
Hostname:	mx
IP CIDR:	103.232.123.167/24
Gateway:	103.232.123.1
DNS:	8.8.8.8

Automatically reboot after successful installation

Abort Previous Install

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

QEMU (ns011-w07-truongpt) - noVNC - Personal - Microsoft Edge
https://lab.vhost.vn:8006/?console=kvm&novnc=1&vmid=432&vmname=ns011-w07-truongpt&node=lab&resize=off

Welcome to the Proxmox Mail Gateway. Please use your web browser to configure this server - connect to:
https://103.232.123.167:8006/

```
mx login: root
Password:
Linux mx 6.5.13-1-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.13-1 (2024-02-05T13:50Z) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@mx:~# ls
root@mx:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether ba:69:94:89:3b:6b brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 103.232.123.167/24 scope global ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::ba69:94ff:fe89:3b6b/64 scope link
        valid_lft forever preferred_lft forever
root@mx:~#
```



The screenshot shows the Proxmox Mail Gateway 8.1.2 dashboard. On the left, a sidebar lists various configuration and monitoring options. The main area displays two charts under 'E-Mail Volume': 'Mail / min' and 'Mail / sec'. Below these charts is a section titled 'E-Mail Processing' with a 'Traffic' summary: '0 B ← In' and '0 B → Out'. A note at the bottom states: 'You have at least one node without subscription.'

Request PTR

The screenshot shows the MxToolbox SuperTool interface. The search bar contains 'ptr:103.232.123.167'. The results table shows a single PTR record:

Type	IP Address	Domain Name	TTL
PTR	103.232.123.167 VHOST-AS-VN (AS56150)	mx.truongptv.id.vn	120 min

Below the table, a 'Test' section shows a green checkmark next to 'DNS Record Published' with the result 'DNS Record found'. A note at the bottom says: 'An error has occurred with your lookup. Please try again.'

On the right side of the interface, there are several promotional boxes for MxToolbox services:

- Free MxToolBox Account
- Delivery Center
- Inbox Placement
- Recipient Complaints
- Adaptive Blacklist Monitoring
- Mailflow Monitoring



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

The screenshot shows the 'Manage' section of the MATBAO domain management interface. It lists various DNS records for the domain '0d-id.vn'. Two specific records are highlighted with red boxes around their IP values: the '@' record has '103.232.123.89' and '103.232.123.167' listed, and the 'mx' record has '103.232.123.167' listed. The interface includes a sidebar with icons for different services and a search bar at the top.

The screenshot shows the 'Manage' section of the MATBAO domain management interface. It lists various DNS records for the domain '0d-id.vn'. One specific record is highlighted with a red box: the '@' record has '1 mx.truongpvt.id.vn.' and '0 webmail.truongpvt.id.vn.' listed. Below it, there are several TXT records, one of which is highlighted with a red box: the '@' record has the SPF configuration 'v=spf1 mx ip4:103.232.123.167 mx ~all' and the DMARC configuration 'v=DMARC1; p=none; rua=mailto:admin@truongpvt.id.vn; ruf=mailto:admin@truongpvt.id.vn; sp=none; adkim...'. The interface includes a sidebar with icons for different services and a search bar at the top.



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.

The screenshot shows the 'Relay Domains' tab of the Proxmox Mail Gateway configuration interface. The left sidebar shows the navigation menu with 'Mail Proxy' selected. The main panel displays a table with columns: Relay Domain, Host, Protocol, Port, Use MX, and Comment. Three entries are listed:

Relay Domain	Host	Protocol	Port	Use MX	Comment
com					
net					
vn					

The screenshot shows the 'Transports' tab of the Proxmox Mail Gateway configuration interface. The left sidebar shows the navigation menu with 'Mail Proxy' selected. The main panel displays a table with columns: Relay Domain, Host, Protocol, Port, Use MX, and Comment. Two entries are listed for the relay domain 'truongpvt.id.vn':

Relay Domain	Host	Protocol	Port	Use MX	Comment
truongpvt.id.vn	103.232.123.89	smtp	25	No	
webmail truongpvt.id.vn	103.232.123.89	smtp	25	No	



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 zimbraMtaSaslPasswordMaps
        lmdb:/opt/zimbra/conf/relay_password
zmprov ms webmail.truongpvt.id.vn zimbraMtaSaslAuthEnable yes
zmprov ms webmail.truongpvt.id.vn zimbraMtaSaslCnameOverridesServername 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



The screenshot shows the Zimbra Administration interface for the server `webmail.truongpvt.id.vn`. The left sidebar is expanded to show the `MTA` section. The main panel displays the configuration for the `webmail.truongpvt.id.vn` service. Key settings include:

- Authentication:** Enable authentication (checked), TLS authentication only (checked).
- Network:** Web mail MTA Hostnames: `webmail.truongpvt.id.vn` (with Add and Remove buttons). Web mail MTA Port: 25. Relay MTA for external delivery: `mx.truongpvt.id.vn` (with port 26). Relay MTA for external delivery (fallback): [empty]. Web mail MTA timeout (s): 60. MTA Trusted Networks: `127.0.0.0/8 [::1]/128 10.0.2.0/24`.
- SMTP DNS:** Enabled.

The screenshot shows the Proxmox Mail Gateway configuration interface. The left sidebar is expanded to show the `Mail Proxy` section. The main panel is titled "Configuration: Mail Proxy" and is currently viewing the `Ports` tab. The configuration details are as follows:

Setting	Value
External SMTP Port	25
Internal SMTP 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



Time ↑	From	To	Status
Aug 07 11:45:32	thientruong01092002@gmail.com	admin@truongpvt.id.vn	accepted/delivered
Aug 07 11:54:02	iamaboylk@gmail.com	admin@truongpvt.id.vn	accepted/deferred
Aug 07 12:00:12	iamaboylk@gmail.com	admin@truongpvt.id.vn	queued/delivered
Aug 07 12:05:09	admin@truongpvt.id.vn	thientruong01092002@gmail.com	accepted/delivered

Cấu hình SSL cho PMG và port mail.

Cách 1:

Theo link dưới

[HOW TO INSTALL SSL LETSENCRYPT IN PROXMOX MAIL GATEWAY 7.3.1](https://origrata.com/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/sites-available/pmg và /etc/nginx/sites-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.



TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN - ĐHQG-HCM
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG
BỘ MÔN AN TOÀN THÔNG TIN

```
GNU nano 7.2                                     /etc/nginx/sites-available/pmg
server {
    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;
    }

    listen 443 ssl; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/mx.truongpvt.id.vn/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/mx.truongpvt.id.vn/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}

server {
    if ($host = mx.truongpvt.id.vn) {
        return 301 https://$host$request_uri;
    } # managed by Certbot

    listen 80;
    server_name mx.truongpvt.id.vn;
    return 404; # managed by Certbot
}
```

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
```

```
root@mx:~# nano /etc/default/pmgproxy
root@mx:~# nano /etc/nginx/sites-available/pmg
root@mx:~# nano /etc/postfix/main.cf
root@mx:~# nano /etc/nginx/sites-available/pmg
root@mx:~# nano /etc/postfix/main.cf
root@mx:~# cp /etc/letsencrypt/live/mx.truongpvt.id.vn/fullchain.pem /etc/pmg/pmg-cert.pem
root@mx:~# cp /etc/letsencrypt/live/mx.truongpvt.id.vn/privkey.pem /etc/pmg/pmg-key.pem
root@mx:~# nano /etc/postfix/main.cf
root@mx:~# nano /etc/postfix/main.cf
root@mx:~#
```



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

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. On the left, there is a sidebar with options: When Objects, Configuration (selected), Mail Proxy, Spam Detector, Virus Detector, and User Management. The main area is titled "Tracking Center" and includes fields for Sender, Receiver, Start date (2024-08-08), End date (2024-08-09), and checkboxes for "Include Empty Senders" and "In". A "Search" button is at the bottom of the tracking center section.

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

The terminal window shows the configuration of the /etc/postfix/main.cf file using the nano editor. The configuration includes setting smtpd_tls_security_level to 'may', specifying smtpd_tls_cert_file and smtpd_tls_key_file paths, and enabling smtpd_use_tls=yes. The file also contains settings for recipient access, sender access, and client access.

```
root@webmail ~ % nano /etc/postfix/main.cf
# /etc/postfix/main.cf *
check_recipient_access regexp:/etc/postfix/rcptaccess
check_sender_access regexp:/etc/postfix/senderaccess
check_client_access cidr:/etc/postfix/clientaccess

smtpd_data_restrictions = reject_unauth_pipeline
smtpd_forbid_bare_newline = normalize
smtpd_forbid_bare_newline_exclusions =
$mynetworks,
cidr:/etc/postfix/clientaccess

smtpd_client_connection_count_limit = 50
smtpd_client_connection_rate_limit = 0
smtpd_client_message_rate_limit = 0

smtpd_tls_security_level = may
smtpd_tls_policy_maps = hash:/etc/pmg/tls_policy
smtpd_CAsfile = /etc/pmg/pmg-cert.pem
smtpd_tls_security_level = encrypt
smtpd_tls_cert_file = /etc/pmg/pmg-cert.pem
smtpd_tls_key_file = /etc/pmg/pmg-key.pem
smtpd_use_tls=yes

lsmtp_tls_security_level = $smtpd_tls_security_level
lsmtp_tls_policy_maps = $smtpd_tls_policy_maps
lsmtp_tls_CAsfile = $smtpd_tls_CAsfile

smtpd_tls_received_header = yes

smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_session_cache
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_session_cache
lsmtp_tls_session_cache_database = btree:/var/lib/postfix/lsmtp_tls_session_cache

^G Help      ^O Write Out    ^W Where Is    ^X Cut        ^T Execute    ^C Location    M-U Undo    M-A Set Mark
^X Exit      ^R Read File    ^R Replace    ^U Paste      ^J Justify    ^Y Go To Line   M-B Redo    M-G Copy     ^Q Where Was
```



mx.truongpvt.id.vn HTTPS Lookup

https://mx.truongpvt.id.vn Monitor This

Certificate

Primary
Common Name: mx.truongpvt.id.vn

> Issuer: E6
> Expires: 3 months
> Valid From: 8/7/2024
> Valid To: 11/5/2024

> Serial: 0476F6B04D8E04936EF95EE094D67AE7104E
> Algorithm: sha384ECDSA

Reminder

Common Name: E6

> Issuer: ISRG Root X1
> Expires: 3 years
> Valid From: 3/12/2024
> Valid To: 3/12/2027

> Serial: 00B053E9173972770DBB487CB3A452B38
> Algorithm: sha256RSA
> Organization: Let's Encrypt
> Location: US

Common Name: ISRG Root X1

> Issuer: ISRG Root X1
> Expires: Never
> Valid From: 6/4/2015
> Valid To: 6/4/2035

> Serial: 00B210CFB0D240E3594463E0BB63828B00
> Algorithm: sha256RSA
> Organization: Internet Security Research Group
> Location: US

Test Result
HTTP Connect 200 OK

Your IP is 113.101.81.210 | Certified Terms & Conditions Site Map Security API Ethics Phishing (88) 696-6852 | © Copyright 2004-2021 | MXToolBox.com All rights reserved. US Patents 10839353 B2 & 11481738 B2

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

ok - thientruong01092002@gmail.com - Gmail

Hộp thư đến (243) ~

MXToolBox.com

Gmail

Tìm kiếm thư

Đang hoạt động

1 trong tổng số 169

113.101.81.210 | Certified Terms & Conditions Site Map Security API Ethics Phishing (88) 696-6852 | © Copyright 2004-2021 | MXToolBox.com All rights reserved. US Patents 10839353 B2 & 11481738 B2

Soạn thư

Hộp thư đến 4

Có gắn dấu sao

Đã tạm án

Đã gửi

Thư nháp 2

Hiện thêm

Nhắn

admin@truongpvt.id.vn confirmed

admin@truongpvt.id.vn

đến tôi

again

từ: admin@truongpvt.id.vn
đến: Thiên Trường Phan Võ <thientruong01092002@gmail.com>
ngày: 09:01 8 thg 8, 2024
tiêu đề: Re: ok
được gửi bởi: truongpvt.id.vn
xác thực bởi: truongpvt.id.vn
bảo mật: ✅ Mã hóa tiêu chuẩn (TLS) [Tìm hiểu thêm](#)
Quan trọng vì các thư trước đó trong cuộc trò chuyện rất quan trọng.

Trả lời Chuyển tiếp

Có cách thứ 2

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



The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar has 'Certificates' selected. In the main area, there's a modal window for the 'default' account. The modal contains the following information:

Account	
E-Mail:	mailto:thientruong01092002@gmail.com
Created:	2024-08-08T01:45:02.2990823Z
Status:	valid
Directory:	https://acme-v02.api.letsencrypt.org/directory
Terms of Services:	https://letsencrypt.org/documents/LE-SA-v1.4-April-3-2024.pdf

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

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar has 'Certificates' selected. In the main area, the 'ACME' section is expanded, showing two certificates:

File	Issuer	Subject	Valid Since	Expires	Subject Alternative Names
pmg-api.pem	/CN=mx	/CN=mx	2024-08-07 11:31:51	2024-08-05 11:31:51	
pmg-fts.pem	/C=US/O=Let's Encrypt/CN=R11	/CN=mx.truongpvt.id.vn	2024-08-09 06:53:25	2024-11-07 06:53:24	mx.truongpvt.id.vn

Below the table, there are buttons for 'Order Certificates Now' (highlighted) and 'Using Account: default'. The 'Domain' dropdown is set to 'mx.truongpvt.id.vn'. The 'Usage' column shows 'api,smtp' and the 'Type' column shows 'standalone'.

SMTP



The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar navigation includes: 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 (selected), Administration, Spam Quarantine, Virus Quarantine, Attachment Quarantine, User Whitelist, and User Blacklist.

The main content area displays a "Task viewer: acmenewcert" window for the "Certificates" section. The "Output" tab is active, showing the following log:

```
Getting authorization details from 'https://acme-v02.api.letsencrypt.org/acme/order/1879773946/294647167126'
The validation for mx.truongpvt.id.vn is pending!
Setting up webserver
Triggering validation
Sleeping for 5 seconds
Status is still 'pending', trying again in 10 seconds
Status is 'valid', domain 'mx.truongpvt.id.vn' OK!
All domains validated!
Creating CSR
Checking order status
Order is ready, finalizing order
Order valid!
Downloading certificate
Setting custom certificate file /etc/pmg/pmg-tls.pem
Reloading postfix
TASK OK
```

The "Status" tab shows a table with one entry:

Type	Plugin
standalone	

API

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar navigation is identical to the previous screenshot.

The main content area displays a "Task viewer: acmenewcert" window for the "Certificates" section. The "Output" tab is active, showing the following log:

```
Getting authorization details from 'https://acme-v02.api.letsencrypt.org/acme/order/1879773946/29464742346'
mx.truongpvt.id.vn is already validated!
All domains validated!
Creating CSR
Checking order status
Order is ready, finalizing order
Order valid!
Downloading certificate
Setting custom certificate file /etc/pmg/pmg-api.pem
Restarting proxmox
TASK OK
```

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



The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar contains a navigation menu with options like Dashboard, Mail Filter, Configuration, Mail Proxy, Spam Detector, Virus Detector, User Management, Cluster, Subscription, Backup/Restore, Certificates, Administration, Spam Quarantine, Virus Quarantine, Attachment Quarantine, User Whitelist, and User Blacklist. The main panel displays two charts under 'E-Mail Volume': 'Mails / min' and 'Spam / min'. Below these charts is a section titled 'E-Mail Processing' with a 'Traffic' summary showing 0 B ← In and 0 B → Out, and an 'Avg. Mail Processing Time' status of 'N/A'. A note at the bottom states 'You have at least one node without subscription.'

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

DKIM

The screenshot shows the 'Configuration: Mail Proxy' screen in Proxmox Mail Gateway 8.1.2. The left sidebar has the same navigation menu as the previous screenshot. The main panel shows tabs for Relaying, Relay Domains, Ports, Options, Transports, Networks, TLS, DKIM (which is selected), and Whitelist. Under the 'DKIM' tab, there's a 'Settings' section with fields for 'Enable DKIM Signing' (Yes), 'Selector' (pmg), 'Get Signing Domain From' (Envelope), and 'Sign all Outgoing Mail' (Yes). Below this is a 'Sign Domain' section with a 'Selector' dropdown set to 'pmg', 'Key Size' of '2048', and a 'DNS TXT Record' input field containing a long string of DKIM key data. A 'Close dialog' button is visible in the top right of this window.

Thêm vào bản ghi DNS của domain



The screenshot shows a web-based interface for managing domain files. On the left is a sidebar with various icons for file types like DEV, PDF, and images. The main area displays a table of files in the root directory of '0d-id.vn'. The columns include file name, type, content, size, and edit/delete icons. Below the table is a section titled 'Thông tin tổng quan' (General Information) with fields for 'Vòng đời tên miền' (Domain lifetime), 'Tình trạng' (Status), and 'Ngày đăng ký' (Registration date). A 'Góp ý trải nghiệm' (Share your experience) button is also present.

Kiểm tra file gửi từ zimbra đi qua proxmox

The screenshot shows an email message in Google Mail. The message is from 'admin@truongpvt.id.vn' to 'thientruong01092002@gmail.com'. The subject is 'Re: ok'. The message body is empty. The 'Thu gốc' (Original Message) tab is selected, showing detailed headers. The 'Match case' and 'Match whole word' search filters are applied. The message was received at 09:01 on August 8, 2024. The SPF result is 'PASS với IP 103.232.123.167'. The DKIM result is 'PASS' and the DMARC result is 'PASS'. The message was delivered to 'thientruong01092002@gmail.com' via SMTP. The X-Google-Smtp-Source header includes a long string of characters representing the SMTP session ID.



```
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=thread-index:thread-topic:mime-version:subject:references
:in-reply-to:message-id:from:date:dkim-signature:dkim-filter;
bh=26kgCg7mqCVwQHsAgeubuhV25IRzawsw9CuzEHZo=;
fh=InKongoghgx1VSeet3TfxVCYhV/20AE1A/gc=g...
b=W4qfjLWvDyv2yvXeJh3n2faw514PHwvnD1+7g4lhdrt
1D7hwmp2lyow/S1e5INTpob3sWHf9NbMojJH1l0+R
gkxZ7RdQztq3uNyAG88oNAleWbEz9Ekoeahd0RVaf...
CmIA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=thread-index:thread-topic:mime-version:subject:references
:in-reply-to:message-id:from:date:dkim-signature:dkim-filter;
bh=26kgCg7mqCVwQHsAgeubuhV25IRzawsw9CuzEHZo=;
fh=InKongoghgx1VSeet3TfxVCYhV/20AE1A/gc=g...
b=W4qfjLWvDyv2yvXeJh3n2faw514PHwvnD1+7g4lhdrt
1D7hwmp2lyow/S1e5INTpob3sWHf9NbMojJH1l0+R
gkxZ7RdQztq3uNyAG88oNAleWbEz9Ekoeahd0RVaf...
eEQ0=;
dara@google.com
ARC-Authentication-Results: i=1; mx.google.com;
dkim-pass header.i=@truongpvt.id.vn header.s=166CA964-4B6A-11EF-948C-47CEA0E91A1E header.b=JH8lkQ78;
spf-pass (google.com: domain of admin@truongpvt.id.vn designates 103.232.123.167 as permitted sender)
smtp.mailfrom=admin@truongpvt.id.vn
dmarc-pass (p=NONE sp=NONE dis=NONE) header.from=truongpvt.id.vn
Return-Path: <admin@truongpvt.id.vn>
Received: by mx.google.com with ESMTPS id d9a43c01a7336-20084d4635f5125349545ad.431.2024.08.07.19.01.46
for <thientruong01092002@gmail.com>
(Version=TLS1.3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
Wed, 07 Aug 2024 19:01:47 +0700 (PDT)
Received-SPF: pass (google.com: domain of admin@truongpvt.id.vn designates 103.232.123.167 as permitted sender) client-ip=103.232.123.167;
Authentication-Results: mx.google.com;
dkim-pass header.i=@truongpvt.id.vn header.s=166CA964-4B6A-11EF-948C-47CEA0E91A1E header.b=JH8lkQ78;
spf-pass (google.com: domain of admin@truongpvt.id.vn designates 103.232.123.167 as permitted sender)
smtp.mailfrom=admin@truongpvt.id.vn
dmarc-pass (p=NONE sp=NONE dis=NONE) header.from=truongpvt.id.vn
Received: from mx.truongpvt.id.vn (localhost.localdomain [127.0.0.1]) by mx.truongpvt.id.vn (Proxmox) with ESMTP id E5DADC1666 for <thientruong01092002@gmail.com>; Thu,
8 Aug 2024 09:01:39 +0700 (+07)
8 Aug 2024 09:01:39 +0700 (+07)
103.232.123.89 is authorized to use 'admin@truongpvt.id.vn' in 'mfrom' identity (mechanism 'mx' matched)
Received: from truongpvt.id.vn [103.232.123.89] (using TLSV1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits))
key-exchange X25519 server-signature ECDSA (prime256v1) server-digest SHA256 (No client certificate requested) by mx.truongpvt.id.vn
(Proxmox) with ESMTPS id 6463AC1664 for <thientruong01092002@gmail.com>; Thu,
8 Aug 2024 09:01:39 +0700 (+07)
```

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

Name ↑	Match if	Value
Blacklist	Any matches	Global blacklist
Whitelist	Type ↑	
	E-Mail	mail@fromthisdomain.com
	E-Mail	ngocnguyen037@gmail.com
	E-Mail	thientruong01092002@gmail.com



Blacklist

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. On the left sidebar, under 'Who Objects', 'Blacklist' is selected. In the main panel, there is a table titled 'Blacklist' with a single entry:

Type	Value
E-Mail	20522091@gm.uit.edu.vn
E-Mail	admin@ngocnguyen037.id.vn
E-Mail	nomaif@fromthisdomain.com

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

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface with the 'Tracking Center' selected. The log table shows two entries for Aug 09 08:01:13 and Aug 09 08:01:47. The second entry, from 20522091@gm.uit.edu.vn to admin@truongpvt.id.vn, is highlighted and has its log message expanded:

```
2024-08-09T08:01:45.259001+07:00 mx postfix/cleanup[1062]: connect from mail-1f1-f50.google.com[209.85.167.50]
2024-08-09T08:01:45.271953+07:00 mx postfix/cleanup[1062]: SAA01C1683: client=mail-1f1-f50.google.com[209.85.167.50]
2024-08-09T08:01:47.372466+07:00 mx postfix/cleanup[1068]: SAA01C1683: message-id=<CAB2MSIfLMer3xKoRgR6bjj1s05up+4kpuWzTfpjaFOae30LkQ@mail.gmail.com>
2024-08-09T08:01:47.389295+07:00 mx postfix/qmgr[800]: SAA01C1683: from=<20522091@gm.uit.edu.vn>, size=3659, nrcpt=1 (queue active)
2024-08-09T08:01:47.507488+07:00 mx png-setp-filter[700]: new mail message-id=<CAB2MSIfLMer3xKoRgR6bjj1s05up+4kpuWzTfpjaFOae30LkQ@mail.gmail.com>#0
2024-08-09T08:01:47.555538+07:00 mx png-setp-filter[700]: C168466B56A7B743E9: block mail to admin@truongpvt.id.vn (rule: Blacklist)
2024-08-09T08:01:47.560039+07:00 mx png-setp-filter[700]: C168466B56A7B743E9: processing time: 0.079 seconds (0, 0.023, 0)
2024-08-09T08:01:47.569587+07:00 mx postfix/lmtp[1069]: SAA01C1683: to=<admin@truongpvt.id.vn>, relay=127.0.0.1[127.0.0.1]:10024, delay=0.52, delays=0.35/0.0/0.08, d
2024-08-09T08:01:47.569716+07:00 mx postfix/qmgr[800]: SAA01C1683: removed
2024-08-09T08:01:47.963118+07:00 mx postfix/smtpd[1062]: disconnect from mail-1f1-f50.google.com[209.85.167.50] ehlo=2 starttls=1 mail=1 rcpt=1 bdat=1 quit=1 commands=7
```



The screenshot shows the Proxmox Mail Gateway interface. On the left, there's a sidebar with various menu items like Dashboard, Mail Filter, Configuration, and Spam Detector. The main area is titled 'Tracking Center' and displays a table of email logs. The table has columns for Sender, Receiver, Start Date, End Date, and Status. The logs show several entries, with one specific entry highlighted in red:

Time ↑	From	To	Status
Aug 09 08:01:13	thientruong01092002@gmail.com	admin@truongpvt.id.vn	accepted/deferred
Aug 09 08:01:47	20522091@gmail.um.edu.vn	admin@truongpvt.id.vn	blocked
Aug 09 08:04:40	thientruong01092002@gmail.com	admin@truongpvt.id.vn	accepted/delivered

Below the table, there is a large block of log entries from the postfix SMTPD process. One entry in the log is highlighted with a red box:

```
2024-08-09T08:04:39.926243+07:00 mx postfix/smtpd[110]: connect from mail-yw1-f171.google.com[209.85.128.371]
2024-08-09T08:04:39.927993+07:00 mx postfix/smtpd[110]: client=mail-yw1-f171.google.com[209.85.128.371]
2024-08-09T08:04:39.927973+07:00 mx postfix/smtpd[110]: C2711C167E: message-id<CAP_vz2Hupdh41cvrMzcF8kGa_c18Y6_P5hzrHvV8+0d4+F2g@mail.gmail.com>
2024-08-09T08:04:39.928132+07:00 mx postfix/qmgr[8801]: C2711C167E: from=<thientruong01092002@gmail.com>, size=4795, nrcpt=1 (queue active)
2024-08-09T08:04:39.936060+07:00 mx qmgr-setp-filter[699]: new mail message-id<CAP_vz2Hupdh41cvrMzcF8kGa_c18Y6_P5hzrHvV8+0d4+F2g@mail.gmail.com>#0
2024-08-09T08:04:39.989025+07:00 mx postfix/smtpd[1117]: connect from localhost.localdomain[127.0.0.1]
2024-08-09T08:04:39.991614+07:00 mx postfix/smtpd[1117]: F20CAC1685: client=localhost.localdomain[127.0.0.1], orig_client=mail-yw1-f171.google.com[209.85.128.171]
2024-08-09T08:04:40.035736+07:00 mx postfix/cleanup[1112]: F20CAC1685: message-id<CAP_vz2Hupdh41cvrMzcF8kGa_c18Y6_P5hzrHvV8+0d4+F2g@mail.gmail.com>
2024-08-09T08:04:40.040155+07:00 mx postfix/qmgr[8801]: F20CAC1685: from=<thientruong01092002@gmail.com>, size=5012, nrcpt=1 (queue active)
2024-08-09T08:04:40.041069+07:00 mx qmgr-setp-filter[699]: C2711C167E: to=<admin@truongpvt.id.vn>, command=qmgr-setp, rule: Whitelist
2024-08-09T08:04:40.041228+07:00 mx postfix/smtpd[1117]: disconnect from localhost.localdomain[127.0.0.1] [client=192.168.1.104], xf�权限不足, mail=reject, d=+, r=reject, ands=5
2024-08-09T08:04:40.045920+07:00 mx qmgr-setp-filter[699]: C168466056027#0C7: processing time: 0.12 seconds (0, 0.03, 0)
2024-08-09T08:04:40.047120+07:00 mx postfix/lmtp[1113]: C2711C167E: to=<admin@truongpvt.id.vn>, relay=127.0.0.1[127.0.0.1]:10024, delay=0.46, delay=0.21/0.07/0.05/0.13
2024-08-09T08:04:40.047835+07:00 mx postfix/qmgr[880]: C2711C167E: removed
2024-08-09T08:04:40.135993+07:00 mx postfix/smtpd[1109]: disconnect from mail-yw1-f171.google.com[209.85.128.171] ehlo=2 starttls=1 mail=1 rcpt=1 bdat=1 quit=1 commands
2024-08-09T08:04:40.763924+07:00 mx postfix/smtpd[1118]: F20CAC1685: to=<admin@truongpvt.id.vn>, relay=10.232.123.89[10.232.123.89]:25, delay=0.77, delays=0.05/0.07/0.24
2024-08-09T08:04:40.764108+07:00 mx postfix/qmgr[880]: F20CAC1685: removed
```

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 chiểu 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.



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

Rule

Name	Type	Value
Dangerous Content		
Images		
Multimedia		
Office Files		
Spam (Level 10)		
Spam (Level 3)		
Spam (Level 5)		
Virus		
spam 0	Spam Filter	Level 0



The screenshot shows a Zimbra webmail interface. On the left, there's a sidebar with 'Mail Folders' (Inbox, Sent, Drafts, Junk, Trash, Chats), 'Searches', 'Tags', and 'Zimlets' (WebEx, Archive, Yahoo! Emoticons). Below the sidebar is a calendar for August 2024. The main area shows a list of 18 conversations. One conversation is selected, showing an email from 'admin@truongpvt.id.vn' to 'thientruong01092002@gmail.com' with the subject 'đại hạ giá đại hạ giá 50%'. The message body contains the text 'đại hạ giá đại hạ giá 50%'. The date is August 9, 2024, at 8:22 AM.

Kết quả

Quarantine

The screenshot shows the Proxmox Mail Gateway 8.1.2 interface. The left sidebar includes 'Dashboard', 'Mail Filter', 'Action Objects', 'Who Objects', 'What Objects', 'When Objects', 'Configuration', 'Administration', 'Spam Quarantine', 'Virus Quarantine', 'Attachment Quarantine', 'User Whitelist', 'User Blacklist', and 'Tracking Center'. The 'Tracking Center' tab is active. The main area displays a 'Tracking Center' table with columns for 'Time', 'From', 'To', and 'Status'. Two entries are listed:

Time	From	To	Status
Aug 09 08:41:01	admin@truongpvt.id.vn	20522091@gm uit.edu.vn	quarantine
Aug 09 08:41:01	.id.vn[103.232.123.89]	20522091@gm uit.edu.vn	quarantine

Below the table, the log details for each entry are shown:

Aug 09 08:41:01 admin@truongpvt.id.vn 20522091@gm uit.edu.vn quarantine

```
[167E: client-truongpvt.id.vn[103.232.123.89]
id:5C167E: message-id:<508129129.65.1723167655944.JavaMail.zimbra@truongpvt.id.vn>
rcpt=2 data=1 quit=1 commands=8
inet: From:admin@truongpvt.id.vn[103.232.123.89] to:20522091@gm uit.edu.vn
size=4326, nrcpt=2, queue active
priority=normal, envelope-to=20522091@gm uit.edu.vn
javaMail: zimbra@truongpvt.id.vn#012
SA score=0/5 time=2.939
moved mail for <20522091@gm uit.edu.vn> to spam quarantine - C1688668573AD480E : (rule: Spam0, 3B869C1687)
notify <thientruong01092002@gmail.com> (rule: Spam0, 2D8C1C1686)
moved mail for <thientruong01092002@gmail.com> to spam quarantine - C1688668573AD480E : (rule: Spam0, 3B869C1687)
processing time: 3.154 seconds (2.939, 0.04, 0)
167E: to<thientruong01092002@gmail.com>, relay=127.0.0.1[127.0.0.1]:10023, delay=3.4, delays=0.02/0.08/0.1/3.2, dsn=2.5.0, status=sent (250 2.5.0 OK (C168366B573AA255B))
167E: to<thientruong01092002@gmail.com>, relay=127.0.0.1[127.0.0.1]:10023, delay=3.4, delays=0.02/0.08/0.1/3.2, dsn=2.5.0, status=sent (250 2.5.0 OK (C168366B573AA255B))
167E: removed
```

Aug 09 08:41:01 .id.vn[103.232.123.89] 20522091@gm uit.edu.vn quarantine

```
[167E: client-truongpvt.id.vn[103.232.123.89]
id:508129129.65.1723167655944.JavaMail.zimbra@truongpvt.id.vn>
pvt.id.vn[103.232.123.89] ehlo=2 starttls=1 mail=1 rcpt=2 data=1 quit=1 commands=8
truongpvt.id.vn[103.232.123.89] size=4326, nrcpt=2, queue active
priority=normal, envelope-to=20522091@gm uit.edu.vn
javaMail: zimbra@truongpvt.id.vn#012
SA score=0/5 time=2.939
moved mail for <20522091@gm uit.edu.vn> to spam quarantine - C1688668573AD480E : (rule: Spam0, 3B869C1687)
notify <admin@truongpvt.id.vn> (rule: Spam0, 2D8C1C1686)
moved mail for <thientruong01092002@gmail.com> to spam quarantine - C1688668573AD480E : (rule: Spam0, 3B869C1687)
notify <admin@truongpvt.id.vn> (rule: Spam0, 2D8C1C1686)
moved mail for <20522091@gm uit.edu.vn> to spam quarantine - C1688668573AD480E : (rule: Spam0, 3B869C1687)
moved mail for <thientruong01092002@gmail.com> to spam quarantine - C1688668573AD480E : (rule: Spam0, 3B869C1687)
processing time: 3.154 seconds (2.939, 0.04, 0)
```

Notify



**TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN - BHQG-HCM
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG
BỘ MÔN AN TOÀN THÔNG TIN**

BỘ MÔN AN TOÀN THÔNG TIN

User Blacklist	[REDACTED]		
Tracking Center	[REDACTED]		
Queues	[REDACTED]		
Statistics	[REDACTED]		
Spam Scores	[REDACTED]		
Virus Charts	[REDACTED]		
Hourly Distribution	[REDACTED]		
Postscreen	[REDACTED]		
Domain	[REDACTED]		

Zimbra: Inbox

https://webmail.truongpvt.id.vn:8443/?adminPreAuth=1&adminPreAuth=1#1

Hộ thư đến (243) ~ Các khóa học của tôi... Security Tham khảo tiêu luậ... English Dashboard Learn from top com... Kino (Kino) lyrics wi... IELTS Online Practice...

zimbra Mail Contacts Calendar Tasks Briefcase Preferences

New Message Reply Reply to All Forward Archive Delete Spam

Mail Folders Sorted by Date 26 conversations

Inbox postmaster 8:41 AM Notification: listing - Proxmox Notification: Sender: admin

admin@truongpvt.id.vn 8:19 AM Service antivirus started on webmail.truongpvt.id.vn - Aut...

admin@truongpvt.id.vn 8:18 AM ***UNCHECKED*** Service antivirus stopped on webmail.

Content-filter 8:18 AM UNCHECKED contents in mail FROM LOCAL [10.0.2.1]:55E

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.co

Thiên, admin 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

Phan Võ Thiên, Truong Aug 07

Notification: listing

From: postmaster@mx.truongpvt.id.vn
To: admin@truongpvt.id.vn

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
Recipient: 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

DNSWL_PASS -0.1 DNSWL pass - a policy

HTML_MESSAGE 0.001 HTML included in message

RCDV_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.

RCDV_IN_VALIDITY_SAFE_BLOCKED 0.001 ADMINISTRATOR NOTICE! The query to Validity was blocked. See http://wiki.apache.org/spamassassin/Dnsblocklists#dnsbl_block for more information.

Chat