Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: November 15, 2012

T. Zink
Microsoft

June 10, 2012

Recommendations for the use of whitelists for email senders transmitting email over IPv6
draft-tzink-ipv6mail-whitelist-02

Abstract

This document contains a plan for how providers of email services can manage one aspect of the problem of email abuse over IPv6. Spammers can send mail from a very large range of IPv6 addresses, and this will make current antispam blocklisting technology less effective. This is because email receivers will have to maintain excessively large lists of IP blocklists which either consume too many resources, or will become stale and therefore ineffective as spammers quickly discard one IP address and move onto the next one.

This document recommends that during the transition of email from IPv4 to IPv6, email receivers implement a whitelisting option where they only allow email from permitted senders over IPv6 and reject or throttle email from everyone else sending email over IPv6.

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 November 15, 2012.

Copyright Notice

Table of Contents

1. Key Terminology

This section defines the key terms used in this document.

1.1. Email

Email is a method of exchanging digital messages from an author to one or more recipients.

1.2. Web mail

A service which offers web based access to email services which would otherwise be accessed by dedicated email programs running on the device used to access the email.

1.3. Host

An end user's host, or computer, as used in the context of this document, is intended to refer to a computing device that connects to the Internet. This encompasses devices used by Internet users such as personal computers, including laptops, desktops, and netbooks, as

well as mobile phones, smart phones, home gateway devices, and other end user computing devices which are connected or can connect to the public Internet and/or private IP networks.

Increasingly, other household systems and devices contain embedded hosts which are connected to or can connect to the public Internet and/or private IP networks. However, these devices may not be under interactive control of the Internet user, such as may be the case with various smart home and smart grid devices.

1.4. SMTP

As defined in RFC5321.

1.5. Internet Customer

An end user who leverages a connection to the Internet via an ISP and is provisioned with a public IP to communicate on the Internet.

1.6. Internet facing server

A server which is addressed with a public IP address that is able to communicate with other publically addressed servers. A server typically hosts a service that can be utilized by the Internet community.

1.7. Internal users

Known corporate users of the ISP entity.

1.8. Blocklist

As defined in section 1 of RFC 5782 and typical usage described in section 6 of that same RFC.

1.9. Whitelist

As defined in section 1 of RFC 5782 and typical usage described in section 6 of that same RFC.

2. Introduction and Problem Statement

With the depletion of IPv4 address space and the transition of Internet infrastructure to IPv6, it is necessary to address the way in which email services can be transitioned from a IPv4 to that of IPv6. There are significant issues to be addressed around the matter of abuse in an IPv6 based environment which have been addressed and largely resolved when operating using IPv4 as a transport mechanism.

The majority of email service providers currently utilize IPv4 blocklists (as defined in section 1 of RFC 5782) to reject mail. This is frequently done upon the initial email connection or sometime during the SMTP transaction (e.g., after the HELO, MAIL FROM or RCPT TO). This is done for multiple reasons:

(a) To save on more expensive downstream content filtering.

(b) To reduce the amount of spam that must be stored for the user in a spam folder and on the mail server.

(c) To improve the quality of spam filtering.

IPv4 blocklists are manageable because the size of IPv4 address space is approximately 4 billion IPs. Even if in the worst case every single IP address were listed, this is very large but still manageable for email filters with sufficient hardware. The size of the total IPv6 address space is 340 trillion trillion trillion IP addresses. This is far too large for filters to handle or backend hardware to process or maintain.

Even if blocklist maintainers listed only the IP addresses that were spamming, a spammer could send spam from an IP address, let the IP address it used get listed on a blocklist, but discard that IP

address and move onto the next IP address. By rotating through IP addresses quickly, a spammer would always be one step ahead of the blocklists, and the lists would lose their effectiveness. This would also result in more spam in users' inboxes, and greatly increased processing load for mail filters.

3. Transition Model - Whitelists

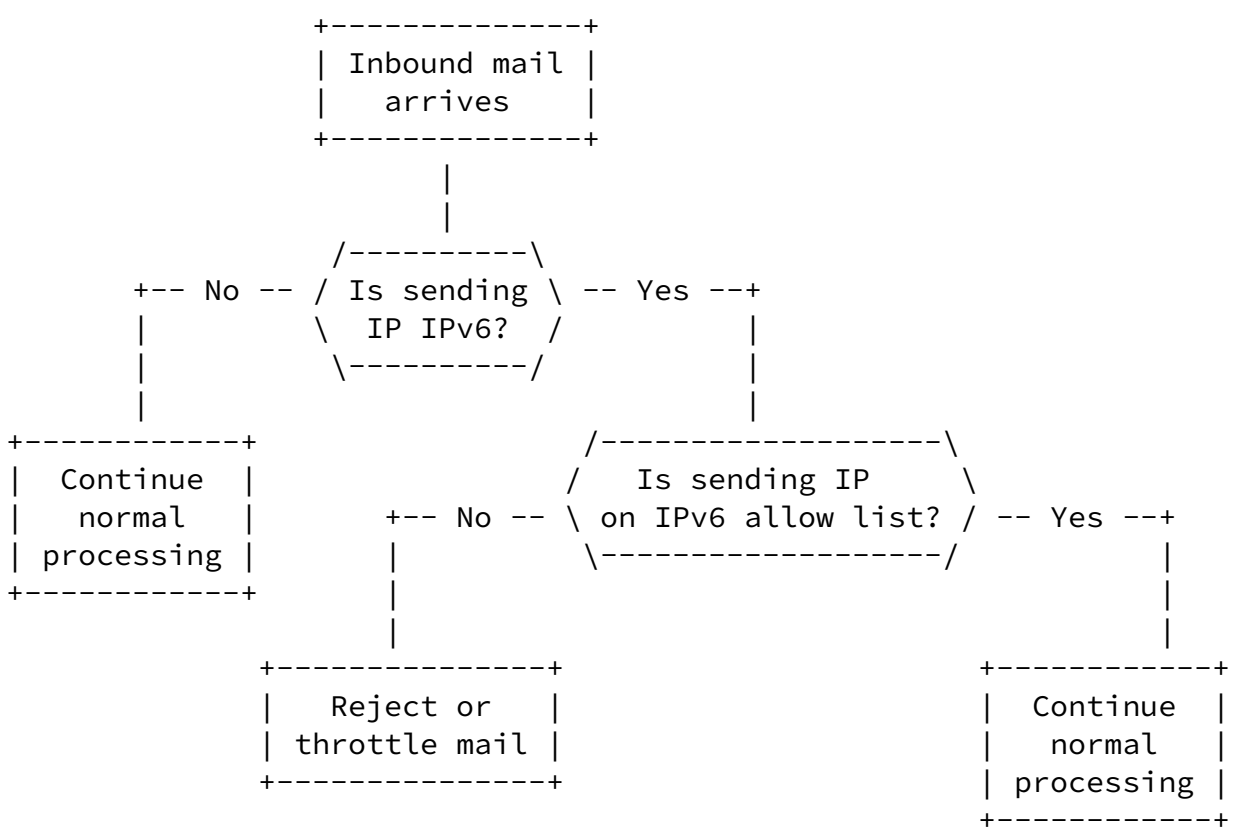
It is assumed that eventually the Internet will come up with a permanent solution to email over IPv6. In the meantime, a transition model is required.

Rather than using IP blocklists to reject mail from known bad IP addresses, email receivers who wish to receive email over IPv6 should use whitelists to only accept mail from known good IP addresses and reject all email from IPv6 IP addresses that are not on the list. Whitelist population is described in section 4.

This IPv6 whitelist is a "Do not reject all mail from this IP address" list; email from these IP addresses may still go through traditional content filtering. IP addresses on this whitelist are there because they send email over IPv6 intentionally, and are not sending email without the computer owner's consent, as part of a botnet.

It is not unusual for email receivers in modern spam filters to use whitelists, or "do not block" lists but still filter the mail by content. For example, many large email receivers do not block the IP address ranges of large webmail providers but still apply content filtering. Other email receivers implement whitelists wherein a small set of IP addresses undergo no spam filtering.

A flowchart of the process is below:



Using an IPv6 whitelist has the following advantages:

(a) It allows email communication between those Internet users who need to do it over IPv6 instead of IPv4.

(b) It does not permit widespread abuse of email over IPv6 since senders must make an effort to get onto the whitelist.

(c) The lists will not take up much memory or bandwidth since the total amount of legitimate senders over IPv6 is projected to be substantially fewer than the total amount of Internet users or devices. There simply are not that many senders who require sending email over IPv6, less than 20 million which is smaller than many IPv4 blocklists.

It is not unusual to put restrictions on IP addresses that are newly sending email. Today (2012) on IPv4, Internet users cannot simply start sending email out a new IP address without encountering problems; most spam filters will view mail from a new IP address as

abusive and either block it or throttle mail from it. Therefore, representatives between those users contact each other, informing them to expect to see mail from their dormant IP addresses in the near future, or else they ask for a pre-emptive whitelisting.

Thus, using an IPv6 whitelist already has precedent. Just as new senders in IPv4 request pre-emptive whitelisting as a courtesy, in IPv6 they will have to acquire pre-emptive whitelisting as a requirement.

Another implementation is that receivers of email over IPv6 do not need to reject non-whitelisted anonymous senders over IPv6. Instead, they can throttle the senders by limiting the amount of mail they can send. As time passes, the IPv6 senders can build up a good reputation and move from the throttle list (where the amount of mail they can send per IP address is limited) to the whitelist (where the amount of mail they can send per IP address is nearly unlimited).

Thus, the key characteristic of the whitelist solution is not a default-treat-everyone-as-potentially-good-until-they-show-otherwise, but instead treat-everyone-as-suspicious-until-they-prove-otherwise. The decision to throttle or reject mail from untrusted senders is up to the recipient.

Email receivers may continue to filter the message by content filter and either store it in the user's spam quarantine, or reject the message based upon spam content, but they must not block messages from those IP addresses due to an IP filtering ban because the sending IP address is IPv6.

IPs addresses in the whitelist can be either single IP addresses or in IP address ranges, it is up to the receiver to decide which format to use.

4. Type of whitelists

It is not necessary to restrict whitelists to use only IP addresess. Email receivers can whitelist based upon sending domain and combine it with an SPF (see RFC 4408) or DKIM (see RFC 6376) validation, or by using certificates such as those exchanged in TLS (see RFC 5246). Using any of these options makes it easier to implement a whitelist

based upon domains because domains change more infrequently than senders' IP addresses do. Secondly, any domain whitelists in IPv4 can be easily implemented in IPv6 when combined with either a DKIM or SPF check.

However, the advantage of using a whitelist based only upon IP addresses is that receiving mail servers can make a Good/Bad decision as soon as the sending IP address connects to the mail server. The drawback of using SPF is that a mail server must wait to perform the whitelist lookup after the MAIL FROM command in the SMTP conversation and wait for a DNS query to return.

Similarly, the drawback using DKIM is that the receiving mail server must wait until it receives the entire message and wait for a DNS query to return from looking up the public key to perform the DKIM validation. This slows down the email transaction and increases load on the email infrastructure.

5. Population of the IPv6 whitelists

It is outside the scope of this Internet Draft to specify how an email receiver should build their own IPv6 whitelists. The following are possible mechanisms to accomplish this:

(a) Administrators may contact each other by email over IPv4, by telephone, by regular mail, by word-of-mouth, or any other form of communication. Both parties may agree to whitelist each other, or one party may whitelist the other without the other doing the same.

(b) Administrators may rely on a third party reputation service that provides lists of IP addresses of known good senders of email over IPv6. An administrator may acquire this list and proactively whitelist all IP addresses on this list, or a subset of them.

(c) If administrators currently use sending domain whitelists in IPv4 by combining them with an SPF or DKIM check, they can use the same domain whitelists in IPv6. SPF supports IPv6, and DKIM

does not require the use of the sending IP address.

(d) Administrators may give email senders a way to do get onto their whitelists by creating a web portal. Senders can go to this web portal and enter in their sending IP addresses. The web portal may do additional forms of validation (CAPTCHAs, SMS verification) and if the sender passes the checks, their sending IPs are added to the whitelist.

(e) Rather than rejecting mail from senders on IPv6, receivers might allow new senders transmitting over IPv6 but throttle them instead. By keeping track of a sending IP addresses' reputation (ratio of spam to non-spam, passing authentication, etc.) over a period of time, a receiver can upgrade the sender from the Untrusted list to the Whitelist. The amount of mail they can send over IPv6 increases as their reputation increases.

This changes the whitelist from a binary decision (Accept/Deny) to a sliding-scale whitelist where a sender's reputation is on a sliding scale.

Any of these methods, or a combination of them, can be used for whitelist population.

6. Removal from the whitelists

If an IP address is added onto the whitelist, its reputation should be tracked to ensure that it is not a spamming IP address. This can be performed by keeping track of complaints, monitoring spam-to-non spam volumes, and so forth. If an IP address is discovered to be malicious, the following are possible methods to deal with this:

(a) The IP should be removed from the whitelist.

(b) Use the sending IP as part of a weight in the spam filter.

(c) Lower the sender's reputation which lowers their throttling limits in the case that the email receiver is throttling IP addresses instead of rejecting mail from them.

Any of these methods, or a combination of them, can be used to remove IP addresses from the whitelist in the even that they are spamming.

7. Security Considerations

This document does not address any security issues inherent in IPv6 itself but acknowledges the security considerations of RFC 5782 do apply to this document. IPv6 security considerations will need to be addressed in this document as it develops.

8. Privacy Considerations

This document describes at a high level activities that ISPs should be sensitive to, where the collection or communication of Personally Identifiable Information (PII) may be possible. In addition, when performing this transition, ISPs should be careful to protect any PII collected whether deliberately or inadvertently.

Any sharing of data from the user to the ISP and/or authorized third parties should be done on an opt-in basis. Additionally the ISP and or authorized third parties should clearly state what data will be shared and with whom the data will be shared with.

Lastly, there my be legal requirements in particular legal jurisdictions concerning how long any subscriber-related or other data is retained, of which an ISP operating in such a jurisdiction should be aware and with which an ISP should comply.

9. IANA Considerations

There are no IANA considerations in this document.

10. Acknowledgements

The authors wish to acknowledge the following individuals and groups

Zink Expires November 15, 2012 [Page 8]

for performing a detailed review of this document and/or providing comments and feedback that helped to improve and evolve this document:

Leiba, B.

11. Normative references

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, July 2009.

[RFC5782] Levine, J., "DNS Blacklists and Whitelists", RFC 5782, February 2010.

12. Informative references

[RFC5321] Wong, M. and Schlitt, W. "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006.

[RFC6376] Allman, E., et al, "DomainKeys Identified Mail (DKIM) Signatures", RFC 6376, July 2009.

[RFC5246] Dierks, T., and Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008

Appendix A. Document Change Log

[RFC Editor: This section is to be removed before publication]

-00 version: Initial version
-01 version: Formatting changes
-02 version: Added more options for how to get onto whitelist,

more documentation around throttling vs rejecting

Appendix B. Open Issues

[RFC Editor: This section is to be removed before publication]

No open issues to date

Authors' Addresses

Terry Zink
Microsoft
1 Microsoft Way
Redmond, WA 98052
US

Email: tzink@microsoft.com
URI: http://www.microsoft.com