

opsec
Internet-Draft
Intended status: Best Current Practice
Expires: April 25, 2014

F. Gont
SI6 Networks / UTN-FRH
W. Liu
Huawei Technologies
G. Van de Velde
Cisco Systems
October 22, 2013

DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers
draft-ietf-opsec-dhcpv6-shield-01

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 at 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](#).

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 April 25, 2014.

Copyright Notice

Copyright (c) 2013 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
2.	Requirements Language	2
3.	Terminology	3
4.	DHCPv6-Shield Configuration	4
5.	DHCPv6-Shield Implementation Advice	4
6.	IANA Considerations	6
7.	Security Considerations	6
8.	Acknowledgements	7
9.	References	7
9.1.	Normative References	7
9.2.	Informative References	8
	Authors' Addresses	8

[1.](#) Introduction

This document specifies a mechanism for protecting hosts connected to a broadcast network against rogue DHCPv6 servers [[RFC3315](#)]. 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 [[RFC4861](#)] messages.

The basic concept behind DHCPv6-Shield is that a layer-2 device filters DHCPv6 messages meant to DHCPv6 clients (henceforth "DHCPv6-server messages"), according to a number of different criteria. The most basic filtering criterion is that DHCPv6-server 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-server messages are to be 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-server messages only if they are received on layer-2 ports that have been explicitly configured for such purpose.

[2.](#) Requirements Language

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](#)].

3. Terminology

For the purposes of this document, the terms Extension Header, Header Chain, First Fragment, and Upper-layer Header are used as follows [[I-D.ietf-6man-oversized-header-chain](#)]:

Extension Header:

Extension Headers are defined in [Section 4 of \[RFC2460\]](#). As a result of [[I-D.ietf-6man-ext-transmit](#)], [[IANA-PROTO](#)] provides a list of assigned Internet Protocol Numbers and designates which of those protocol numbers also represent extension headers.

First Fragment:

An IPv6 fragment with fragment offset equal to 0.

IPv6 Header Chain:

The header chain contains an initial IPv6 header, zero or more IPv6 extension headers, and optionally, a single upper-layer header. If an upper-layer header is present, it terminates the header chain; otherwise the "No Next Header" value (Next Header = 59) terminates it.

The first member of the header chain is always an IPv6 header. For a subsequent header to qualify as a member of the header chain, it must be referenced by the "Next Header" field of the previous member of the header chain. However, if a second IPv6 header appears in the header chain, as is the case when IPv6 is tunneled over IPv6, the second IPv6 header is considered to be an upper-layer header and terminates the header chain. Likewise, if an Encapsulating Security Payload (ESP) header appears in the header chain it is considered to be an upper-layer header and it terminates the header chain.

Upper-layer Header:

In the general case, the upper-layer header is the first member of the header chain that is neither an IPv6 header nor an IPv6 extension header. However, if either an ESP header, or a second IPv6 header occur in the header chain, they are considered to be upper layer headers and they terminate the header chain.

Neither the upper-layer payload, nor any protocol data following the upper-layer payload, is considered to be part of the header chain. In a simple example, if the upper-layer header is a TCP header, the TCP payload is not part of the header chain. In a more complex example, if the upper-layer header is an ESP header, neither the payload data, nor any of the fields that follow the payload data in the ESP header are part of the header chain.

4. DHCPv6-Shield Configuration

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

5. DHCPv6-Shield Implementation Advice

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

1. DHCPv6-Shield MUST parse the IPv6 entire header chain present in the packet, to identify whether it is a DHCPv6 packet meant for a DHCPv6 client (i.e., a DHCPv6-server message).

RATIONALE: [[RFC6564](#)] specifies a uniform format for IPv6 Extension Headers, thus meaning that an IPv6 node can parse an IPv6 header chain even if it contains Extension Headers that are not currently supported by that node. Additionally, [[I-D.ietf-6man-oversized-header-chain](#)] requires that if a packet is fragmented, the first fragment contains the entire IPv6 header chain.

DHCPv6-Shield implementations MUST NOT enforce a limit on the number of bytes they can inspect (starting from the beginning of the IPv6 packet), since this could introduce false-positives: legitimate packets could be dropped simply because the DHCPv6-Shield device does not parse the entire IPv6 header chain present in the packet. An implementation that has such an implementation-specific limit MUST NOT claim compliance with this specification, and MUST pass the packet when such implementation-specific limit is reached.

2. When parsing the IPv6 header chain, if the packet is a first-fragment (i.e., a packet containing a Fragment Header with the Fragment Offset set to 0) and it fails to contain the entire IPv6 header chain (i.e., all the headers starting from the IPv6 header

up to, and including, the upper-layer header), DHCPv6-Shield MUST drop the packet, and SHOULD log the packet drop event in an implementation-specific manner as a security fault.

RATIONALE: [[I-D.ietf-6man-oversized-header-chain](#)] specifies that the first-fragment (i.e., the fragment with the Fragment Offset set to 0) MUST contain the entire IPv6 header chain, and allows intermediate systems such as routers to drop those packets that fail to comply with this requirement.

NOTE: This rule should only be applied to 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 they are part of a DHCPv6 packet meant for a DHCPv6 client received on a port where such packets are not allowed).

3. When parsing the IPv6 header chain, if the packet is identified to be a DHCPv6 packet meant for a DHCPv6 client, DHCPv6-Shield MUST drop the packet, and SHOULD log the packet drop event in an implementation-specific manner as a security fault.
4. In all other cases, DHCPv6-Shield MUST 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 encapsulates a DHCPv6 message, it is up to the receiving host what to do with such packet.

If a packet is dropped due to this filtering policy, then the packet drop event SHOULD be logged in an implementation-specific manner as a security fault. The logging mechanism SHOULD include a drop counter dedicated to DHCPv6-Shield packet drops.

In order to protect current end-node IPv6 implementations, Rule #2 has been defined as a default rule to drop packets that cannot be positively identified as not being DHCPv6-server packets (because the packet is a fragment that fails to include 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-server) packets. However, as noted in [\[I-D.ietf-6man-oversized-header-chain\]](#), IPv6 packets that fail to include the entire IPv6 header chain are virtually impossible to police with state-less filters and firewalls, and hence are unlikely to survive in real networks. [\[I-D.ietf-6man-oversized-header-chain\]](#) requires that hosts employing fragmentation include the entire IPv6 header chain in the first fragment (the fragment with the Fragment Offset set to 0), thus eliminating the aforementioned false positives.

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 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 [\[RFC5722\]](#).

6. IANA Considerations

This document has no actions for IANA.

7. 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.

As noted in [Section 5](#), 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 packet 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.

8. Acknowledgements

The authors would like to thank (in alphabetical order) Jean-Michel Combes, Juergen Schoenwaelder, and Mark Smith, for providing valuable comments on earlier versions of this document.

[Section 3](#) of this document was borrowed from [[I-D.ietf-6man-oversized-header-chain](#)], authored by Fernando Gont, Vishwas Manral, and Ron Bonica.

This document is heavily based on the document [[I-D.ietf-v6ops-ra-guard-implementation](#)] authored by Fernando Gont. Thus, the authors 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.

9. References

9.1. 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.
- [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.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [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.

[I-D.ietf-6man-ext-transmit]
Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", [draft-ietf-6man-ext-transmit-05](#) (work in progress), October 2013.

9.2. 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.ietf-6man-oversized-header-chain]
Gont, F., Manral, V., and R. Bonica, "Implications of Oversized IPv6 Header Chains", [draft-ietf-6man-oversized-header-chain-08](#) (work in progress), October 2013.

[I-D.ietf-v6ops-ra-guard-implementation]
Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", [draft-ietf-v6ops-ra-guard-implementation-07](#) (work in progress), November 2012.

[IANA-PROTO]
Internet Assigned Numbers Authority, "Protocol Numbers", February 2013, <<http://www.iana.org/assignments/protocol-numbers/protocol-numbers.txt>>.

[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).

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>

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

Email: liushucheng@huawei.com

Gunter Van de Velde
Cisco Systems
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 2704 5473
Email: gunter@cisco.com

