Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 5, 2014

W. Liu
Huawei Technologies
F. Gont
SI6 Networks / UTN-FRH
T. Tsou
Huawei Technologies (USA)
January 1, 2014

DS-lite security
draft-liu-opsec-ds-lite-security-00

Abstract

More and more operators have deployed or are about to deploy IPv6 transition technologies such as DS-lite, MAP, LAFT6, etc. The fundamental elements of these technologies are Network Address Translation (NAT) and Tunneling. The elements of these transition technologies may be subject to a number of attacks, unless appropriate mitigations are in place. This memo discusses the security implications of the aforementioned points, and additionally, provides a number of operational mitigations that could be deployed against these attacks.

Table of Contents

1. Introduction

Due to the world-wide IPv4 address exhaustion, more and more operators have deployed or are about to deploy IPv6 transition technologies such as DS-lite, MAP, LAFT6, etc. The fundamental elements of these technologies are Network Address Translation (NAT) and Tunneling. The traffic traversing a NAT or Tunneling function may be under attack due to the lack of protection on the node where the NAT or/and Tunneling is placed. In addition, the node conducting the function of NAT or/and Tunneling may also be the victim of DDOS attack. This memo discusses the security implications of the aforementioned points, and additionally, provides a number of operational mitigations that could be deployed against these attacks.

Dual-Stack Lite (DS-Lite) technology, which enables a broadband service provider to share IPv4 addresses among customers by combining two well-known technologies: IP in IP (IPv4- in-IPv6) and Network Address Translation (NAT), was proposed aiming at better aligning the costs and benefits of deploying IPv6 in service provider networks. [RFC6333] A typical DS-Lite deployment is shown in the figure below. the Dual-Stack Lite model is built on to cross the network to reach a carrier-grade IPv4-IPv4 NAT (the AFTR), where customers will share IPv4 addresses. A IPv4-in-IPv6 tunnel(DS-Lite Tunnel) is built from Bridging BroadBand (B4) element crossing the network to reach a DS-Lite Address Family Transition Router (AFTR) element, where a carrier-grade IPv4-IPv4 NAT is implemented. In such an end to end DS-Lite deployment, there are several points that are vulnerable and will be discussed in the rest of this document.

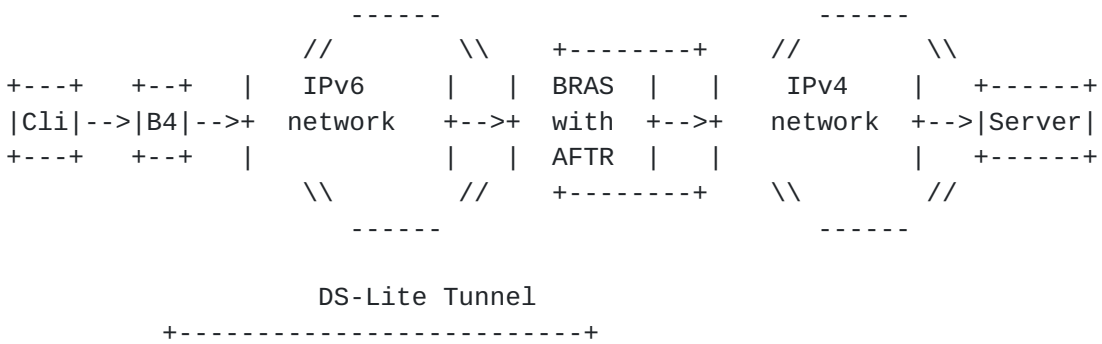

Figure 1: DS-Lite deployment

2. Terminology

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].

3. DHCPv6-based attacks

In DS-Lite, DHCPv6 [RFC3115] is used to assign address for CPE, so DHCPv6 can be exploited as an attack vector. The following aspects should be considered:

1. Authentication between client and server.

   a) Rogue/malicious DHCP server: A rogue server may allocate fake IP address to the client requesting address and causes the client unable to communicate. This has been well discussed in draft-ietf-opsec-dhcpv6-shield.

   b) Rogue/malicious client: A rogue client may make DoS attacks by following two ways:

      i)Using up all the resources of DHCP server. A client may unremittingly send forged DHCP requests to DHCP server to use up the resources of DHCP server.

      ii)Dos attack other client by forging its IP address. A malicious client may unremittingly send forged DHCP requests to cause it unable to communicate.

We note that these attacks are not different than in the typical home network case where a DHCPv6 server is employed.

4. IPv6 fragmentation

Since the encapsulation of IPv4 traffic in IPv6 may rely on the use of IPv6 fragmentation, DS-lite may be subject to fragmentation-based attacks.

Operational mitigation: Limit resources used by per client and/or globally.

5. Attacks against the AFTR/CPE //neet to reorganize the arch

1. Forge tunnel source addresses of CPE(B4). An attacker may forge many IPv6 addresses as DS-lite tunnel source addresses and create many tunnels, and/or entries in the NAT state table with AFTR, causing a DoS attack to the CGN(AFTR).

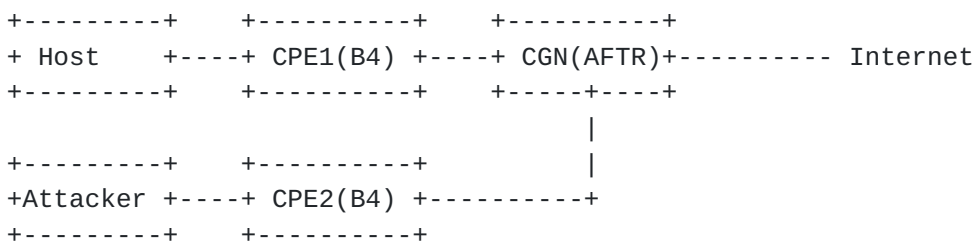

Figure 2: Forge tunnel source addresses of CPE(B4)

As shown in Figure 2, the attacker can cause a DoS attack to the CGN(AFTR) by creating tunnels on CPE2(B4), and/or entries in the NAT state table with the CGN(AFTR).

2. Forge CPE's address. One or many hackers may forge IPv6 addresses of CPEs of other users and send lots of packets to CGN(AFTR). After receiving too many such packets, the CNG(AFTR) may deny the further request from those victim CPEs whose addresses are forged.

Take Figure 2 as an example, Attacker may make CPE2(B4) to forge the address of CPE1 and start an attack. With too many packets from with the v6 address of CPE1 received, the CGN might deny the service of CPE1.

3. Session attack. An attacker may create many sessions at the same time within one tunnel. This may cause a DoS attack that other user can hardly create sessions due to resource excessive occupancy.

4. Big header attack. An attacker forges DS-lite packet with multiple Next Headers in IP header to cause an excessive occupancy of the CPU resource.

Operational mitigation: Limit on the number of sessions per client and globally. Limit on the rate of building sessions to avoid the memory being used up. Limit on the number of next headers of packet to avoid the CPU resource being used up.

6. Attacks based on encapsulation/decapsulation

Not sure about this one. Could you please write more about this? Thanks.

e.g. Can clients leverage DS-LITE to spoof the sure address? [fgont] Yes Can clients diretly acess themselves with DS-list (to avoid being monitored)? [fgont] This would be another possible one. [fgont] You might find this reference useful: RFC 6169

7. Security Considerations

N/A.

8. Acknowledgements

N/A.

9. 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.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

Authors' Addresses

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

Email: liushucheng@huawei.com

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

Tina Tsou
Huawei Technologies (USA)
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4424
Email: tina.tsou.zouting@huawei.com