opsec   F. Gont
Internet-Draft   SI6 Networks / UTN-FRH
Intended status: Informational   M. Ermini
Expires: September 22, 2016   ResMed
                                                                    W. Liu
                                                        Huawei Technologies
                                                            March 21, 2016

Requirements for IPv6 Enterprise Firewalls
draft-gont-opsec-ipv6-firewall-reqs-03

Abstract

   While there has been some work in the area of firewalls, concrete
   requirements for IPv6 firewalls have never been specified in the RFC
   series. The more limited experience with the IPv6 protocols and the
   more reduced number of firewalls that support IPv6 has made it rather
   difficult to infer what are reasonable features to expect in an IPv6
   firewall. This has typically been a problem for network operators,
   who typically have to produce a "Request for Proposal" from scratch
   that describes such features. This document specifies a set of
   requirements for IPv6 firewalls, in order to establish some common-
   ground in terms of what features can be expected in them.

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 September 22, 2016.

Copyright Notice

Table of Contents

[1](#). DISCLAIMER

   This initial version of the document is based on a typical IPv6
   firewall "Request for Proposal" (RFP), and is mostly meant to trigger
   discussion in the community, and define a direction for the document.
   Future versions of this document may contain all, more, or a subset
   of the requirements present in the current version of this document.
   Additionally, the current version DOES NOT yet properly separate
   requirements among MUST/REQUIRED, SHOULD/RECOMMENDED, and MAY/
   OPTIONAL.

   Please DO read [Section 3](#) of this document, since it provides
   important information about the conventions used throughout this
   document that is mandatory to be able to understand it.

   Finally, please note this version is meant to provide requirements,
   rather than implementation guidelines.

2. Introduction

   While the IETF has published a large number of documents discussing
   IP and IPv6 packet filtering (see e.g. [RFC7126] and some documents
   on the topic of IP firewalls (see e.g. [RFC2979] and [RFC3511]),
   concrete requirements for IP firewalls have never been specified in
   the RFC series. When it comes to IPv4, a number of features have
   become common over the years, and firewall requirements have somehow
   become operational wisdom. When it comes to IPv6 [RFC2460], the more
   limited experience with the protocols, and the reduced variety of
   IPv6 firewalls has made it rather difficult to specify what are
   reasonable features to be expected of an IPv6 firewall. This has
   proven to be a problem for network operators (who have typically had
   to produce a "Request for Proposal" from scratch), but also for
   vendors (who lack a well defined set of requirements that can serve
   as a roadmap for implementation).

   This situation has not only made the process of purchasing an IPv6
   firewall harder, but at times has also meant that a number of
   important/basic features have remained unimplemented by major
   firewall vendors, or that aforementioned features have not behaved as
   expected.

   This document aims to provide a set of requirements for firewall
   vendors, which are specified as "MUST", "SHOULD", or "MAY". An IPv6
   firewall product is said to be "fully-compliant" with this
   specification provided it implements all requirements marked as
   "MUST" and "SHOULD". An IPv6 firewall product is said to be
   "conditionally-compliant" with this specification provided it
   implements all requirements marked as "MUST", but fails to implement
   one or more of the requirements marked as "SHOULD".

3. Conventions

3.1. Requirements Language

   Take careful note: Unlike other IETF documents, the key words "MUST",
   "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",
   "RECOMMENDED", "MAY", and "OPTIONAL" in this document are not used as
   described in [RFC2119]. This document uses these keywords not

strictly for the purpose of interoperability, but rather for the
purpose of establishing industry-common baseline functionality.

In this document, the words that are used to define the significance
of each particular requirement are capitalized. These words are:

o "MUST" This word, or the words "REQUIRED" and "SHALL" mean that
   the item is an absolute requirement of the specification.

o "SHOULD" This word or the adjective "RECOMMENDED" means that there
   may exist valid reasons in particular circumstances to ignore this
   item, but the full implications should be understood and the case
   carefully weighed before choosing a different course.

o "MAY" This word or the adjective "OPTIONAL" means that this item
   is truly optional. One vendor may choose to include the item
   because a particular marketplace requires it or because it
   enhances the product, for example; another vendor may omit the
   same item.

A firewall implementation is a module that supports at least one of
the feature types defined in this document. Firewall implementations
may support multiple feature types, but conformance is considered
individually for each type.

A firewall implementation is not compliant with a specific feature
type if it fails to satisfy one or more of the MUST requirements of
such specific feature type. An implementation that satisfies all the
MUST and all the SHOULD requirements of a specific feature is said to
be "unconditionally compliant" with such feature type; one that
satisfies all the MUST requirements but not all the SHOULD
requirements is said to be "conditionally compliant" with such
feature type.

3.2. Terminology

Where possible, this document employs the terminology defined in
[RFC2647]. Other additional terms are defined below:

session:
   The term session refers to any protocol instance that involves
   some sort of stateful exchange. Examples of "sessions" could be
   TCP connections, UDP query/response pairs, ICMPv6 echo/response
   pairs, etc. Our definition of session corresponds to the
   definition of "connection" in Section 3.7 of [RFC2647], but we
   rather employ "session" to avoid possible confusion.

      XXX: Should we just get rid of the term "session" and use
      "connection" throughout this document, with a big reference to the
      definition in RFC2647?

3.3. Numbering Conventions

   The items for each feature type will follow a monotonically-
   increasing order -- typically in increments to 10. This is to
   prevent the insertion of an item in the list of requirements to
   change the numbering of all the following requirements. Prior to the
   final publication of this document, each of items of each the feature
   types will be numbered starting from 1, with increments of 1 (1, 2,
   3, 4, etc.).

      NOTE: Those with BASIC language programming experience may find
      the idea familiar.

4. General Security Features

   REQ GEN-5:
      The firewall MUST include performance benchmarking documentation.
      Such documentation MUST include information that reflects firewall
      performance with respect to IPv6 packet, but also regarding how
      IPv6 traffic may affect the performance of IPv4 traffic. The
      aforementioned documentation MUST be, at the very least,
      conditionally-compliant with both [RFC3511] and [RFC5180] (that
      is, it MUST support all "MUST" requirements in such documents, and
      may also support the "SHOULD" requirements in such documents).

         NOTE: This is for operators to spot be able to identify cases
         where a devices may under-perform in the presence of IPv6
         traffic (see e.g. [FW-Benchmark]). XXX: This note may be
         removed before publication if deemed appropriate.

   REQ GEN-10:
      All features of the firewall MUST be able to be individually
      configured (at least ON or OFF, with other configurable parameters
      as applicable). A well-documented default initial setting must be
      provided for each feature.

   REQ GEN-20:
      MUST support basic Access Control Lists (ACLs).

   REQ GEN-30:
      MUST support stateless packet inspection and filtering at
      transport layer.

   REQ GEN-40:

      MUST support stateful packet inspection and filtering at transport
      layer.

   REQ GEN-50:
      SHOULD support full-proxy for the TCP [RFC0793] connections (the
      handshake is validated on the firewall before reaching the target
      system).

         Some products identify this feature with terms such as "TCP
         Intercept and Limiting Embryonic Connections".

   REQ GEN-60:
      MUST be able to enforce timeouts on protocol sessions based on the
      upper-layer protocol (e.g. enforce a timeout on the FIN-WAIT state
      for TCP connections, a timeout for DNS query/respose pair, etc.).
      In general, it MUST have different timeout parameters and
      thresholds to be used to prevent idle sessions from exhausting
      resources on the device and/or the service that is defended. For
      sessions composed of multiple packets (such as TCP connections),
      the exchange of valid packets MUST refresh the timers employed for
      enforcing the aforementioned timeouts.

         NOTE: This is to avoid the known and buggy behavior where
         firewalls enforce a maximum lifetime for the protocol session
         (e.g. TCP connection) regardless of whether there is ongoing
         exchange of legitimate packets for such session.

   REQ GEN-70:
      MUST be able to provide anti-spoofing features (e.g. uRPF).

   REQ GEN-80:
      MUST be able to redirect specific traffic to a proxy server e.g.
      for HTTP/S protocols.

         NOTE: "Redirection means that the firewall should be able to
         divert the traffic to a proxy - i.e., take the traffic, send it
         to an inspection engine, receive it back and forward it (all
         this completely transparent to the users).

   REQ GEN-90:
      MUST be able to detect and reject invalid source or destination
      addresses (e.g. local-link addresses that try to traverse the
      firewall) with a single policy.

5. **IPv6-Specific Features**

   REQ SPC-10:
      MUST be able to filter ICMPv6 [RFC4443] traffic at a message type/
      code granularity. [RFC4890] MUST be employed for the default
      filtering configuration.

   REQ SPC-20:
      MUST be able to block packets containing any specified extension
      header type (based on its Next Header value), on a specified
      number of instances of a specified extension header type, and on a
      specified overall number of IPv6 extension headers.

   REQ SPC-30:
      MUST be able to block IPv6 packets that employ a Routing Header
      both at the granularity of Extension Header Type (as required in
      SPC-20) and Routing Header Type.

   REQ SPC-40:
      SHOULD be able to drop packets based on IPv6 option types.

   REQ SPC-50:
      MUST be able to detect IPv6 tunnels such as SIIT [RFC6145], 6to4
      [RFC3056], 6in4 [RFC4213], ISATAP [RFC5214] and Teredo [RFC4380]
      (please see [RFC7123], and MUST be able to selectively block or
      allow them for specific sources, destinations, routes or
      interfaces.

   REQ SPC-60:
      MUST be able to validate IPv6 Neighbor Discovery [RFC4861] packets
      (RS, RA, NS, NA, Redirect) according to
      [I-D.ietf-opsec-ipv6-nd-security].

   REQ SPC-70:
      MUST be able to statefully match ICMPv6 errors to TCP [RFC0793],
      UDP [RFC0768], and ICMPv6 [RFC4443] communication instances (see
      [RFC5927]).

   REQ SPC-80:
      MUST be able to parse all defined extension headers according to
      [RFC7045], and SHOULD filter packets containing IPv6 Extension
      Headers as recommended in [draft-gont-opsec-ipv6-eh-filtering].

   REQ SPC-90:
      MUST be able to find the upper-layer protocol in an IPv6 header
      chain (see [RFC7112].

   REQ SPC-100:

     SHOULD be able to normalize (rewrite) the following IPv6 header
     fields on a per-interface basis:

     * Hop Limit

6. VPN Security Requirements

   REQ VPN-10:
      MUST implement IPsec-based [RFC4301] VPN technology.

   REQ VPN-20:
      MUST implement "hub-and-spoke" Dynamic Multipoint VPN-like
      technology, allowing creation of dynamic-meshed VPN without having
      to pre-configure all of possible tunnels.

   REQ VPN-30:
      MUST implement SSL/TLS-based [SSL-VPNs] VPN technology.

   REQ VPN-40:
      MUST be able to use digital certificates, including CRL and OCSP
      revocation checking methods, to mutually authenticate VPN peers.

   REQ VPN-50:
      MUST be able to disable or enable split-tunnelling feature on VPN
      as required.

   REQ VPN-60:
      MUST support the enrollment of the system in a PKI infrastructure
      for the regular renewal of certificates.

   REQ VPN-70:
      MUST be able to transit IPv4 and IPv6 packets providing full
      parity for services, and also offer both protocols in dual-stack
      in the same VPN connection.

   REQ VPN-80:
      MUST be able to apply to the tunnelled content that is terminated
      on the device, the same inspection policies that are possible in
      the non tunnelled traffic.

   REQ VPN-90:
      MUST perform a full validation of the certificates' chains when
      verifying the validity of the OCSP/CLR responses. Caching of
      responses SHOULD be configurable by end users, and the default
      response SHOULD be not to accept a non-valid certificate. The
      default response MAY be overridden by the administrators, but it
      MUST be configurable on a per-domain basis (e.g. accept incomplete

certificate chains for "intranet_of_internal_corp.example.org",
but refuse it for all of the other domains).

7. Denial of Service (DoS) Protection

REQ DoS-10:
   MUST be able to protect against implementation-specific attacks,
   including:

   * Winnuke [Myst1997]

   * ping-of-death [Kenney1996]

   * Smurf [CERT1998a]

   * LAND Attack [Meltman1997]

   * Teardrop Attack [CERT1997] [Junos-Teardrop]

REQ DoS-20:
   MUST be able to protect against IPv6 resource exhaustion attacks,
   including:

   * fragment flooding attacks

   * Neighbor Cache Exhaustion attacks, whether launched from a
      local network (see [I-D.ietf-opsec-ipv6-nd-security] or from
      remote networks (see [RFC6583]

REQ DoS-30:
   MUST be able to protect against TCP flooding attacks: connection-
   flooding, FIN-WAIT-1 flooding, etc. (see e.g. [CPNI-TCP])

REQ DoS-40:
   MUST be able to protect against TCP resource exhaustion attacks:
   zero-window attacks, SYN-floods, etc. (see e.g. [CPNI-TCP])

REQ DoS-50:
   MUST be able to detect and drop malformed IPv6 packets (incorrect
   header/option lengths, etc.).

REQ DoS-60:
   MUST be able to detect and drop malformed TCP packets (incorrect
   segment/options lengths, etc.).

REQ DoS-70:

      MUST be able to provide bandwidth management (QoS or anti-
      flooding) policies customizable for specific source and
      destination networks, or by VLAN or MPLS ID.

   REQ DoS-80:
      MUST be able to participate to a blackhole/synkhole routing
      infrastructure as per [RFC5635].

   REQ DoS-85:
      MUST be able to fetch and use third party "reputational" IP white-
      and black-lists (e.g. download them via RSS feeds or query via
      them DNS record) and use them in policy constructs/ACLs. In
      general, it MUST be able to provide some form of reputational
      service for IP addresses which must include IPv6 networks.

   REQ DoS-90:
      MUST be able to set up a maximum session setup rate, and detect
      hosts or networks exceeding it.

   REQ DoS-100:
      MUST be able to set up a maximum IPv6 source and/or destination
      session limit, and detect when they are exceeded.

   REQ DoS-110:
      For each of the previous detection controls, different
      configurable reactions SHOULD be possible by IPv6 address and
      network sources and/or destinations. The minimum actions required
      are the following:

      1.   allow the traffic ("ignore" or "whitelist")

      2.   allow the traffic but log ("bypass" or "detection only" mode)

      3.   drop the packet (only the offending packet but do not reset
           the connection)

      4.   drop session (drop the entire connection, but do not send a
           reset back)

      5.   "greylist" - put it in a list of blocked addresses, but
           remove it from the list after a configurable amount of time

      6.   send an email/SMS/pager text to the firewall administrator

      7.   send TCP reset to source only

      8.   send TCP reset to destination only

    9.   send TCP reset to both source and destination

    10. perform a specific, preconfigured change on the firewall
         policy

    11. feed a third party source such as a switch/NAC/NAP or RADIUS
         system, to isolate/quarantine the offending port/MAC address/
         user

    12. quarantine the specific traffic or source (block them for a
         configurable amount of time, e.g. 5 minutes, and then allow
         them again; eventually, the quarantine time may get longer if
         the offense is repeated)

[8]. Application Layer Firewall

   REQ APP-10:
      MUST be able to provide web filtering features, such as enforcing
      access to allowed web content and filtering high risk URLs such as
      anonymizers and known hostile addresses.

   REQ APP-20:
      MUST be able to provide email filtering features, such as
      mitigating spam, phishing and email harvesting, and enforce email
      policies.

[9]. Logging, Auditing and Security Operation Centre (SOC) requirements

   REQ SOC-10:
      MUST generate log for all the changes performed to the system,
      including change of group membership for a device, new or removed
      devices in a group, new or removed administrators.

   REQ SOC-20:
      MUST provide the following features:

    1. Connection logs

    2. Local log storage

    3. Network logging

    4. Real time log viewer

    5. Attack detected

    6. Per rule logging

   7. Automatic log file compression

   8. Log file rotation

REQ SOC-30:
   MUST be able to generate a log for:

   1. all the logins, logouts and failed login attempts from
       firewall administrators

   2. any modifications or disabling of the firewall rules

REQ SOC-40:
   Any security event detected - malicious traffic, hit of a policy,
   policy violation, termination of a session and so on - MUST be
   able to generate a log, and be configurable to do that or not by
   administrators.

REQ SOC-50:
   There MUST be a mechanism to prevent log flooding from the device
   against the management system, such as aggregation of like events.

REQ SOC-60:
   The amount of information in the alerts MUST be configurable; it
   SHOULD possible to have the date/time and type of event and the
   full payload of the traffic that has triggered the signature/
   event.

REQ SOC-70:
   The firewall MUST minimize the number of log entries generated for
   a single event - e.g. when repeated similar events for a short
   period of time are detected, they are aggregated and the
   cumulative number of events is reported.

REQ SOC-80:
   The firewall MUST be able to send logs in multiple ways and
   formats, for instance UDP syslog, TCP syslog, SMTP, SNMP and so
   on. It must be possible to configure different ways and formats
   for different policies and configure some ways and formats as a
   "backup" in the case that the main way fails. Please describe the
   different possibilities.

REQ SOC-90:
   The firewall SHOULD alert the firewall administrator when the
   policy to be enforced does not follow the advice in [RFC4890] --
   particularly if the filtering policy would block/drop ICMPv6
   Packet Too Big error messages.

[10]. Console and Events Visualization requirements

REQ CON-10:
   MUST provide a dashboard view, which must be customizable by end-
   user and end-users' group (e.g. their Microsoft Active Directory
   or LDAP group).

REQ CON-20:
   The dashboard must be able to include system health monitoring
   information, such as the following:

   1. CPU idle

   2. Real and Swap memory usage

   3. Disk usage

   4. Number of accepted and dropped packets

   5. Operating status for all supported facilities (HA, QoS, VPN)

   6. VPN tunnels status

   7. NIC link state

REQ CON-30:
   MUST have the possibility to select a particular piece of data or
   individual alert, and visualize the policy that has triggered the
   event.

REQ CON-40:
   MUST be able to create exception filters that will suppress
   visualization of a specific alert (e.g. from specific sources, or
   specific events), without actually affecting the detection and log
   retention.

REQ CON-50:
   MUST provide a remote access method to obtain all current
   operational data on demand, in a documented format, covering items
   such as those listed in REQ CON-20.

      Note: This is to be able to integrate firewall operations in an
      existing NMS.

11. Reporting requirements

   REQ REP-10:
      Built in reports MUST be provided by default, such as protocol
      distribution, policy and rule matched, top attacks, top sources/
      destinations, top targets, top geographical sources, device status
      including utilizations, and so on.

   REQ REP-20:
      SHOULD allow to run reporting over historical and archived logs,
      automatically restoring and re-archiving them.

12. IANA Considerations

   There are no IANA registries within this document. The RFC-Editor
   can remove this section before publication of this document as an
   RFC.

13. Security Considerations

   [TBD]

14. Acknowledgements

   The initial version was based on an (unpublished) document authored
   by Marco Ermini.

   The authors would like to thank (in alphabetical order), Mikael
   Abrahamsson, Cameron Byrne, Brian Carpenter, Tim Chown, Jakub (Jake)
   Czyz, Marc Heuse, Simon Perreault, Carsten Schmoll, Robert Sleigh,
   Donald Smith, Qiong Sun, Gunter Van de Velde, and Scott Weeks, for
   providing valuable comments on earlier versions of this document.

15. References

15.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <http://www.rfc-editor.org/info/rfc2119>.

   [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6
              (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460,
              December 1998, <http://www.rfc-editor.org/info/rfc2460>.

   [RFC4301] Kent, S. and K. Seo, "Security Architecture for the
              Internet Protocol", RFC 4301, DOI 10.17487/RFC4301,
              December 2005, <http://www.rfc-editor.org/info/rfc4301>.

   [RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet
              Control Message Protocol (ICMPv6) for the Internet
              Protocol Version 6 (IPv6) Specification", RFC 4443,
              DOI 10.17487/RFC4443, March 2006,
              <http://www.rfc-editor.org/info/rfc4443>.

   [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
              "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
              DOI 10.17487/RFC4861, September 2007,
              <http://www.rfc-editor.org/info/rfc4861>.

   [RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768,
              DOI 10.17487/RFC0768, August 1980,
              <http://www.rfc-editor.org/info/rfc768>.

   [RFC0793] Postel, J., "Transmission Control Protocol", STD 7,
              RFC 793, DOI 10.17487/RFC0793, September 1981,
              <http://www.rfc-editor.org/info/rfc793>.

   [RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing
              of IPv6 Extension Headers", RFC 7045,
              DOI 10.17487/RFC7045, December 2013,
              <http://www.rfc-editor.org/info/rfc7045>.

   [RFC7112] Gont, F., Manral, V., and R. Bonica, "Implications of
              Oversized IPv6 Header Chains", RFC 7112,
              DOI 10.17487/RFC7112, January 2014,
              <http://www.rfc-editor.org/info/rfc7112>.

   [RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation
              Algorithm", RFC 6145, DOI 10.17487/RFC6145, April 2011,
              <http://www.rfc-editor.org/info/rfc6145>.

   [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains
              via IPv4 Clouds", RFC 3056, DOI 10.17487/RFC3056, February
              2001, <http://www.rfc-editor.org/info/rfc3056>.

   [RFC5214] Templin, F., Gleeson, T., and D. Thaler, "Intra-Site
              Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214,
              DOI 10.17487/RFC5214, March 2008,
              <http://www.rfc-editor.org/info/rfc5214>.

   [RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through
              Network Address Translations (NATs)", RFC 4380,
              DOI 10.17487/RFC4380, February 2006,
              <http://www.rfc-editor.org/info/rfc4380>.

15.2. Informative References

   [RFC2647] Newman, D., "Benchmarking Terminology for Firewall
              Performance", RFC 2647, DOI 10.17487/RFC2647, August 1999,
              <http://www.rfc-editor.org/info/rfc2647>.

   [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms
              for IPv6 Hosts and Routers", RFC 4213,
              DOI 10.17487/RFC4213, October 2005,
              <http://www.rfc-editor.org/info/rfc4213>.

   [RFC4890] Davies, E. and J. Mohacsi, "Recommendations for Filtering
              ICMPv6 Messages in Firewalls", RFC 4890,
              DOI 10.17487/RFC4890, May 2007,
              <http://www.rfc-editor.org/info/rfc4890>.

   [RFC5180] Popoviciu, C., Hamza, A., Van de Velde, G., and D.
              Dugatkin, "IPv6 Benchmarking Methodology for Network
              Interconnect Devices", RFC 5180, DOI 10.17487/RFC5180, May
              2008, <http://www.rfc-editor.org/info/rfc5180>.

   [RFC5635] Kumari, W. and D. McPherson, "Remote Triggered Black Hole
              Filtering with Unicast Reverse Path Forwarding (uRPF)",
              RFC 5635, DOI 10.17487/RFC5635, August 2009,
              <http://www.rfc-editor.org/info/rfc5635>.

   [RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational
              Neighbor Discovery Problems", RFC 6583,
              DOI 10.17487/RFC6583, March 2012,
              <http://www.rfc-editor.org/info/rfc6583>.

   [RFC7123] Gont, F. and W. Liu, "Security Implications of IPv6 on
              IPv4 Networks", RFC 7123, DOI 10.17487/RFC7123, February
              2014, <http://www.rfc-editor.org/info/rfc7123>.

   [RFC7126] Gont, F., Atkinson, R., and C. Pignataro, "Recommendations
              on Filtering of IPv4 Packets Containing IPv4 Options",
              BCP 186, RFC 7126, DOI 10.17487/RFC7126, February 2014,
              <http://www.rfc-editor.org/info/rfc7126>.

   [RFC2979] Freed, N., "Behavior of and Requirements for Internet
              Firewalls", RFC 2979, DOI 10.17487/RFC2979, October 2000,
              <http://www.rfc-editor.org/info/rfc2979>.

   [RFC3511] Hickman, B., Newman, D., Tadjudin, S., and T. Martin,
              "Benchmarking Methodology for Firewall Performance",
              RFC 3511, DOI 10.17487/RFC3511, April 2003,
              <http://www.rfc-editor.org/info/rfc3511>.

   [RFC5927] Gont, F., "ICMP Attacks against TCP", RFC 5927,
              DOI 10.17487/RFC5927, July 2010,
              <http://www.rfc-editor.org/info/rfc5927>.

   [I-D.ietf-opsec-ipv6-nd-security]
              Gont, F., Bonica, R., and W. Will, "Security Assessment of
              Neighbor Discovery (ND) for IPv6", draft-ietf-opsec-ipv6-
              nd-security-00 (work in progress), October 2013.

   [RFC6274] Gont, F., "Security Assessment of the Internet Protocol
              Version 4", RFC 6274, DOI 10.17487/RFC6274, July 2011,
              <http://www.rfc-editor.org/info/rfc6274>.

   [CPNI-TCP]
              CPNI, , "Security Assessment of the Transmission Control
              Protocol (TCP)", http://www.gont.com.ar/papers/
              tn-03-09-security-assessment-TCP.pdf, 2009.

   [SSL-VPNs]
              Hoffman, P., "SSL VPNs: An IETF Perspective", IETF 72,
              SAAG Meeting., 2008,
              <http://www.ietf.org/proceedings/72/slides/saag-4.pdf>.

   [FW-Benchmark]
              Zack, E., "Firewall Security Assessment and Benchmarking
              IPv6 Firewall Load Tests", IPv6 Hackers Meeting #1,
              Berlin, Germany. June 30, 2013,
              <http://www.ipv6hackers.org/meetings/ipv6-hackers-1/zack-
              ipv6hackers1-firewall-security-assessment-and-
              benchmarking.pdf>.

   [Junos-Teardrop]
              Juniper, j., "Understanding Teardrop Attacks", Junos OS
              Security Configuration Guide, 2010,
              <http://www.juniper.net/techpubs/software/junos-es/junos-
              es93/junos-es-swconfig-security/
              understanding-teardrop-attacks.html>.

   [draft-gont-opsec-ipv6-eh-filtering]
              Gont, F., Ermini, M., and W. Liu, "Recommendations on
              Filtering of IPv6 Packets Containing IPv6 Extension
              Headers", draft-gont-opsec-ipv6-filtering-00, Work
              in Progress, April 2014.

   [Kenney1996]
             Kenney, M., "The Ping of Death Page", 1996,
             <http://www.insecure.org/sploits/ping-o-death.html>.

   [Meltman1997]
             Meltman, M., "new TCP/IP bug in win95", 1997,
             <http://insecure.org/sploits/land.ip.DOS.html>.

   [Myst1997]
             Myst, M., "Windows 95/NT DoS", 1997,
             <http://insecure.org/sploits/land.ip.DOS.html>.

   [CERT1997]
             CERT, , "CERT Advisory CA-1997-28: IP Denial-of-Service
             Attacks", 1997,
             <http://www.cert.org/advisories/CA-1997-28.html>.

   [CERT1998a]
             CERT, , "CERT Advisory CA-1998-01: Smurf IP Denial-of-
             Service Attacks", 1998,
             <http://www.cert.org/advisories/CA-1998-01.html>.

Authors' Addresses

   Fernando Gont
   SI6 Networks / UTN-FRH
   Evaristo Carriego 2644
   Haedo, Provincia de Buenos Aires 1706
   Argentina

   Phone: +54 11 4650 8472
   Email: fgont@si6networks.com
   URI: http://www.si6networks.com

   Marco Ermini
   ResMed
   Fraunhoferstrasse 16
   Munich, Bayern 82152
   Deutschland

   Phone: +49 175 4395642
   Email: marco.ermini@resmed.com
   URI: http://www.resmed.com

   Will Liu
   Huawei Technologies
   Bantian, Longgang District
   Shenzhen 518129
   P.R. China

   Email: liushucheng@huawei.com