

Operational Security Capabilities for  
IP Network Infrastructure (opsec)  
Internet-Draft  
Intended status: BCP  
Expires: November 19, 2012

F. Gont  
SI6 Networks / UTN-FRH  
May 18, 2012

**DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers**  
**draft-gont-opsec-dhcpv6-shield-00**

Abstract

This document specifies a mechanism for protecting hosts connected to a broadcast network against rogue DHCPv6 servers. The aforementioned mechanism is based on DHCPv6 packet-filtering at the layer-2 device on which the packets are received. The aforementioned mechanism has been widely deployed in IPv4 networks ('DHCP snooping'), and hence it is desirable that similar functionality be provided for IPv6 networks.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 19, 2012.

Copyright Notice

Copyright (c) 2012 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	DHCPv6-Shield Configuration . . . . .	<a href="#">4</a>
<a href="#">3.</a>	DHCPv6-Shield Implementation Advice . . . . .	<a href="#">5</a>
<a href="#">4.</a>	IANA Considerations . . . . .	<a href="#">7</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">8</a>
<a href="#">6.</a>	Acknowledgements . . . . .	<a href="#">9</a>
<a href="#">7.</a>	References . . . . .	<a href="#">10</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">10</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">10</a>
	Author's Address . . . . .	<a href="#">12</a>



## **1. Introduction**

This document specifies a mechanism for protecting hosts connected to a broadcast network against rogue DHCPv6 servers. This mechanism is analogous to the RA-Guard mechanism [[RFC6104](#)] [[RFC6105](#)] [[I-D.ietf-v6ops-ra-guard-implementation](#)] intended for protection against rogue Router Advertisement messages.

The basic concept behind DHCPv6-Shield is that a layer-2 device filters DHCPv6 messages meant to DHCPv6 clients, according to a number of different criteria. The most basic filtering criterion being that the aforementioned DHCPv6 messages are discarded by the layer-2 device unless they are received on a specified port of the layer-2 device.

Before the DHCPv6-Shield device is deployed, the administrator specifies the layer-2 port(s) on which DHCPv6 packets meant for DHCPv6 clients are allowed. Only those ports to which a DHCPv6 server is to be connected should be specified as such. Once deployed, the DHCPv6-Shield device inspects received packets, and allows (i.e. passes) DHCPv6 messages meant for DHCPv6 clients only if they are received on layer-2 ports that have been explicitly configured for such purpose.

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



## **2. DHCPv6-Shield Configuration**

Before being deployed for production, the DHCPv6-Shield device MUST be configured with respect to which layer-2 ports are allowed to send DHCPv6 packets to DHCPv6 clients. Only those layer-2 ports explicitly configured for such purpose will be allowed to send DHCPv6 packets to DHCPv6 clients.

### **3. DHCPv6-Shield Implementation Advice**

The following filtering rules MUST be enforced as part of an DHCPv6-Shield implementation on those ports that are not allowed to send DHCPv6 packets to DHCPv6 clients:

1. Try to identify whether the packet is a DHCPv6 packet meant for a DHCPv6 client, by parsing the IPv6 header chain. When doing so, enforce a limit on the maximum number of Extension Headers that is allowed for each packet, and if such limit is hit before the upper-layer protocol is identified, silently drop the packet.

[RFC6564] specifies a uniform format for IPv6 Extension Header, thus meaning that an IPv6 node should be able to parse an IPv6 header chain even if it contains Extension Headers that are not currently supported by that node.

2. If the layer-2 device is unable to identify whether the packet is a DHCPv6 packet meant for a DHCPv6 client or not (i.e., the packet is a first-fragment, and the necessary information is missing), silently drop the packet.

Note: This rule should only be applied to non-fragmented IPv6 datagrams and IPv6 fragments with a Fragment Offset of 0 (non-first fragments can be safely passed, since they will never reassemble into a complete datagram if the first fragment is successfully dropped by DHCPv6-Shield).

3. If the packet is identified to be a DHCPv6 packet meant for a DHCPv6 client, silently drop the packet.

A packet is said to be "a DHCPv6 packet meant for a DHCPv6 client" if the encapsulated transport protocol is UDP, and the UDP Destination Port is 546.

4. In all other cases, pass the packet as usual.

Note: For the purpose of enforcing the DHCPv6-Shield filtering policy, an ESP header [RFC4303] should be considered to be an "upper-layer protocol" (that is, it should be considered the last header in the IPv6 header chain). This means that packets employing ESP would be passed by the DHCPv6-Shield device to the intended destination. If the destination host does not have a security association with the sender of the aforementioned IPv6 packet, the packet would be dropped. Otherwise, if the packet is considered valid by the IPsec implementation at the receiving host and it encapsulates a DHCPv6 message, it is up to the receiving host what to do with such packet.





Rule #2 has been defined as a default rule to drop packets that cannot be positively identified as not being DHCPv6 packets meant for DHCPv6 clients (possibly because the packet contains fragments that do not contain the entire IPv6 header chain). This means that, at least in theory, DHCPv6-Shield could result in false-positive blocking of some legitimate non-DHCPv6 packets that could not be positively identified as being non-DHCPv6. However, as noted in [[I-D.gont-6man-oversized-header-chain](#)], IPv6 packets that fail to include the entire IPv6 header chain are anyway unlikely to survive in real networks. Whilst currently legitimate from a specifications standpoint, they are virtually impossible to police with state-less filters and firewalls, and are hence likely to be blocked by such filters and firewalls.

The aforementioned filtering rules implicitly handle the case of fragmented packets: if the DHCPv6-Shield device fails to identify the upper-layer protocol as a result of the use of fragmentation, the corresponding packets would be silently dropped.

Finally, we note that IPv6 implementations that allow overlapping fragments (i.e. that do not comply with [[RFC5722](#)]) might still be subject of DHCPv6-based attacks. However, a recent assessment of IPv6 implementations [[SI6-FRAG](#)] with respect to their fragment reassembly policy seems to indicate that most current implementations comply with [[RFC5722](#)].



#### **4. IANA Considerations**

This document has no actions for IANA.

## 5. Security Considerations

The mechanism specified in this document can be used to mitigate DHCPv6-based attacks. Attack vectors based on other messages (such as ICMPv6 Router Advertisements) are out of the scope of this document.

Mitigation of such attack vectors is discussed in other documents, such as [[RFC6105](#)], [[I-D.ietf-v6ops-ra-guard-implementation](#)] and [[draft-gont-opsec-ipv6-ndp-shield](#)].

As noted in [Section 3](#), IPv6 implementations that allow overlapping fragments (i.e. that do not comply with [[RFC5722](#)]) might still be subject of DHCPv6-based attacks. However, most current implementations seem to comply with [[RFC5722](#)], and hence forbid IPv6 overlapping fragments.

We note that if an attacker sends a fragmented DHCPv6 packets on a port not allowed to send such packets, the first-fragment would be dropped, and the rest of the fragments would be passed. This means that the victim node would tie memory buffers for the aforementioned fragments, which would never reassemble into a complete datagram. If a large number of such packets were sent by an attacker, and the victim node failed to implement proper resource management for the fragment reassembly buffer, this could lead to a Denial of Service (DoS). However, this does not really introduce a new attack vector, since an attacker could always perform the same attack by sending forged fragmented datagram in which at least one of the fragments is missing. [[CPNI-IPv6](#)] discusses some resource management strategies that could be implemented for the fragment reassembly buffer.



## **6. Acknowledgements**

This document is heavily based on the document [[I-D.ietf-v6ops-ra-guard-implementation](#)] authored by Fernando Gont. Thus, the author would like to thank Ran Atkinson, Karl Auer, Robert Downie, Washam Fan, David Farmer, Marc Heuse, Nick Hilliard, Ray Hunter, Joel Jaeggli, Simon Perreault, Arturo Servin, Gunter van de Velde, James Woodyatt, and Bjoern A. Zeeb, for providing valuable comments on [[I-D.ietf-v6ops-ra-guard-implementation](#)], on which this document is based.

## **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.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", [RFC 4303](#), December 2005.
- [RFC5722] Krishnan, S., "Handling of Overlapping IPv6 Fragments", [RFC 5722](#), December 2009.
- [RFC6564] Krishnan, S., Woodyatt, J., Kline, E., Hoagland, J., and M. Bhatia, "A Uniform Format for IPv6 Extension Headers", [RFC 6564](#), April 2012.

### **7.2. Informative References**

- [RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", [RFC 6104](#), February 2011.
- [RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", [RFC 6105](#), February 2011.
- [I-D.gont-6man-oversized-header-chain]  
Gont, F. and V. Manral, "Security and Interoperability Implications of Oversized IPv6 Header Chains", [draft-gont-6man-oversized-header-chain-01](#) (work in progress), April 2012.
- [I-D.ietf-v6ops-ra-guard-implementation]  
Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", [draft-ietf-v6ops-ra-guard-implementation-03](#) (work in progress), May 2012.
- [[draft-gont-opsec-ipv6-ndp-shield](#)]  
Gont, F., "Neighbor Discovery Shield (ND-Shield)", IETF Internet Draft, [draft-gont-opsec-ipv6-ndp-shield](#), work in progress, May 2012.
- [SI6-FRAG]





SI6 Networks, "IPv6 NIDS evasion and improvements in IPv6 fragmentation/reassembly", 2012, <<http://blog.si6networks.com/2012/02/ipv6-nids-evasion-and-improvements-in.html>>.

[CPNI-IPv6]

Gont, F., "Security Assessment of the Internet Protocol version 6 (IPv6)", UK Centre for the Protection of National Infrastructure, (available on request).

Author's Address

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>