               Time to Remove Filters for Previously Unallocated IPv4 /8s

Abstract

   It has been common for network administrators to filter IP traffic
   from and BGP prefixes of unallocated IPv4 address space. Now that
   there are no longer any unallocated IPv4 /8s, this practise is more
   complicated, fragile, and expensive. Network administrators are
   advised to remove filters based on the registration status of the
   address space.

   This document explains why any remaining packet and BGP prefix
   filters for unallocated IPv4 /8s should now be removed on border
   routers and documents those IPv4 unicast prefixes that should not be
   routed across the public Internet.

Status of This Memo

   This memo documents an Internet Best Current Practice.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   BCPs is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6441.

Copyright Notice

include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction

   It has been common for network administrators to filter IP traffic
   from and BGP prefixes of unallocated IPv4 address space. Now that
   there are no longer any unallocated IPv4 /8s, this practise is more
   complicated, fragile, and expensive. Network administrators are
   advised to remove filters based on the registration status of the
   address space.

   This document explains why any remaining packet and BGP prefix
   filters for unallocated IPv4 /8s should now be removed on border
   routers and documents those IPv4 unicast prefixes that should not be
   routed across the public Internet.

2. Terminology

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in BCP 14, RFC 2119
   [RFC2119].

   Martians [RFC1208] is a humorous term applied to packets that turn up
   unexpectedly on the wrong network because of bogus routing entries.
   It is also used as a name for a packet that has an altogether bogus
   (non-registered or ill-formed) Internet address. Bogons [RFC3871]
   are packets sourced from addresses that have not yet been allocated

by IANA or the Regional Internet Registries (RIRs), or addresses
reserved for private or special use by RFCs [RFC5735]. Bogons are
referred to as "Dark IP" in some circles.

3. Traffic Filtering Options

3.1. No Longer Filtering Based on Address Registration Status

Network administrators who implemented filters for unallocated IPv4
/8s did so in the knowledge that those /8s were not a legitimate
source of traffic on the Internet and that there was a small number
of bogon filters to implement. Now that there are no longer any
unallocated unicast IPv4 /8s, there will be legitimate Internet
traffic coming from all unicast /8s that are not reserved for special
purposes in an RFC.

Removing packet and prefix filters based on the registration status
of the IPv4 address is a simple approach that will avoid blocking
legitimate Internet traffic. Network operators SHOULD remove both
ingress and egress packet filters as well as BGP prefix filters for
previously unallocated IPv4 /8s.

3.2. Continuing to Filter Traffic from Unallocated IPv4 Space

Some network administrators might want to continue filtering
unallocated IPv4 addresses managed by the RIRs. This requires
significantly more granular ingress filters and the highly dynamic
nature of the RIRs' address pools means that filters need to be
updated on a daily basis to avoid blocking legitimate incoming
traffic.

4. Prefixes That Should Not be Routed across the Internet

Network operators may deploy filters that block traffic destined for
Martian prefixes. Currently, the Martian prefix table is defined by
[RFC5735] which reserves each Martian prefix for some specific,
special use. If the Martian prefix table ever changes, that change
will be documented in an RFC that either updates or obsoletes
[RFC5735].

5. Security Considerations

The cessation of filters based on unallocated IPv4 /8 allocations is
an evolutionary step towards reasonable security filters. While
these filters are no longer necessary, and in fact harmful, this does
not obviate the need to continue other security solutions. These
other solutions are as necessary today as they ever were.

6. References

6.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC5735] Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses",
              BCP 153, RFC 5735, January 2010.

6.2. Informative References

   [RFC1208] Jacobsen, O. and D. Lynch, "Glossary of networking terms",
              RFC 1208, March 1991.

   [RFC3871] Jones, G., "Operational Security Requirements for Large
              Internet Service Provider (ISP) IP Network
              Infrastructure", RFC 3871, September 2004.

Appendix A. Acknowledgments

   Thanks are owed to Kim Davies, Terry Manderson, Dave Piscitello, and
   Joe Abley for helpful advice on how to focus this document. Thanks
   also go to Andy Davidson, Philip Smith, and Rob Thomas for early
   reviews and suggestions for improvements to the text, and to Carlos
   Pignataro for his support and comments.

Author's Address

   Leo Vegoda
   Internet Corporation for Assigned Names and Numbers
   4676 Admiralty Way, Suite 330
   Marina del Rey, CA 90292
   United States of America

   Phone: +1-310-823-9358
   EMail: leo.vegoda@icann.org
   URI: http://www.iana.org/