Internet Engineering Task Force
Internet-Draft
Intended status: BCP
Expires: October 21, 2011

A. Durand
Juniper Networks
I. Gashinsky
Yahoo! Inc.
D. Lee
Facebook, Inc.
S. Sheppard
ATT Labs

April 19, 2011

Logging recommendations for Internet facing servers
draft-ietf-intarea-server-logging-recommendations-04

Abstract

In the wake of IPv4 exhaustion and deployment of IP address sharing techniques, this document recommends that Internet facing servers log port number and accurate timestamps in addition to the incoming IP address.

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 October 21, 2011.

Copyright Notice

Table of Contents

1. Introduction 3
2. Recommendations 3
3. ISP Considerations 4
4. IANA Considerations 5
5. Security Considerations 5
6. References 5
6.1. Normative references 5
6.2. Informative references 5
Authors' Addresses 6

1. Introduction

The global IPv4 address free pool at IANA was exhausted in February 2011. Service providers will now have a hard time finding enough IPv4 global addresses to sustain product and subscriber growth. Due to the huge global existing infrastructure, both hardware and software, vendors and service providers must continue to support IPv4 technologies for the foreseeable future. As legacy applications and hardware are retired the reliance on IPv4 will diminish but this is a years long perhaps decades long process.

To maintain legacy IPv4 address support, service providers will have little choice but to share IPv4 global addresses among multiple customers. Techniques to do so are outside of the scope of this document. All include some form of address translation/address sharing, being NAT44 [RFC3022], NAT64 [I-D.ietf-behave-v6v4-xlate-stateful] or DS-Lite [I-D.ietf-softwire-dual-stack-lite].

The effects on the Internet of the introduction of those address sharing techniques have been documented in [I-D.ietf-intarea-shared-addressing-issues].

Address sharing techniques come with their own logging infrastructure to track the relation between which original IP address and source port(s) were associated with which user and external IPv4 address at any given point in time. In the past to support abuse mitigation or public safety requests, the knowledge of the external global IP address was enough to identify a subscriber of interest. With address sharing technologies, only providing information about the external public address associated with a session to a service provider is no longer sufficient information to unambiguously identify customers.

Note: this document provides recommendations for Internet facing servers logging incoming connections. It does not provide any

recommendations about logging on carrier-grade NAT or other address sharing tools.

2. Recommendations

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 RFC 2119 [RFC2119].

It is RECOMMENDED as best current practice that Internet facing servers logging incoming IP addresses from inbound IP traffic also

log:

- The source port number.
- A timestamp, RECOMMENDED in UTC, accurate to the second, from a traceable time source (e.g., NTP [RFC5905]).
- The transport protocol (usually TCP or UDP) and destination port number, when the server application is defined to use multiple transports or multiple ports.

Discussion: Carrier-grade NATs may have different policies to recycle ports, some implementations may decide to reuse ports almost immediately, some may wait several minutes before marking the port ready for reuse. As a result, servers have no idea how fast the ports will be reused and, thus, should log timestamps using a reasonably accurate clock. At this point the RECOMMENDED accuracy for timestamps is to the second or better. Representation of timestamps in UTC is prefered to localtime with UTC-offset or time zone as this extra information can be lost in the reporting chain.

Examples of Internet facing servers include, but are not limited to, web servers and email servers.

Although the deployment of address sharing techniques is not foreseen in IPv6, the above recommendations apply to both IPv4 and IPv6, if only for consistency and code simplification reasons.

Discussions about data retention policies are out of scope for this

document. Server security and transport security is important for the protection of logs for Internet facing systems. The operator of the Internet facing server must consider the risks, including the data and services on the server to determine the appropriate measures. The protection of logs is critical in incident investigations. If logs are tampered with, evidence could be destroyed.

The above recommendations also apply to devices such as load-balancers logging incoming connections on behalf of actual servers.

The above recommendations apply to current logging practices. They do not require any changes in the way logging is performed; e.g., which packets are examined and logged.

3. ISP Considerations

ISP deploying IP address sharing techniques should also deploy a

corresponding logging architecture to maintain records of the relation between a customer's identity and IP/port resources utilized. However, recommendations on this topic are out of scope for this document.

4. IANA Considerations

None.

5. Security Considerations

In the absence of source port number and accurate timestamp, operators deploying any address sharing techniques will not be able to identify unambiguously customers when dealing with abuse or public safety queries.

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.

6.2. Informative references

[I-D.ietf-behave-v6v4-xlate-stateful]
Bagnulo, M., Matthews, P., and I. Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", draft-ietf-behave-v6v4-xlate-stateful-12 (work in progress), July 2010.

[I-D.ietf-intarea-shared-addressing-issues]
Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", draft-ietf-intarea-shared-addressing-issues-05 (work in progress), March 2011.

[I-D.ietf-softwire-dual-stack-lite]
Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", draft-ietf-softwire-dual-stack-lite-07 (work in progress), March 2011.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network

Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC5905] Mills, D., Martin, J., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

Authors' Addresses

Alain Durand
Juniper Networks
1194 North Mathilda Avenue
Sunnyvale, CA 94089-1206
USA

Email: adurand@juniper.net

Igor Gashinsky
Yahoo! Inc.
45 West 18th St.
New York, NY 10011
USA

Email: igor@yahoo-inc.com

Donn Lee
Facebook, Inc.
1601 S. California Ave.
Palo Alto, CA 94304
USA

Email: donn@fb.com

Scott Sheppard
ATT Labs
575 Morosgo Ave, 4d57
Atlanta, GA 30324
USA

Email: Scott.Sheppard@att.com