

opsec  
Internet-Draft  
Intended status: Best Current Practice  
Expires: January 5, 2015

F. Gont  
UTN-FRH / SI6 Networks  
W. Liu  
Huawei Technologies  
R. Bonica  
Juniper Networks  
July 4, 2014

Recommendations on filtering of IPv6 packets containing IPv6 Extension  
Headers  
draft-gont-opsec-ipv6-eh-filtering-00.txt

Abstract

This document provides advice on the filtering of IPv6 packets based on the IPv6 Extension Headers and the IPv6 options they contain. Additionally, it discusses the operational and interoperability implications of dropping packets based on the IPv6 Extension Headers and IPv6 options they contain.

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 5, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must 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 . . . . .	2
1.1. Terminology and Conventions Used in This Document . . . . .	3
2. IPv6 Extension Headers . . . . .	3
2.1. General Discussion . . . . .	3
2.2. General Security Implications . . . . .	3
2.3. Advice on the Handling of IPv6 Packets with Specific IPv6 Extension Headers . . . . .	3
3. IPv6 Options . . . . .	10
3.1. General Discussion . . . . .	10
3.2. General Security Implications of IPv6 Options . . . . .	10
3.3. Advice on the Handling of Packets with Specific IPv6 Options . . . . .	11
4. IANA Considerations . . . . .	22
5. Security Considerations . . . . .	22
6. Acknowledgements . . . . .	22
7. References . . . . .	22
7.1. Normative References . . . . .	22
7.2. Informative References . . . . .	24
Authors' Addresses . . . . .	25

## 1. Introduction

This document discusses the filtering of IPv6 packets based on the IPv6 Extension Headers and the IPv6 options they contain. Since various protocols may use IPv6 Extension Headers (possibly with IPv6 options), dropping packets based on the the IPv6 Extension Headers or IPv6 options they contain may have implications on the proper functioning of such protocols. Thus, this document attempts to discuss the operational and interoperability implications of such dropping, and provide advice in this area. Additionally, it outlines what an administrator should do in a typical enterprise environments. This document is similar in nature to [RFC7123], which addresses the same problem for the IPv4 case.

Section 2 of this document discusses IPv6 extension headers and IPv6 options, and provides advice in the area of filtering IPv6 packets that contain such IPv6 Extension Headers and/or options.

### 1.1. Terminology and Conventions Used in This Document

The terms "fast path", "slow path", and associated relative terms ("faster path" and "slower path") are loosely defined as in Section 2 of [RFC6398].

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 [RFC2119].

## 2. IPv6 Extension Headers

### 2.1. General Discussion

IPv6 Extension Headers allow for the extension of the IPv6 [RFC2460] protocol. Since both IPv6 Extension Headers and upper-layer protocols share the same namespace ("Next Header" registry/namespace), [RFC7045] identifies which of the currently assigned Internet Protocol numbers identify IPv6 Extension Headers vs. upper-layer protocols. This document discusses the filtering of packets based on the IPv6 Extension Headers (as specified by [RFC7045]) they contain. .

NOTE: [RFC7112] specifies that non-fragmented IPv6 datagrams and IPv6 First-Fragments, must contain the entire IPv6 header chain [RFC7112]. Therefore, intermediate systems can always enforce the filtering policies discussed in this document, or resort to simply dropping the offending packets when they fail to comply with the requirements in [RFC7112].

### 2.2. General Security Implications

Depending on the specific device architecture, IPv6 packets that contain IPv6 Extension Headers may require processing by the device's general-purpose CPU, and hence can be leveraged for the purpose of Denial of Service (DoS) attacks [Cisco-EH] [FW-Benchmark].

Operators are urged to consider IPv6 Extension Header filtering and IPv6 options handling capabilities of different devices as they make deployment decisions in future.

### 2.3. Advice on the Handling of IPv6 Packets with Specific IPv6 Extension Headers

### 2.3.1. IPv6 Hop-by-Hop Option (Number=0)

#### 2.3.1.1. Uses

The Hop-by-Hop Options header is used to carry optional information that must be examined by every node along a packet's delivery path. At the time of this writing, the following options have been specified for the Hop-by-Hop Options extension header:

- o Router Alert [RFC2711]
- o Jumbo Payload [RFC2675]
- o RPL Option [RFC6553]
- o SMF\_DPD [RFC6621]
- o MPL Option [I-D.ietf-roll-trickle-mcast]
- o IPv6 DFF Header [RFC6971]

#### 2.3.1.2. Specification

This Extension Header is specified in [RFC2460].

#### 2.3.1.3. Specific Security Implications

Since this Extension Header must be processed by all intermediate-systems en route, it can be leveraged to perform Denial of Service attacks against the network infrastructure.

#### 2.3.1.4. Operational and Interoperability Impact if Blocked

Dropping of packets containing a Hop-by-Hop Option extension header would break RSVP and multicast deployments. Additionally, it would cause IPv6 jumbograms to be dropped.

#### 2.3.1.5. Advice

Intermediate systems should, by default, drop packets containing a IPv6 Hop-by-Hop Option Extension Header. For obvious reasons, RPL routers must not drop packets based on the presence of an IPv6 Hop-by-Hop Option Extension Header.

Those intermediate systems processing the contents of this extension header should drop packets that contain more than one instance of the Router Alert option (see [RFC2711]).

### 2.3.2. Routing Header for IPv6 (Number=43)

#### 2.3.2.1. Uses

The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination.

#### 2.3.2.2. Specification

This Extension Header is specified in [RFC2460]. [RFC2460] originally specified the Routing Header Type 0, which has been later obsoleted by [RFC5095].

At the time of this writing, the following Routing Types have been specified:

- o Type 0: Source Route (DEPRECATED) [RFC2460] [RFC5095]
- o Type 1: Nimrod (DEPRECATED 2009-05-06)
- o Type 2: Type 2 Routing Header [RFC6275]
- o Type 3: RPL Source Route Header [RFC6554]
- o Types 4-252: Unassigned
- o Type 253: RFC3692-style Experiment 1 [RFC4727]
- o Type 254: RFC3692-style Experiment 2 [RFC4727]
- o Type 255: Reserved

#### 2.3.2.3. Specific Security Implications

The security implications of RHT0 have been discussed in detail in [Biondi2007] and [RFC5095].

#### 2.3.2.4. Operational and Interoperability Impact if Blocked

Blocking packets containing a RHT0 has no operational implications.

#### 2.3.2.5. Advice

Drop packets containing a RHT0.

### 2.3.3. Fragment Header for IPv6 (Number=44)

#### 2.3.3.1. Uses

This Extension Header provides the fragmentation functionality for IPv6.

#### 2.3.3.2. Specification

This Extension Header is specified in [RFC2460].

#### 2.3.3.3. Specific Security Implications

The security implications of the Fragment Header range from Denial of Service attacks (based on flooding a target with IPv6 fragments) to information leakage attacks [I-D.ietf-6man-predictable-fragment-id].

#### 2.3.3.4. Operational and Interoperability Impact if Blocked

Blocking packets that contain a Fragment Header would break any protocols that might rely on fragmentation (e.g., the DNS).

#### 2.3.3.5. Advice

Intermediate systems should, by default, pass packets that contain a Fragment Header.

### 2.3.4. Encapsulating Security Payload (Number=50)

#### 2.3.4.1. Uses

This extension Header is employed for the IPsec suite [RFC4303].

#### 2.3.4.2. Specification

This extension header is specified in [RFC4303].

#### 2.3.4.3. Specific Security Implications

Besides the general implications of IPv6 Extension Headers, this extension header could be employed to potentially perform a DoS attack at the destination system by wasting CPU resources in validating the contents of the packet.

#### 2.3.4.4. Operational and Interoperability Impact if Blocked

Dropping packets that employ this extension header would break IPsec deployments.

#### 2.3.4.5. Advice

Intermediate systems should pass packets containing the Encapsulating Security Payload extensio header.

### 2.3.5. Authentication Header (Number=51)

#### 2.3.5.1. Uses

The Authentication Header can be employed for provide authentication services in IPv4 and IPv6. .

#### 2.3.5.2. Specification

This Extension Header is specified in [RFC4302].

#### 2.3.5.3. Specific Security Implications

This header could be employed for performing a CPU-consumption attack at the target system.

#### 2.3.5.4. Operational and Interoperability Impact if Blocked

Traffic employing the Authentication Header would be dropped.

#### 2.3.5.5. Advice

Intermediary systems should not drop packets containing an Authentication Header.

### 2.3.6. Destination Options for IPv6 (Number=60)

#### 2.3.6.1. Uses

The Destination Options header is used to carry optional information that need be examined only by a packet's destination node(s).

#### 2.3.6.2. Specification

This Extension Header is specified in [RFC2460]. At the time of this writing, no options have been specified for this extension header.

#### 2.3.6.3. Specific Security Implications

No security implications are known, other than the general implications of IPv6 extension headers.

#### 2.3.6.4. Operational and Interoperability Impact if Blocked

None.

#### 2.3.6.5. Advice

Pass packets that contain the Destination Options Header.

#### 2.3.7. Mobility Header (Number=135)

##### 2.3.7.1. Uses

The Mobility Header is an extension header used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings in Mobile IPv6.

##### 2.3.7.2. Specification

This Extension Header is specified in [RFC6275].

##### 2.3.7.3. Specific Security Implications

TBD.

##### 2.3.7.4. Operational and Interoperability Impact if Blocked

Dropping packets containing this extension header would break Mobile IPv6.

##### 2.3.7.5. Advice

Pass packets containing this extension header.

#### 2.3.8. Host Identity Protocol (Number=139)

##### 2.3.8.1. Uses

This extension header is employed with the Host Identity Protocol (HIP), an experimental protocol that allows consenting hosts to securely establish and maintain shared IP-layer state, allowing separation of the identifier and locator roles of IP addresses, thereby enabling continuity of communications across IP address changes.



#### 2.3.8.2. Specification

This extension Header is specified in [RFC5201].

#### 2.3.8.3. Specific Security Implications

TBD.

#### 2.3.8.4. Operational and Interoperability Impact if Blocked

Dropping packets that contain the Host Identity Protocol would break HIP deployments.

#### 2.3.8.5. Advice

Pass packets that contain a Host Identity Protocol extension header.

#### 2.3.9. Shim6 Protocol (Number=140)

##### 2.3.9.1. Uses

This extension header is employed by the Shim6 Protocol.

##### 2.3.9.2. Specification

This Extension Header is specified in [RFC5533].

##### 2.3.9.3. Specific Security Implications

TBD.

##### 2.3.9.4. Operational and Interoperability Impact if Blocked

Dropping packets that contain this extension header would break Shim6.

##### 2.3.9.5. Advice

Pass packets containing this extension header.

#### 2.3.10. Use for experimentation and testing (Numbers=253 and 254)

##### 2.3.10.1. Uses

.

#### 2.3.10.2. Specification

This Extension Header is specified in [RFC3692] and [RFC4727].

#### 2.3.10.3. Specific Security Implications

None.

#### 2.3.10.4. Operational and Interoperability Impact if Blocked

.

#### 2.3.10.5. Advice

Routers, security gateways, and firewalls SHOULD have configuration knobs for IP packets that contain this extension header to select between "ignore & forward" and "drop & log". Otherwise, no legitimate experiment using these options will be able to traverse any IP router.

The aforementioned configuration knob SHOULD default to "drop & log".

Special care needs to be taken in the case of "drop & log". Devices SHOULD count the number of packets dropped, but the logging of drop events SHOULD be limited so as to not overburden device resources.

### 3. IPv6 Options

#### 3.1. General Discussion

The following subsections describe specific security implications of different IPv6 options, and provide advice regarding filtering packets that contain such options.

#### 3.2. General Security Implications of IPv6 Options

The general security implications of IPv6 options are closely related to those discussed in Section 2.2. Essentially, packets that contain IPv6 options might need to be processed by IPv6 router's general-purpose CPU can be a DDoS risk to that router's general-purpose CPU (and thus to the router itself). For some architectures, a possible mitigation would be to rate-limit the packets that are to be processed by the general-purpose CPU (see e.g. [Cisco-EH]).

### 3.3. Advice on the Handling of Packets with Specific IPv6 Options

The following subsections contain a description of each of the IPv6 options that have so far been specified, a discussion of possible interoperability implications if packets containing such options are dropped, and specific advice on whether to drop packets containing these options in a typical enterprise firewall.

#### 3.3.1. Pad1 (Type=0x00)

##### 3.3.1.1. Uses

This option is used when necessary to align subsequent options and to pad out the containing header to a multiple of 8 octets in length.

##### 3.3.1.2. Specification

This option is specified in [RFC2460].

##### 3.3.1.3. Specific Security Implications

None.

##### 3.3.1.4. Operational and Interoperability Impact if Blocked

Dropping packets that contain this option would potentially break any protocol that relies on IPv6 extension headers.

##### 3.3.1.5. Advice

Do not drop packets based on the presence of this option.

#### 3.3.2. PadN (Type=0x01)

##### 3.3.2.1. Uses

This option is used when necessary to align subsequent options and to pad out the containing header to a multiple of 8 octets in length.

##### 3.3.2.2. Specification

This option is specified in [RFC2460].

##### 3.3.2.3. Specific Security Implications

Because of the possible size of this option, it could be leveraged as a large-bandwidth covert channel.

#### 3.3.2.4. Operational and Interoperability Impact if Blocked

Dropping packets that contain this option would potentially break any protocol that relies on IPv6 extension headers.

#### 3.3.2.5. Advice

Do not drop packets based on the presence of this option.

#### 3.3.3. Jumbo Payload (Type=0XC2)

##### 3.3.3.1. Uses

The Jumbo payload option provides the means of specifying payloads larger than 65535 bytes.

##### 3.3.3.2. Specification

This option is specified in [RFC2675].

##### 3.3.3.3. Specific Security Implications

TBD.

##### 3.3.3.4. Operational and Interoperability Impact if Blocked

Dropping packets based on the presence of this option would cause IPv6 jumbograms to be dropped.

##### 3.3.3.5. Advice

By default, intermediate systems should drop packets that contain this option. This policy could be overridden in specific environments where support for IPv6 jumbograms is desired.

#### 3.3.4. RPL Option (Type=0x63)

##### 3.3.4.1. Uses

The RPL Option provides a mechanism to include routing information with each datagram that an RPL router forwards.

##### 3.3.4.2. Specification

This option is specified in [RFC6553].

#### 3.3.4.3. Specific Security Implications

TBD.

#### 3.3.4.4. Operational and Interoperability Impact if Blocked

This options is meant to be employed within an RPL instance. As a result, dropping packets based on the presence of this option at e.g. an ISP does will not result in operational implications.

#### 3.3.4.5. Advice

Non-RPL routers should drop packets that contain an RPL option.

#### 3.3.5. Tunnel Encapsulation Limit (Type=0x04)

##### 3.3.5.1. Uses

The Tunnel Encapsulation Limit option can be employed to specify how many further levels of nesting the packet is permitted to undergo.

##### 3.3.5.2. Specification

This option is specified in [RFC2473].

##### 3.3.5.3. Specific Security Implications

TBD.

##### 3.3.5.4. Operational and Interoperability Impact if Blocked

Filtering packets based on the presence of this option could result in tunnel traffic being dropped.

##### 3.3.5.5. Advice

Intermediate systems should not drop packets based on the presence of this option.

Since this option is meant to be included in the Destination Options Header, an intermediate system should drop packets that employ this option in any other extension header type.

#### 3.3.6. Router Alert (Type=0x05)

#### 3.3.6.1. Uses

Router Alert option [RFC2711], which is typically employed for the RSVP protocol [RFC2205] and the MLD protocol [RFC2710].

#### 3.3.6.2. Specification

This option is specified in [RFC2711].

#### 3.3.6.3. Specific Security Implications

Since this option causes the contents of the packet to be inspected by the handling device, this option could be leveraged for performing DoS attacks.

#### 3.3.6.4. Operational and Interoperability Impact if Blocked

Dropping packets that contain this option would break RSVP and multicast deployments.

#### 3.3.6.5. Advice

Intermediate systems should, by default, drop packets that contain this option.

#### 3.3.7. Quick-Start (Type=0x26)

##### 3.3.7.1. Uses

This IP Option is used in the specification of Quick-Start for TCP and IP, which is an experimental mechanism that allows transport protocols, in cooperation with routers, to determine an allowed sending rate at the start and, at times, in the middle of a data transfer (e.g., after an idle period) [RFC4782].

##### 3.3.7.2. Specification

This option is specified in [RFC4782], on the "Experimental" track.

##### 3.3.7.3. Specific Security Implications

Section 9.6 of [RFC4782] notes that Quick-Start is vulnerable to two kinds of attacks:

- o attacks to increase the routers' processing and state load, and,

- o attacks with bogus Quick-Start Requests to temporarily tie up available Quick-Start bandwidth, preventing routers from approving Quick-Start Requests from other connections.

#### 3.3.7.4. Operational and Interoperability Impact if Blocked

The Quick-Start functionality would be disabled, and additional delays in TCP's connection establishment (for example) could be introduced. (Please see Section 4.7.2 of [RFC4782].) We note, however, that Quick-Start has been proposed as a mechanism that could be of use in controlled environments, and not as a mechanism that would be intended or appropriate for ubiquitous deployment in the global Internet [RFC4782].

#### 3.3.7.5. Advice

A given router, security gateway, or firewall system has no way of knowing a priori whether this option is valid in its operational environment. Therefore, routers, security gateways, and firewalls SHOULD, by default, ignore the Quick-Start option. Additionally, routers, security gateways, and firewalls SHOULD have a configuration setting that governs their reaction in the presence of packets containing the Quick-Start option. This configuration setting SHOULD allow to honor and process the option, ignore the option, or drop packets containing this option. The default configuration is to ignore the Quick-Start option.

We note that if routers in a given environment do not implement and enable the Quick-Start mechanism, only the general security implications of IP options (discussed in Section 3.2) would apply.

#### 3.3.8. CALIPSO (Type=0x07)

##### 3.3.8.1. Uses

This option is used for encoding explicit packet Sensitivity Labels on IPv6 packets. It is intended for use only within Multi-Level Secure (MLS) networking environments that are both trusted and trustworthy.

##### 3.3.8.2. Specification

This option is specified in [RFC5570].

#### 3.3.8.3. Specific Security Implications

Presence of this option in a packet does not by itself create any specific new threat. Packets with this option ought not normally be seen on the global public Internet.

#### 3.3.8.4. Operational and Interoperability Impact if Blocked

If packets with this option are blocked or if the option is stripped from the packet during transmission from source to destination, then the packet itself is likely to be dropped by the receiver because it is not properly labeled. In some cases, the receiver might receive the packet but associate an incorrect sensitivity label with the received data from the packet whose CALIPSO was stripped by an intermediate router or firewall. Associating an incorrect sensitivity label can cause the received information either to be handled as more sensitive than it really is ("upgrading") or as less sensitive than it really is ("downgrading"), either of which is problematic.

#### 3.3.8.5. Advice

A given IP router, security gateway, or firewall has no way to know a priori what environment it has been deployed into. Even closed IP deployments generally use exactly the same commercial routers, security gateways, and firewalls that are used in the public Internet.

Since operational problems result in environments where this option is needed if either the option is dropped or IPv6 packets containing this option are dropped, but no harm results if the option is carried in environments where it is not needed, the default configuration SHOULD NOT (a) modify or remove this IPv6 option or (b) drop an IPv6 packet because the IPv6 packet contains this option.

A given IPv6 router, security gateway, or firewall MAY be configured to drop this option or to drop IP packets containing this option in an environment known to not use this option.

For auditing reasons, routers, security gateways, and firewalls SHOULD be capable of logging the numbers of packets containing the CALIPSO on a per-interface basis. Also, routers, security gateways, and firewalls SHOULD be capable of dropping packets based on the CALIPSO presence as well as the CALIPSO values.



### 3.3.9. SMF\_DPD (Type=0x08)

#### 3.3.9.1. Uses

This option is employed in the (experimental) Simplified Multicast Forwarding (SMF) for unique packet identification for IPv6 I-DPD, and as a mechanism to guarantee non-collision of hash values for different packets when H-DPD is used. .

#### 3.3.9.2. Specification

This option is specified in [RFC6621].

#### 3.3.9.3. Specific Security Implications

TBD.

#### 3.3.9.4. Operational and Interoperability Impact if Blocked

TBD.

#### 3.3.9.5. Advice

TBD.

### 3.3.10. Home Address (Type=0xC9)

#### 3.3.10.1. Uses

The Home Address option is used by a Mobile IPv6 node while away from home, to inform the recipient of the mobile node's home address.

#### 3.3.10.2. Specification

This option is specified in [RFC6275].

#### 3.3.10.3. Specific Security Implications

TBD.

#### 3.3.10.4. Operational and Interoperability Impact if Blocked

TBD.

## 3.3.10.5. Advice

TBD.

## 3.3.11. Endpoint Identification (Type=0x8A)

## 3.3.11.1. Uses

The Endpoint Identification option was meant to be used with the Nimrod routing architecture [NIMROD-DOC], but has never seen widespread deployment.

## 3.3.11.2. Specification

This option is specified in [NIMROD-DOC].

## 3.3.11.3. Specific Security Implications

TBD.

## 3.3.11.4. Operational and Interoperability Impact if Blocked

None.

## 3.3.11.5. Advice

An intermediate system should drop packets that contain this option.

## 3.3.12. ILNP Nonce (Type=0x8B)

## 3.3.12.1. Uses

This option is employed by Identifier-Locator Network Protocol for IPv6 (ILNPv6) for providing protection against off-path attacks for packets when ILNPv6 is in use, and as a signal during initial network-layer session creation that ILNPv6 is proposed for use with this network-layer session, rather than classic IPv6.

## 3.3.12.2. Specification

This option is specified in [RFC6744].

## 3.3.12.3. Specific Security Implications

TBD.

#### 3.3.12.4. Operational and Interoperability Impact if Blocked

TBD.

#### 3.3.12.5. Advice

TBD.

### 3.3.13. Line-Identification Option (Type=0x8C)

#### 3.3.13.1. Uses

This option is used by an Edge Router to identify the subscriber premises in scenarios where several subscriber premises may be logically connected to the same interface of an Edge Router.

#### 3.3.13.2. Specification

This option is specified in [RFC6788].

#### 3.3.13.3. Specific Security Implications

TBD.

#### 3.3.13.4. Operational and Interoperability Impact if Blocked

Since this options is meant to be employed in Router Solicitation messages, dropping packets based on the presence of this option at intermediate systems will result in no interoperability implications.

#### 3.3.13.5. Advice

Intermediate devices should drop packets that contain this option.

### 3.3.14. Deprecated (Type=0x4D)

#### 3.3.14.1. Uses

TBD.

#### 3.3.14.2. Specification

TB.

#### 3.3.14.3. Specific Security Implications

TBD.

#### 3.3.14.4. Operational and Interoperability Impact if Blocked

TBD.

#### 3.3.14.5. Advice

TBD.

### 3.3.15. MPL Option (Type=0x6D)

#### 3.3.15.1. Uses

This option is specified in [I-D.ietf-roll-trickle-mcast], and is meant to be included only in Hop-by-Hop Option headers..

#### 3.3.15.2. Specification

This option is specified in [I-D.ietf-roll-trickle-mcast].

#### 3.3.15.3. Specific Security Implications

TBD.

#### 3.3.15.4. Operational and Interoperability Impact if Blocked

TBD.

#### 3.3.15.5. Advice

TBD.

### 3.3.16. IP\_DFF (Type=0xEE)

#### 3.3.16.1. Uses

This options is employed with the (Experimental) Depth-First Forwarding (DFF) in Unreliable Networks.

#### 3.3.16.2. Specification

This option is specified in [RFC6971].

## 3.3.16.3. Specific Security Implications

TBD.

## 3.3.16.4. Operational and Interoperability Impact if Blocked

TBD.

## 3.3.16.5. Advice

TBD.

## 3.3.17. RFC3692-style Experiment (Types = 0x1E, 0x3E, 0x5E, 0x7E, 0x9E, 0xBE, 0xDE, 0xFE)

## 3.3.17.1. Uses

It is only appropriate to use these values in explicitly configured experiments; they MUST NOT be shipped as defaults in implementations.

## 3.3.17.2. Specification

Specified in RFC 4727 [RFC4727] in the context of RFC3692-style experiments.

## 3.3.17.3. Specific Security Implications

No specific security issues are known for this IPv4 option.

## 3.3.17.4. Operational and Interoperability Impact if Blocked

None.

## 3.3.17.5. Advice

Routers, security gateways, and firewalls SHOULD have configuration knobs for IPv6 packets that contain RFC3692-style Experiment options to select between "ignore & forward" and "drop & log". Otherwise, no legitimate experiment using these options will be able to traverse any IP router.

Special care needs to be taken in the case of "drop & log". Devices SHOULD count the number of packets dropped, but the logging of drop events SHOULD be limited so as to not overburden device resources.

The aforementioned configuration knob SHOULD default to "drop & log".

#### 4. IANA Considerations

This document has no actions for IANA.

#### 5. Security Considerations

This document provides advice on the filtering of IPv6 packets that contain IPv6 Extension Headers (and possibly IPv6 options). Dropping such packets can help to mitigate the security issues that arise from the use of different IPv6 Extension Headers and options.

#### 6. Acknowledgements

This document borrows some text and analysis from [RFC7126], authored by Fernando Gont, Randall Atkinson, and Carlos Pignataro.

#### 7. References

##### 7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
- [RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.
- [RFC2675] Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", RFC 2675, August 1999.
- [RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
- [RFC2711] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, October 1999.
- [RFC3692] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3692, January 2004.
- [RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
- [RFC4304] Kent, S., "Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)", RFC 4304, December 2005.
- [RFC4727] Fenner, B., "Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers", RFC 4727, November 2006.
- [RFC4782] Floyd, S., Allman, M., Jain, A., and P. Sarolahti, "Quick-Start for TCP and IP", RFC 4782, January 2007.
- [RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.
- [RFC5201] Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.
- [RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, June 2009.
- [RFC5570] StJohns, M., Atkinson, R., and G. Thomas, "Common Architecture Label IPv6 Security Option (CALIPSO)", RFC 5570, July 2009.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6398] Le Faucheur, F., "IP Router Alert Considerations and Usage", BCP 168, RFC 6398, October 2011.
- [RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", RFC 6553, March 2012.
- [RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, March 2012.
- [RFC6621] Macker, J., "Simplified Multicast Forwarding", RFC 6621, May 2012.

- [RFC6744] Atkinson,, RJ., "IPv6 Nonce Destination Option for the Identifier-Locator Network Protocol for IPv6 (ILNPv6)", RFC 6744, November 2012.
- [RFC6788] Krishnan, S., Kavanagh, A., Varga, B., Ooghe, S., and E. Nordmark, "The Line-Identification Option", RFC 6788, November 2012.
- [RFC6971] Herberg, U., Cardenas, A., Iwao, T., Dow, M., and S. Cespedes, "Depth-First Forwarding (DFF) in Unreliable Networks", RFC 6971, June 2013.
- [RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, December 2013.
- [RFC7112] Gont, F., Manral, V., and R. Bonica, "Implications of Oversized IPv6 Header Chains", RFC 7112, January 2014.
- [RFC7123] Gont, F. and W. Liu, "Security Implications of IPv6 on IPv4 Networks", RFC 7123, February 2014.

## 7.2. Informative References

- [Biondi2007] Biondi, P. and A. Ebalard, "IPv6 Routing Header Security", CanSecWest 2007 Security Conference, 2007, <[http://www.secdev.org/conf/IPv6\\_RH\\_security-csw07.pdf](http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf)>.
- [Cisco-EH] Cisco Systems, , "IPv6 Extension Headers Review and Considerations", Whitepaper. October 2006, <[http://www.cisco.com/en/US/technologies/tk648/tk872/technologies\\_white\\_paper0900aecd8054d37d.pdf](http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.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>>.
- [I-D.ietf-6man-predictable-fragment-id] Gont, F., "Security Implications of Predictable Fragment Identification Values", draft-ietf-6man-predictable-fragment-id-01 (work in progress), April 2014.



[I-D.ietf-roll-trickle-mcast]

Hui, J. and R. Kelsey, "Multicast Protocol for Low power and Lossy Networks (MPL)", draft-ietf-roll-trickle-mcast-09 (work in progress), April 2014.

[IANA-IPV6]

Internet Assigned Numbers Authority, "Internet Protocol Version 6 (IPv6) Parameters", December 2013, <<http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml>>.

[NIMROD-DOC]

Nimrod Documentation Page, ,  
"<http://ana-3.lcs.mit.edu/~jnc/nimrod/>", .

[RFC7126] Gont, F., Atkinson, R., and C. Pignataro, "Recommendations on Filtering of IPv4 Packets Containing IPv4 Options", BCP 186, RFC 7126, February 2014.

Authors' Addresses

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

Phone: +54 11 4650 8472  
Email: [fgont@si6networks.com](mailto:fgont@si6networks.com)  
URI: <http://www.si6networks.com>

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

Email: [liushucheng@huawei.com](mailto:liushucheng@huawei.com)

Ronald P. Bonica  
Juniper Networks  
2251 Corporate Park Drive  
Herndon, VA 20171  
US

Phone: 571 250 5819  
Email: rbonica@juniper.net

opsec  
Internet-Draft  
Intended status: Informational  
Expires: October 18, 2014

F. Gont  
SI6 Networks / UTN-FRH  
M. Ermini  
ResMed  
W. Liu  
Huawei Technologies  
April 16, 2014

Requirements for IPv6 Enterprise Firewalls  
draft-gont-opsec-ipv6-firewall-reqs-01

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 October 18, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must 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. DISCLAIMER . . . . .	2
2. Introduction . . . . .	3
3. Conventions . . . . .	3
3.1. Requirements Language . . . . .	3
3.2. Terminology . . . . .	4
3.3. Numbering Conventions . . . . .	5
4. General Security Features . . . . .	5
5. IPv6-Specific Features . . . . .	7
6. VPN Security Requirements . . . . .	8
7. Denial of Service (DoS) Protection . . . . .	9
8. Application Layer Firewall . . . . .	11
9. Logging, Auditing and Security Operation Centre (SOC) requirements . . . . .	11
10. Console and Events Visualization requirements . . . . .	13
11. Reporting requirements . . . . .	14
12. IANA Considerations . . . . .	14
13. Security Considerations . . . . .	14
14. Acknowledgements . . . . .	14
15. References . . . . .	14
15.1. Normative References . . . . .	14
15.2. Informative References . . . . .	15
Authors' Addresses . . . . .	17

## 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/response 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 be 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 Sleight, 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, March 1997.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.



- [RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.
- [RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.
- [RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.
- [RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, December 2013.
- [RFC7112] Gont, F., Manral, V., and R. Bonica, "Implications of Oversized IPv6 Header Chains", RFC 7112, January 2014.
- [RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.
- [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.
- [RFC5214] Templin, F., Gleeson, T., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214, March 2008.
- [RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.

## 15.2. Informative References

- [RFC2647] Newman, D., "Benchmarking Terminology for Firewall Performance", RFC 2647, August 1999.
- [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.
- [RFC4890] Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, May 2007.
- [RFC5180] Popoviciu, C., Hamza, A., Van de Velde, G., and D. Dugatkin, "IPv6 Benchmarking Methodology for Network Interconnect Devices", RFC 5180, May 2008.

- [RFC5635] Kumari, W. and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)", RFC 5635, August 2009.
- [RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, March 2012.
- [RFC7123] Gont, F. and W. Liu, "Security Implications of IPv6 on IPv4 Networks", RFC 7123, February 2014.
- [RFC7126] Gont, F., Atkinson, R., and C. Pignataro, "Recommendations on Filtering of IPv4 Packets Containing IPv4 Options", BCP 186, RFC 7126, February 2014.
- [RFC2979] Freed, N., "Behavior of and Requirements for Internet Firewalls", RFC 2979, October 2000.
- [RFC3511] Hickman, B., Newman, D., Tadjudin, S., and T. Martin, "Benchmarking Methodology for Firewall Performance", RFC 3511, April 2003.
- [RFC5927] Gont, F., "ICMP Attacks against TCP", RFC 5927, July 2010.
- [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, July 2011.
- [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](mailto: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](mailto:liushucheng@huawei.com)