Applications Area Working Group
Internet-Draft
Intended status: Informational
Expires: January 28, 2018

T. Akagiri
Regumi, Inc.
K. Wakamatsu
SoftBank Mobile Corp.
G. Yasutaka
Rakuten, Inc.
K. Okada
Lepidum Co. Ltd.
July 27, 2017

Outbound Port 25 Blocking for Dynamic IP Addresses
draft-akagiri-op25b-dynamicip-01.txt

Abstract

Outbound Port 25 Blocking has been widely used over a decade as a countermeasure against mail spams. It is the operation to filter TCP traffic which (1) the source IP addresses are dynamic IP addresses and (2) the destination port is 25. Since ordinal mail message submissions from dynamic IP addresses can be done via submission port (port number 587), operators can introduce the blocking without preventing ordinal mail message submissions. We explain current OP25B operations in this document.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 28, 2018.

Copyright Notice

Table of Contents

1. Introduction

Countermeasures for spam mails are categorized into two types, "to block sending spam mails" and "not to receive spam mails". Outbound Port 25 Blocking (OP25B) is one of the former approaches. Blocking a spam mail inside the spam origin domain is more desirable as the spam distributed domain is limited to one domain.

The way spam senders send spam mails are categorized into three types.

1. Spam senders refer MX RR from dynamic IP addresses to send spam mails directly to target MTAs.

2. Spam senders send spams via webmail MSAs.

3. Spam senders obtain static IP addresses to send spam mails.

OP25B prevents approach 1. By introducing OP25B, network operators can focus on actions against spam mails from static addresses.

At the time OP25B was first introduced, there were two issues that we needed to consider. Submission port (port number 587) was not yet fully adopted, and the number of filtering rules hit performance of network routers. These have been solved these days, enabling easier OP25B deployment. While OP25B becomes widespread in this decade, this document summarize current OP25B practices to help newly introducing the blocking.

2. Terminology

- Mail User Agent(MUA): user application which submit email messages to MSA

- Mail Submission Agent(MSA): program which receive submitted email messages from MUA and forward them

- Mail Transfer Agent(MTA): programs which receive forwarded email messages from MSA or MTA and forward them

- submit: The action by the MUA of entrusting the deliveries of email messages to MSA

- forward: actions which MTA(or MSA) entrust the deliveries of email messages to other MTAs

- subscriber: User who establishes account(s) with some ISP(s) to obtain Internet connectivity

Figure 1 and Figure 2 are the typical pattern diagrams of mail components. Figure 1 is the diagram which single server doubles as MSA and MTA. Figure 2 is the diagram which MSA and MTA are separated.

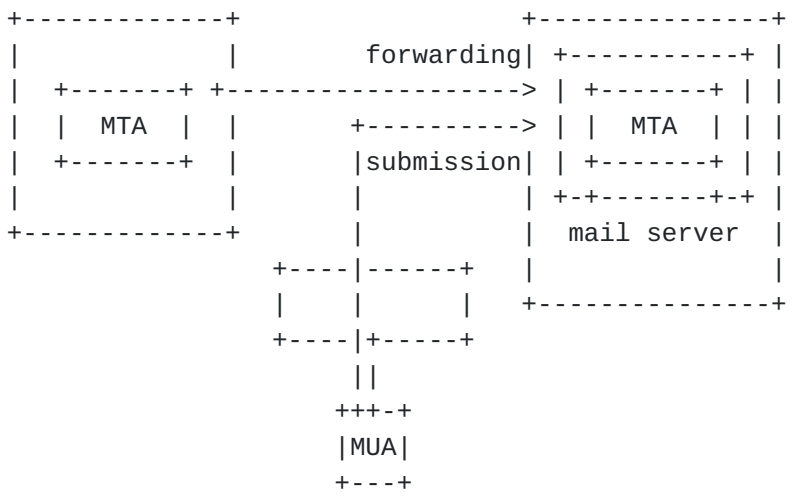

Figure 1: Single server model

In Figure 1, single SMTP server utilizes port 25 both for submissions and forwarding, that is, MSA and MTA cannot be distinguished. In this document, submissions to this kind of SMTP servers are called "submissions to MTA". In Figure 2, different SMTP servers engage in submissions and forwarding respectively, that is, MSA and MTA can be distinguished. In this document, SMTP servers which serve port 25 for mail submissions are called MSA[25].

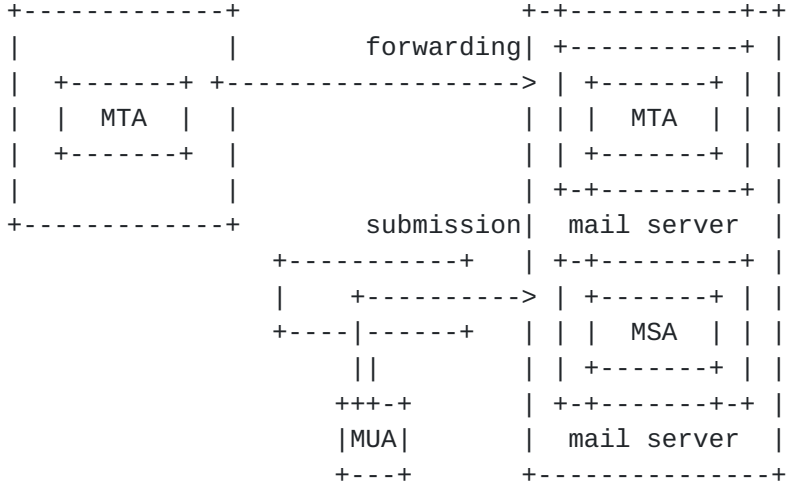

Figure 2: Separate server model

3. Mail Distribution Models

3.1. ISP models

In this document, we categorize ISPs into 3 types:

1. ISP model A: ISP that provides Internet connectivity services to other ISPs (model B)

2. ISP model B: ISP that depends on end-user Internet connectivity on other ISPs (model A)

3. ISP model C: ISP that utilize their internet connectivity for their own services only.

Figure 3 shows how end clients are connected to the Internet through 3 types of ISPs.

- (A): the Internet connectivity for subscribers of ISPs of model A

- (B): the Internet connectivity for subscribers of ISPs of model B

- (C): the Internet connectivity for subscribers of ISPs of model C

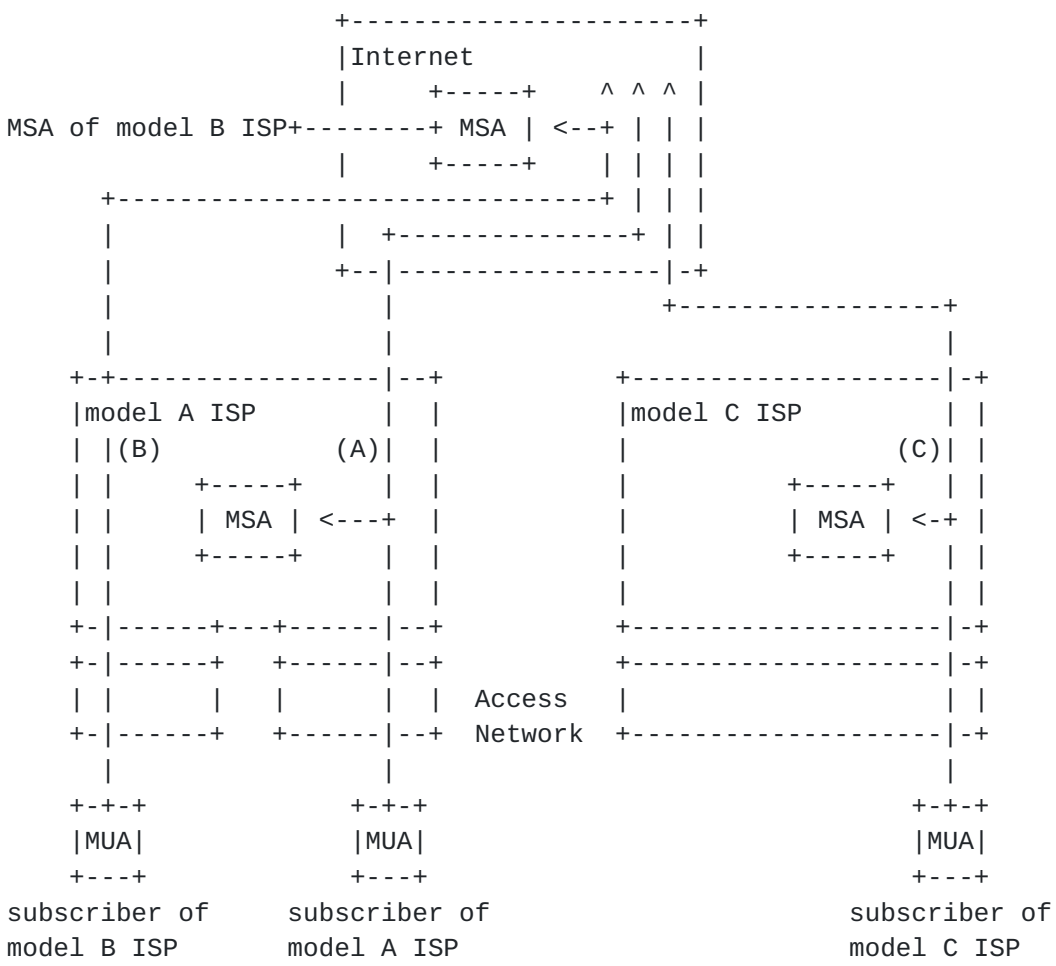

Figure 3: ISP models

All subscribers of ISPs of model A and model C are connected to the Internet via ISPs to which they subscribe. In Figure 3, MSAs for these subscribers are located in ISPs users are subscribing to. Lines with labels (A) and (C) in the figure depict the communication between MSAs and clients in ISPs of model A and model C respectively. Subscribers in the ISPs of model B are connected to the Internet via ISPs of model A. This is shown by the line labeled as (B) in the figure. In this case, MSAs are located somewhere on the Internet.

3.2. Mail distribution path

3 figures in this section show the mail distribution paths in the current mail architecture. These figures depict "valid mail submission" scenario, "invalid mail submission" scenario and "valid mail forwarding" scenario respectively. In the figures, ISP A is the mail sender, and ISP B, ISP C and "ASP/Hosting/Business Enterprise/ Academic institution" are mail receivers.

- ISP A: ISP of model A
- ISP B: ISP of model B
- ISP C: ISP of model C
- MUA: Client PCs which obtain dynamic IP addresses and run MUAs. These MUAs include:
  - Valid User PCs: ISP subscribers' PCs (not include spam senders or bots)
  - Spam senders
  - Bots

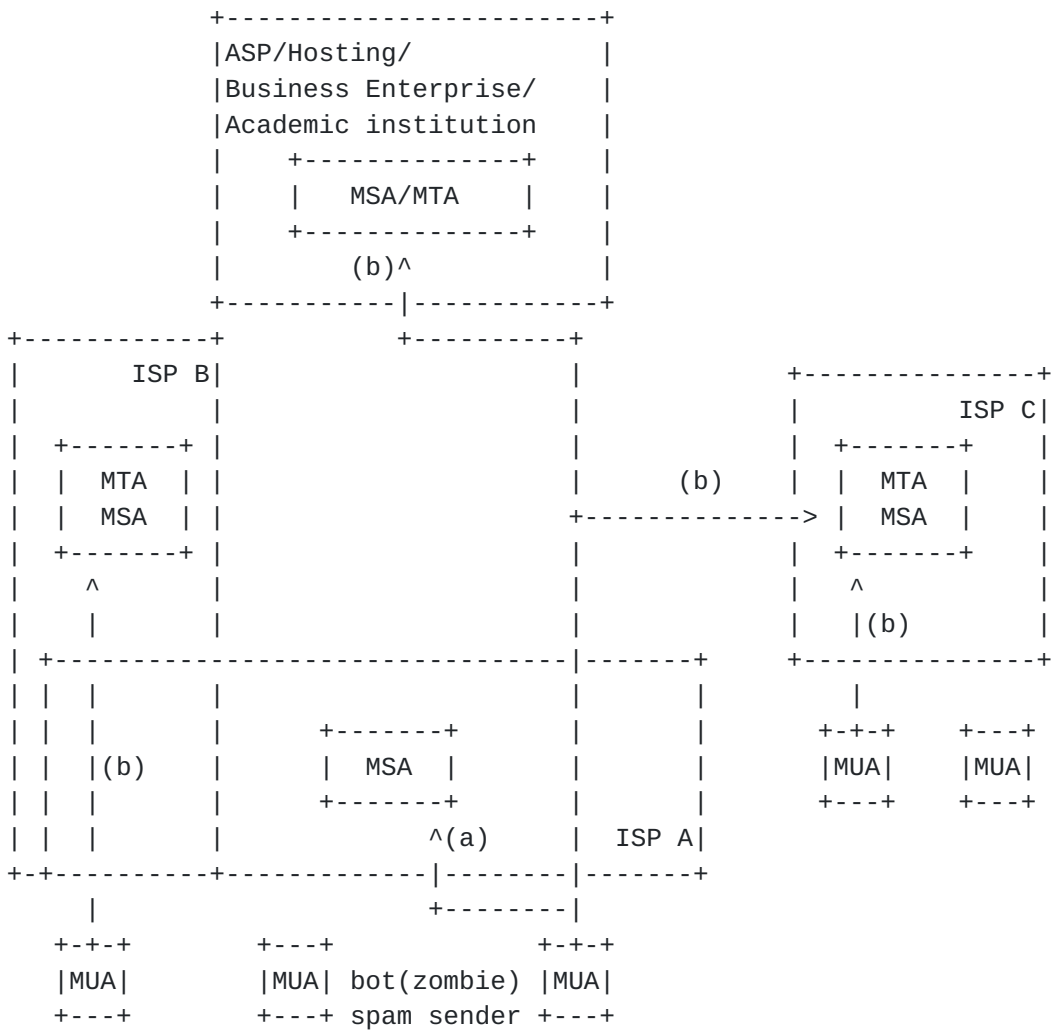

Figure 4: Valid Mail Submission

Figure 4 shows valid mail submissions by ISP subscribers. These submissions MUST NOT be disrupted by OP25B.

- (a): submissions from MUA to MSA of ISP A

- (b): submissions from MUA to MSA located outside of ISP A

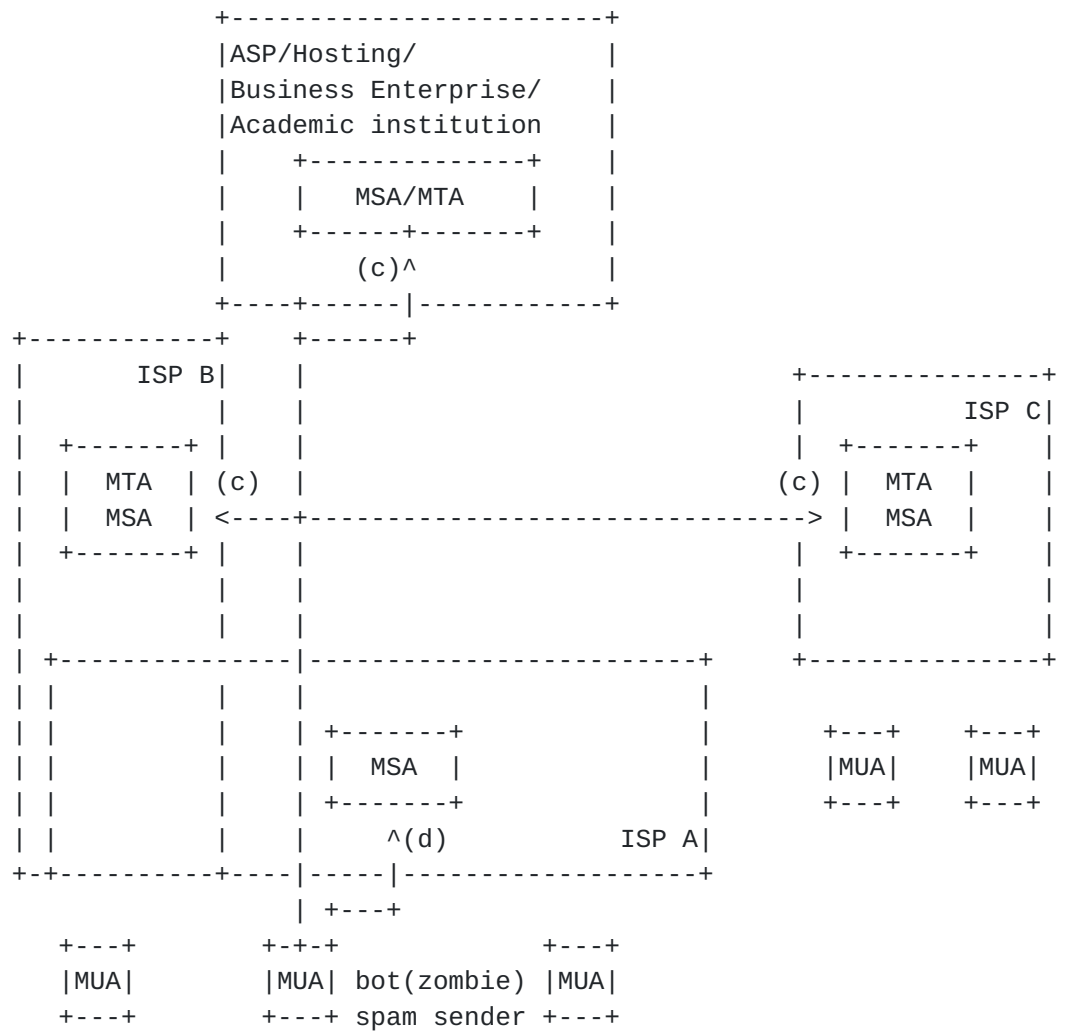

Figure 5

Figure 5 shows invalid mail submissions by spam senders or bots. These submissions are the block target of OP25B.

- (c): submissions from spam senders or bots to MTAs located outside of ISP A

- (d): submissions from spam senders or bots to MSAs of ISP A

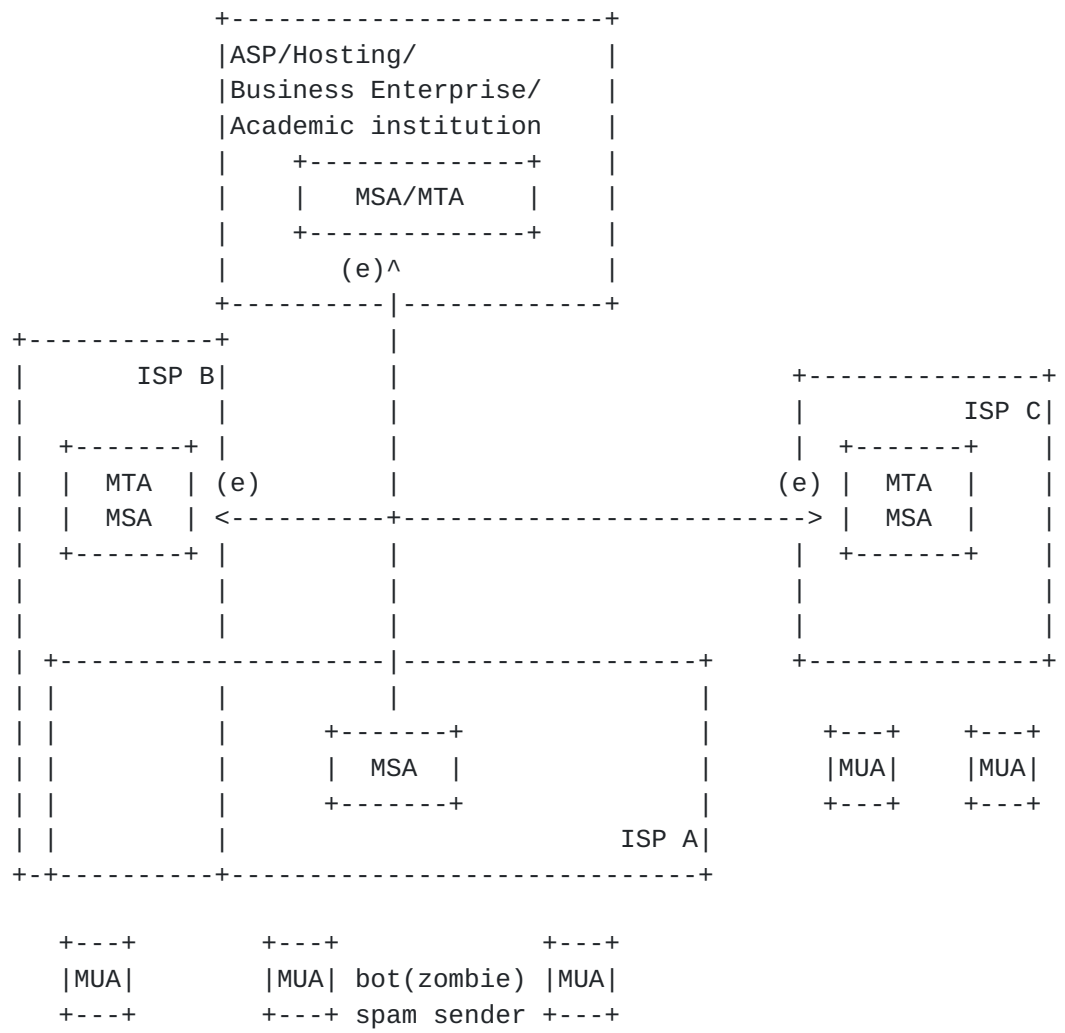

Figure 6: Valid Mail Forwarding

Figure 6 shows valid mail forwarding between MSAs and MTAs. The forwarding MUST NOT be disrupted by OP25B.

o (e): mail deliveries between MTAs or deliveries from MSAs to MTAs

3.3. Spam sender strategies and countermeasures

Spam senders' strategies can be categorized into two patterns:

1. Pattern I: submit spam mails to MSA and let the MSA to distribute them.

2. Pattern II: submit spam mails directly to target MSAs from dynamic IP addresses.

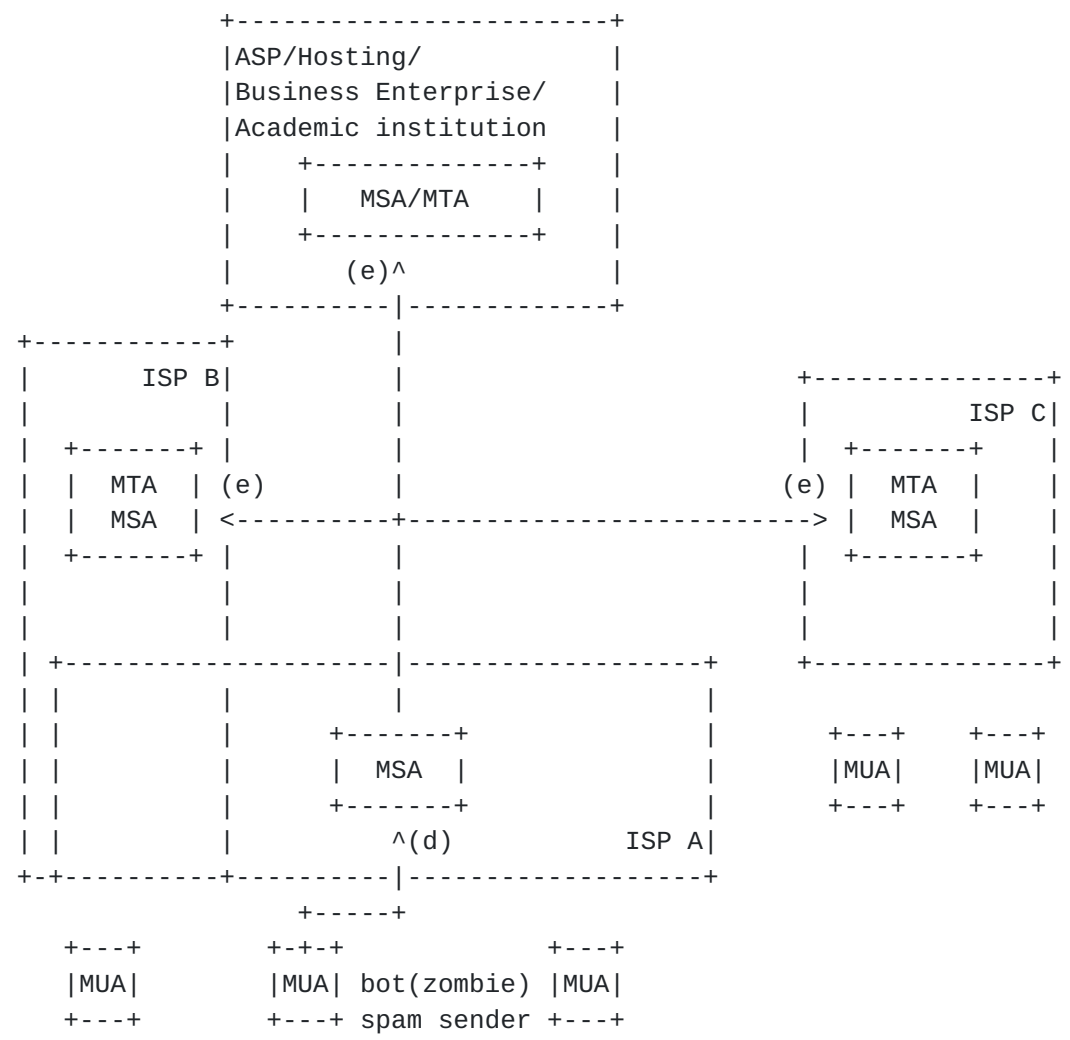

Figure 7: Spam sender strategy: Pattern I

Figure 7 shows a spam sender strategy of pattern I. First, spam senders submit spam mails to the MSA (line labeled with (d)). Then, the submitted spam mails are delivered to MTAs of target domains (line labeled with (e)). In this scenario, the mail distribution paths are same as one via which subscribers send valid email messages. Possible countermeasure is to set a quota with user authentication.

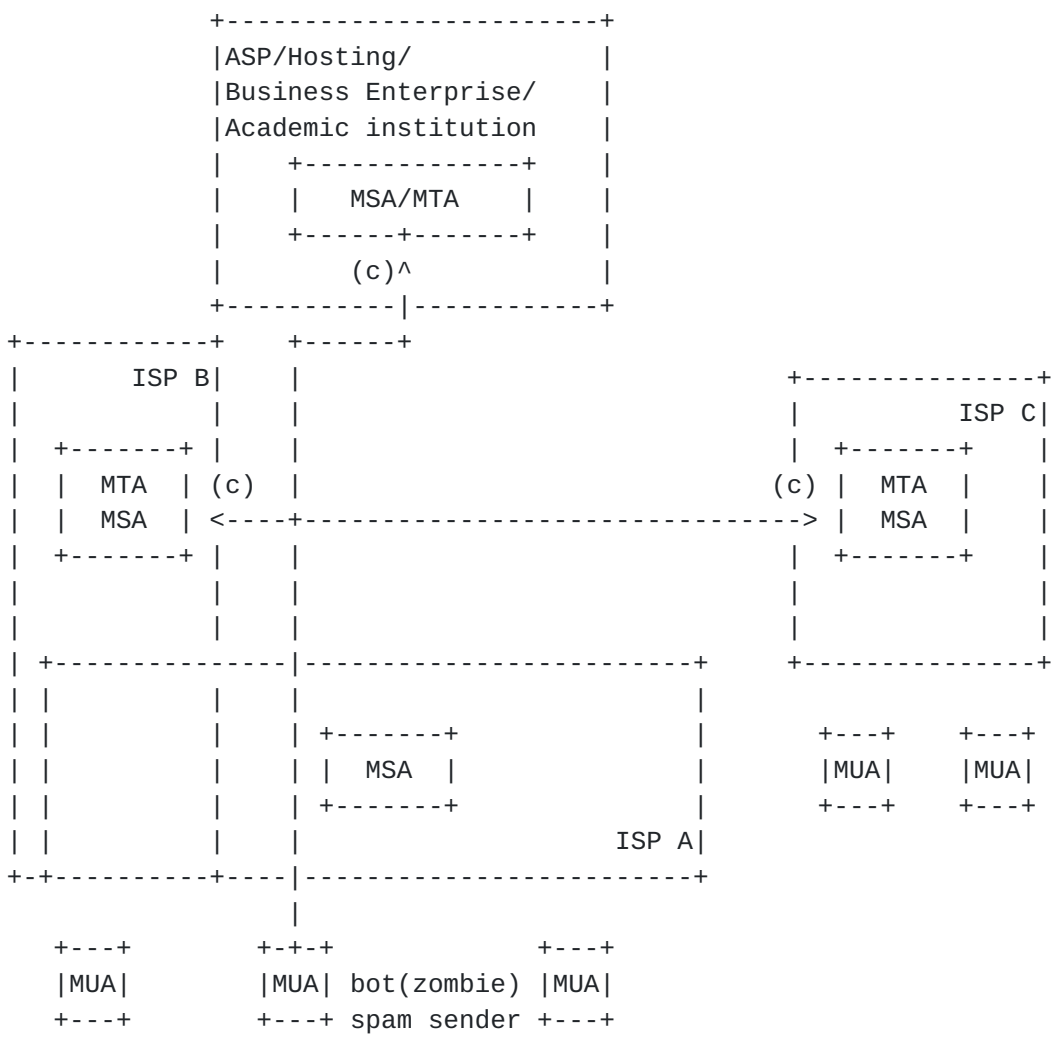

Figure 8: Spam sender strategy: Pattern II

Figure Figure 8 shows a spam sender strategy of pattern II. First, spam senders obtain dynamic IP addresses on their client PCs. Then, spam senders send spam mails directly to MTAs in target domains from the dynamic IP addresses. (lines labeled with (c)) A countermeasure for this strategy is OP25B.

4. Outbound Port 25 Blocking

In this document, we define OP25B as "filtering of the TCP traffic which the source addresses are dynamic IP addresses and the destination port is 25". In Section 3.2, we explained the relation between mail distribution paths and OP25B in Figure 4, Figure 5, and Figure 6. The alphabets "a" to "g" in the following paragraph refers to the arrows labeled with those alphabets in the above three figures.

After ISP A implements OP25B, a mail sender can send email messages via MSA which ISP A serves (a, e) while they cannot send email messages via other paths (c). Thus subscribers of ISP A are ensured a method to send email messages via MSAs. By OP25B, operators can prevent spams sent by spam sender strategy pattern II.

OP25B is implemented by configuring access control lists (ACL) on the network devices located on the ISP backbone networks. We call the location where those network devices are located "blocking points".

Below is an example of filtering policies to filter spams from dynamic IP addresses.

1. Allow traffic from dynamic IP addresses to port 25 of designated MSAs

2. Deny all traffic to port 25 of MSAs other than MSAs described in 1

3. No filtering rules for static IP addresses

This is one of the simplest filtering policies. The access control rules could differ depending on the specifications of the devices to filter or services policies of network domains.

The numbers of ACL rules are calculated using this formula:

(# of ACL rules) = (# of dynamic IP address blocks) * (# of MSA address blocks + 1)

For example, if the number of dynamic IP address blocks is 100 and the number of MSA address blocks is 10, the number of ACL rules is 1100 = 100 * (10+1). The number of ACL rules directly influences the costs such as filter performance of the network devices and/or filter rule management of network operators. In this example, the ISP which intends to implement OP25B has to introduce network devices that have enough performance to handle 1100 ACL entries. In the model A ISPs, the number of MSA address blocks to "permit" can be increased dependent on the numbers of ISPs of model B to serve connectivity. On the other hand, the number of ACL entities are generally fewer in ISPs of model C, because they can concentrate on their internal MSAs only.

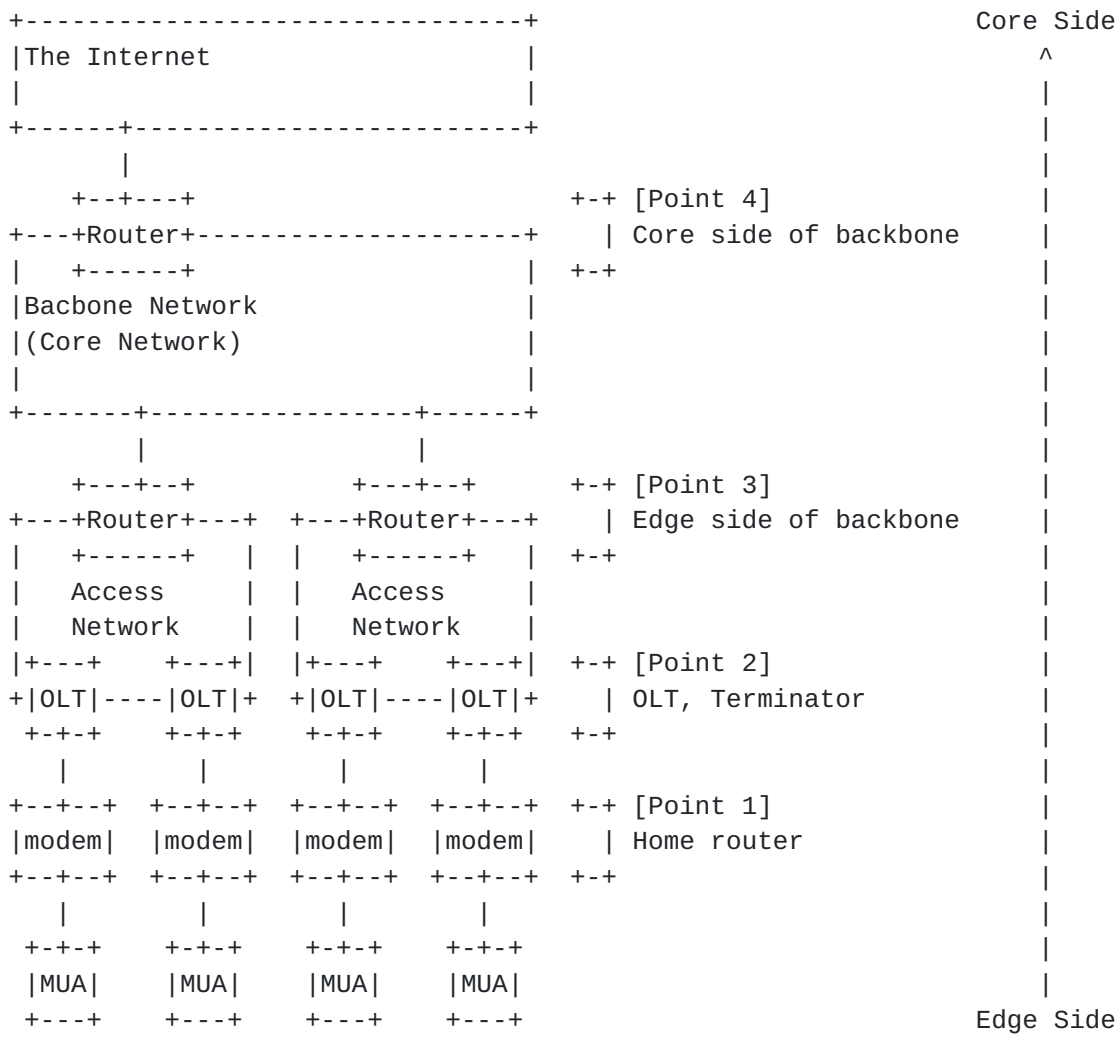

Figure 9: Blocking point analysis

Figure 9 shows a blocking point analysis in a backbone network. If the blocking point get closer to the "core side", the performance requirements for the filtering network devices increase while the number of the network devices operators have to configure comes down. On the other hand, If the blocking point get closer to the "edge side", the performance requirements for the filtering network devices decrease while the number of the network devices operators have to configure comes up.

In the case point 1 is selected as the blocking point, the filtering configurations are set to home routers in subscribers' home networks. The advantages of this approach are:

- Fewer ACL rules on each network devices

- No spam mail traffic to the backbone network
- No additional configurations to the network devices in the backbone network

The ISPs who can employ this method are the ISPs which can control home routers from network operations centers.

In the case of point 2, the blocking point is set to the terminating devices of the access networks. The configurations are done using Radius attributes.

In the case of point 3, the blocking points are the routers located between access networks and the backbone networks. This approach is expected to be most common.

In the case of point 4, the network devices located near to the ISP border gateways are the blocking point. In this case, relatively small amount of the devices are engaged in filtering and huge amount of ACL rules are configured to each network devices. The performance requirements for the devices are high enough to withstand the load.

4.1. Deployment Considerations

As mentioned in Section 2, currently port 25 is used for mail submissions. When the complete OP25B is employed by an ISP, the subscribers in the ISP get not to be able to send email messages in the cases below.

1. Subscribers use other MSAs than ones located inside the ISP. In this case, the subscribers subscribe to multiple ISPs.
2. Subscribers use the MSAs served by hosting providers or ASPs.
3. The ISP is a model B ISP.

In all the cases listed above, subscribers uses the MSAs located outside of the ISPs which they subscribe. In this document, we call this kind of submission "submissions to third-party servers". The implementation of OP25B causes problems with submissions to third-party servers. Figure 10 shows this problem. The number of the arrows in Figure 10 is correspondent to the number in the list above.

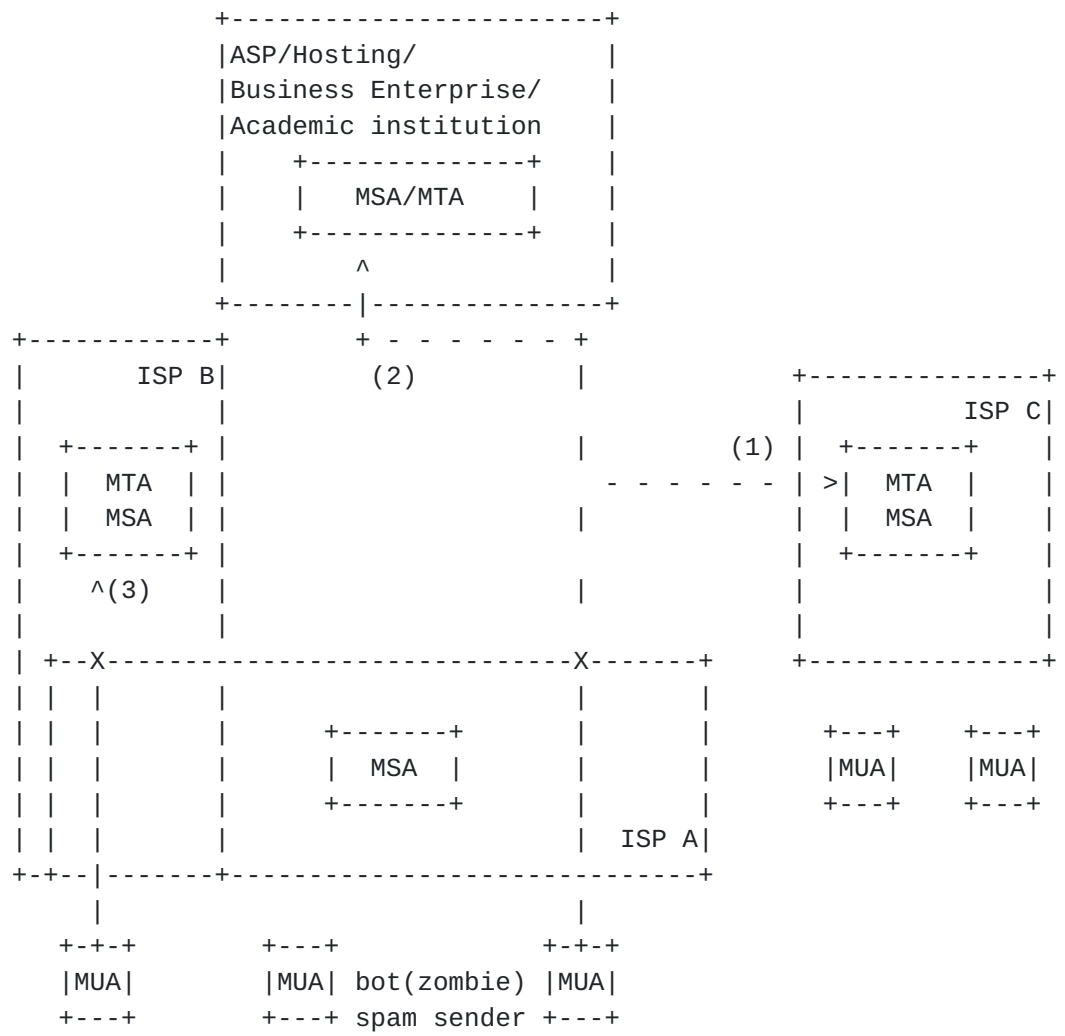

Figure 10: Problem with complete OP25B

ISP A in the figure is an ISP of model A, and ISP B is an ISP of model B. As described in former sections, mail submissions of subscribers in ISP B are forwarded through the backbone network of ISP A to MSAs of ISP B. When ISP A implements OP25B, the path of the line (3) is blocked by the operation. Then subscribers of ISP B cannot submit to their MSAs.

MUAs can use port number other than 25 for submissions to avoid this problem.
As described in [RFC6409], MUAs can use the submission port (port 587) for submissions.

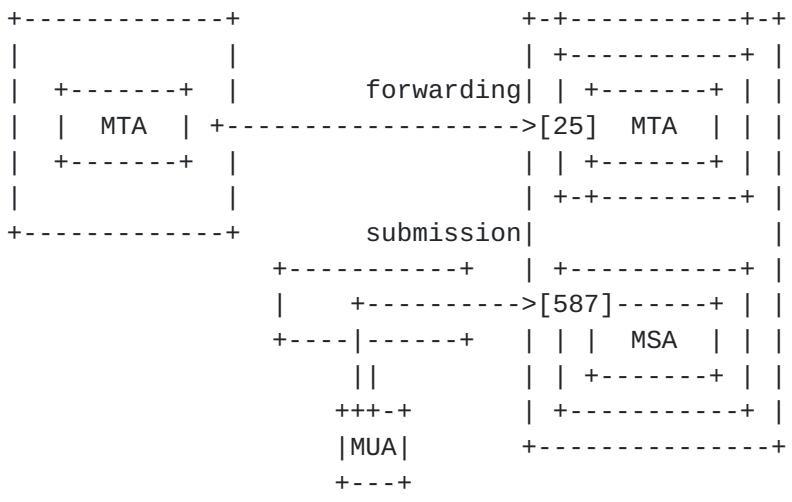

Figure 11: Complete OP25B with submission port

Figure 11 shows a typical SMTP server configuration for complete OP25B. In this figure, MTA receives forwarded email messages on port 25 and MSA accept submissions from MUAs on port 587. With this configuration, users can keep submitting to their MSAs using the submission port that OP25B does not affect. We detail the use of submission port in a following section (Section 4.2).

4.2. Submission port (587)

- Mail system operators MUST serve MSAs which support the submission port (port number 587).
- The operators MUST implement SMTP Auth on the MSAs.
- Even for the local mail distributions, the subscribers SHOULD use SMTP Auth.
- The POP ID/Password pairs SHOULD be identical with AUTH ID/ Password of SMTP Auth.
- MSAs MUST NOT serve POP before SMTP.
- These operations are for the operators of MSAs which accept submissions from global IP addresses.

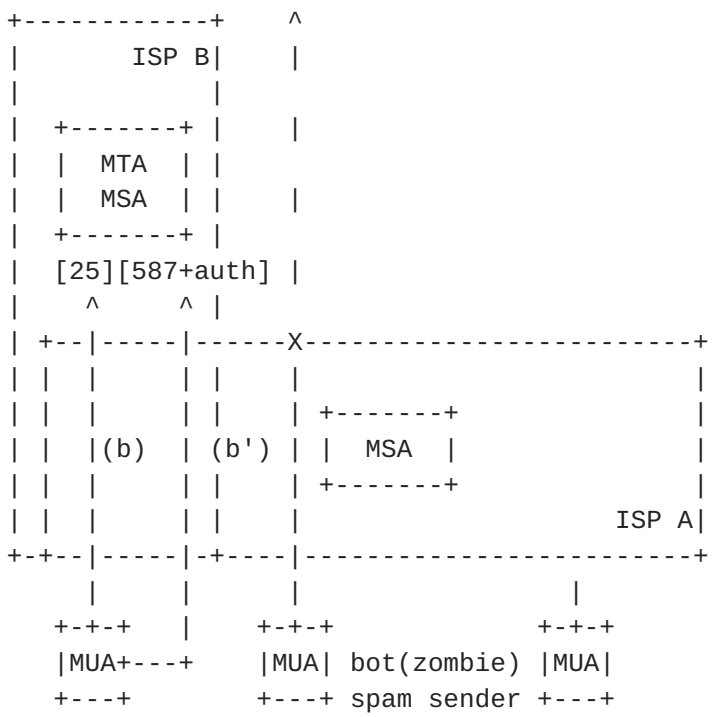

Figure 12: OP25B with submission port

In Figure 12, if the ISP A implements OP25B, the line (b) becomes a blocking target of the operation. In this case, subscribers become not to be able to keep using services they could utilize before. The ISP have to serve alternatives for the subscribers of ISP B to perform valid submissions to third-party MSAs of ISP B. One of the alternatives is the submission port (port number 587). A submission to the submission port of an MSA in ISP B is depicted as the line (b'). The operators of MSAs which are used as third-party servers MUST serve the submission port immediately after the implementation of OP25B on ISP A. Then, subscribers can send email messages by re-configuring their MUAs properly.

When an MSA provides submission port, operators of the MSA MUST implement SMTP AUTH on it. In this case, the local mail distribution SHOULD be achieved via SMTP AUTH to prevent spam mails to the local domain.

The POP ID/Password pairs SHOULD be identical with AUTH ID/Password of SMTP Auth. In this case, MUAs can use POP ID/Password pairs to the authentications if AUTH ID/Password pair is not configured.

If SMTP AUTH is not implemented in the domain, spam sender simply switch their mail submission port from 25 to 587 and keep sending spams using the spam sender strategy pattern I as described in Section 3.3. After the implementation of SMTP AUTH on port 587, the

operators can limit the number of email messages sent by single user ID.

MSAs MUST NOT serve POP before SMTP because of its architectural defect. In the POP before SMTP architecture, POP servers store the IP addresses from which the POP authentications succeeded for certain periods, and verify mail submissions using the IP address list. That is, if the IP addresses from which the MTA receives submitted email messages are in the IP address list, the submissions are taken as valid.

This IP address based authentication causes a serious security problem. Suppose a client which has successfully succeeded the POP authentication leaves the network. If a malicious node obtains the same IP address while the POP server still hold the IP address in the valid IP address list, the malicious node can send spams freely.

When the valid IP addresses are the global addresses of the NAT routers, the situation gets worse. In the case multiple MUAs behind a NAT router utilizes a same MSA located on the WAN side and a client PC which runs MUA get infected by a bot, the bot can send email messages via the MSA after an MUA on another PC has done the POP authentication for the MSA. If the healthy PC is configured to do the POP authentications periodically, it effectively cancels POP before SMTP authentication from the LAN behind the NAT router.

4.3. Complete migration to submission port(587)

- For mail submissions, MUAs MUST utilize MSAs which support both of the submission port(port 587) and SMTP Auth.
- The mail system operators MUST abolish the use of MSAs which utilize the port 25.
- The operators MUST deny submissions to MTAs.
- This operation is for the operators of MSAs which accept the submissions from global IP addresses.

As mentioned in Section 3.3, the mail quota using SMTP AUTH is workable against the spam senders' strategy pattern I. For this operation, all the mail submissions must be done with SMTP AUTH. While ISPs of model C do not need to sweep away the MSAs with port 25 and MTAs after all the submissions are completely done with SMTP Auth, the ISPs SHOULD migrate to port 587 for the users' convenience if deployments of SMTP AUTH are still not be completed. The operation in the model C ISP is described in the following section(Section 4.3.1).

For the completion of this operation, all the subscribers have to change the configurations of their MUAs. ISPs MUST encourage their subscribers to change the configurations of their MUAs.

Proposed migration steps are:

1. Operators of mail systems prepare MSA(s)[587+Auth] other than MTA/MSA[25].

2. For new subscribers, prepare the guidance of MSA[587+Auth] only.

3. For subscribers who need to change the configuration of MTAs on their MUAs (for example, users who want to change their mail addresses), show them a configuration guideline of MSA[587+Auth] only.

4. encourage all other subscribers to change their MUA configurations to MSA[587+Auth]

The focuses or problems of the complete migration vary by the ISP models and network configurations. We explain the focuses and problems for 3 models below in the following sections.

1. ISP of model C

2. ISP of model A and B

3. providers which cannot identify submission sources (ex) ASP)

Essentially, the categorization of the ISPs (model A, B and C) is not the categorization of the ISPs themselves but of the services which the ISPs provide for their subscribers. (An ISP can provide one service categorized as model A and another service of model B simultaneously) For simplicity, we use the above categorization over ISPs themselves in the following sections.

4.3.1. ISP of model C

Operators of model C ISPs are able to implement OP25B while their MSAs and MTAs keep accepting submissions for port 25. This is because their OP25B implementations do not influence on mail services on other ISPs. Therefore, the operations described in Section 4.3 are not required in IPSs of model C.

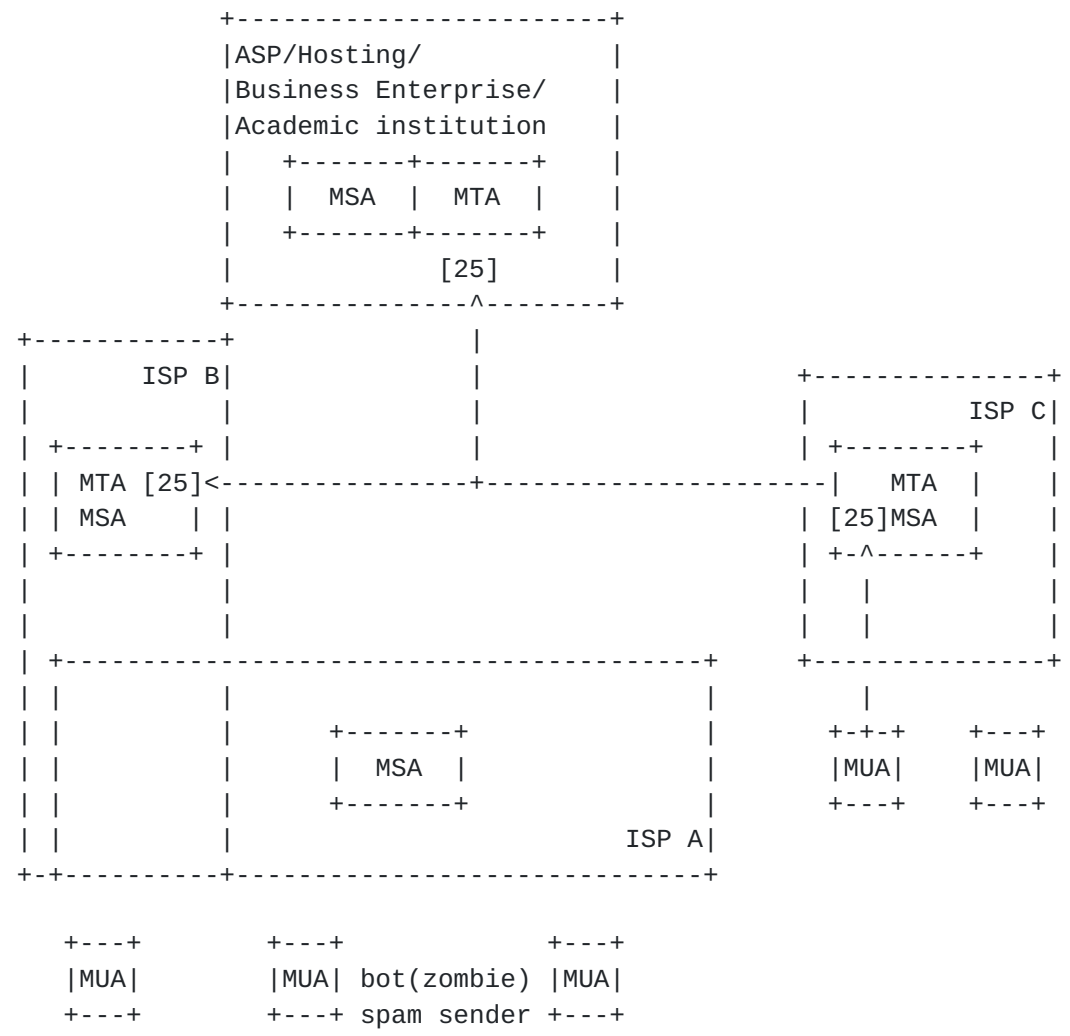

Figure 13: Mail distribution path after OP25B in ISPs of model C

4.3.2. ISP of model A and B

- Operators of model B ISPs SHOULD cooperate with operators of model A ISPs.

- Operators of model A ISPs SHOULD accept the requests from model B ISPs.

- Operators of model A ISPs MUST keep their mail distribution paths for MSA[25] and MTA[25] until all the subscribers of model B ISPs complete the migrations to MSA[587+Auth].

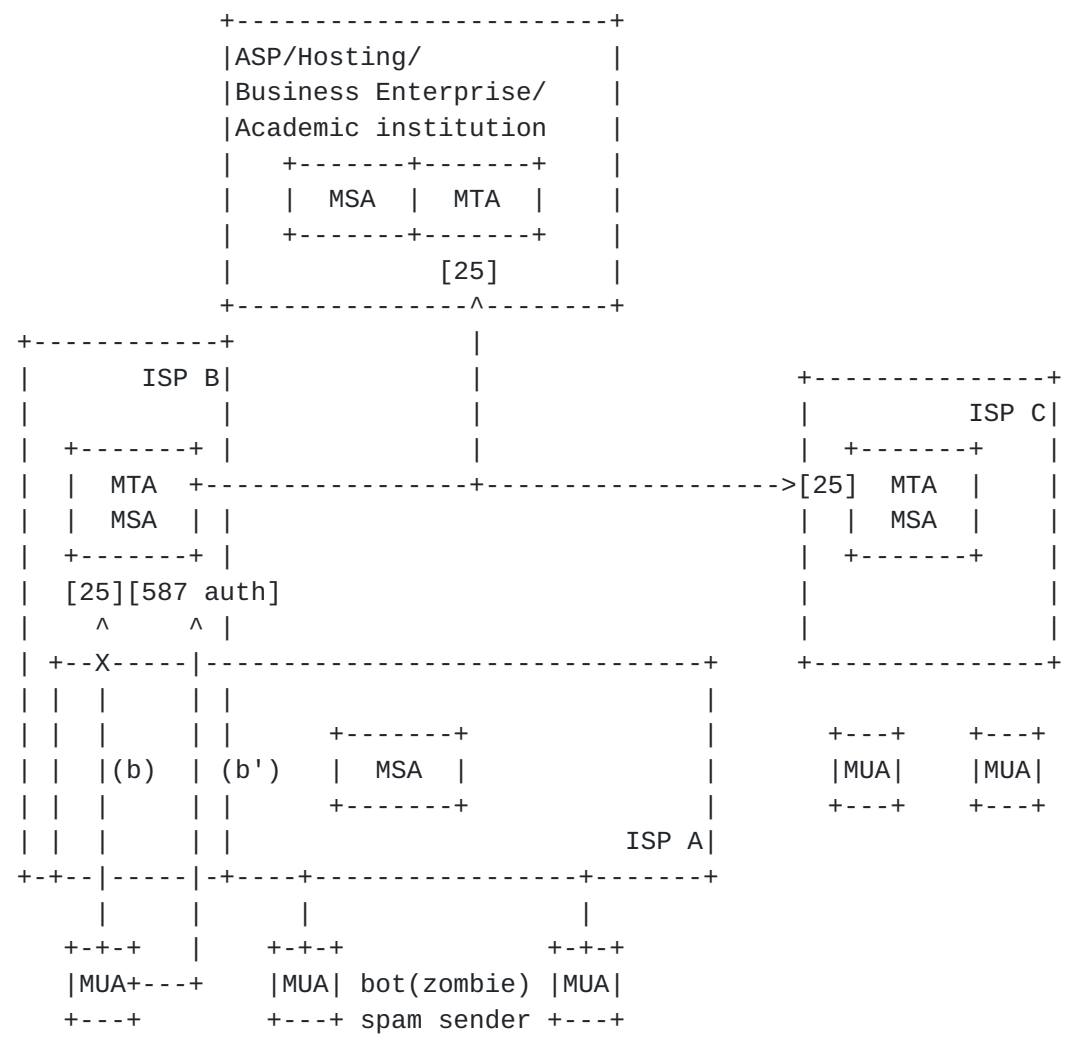

Figure 14: Mail distribution path of model B ISP

In Figure 14, after ISP A implements OP25B, the subscribers in ISP B become not to be able to submit to their MTAs[25] and MSAs[25] (line (b)). Because ISP B does not have own backbone network and IP address blocks for subscribers, ISP B depends the implementation of OP25B on ISP A. Therefore, ISP A and ISP B have to cooperate with the implementation of OP25B.

Before the implementation of OP25B, ISP A and ISP B MUST choose one of the operations below.

1. ISP A permit the mail submissions from MUAs in ISP B to MSA[25] or MTA[25] of ISP B.

2. Subscribers of ISP B "completely" migrate SMTP server configurations of their MUAs to MSA[587+Auth]

If ISP A and ISP B choose 1, the ACL problems arise in ISP A as described in Section 4. Regarding to the choice 2, the implementation of OP25B will be delayed. Below is a practical procedure of the OP25B implementation of ISP A and ISP B.

1. ISP B aggregates the address blocks for MSAs as few as possible.

2. ISP A permits submissions from subscribers of ISP B to MSAs[25] or MTA[25].

3. ISP A implements OP25B.

4. Subscribers of ISP B migrates SMTP server configurations of their MUAs to MSA[587+Auth].

5. ISP B stops to accept submissions to MSA[25] or MTA[25].

The transition period is desirable to be as short as possible.

4.3.3. Providers which cannot identify submission sources

Providers which cannot identify submission sources MUST migrate to MSA[587+Auth] immediately. This operations is for the operators of MSAs which accept submissions from global IP addresses (especially for the operators of ASP or hosting companies).

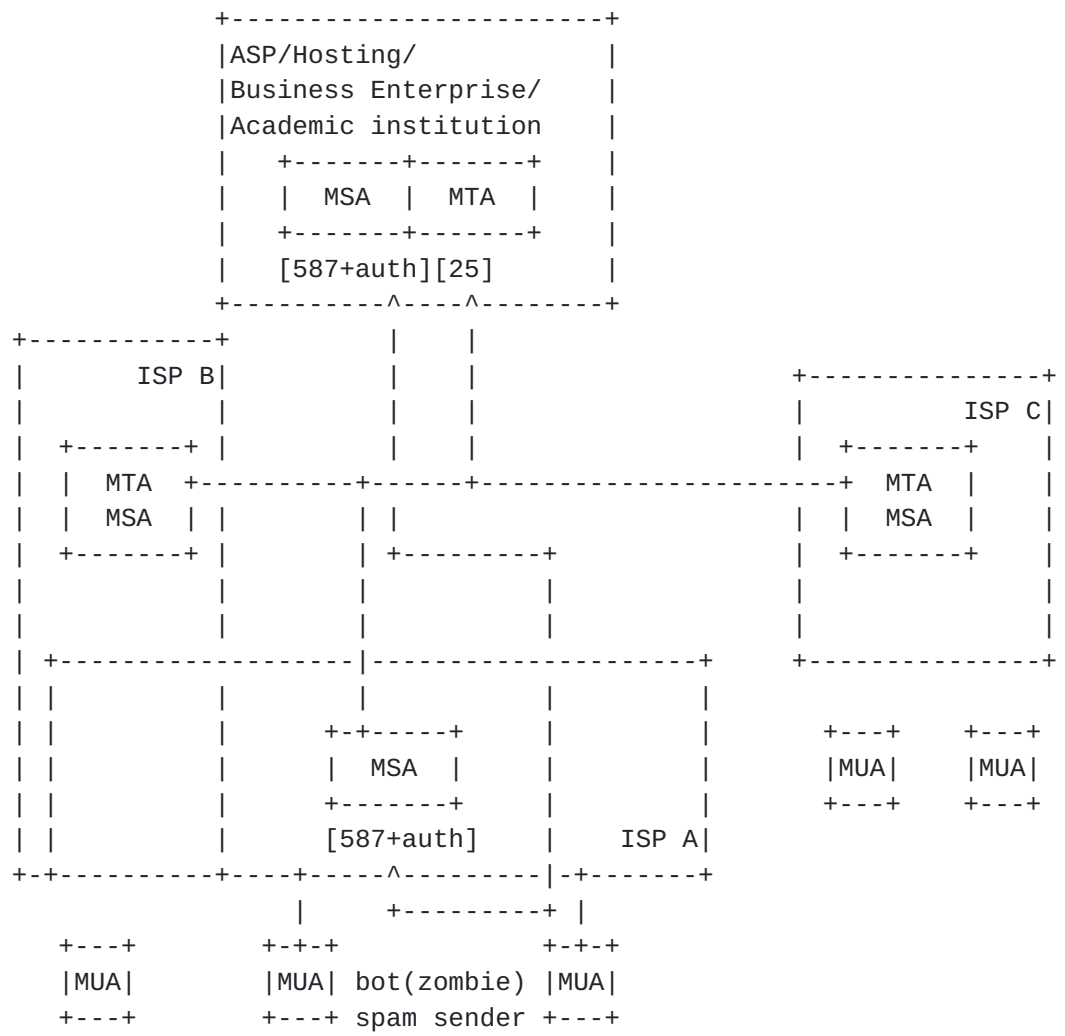

Figure 15: Mail distribution path after OP25B in ASP of Hosting Providers

Providers which provide ASP services or hosting services cannot identify which ISP their users submit their email messages from. Such is the case with companies or academic institutions which allow submissions from the Internet. These providers MUST setup MSA[587+Auth] immediately and encourage their users to change their MUA configurations.

Because it requires time to implement SMTP AUTH, it is expected that these provides need to utilize POP before SMTP on the submission port as a temporary solution. Even in this case, as described in Section 4.2, the use of POP before SMTP is not recommended. It MUST be migrated to SMTP Auth as soon as possible.

4.3.4. Related item

In the case implementations of OP25B proceed, spam senders are expected to subscribe to the target ISP and send spams to the MTAs on the local domain. For this problem, ISPs SHOULD block the traffic from dynamic IP addresses of their IP address blocks to port 25 of MTAs. For this purpose, MSA and MTA have to obtain separated port numbers or separated IP addresses.

4.4. Considerations

4.4.1. Attacks against OP25B

- TCP traffic which the source IP addresses are dynamic IP addresses and the destination port is 25 MUST be blocked.

- Operators SHOULD implement some countermeasure for asymmetric routing attack and triangular spamming.

These operations are for the operators of ISPs.

As OP25B blocks the email messages directly submitted to MTAs (not via MSAs), spam senders cannot send spam mails to the target directly after the implementations of OP25B. At the same time, valid users can keep sending email messages via submission port. How to implement OP25B is shown in Section 4. In this section, we explain two notes while implementing OP25B.

We defined OP25B as "filtering of the TCP traffic which the source addresses are dynamic IP addresses and the destination ports are 25" in a former section (Section 4). Even after the implementations of OP25B, it is known that the spam senders keep sending spam mails using some characteristics of IP communications. This attack is called "asymmetric routing attack".

Figure 16 illustrates the asymmetric routing attack. First, the spam sender obtains two IP addresses, a static address and a dynamic IP address. The spam sender send spam mails which the source address is dynamic IP address via the network interface which has static IP address. Thus, the spam mails are transferred through the static IP address segment. If ACL for OP25b is not set on the gateway of the static IP address segment, the junk mails sent by the sender will be submitted to the target MSAs. The target MSA sends TCP responses to the dynamic IP address of the spam sender and the TCP connections from the spam sender to the target MSA are established.

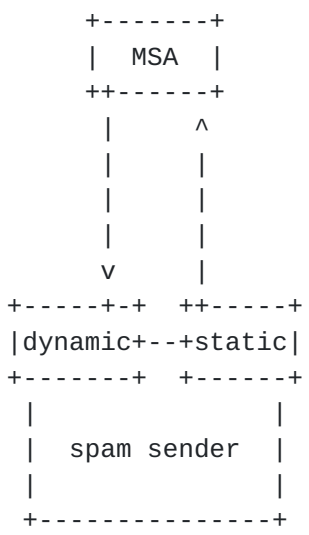

Figure 16: Asymmetric routing attack

"Triangular spamming"[Triangular] is a more generalized attack. Triangular spamming enables spam senders to bypass OP25B utilizing relaying nodes. Figure 17 illustrates triangular spamming. First, a spam sender sends IP packets which the source address is IP address of the spam relay node and the destination is the target MSA. As the source addresses are not the dynamic IP addresses of ISP1, the packets pass the ACL(s) of ISP1. The target MSA send responses which the destination is the spam relay node. The spam relay node forwards the packets modifying the destination IP address to the address of the original spam sender. This forwarded packets will be received by the spam sender not being blocked, because the in-bound ACLs are not configured in ISP1. Thus OP25B can be bypassed by triangular spamming.

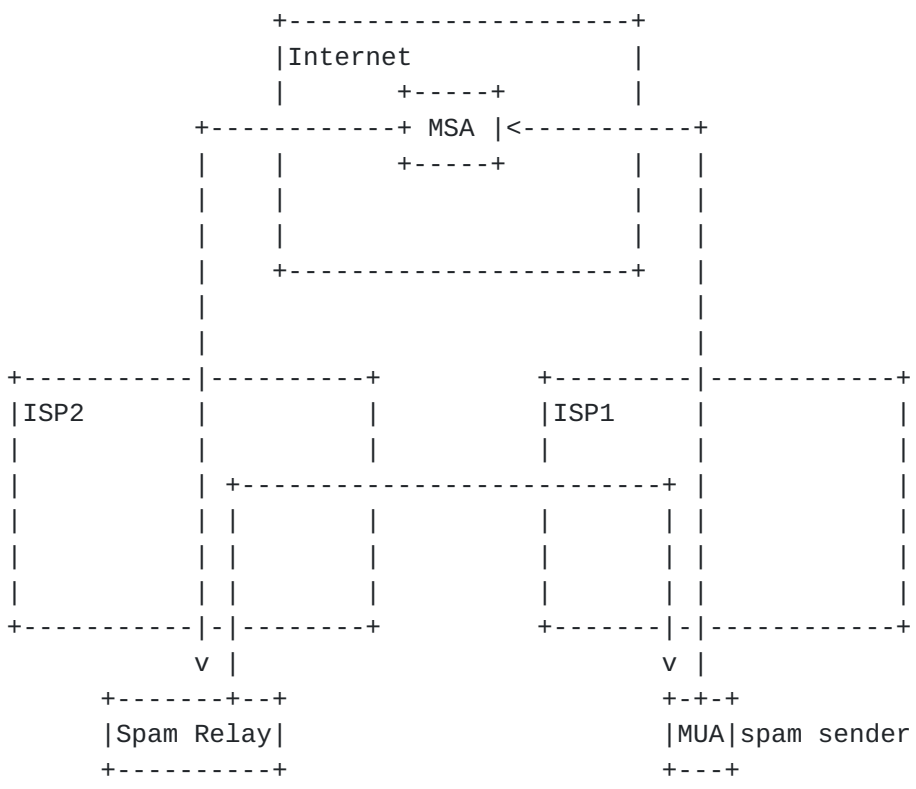

Figure 17: Triangular spamming

Countermeasures for these attacks are shown below.

1. Out of all the mail traffic from backbone networks to dynamic IP addresses, only the traffic which is from port 25 of designated MSAs are permitted. (traffic from "other MSAs" are blocked)

2. Prevent source address spoofing of the traffic from static or dynamic addresses to the backbone networks by source address validation.

For asymmetric routing attack and triangular spamming, the adoption of source address validation (item 2) is more desirable than inbound ACL (item 1). However, as the implementations of source address validation are burdens in many cases, at least the operators SHOULD employ the inbound ACL (item 1) until source address validation is ready on the domain.

4.4.2. Alternative MSA

o Operators SHOULD provide third-party alternative MSAs.

This operation is for the operators of ISPs.

To explain the need for alternative MSAs, we illustrate a mail user disrupted by OP25B.

1. User A is a subscriber of ISP A.

2. ISP A does not allow relays other than that for the email messages which the MAIL FROM field is within its own domain.

3. The user has another mail address "foo@example.com" than that of ISP A.

4. The MSA of "example.com" is located outside of ISP A and does not provide submission port.

5. The user cannot configure different FROM between Envelop and Header on her/his MUA.

If the ISP A implements OP25B in this situation, the illustrated user gets to lose MSA and is not able to submit email messages. In this case, ISPs SHOULD provide the MSA[587+Auth] which users can configure their MAIL FROM field freely. This operation is not only for the users subscribed to ISPs themselves but for the providers which still have not implemented MSA[587+Auth].

4.4.3. Mail quota

Operators SHOULD implement mail quota on MSAs utilizing SMTP AUTH. The number of the email messages SHOULD be counted by "RCPT TO".

After the implementations of OP25B and submission port, the only way mail senders submit their email messages is to use MSA[587+Auth] if the senders are using dynamic IP addresses. The way spam senders try to send junk mails via MSA[587+Auth] resembles to the spam sender strategy pattern I described in Section 3.1. As MSAs[587+Auth] can figure out the number of email messages sent from single user ID, operators SHOULD implement the mail quota using these mail sent counts. Operators have to decide the limit rate carefully not to influence on the mail deliveries of users other than the spam senders.

The number of outgoing email messages SHOULD be measured sorely by "RCPT TO". In [RFC5321], the minimum total number of recipients is defined as 100. If the maximum number of the MAIL FROM is also limited to 100, mail senders can send 10,000 email messages("MAIL FROM" * "RCPT TO") from single MUA. If the number is measured by "MAIL FROM" and not considering "RCPT TO", the combination tends to allow huge amount of outgoing email messages for each spam sender.

4.4.4. IPv6 Consideration

TBD

4.4.5. ACL rules to permit submission port

- Operators MUST configure to permit tcp 587 traffic to the Internet if MSAs which users have to communicate with are outside of their LANs.

In this section, we describe the problems with OP25B other than the problems related to submissions to third-party servers. After the implementations of OP25B, there are cases caused by the ACL configurations on routers or firewalls. For example, MUAs cannot submit email messages in the case "some companies or academic institutions are using dynamic IP addresses and rely the capability of MSAs on ASP or hosting providers, and the submission port (587) is blocked". In this case, operators of the routers and firewalls MUST permit the traffic to submission port (587). In the case of proxies, the situation is the same. Proxies MUST forward the mail traffic to submission port (587).

4.4.6. MTAs with dynamic IP addresses

- MTAs utilizing dynamic IP addresses SHOULD obtain static addresses.

If there is an SMTP server which obtain a dynamic IP address and resolves MX records to forward email messages directly to the destination MTAs, these forwarded traffic are blocked by OP25B configurations. Below are examples of this case.

1. The case the MTA is using dynamic IP address(es) and dynamic DNS.

2. The case send-only SMTP servers have dynamic IP addresses only.

In these cases, operators of the servers SHOULD obtain static IP addresses.

5. The goal of this document

After the implementation of OP25B, the mail distribution paths from ISP A are reformed as three figures below (Figure 18, Figure 19, Figure 20).

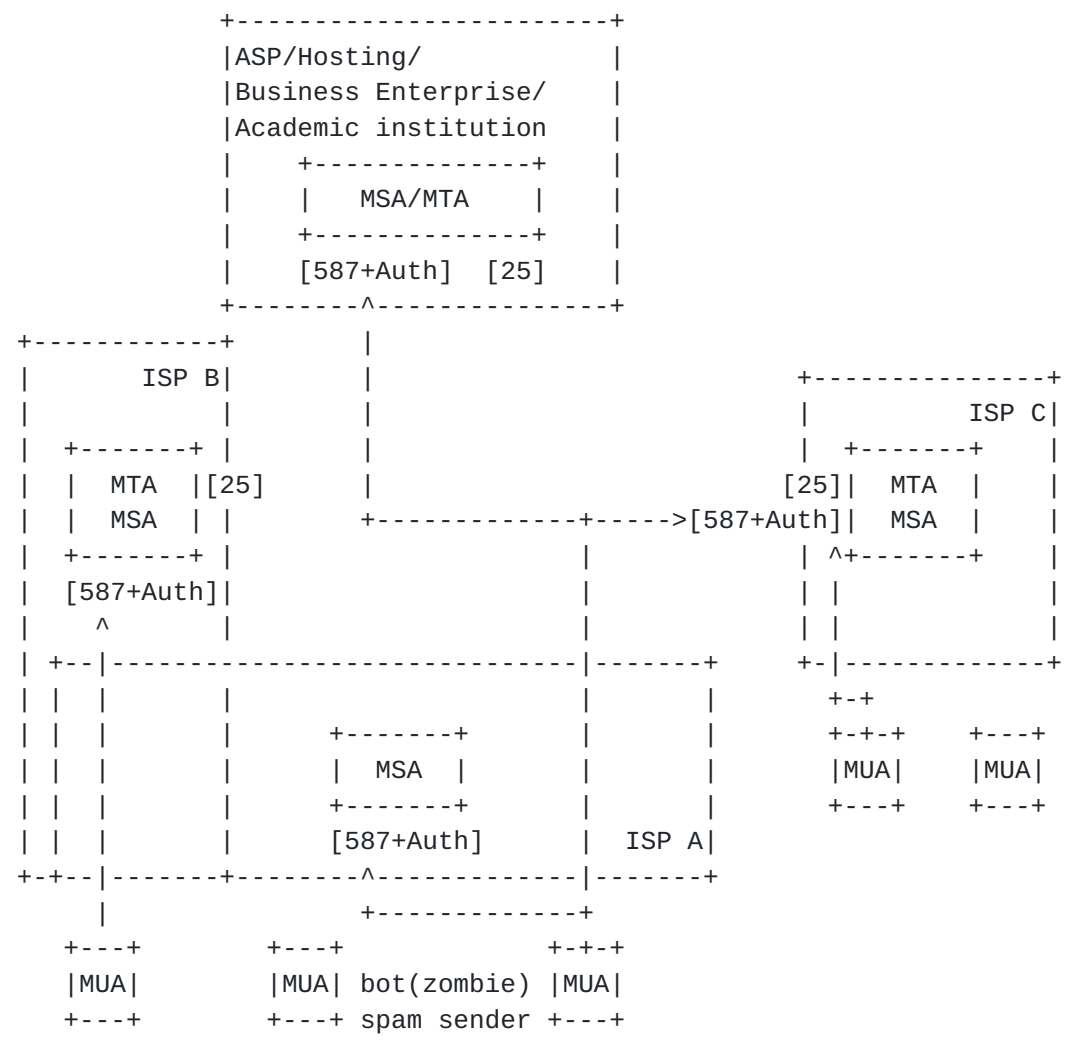

Figure 18: Valid mail submission after OP25B

Figure 18 depicts the valid mail submissions from MUA in ISP A. All the email messages are submitted to port 587 of MSAs. Even for the local domain submissions, MUA SHOULD use the submission port(587).

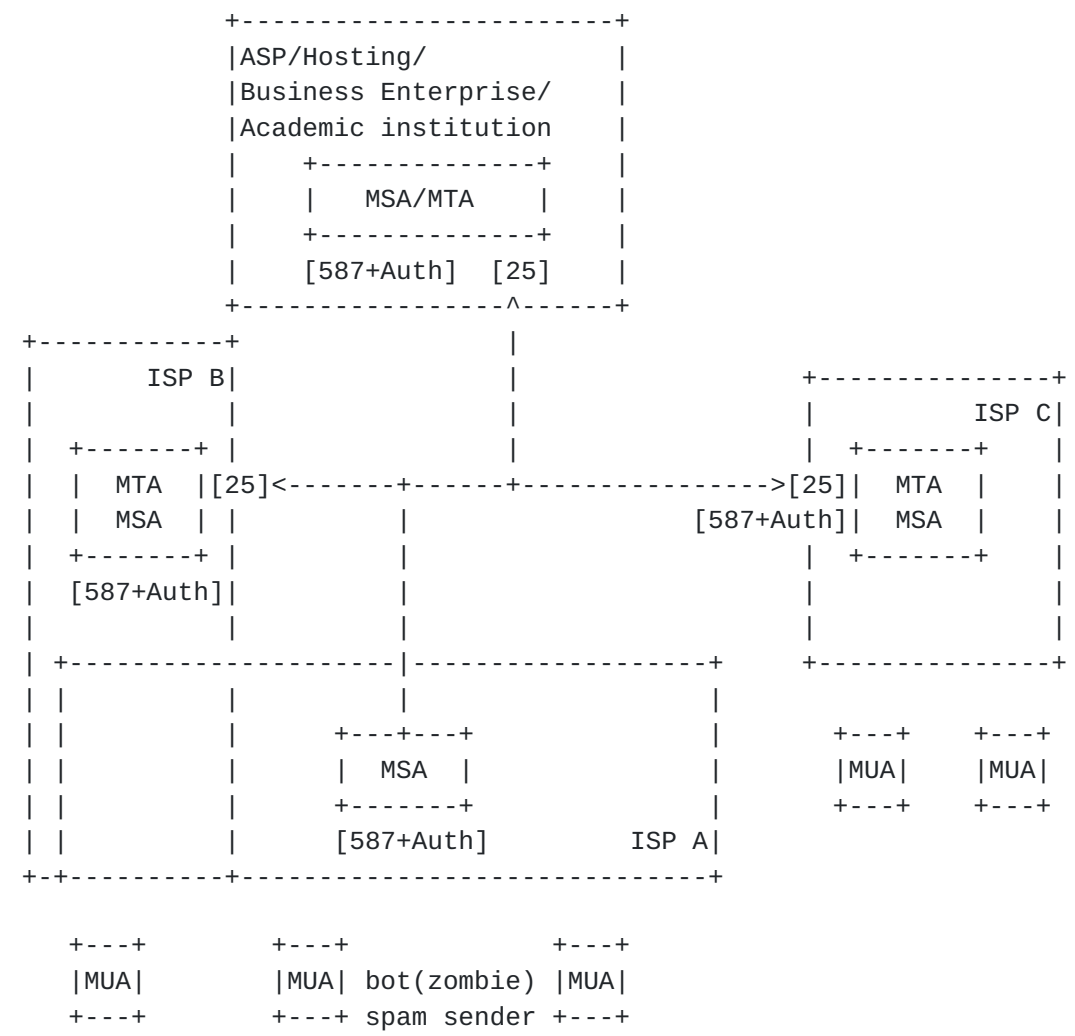

Figure 19: Valid mail forwarding after OP25B

MSAs in ISP A forward submitted email messages to port 25 of MTAs outside of ISP A. Because MSAs are allocated static IP addresses, the ACL rules of OP25B do not match the traffic.

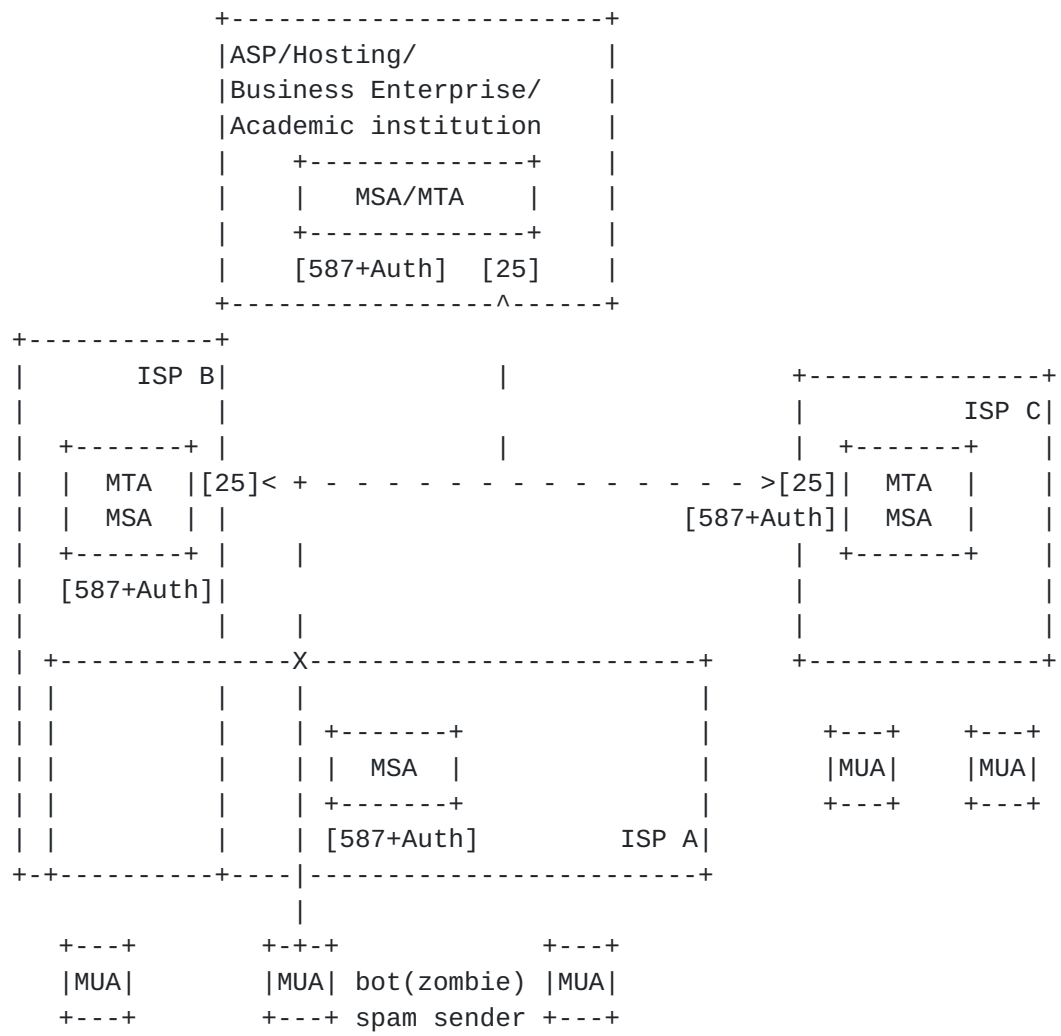

Figure 20: Invalid mail submission after OP25B

All the submissions from dynamic IP addresses to port 25 of MSAs outside of ISP A are blocked by ACL rules of OP25B.

6. Acknowledgements

The author would like to thank Rodney Van Meter for his good contributions to this memo.

7. References

7.1. Normative References

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <http://www.rfc-editor.org/info/rfc5322>.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, DOI 10.17487/RFC5598, July 2009, <http://www.rfc-editor.org/info/rfc5598>.

[RFC6409] Gellens, R. and J. Klensin, "Message Submission for Mail", STD 72, RFC 6409, DOI 10.17487/RFC6409, November 2011, <http://www.rfc-editor.org/info/rfc6409>.

7.2. Informative References

[Triangular] Qian, Z., "Investigation of Triangular Spamming a Stealthy and Efficient Spamming Technique", In proceedings of IEEE Symposium on Security and Privacy (Oakland) 2010 , May 2010.

Authors' Addresses

Takehito Akagiri
Regumi, Inc.

Email: akagiri@regumi.net

Koji Wakamatsu
SoftBank Mobile Corp.

Email: koji.wakamatsu@g.softbank.co.jp

Genki Yasutaka
Rakuten, Inc.

Email: genki.yasutaka@rakuten.com

Kouji Okada
Lepidum Co. Ltd.

Email: okd@lepidum.co.jp