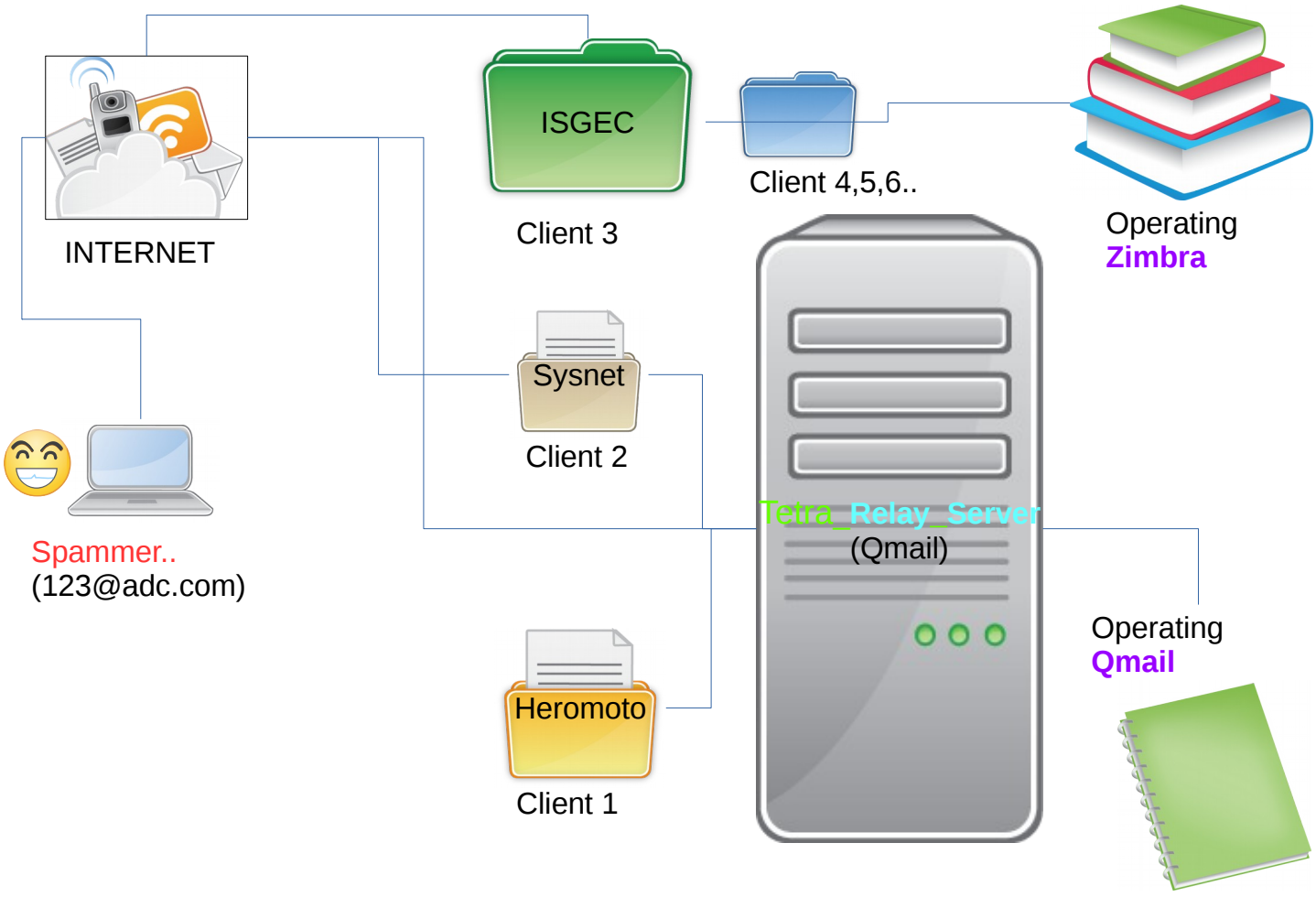
Analyzing & Resolution:

To Spamming

Spamming Architecture:



Description:
Above diagram explins below points:

1) Spammer is anyone who is located at external world from the domain network with miscellaneous prospectus to stole, corrupt or hamper the operation of server(s).

2) Spammer is located at any location on the internet.

3) It tries to attack client servers {like heromotocorp, sysnet, blsinternational (critical)}. Now either the client's mail are being relayed independantly from their own server or through tetra servers.

4) Now the server may be running either qmail/postfix or Zimbra mail server. So the workaround for stopping spamming in regard to both type of servers are described below:

Zimbra Server:

After getting the information about spam either throgh (Nagios/Call/Email), I perform the following steps:

1. Login into the reported server's admin panel & check the realy information in MTA server section.
2. Unlink relay IP with the corresponding server by removing the IP & port and save the configuration in Zimbra Admin Panel of client server.
3. Now login into the reported server with provided credetails. Then switch with zimbra server.

```
su - zimbra
postqueue -q  to chek the numbers of mailq
```

5. Check the email Id/username from which maximum number of email has been shooted by the following command :

```
grep sasl_user /var/log/zimbra.log | sed 's/.*sasl_username=//g' | sort | uniq -c | sort -nr | tail -n 1000 | less
```

6. Try to read the content of the Email of suspicious email id by the following command

```
postcat -p queue_id | less
```

7. If content is not genuine/malicious, remove those emails by the following command:

```
postqueue -p |grep "EMAIL_ID" |awk {'print $1'} |grep -v @ | tr -d '*!' | postsuper -d -
```

8. Also,we can check the supicious account by monitioring the overseas domain email ID and their content.
9. Change the password of the concern Email ID by Admin panel

OPTIONAL..

10. If needed, we can check the Spammers IP Address from log & will enter that entry in IPTABLES . (I havn't done this yet!!)

To do so:

1. cat /var/log/zimbra.log | less (Will check Spammer's IP, which will be there with Spammer Email ID)

Then we can block it by creating a REJECT rule for that IP either on the MailServer or on our relay server. Then restart Iptables service (I havn't done this yet!!)

We will keep monitor the mailq by postqueue -q | less for 10/15 minutes(depends on Spamming level)
After making sure the mailq is genuine, we can relay to the suggested relay server.
Even, after linking with relay server, we will keep eye on mailq for some time.

QMAIL Server:

1. Log in on the qmail server with root and check mail queue with this command.

```
qmHandle -l | less
```

2. To know which user account has been compromised. this command shows which user sending maximum mail.

```
qmHandle -l |grep From:|sort|uniq -c|sort -nr|head
```

OR

```
qmHandle -l|less
```

3. get message ID

```
qmHandle -m'message ID'|less
```

4. Change password for it first and delete mail in queue.

5. You can delete mail from queue using different option to from qmHandle -h (help)

```
qmHandle -h'Subject: limited offer'
```

or

```
qmHandle -d1234 -d2345 -d3456
```