Network Working Group L. Xue
Internet-Draft B. Sarikaya
Intended status: Informational Huawei
Expires: October 23, 2014 April 21, 2014

Host Identification Problem in Service Function Chaining Use Cases
draft-xue-sfc-address-sharing-in-sfc-use-cases-00.txt

Abstract

The purpose of this document is to present host identification problem due to the address and prefix sharing in service function chaining. So far we have identified this problem in the two use cases of the parental control service and offloading service but it is likely that more use cases can be identified.

Table of Contents

1. Introduction

The use cases described in this document belong to service function chaining (SFC) area [I-D.liu-sfc-use-cases], [I-D.haeffner-sfc-use-case-mobility]. Service functions like Parental Control, Traffic Offloader, Web Proxy, Load Balancer, etc. can be executed in a chained fashion. The order of execution of each function is controlled by an abstract entity called Service Chaining Enforcement Points (SCEP) [I-D.beliveau-sfc-architecture]. Each service function is directly connected to an SCEP.

Traffic policy control, such as Parental Control Function and Traffic Offloader are commonly used by operators to enable flexible service to the customers. The architecture we assume is shown in Figure 1. It is a typical home network architecture.

Address sharing/host identification issue comes up if the residential gateway (RG) is a NAT box in IPv4 or a single prefix is assigned to the RG in DHCPv6-Prefix Delegation in IPv6 [I-D.boucadair-intarea-host-identifier-scenarios]. Multiple hosts are sharing the same public IPv4 address or single IPv6 prefix.

Some earlier solution approaches to the host identification problem are analysed in [RFC6967]. It is not clear if those approaches can also be used in the service function chaining use cases.

2. Conventions and 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 RFC 2119 [RFC2119].

3. Service Function Execution

We assume a service function chaining architecture similar to [I-D.beliveau-sfc-architecture]. In its simplified form, possibly suitable in home networks, the service chain enforcement point is also the ingress router or edge router, e.g. Broadband Network Gateway. In this case parental control function and all other functions are directly connected to SCEP. There is an egress router that routes traffic to the edge router, see Figure 1.

Parental control service function is needed to filter the traffic from the Internet for certain content. Home users connect to the Internet after getting their address from RG. In case of NAT at the RG, all outgoing traffic carries the same address for all users, i.e. RG address for its WAN interface. In case RG is assigned a single prefix, all outgoing IPv6 packets contain the same prefix.

Encrypted web traffic (https) represents a very significant part of Web traffic and is likely to become the main or even the only method to carry Web data over the Internet. Service functions MUST be able to decrypt such encrypted traffic, e.g. using Secure Socket Layer (SSL). In case of address sharing/host identification, being able to decrypt encrypted data becomes a requirement in order to be able to access the URL and user information to filter.

With data services rapidly increasing, the traditional cellular network becomes the bottleneck in providing mobile services mainly because of the increasing bandwidth demand. Operators are trying to offload the data traffic from the mobile subscribers to the broadband network. Traffic offloader service function is needed in the broadband access network for this purpose.

One common broadband access network for offload is home network. Traffic offloader service function decides on each flow/service coming from the hosts at home if they should be routed to the broadband network, i.e. offloaded or they should be sent to the packet data network gateway fo the mobile network.

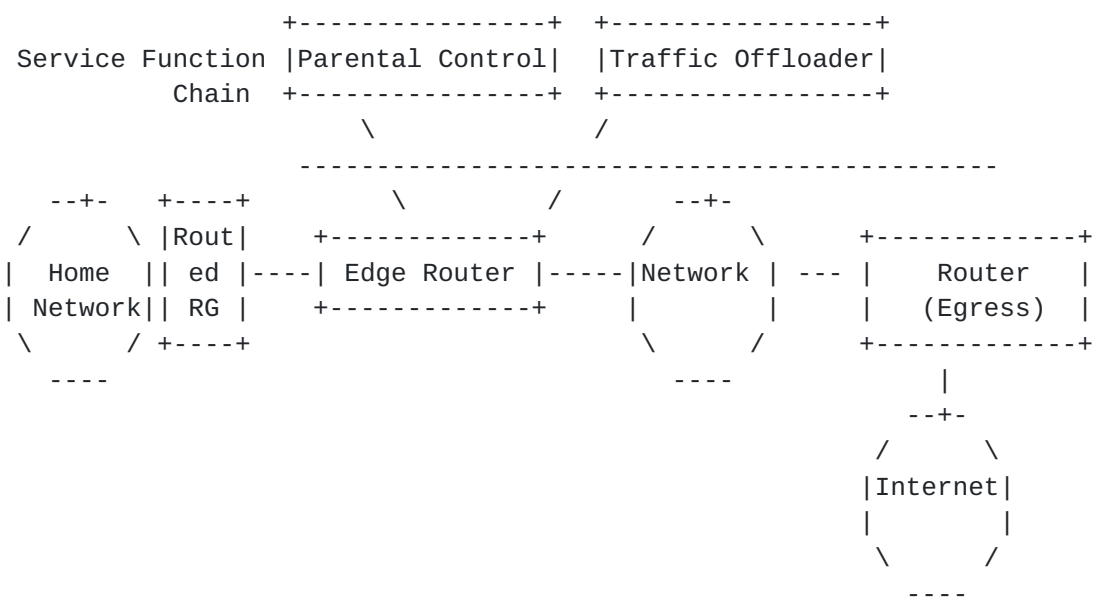

Figure 1: Service Chaining in Home Network

4. Issue Description

4.1. Parental Control Use Case

Parental control service function searches each packet for certain content, e.g. certain URL like www.thisbizarresite.com. Parental control function should keep this information (URL and source IP address) in its cache so that all subsequent packets can be filtered for certain users from the Web server. Parental control service should send the packet back to SCEP to be forwarded to the home network.

Parental control function receives next packet from the recorded URL. Now it needs to decide to filter it or not. Filtering for specific host should depend on the source address, i.e. the address of the host that is being subject to the parental control in IPv4 or the prefix of the host that is being subject to the parental control in IPv6. In case of NAT'ed RG, all incoming packets from one RG contain the same address, i.e. WAN interface address of RG. In case of IPv6, all incoming packets contain the same prefix.

In order to do the parental control on the incoming traffic, parental control service function needs to identify each host. A typical host identity is its IP address in broadband network. In Figure 1, RG knows identifiers of each host in the home network. Edge router needs to identify the host so that it can inform the service functions and set the proper service chain.

Edge router MUST set host identifier state in the service functions that need it, e.g. parental control. Parental control function MUST be able to identify incoming traffic to be filtered, e.g. specific URL information. All other traffic is not subject to filtering. Parental control function filters all traffic coming from indicated URL only for the specific hosts identified by the service control enforcement point.

4.2. Traffic Offload Use Case

Traffic offloader service function works on each flow/service and decides if it should be offloaded to the broadband network or sent back to the mobile network. In this scenario, the broadband network MUST obtain the subscriber subscription from the mobile network and decide if the traffic coming from this subscriber needs to be offloaded or not. If offloading is needed, This usually means that the source address of the subscriber needs to be known on edge router. In case of NAT'ed RG, all the hosts information lost, this introduces a major challenge on how to obtain host identification to decide to offload the traffic or not.

5. IANA Considerations

This document makes no request to IANA.

6. Security Considerations

Any security considerations arising from Service Function Chaining use cases are TBD.

7. Acknowledgements

TBD.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[TS29.212]
"3GPP TS29.212, Policy and Charging Control (PCC) over Gx/Sd reference point", December 2011.

8.2. Informative References

[I-D.beliveau-sfc-architecture]
Beliveau, A., "Service Function Chaining Architecture", draft-beliveau-sfc-architecture-00 (work in progress), October 2013.

[I-D.boucadair-intarea-host-identifier-scenarios]
Boucadair, M., Binet, D., Durel, S., Chatras, B., Reddy, T., Williams, B., Sarikaya, B., and L. Xue, "Host Identification: Use Cases", draft-boucadair-intarea-host-identifier-scenarios-05 (work in progress), April 2014.

[I-D.haeffner-sfc-use-case-mobility]
Haeffner, W., Napper, J., Stiemerling, M., and D. Lopez, "Service Function Chaining Use Cases in Mobile Networks", draft-haeffner-sfc-use-case-mobility-01 (work in progress), February 2014.

[I-D.liu-sfc-use-cases]
Will, W., Li, H., Huang, O., Boucadair, M., Leymann, N., Cao, Z., Qiong, Q., and C. Pham, "Service Function Chaining (SFC) Use Cases", draft-liu-sfc-use-cases-05 (work in progress), April 2014.

[RFC6967] Boucadair, M., Touch, J., Levis, P., and R. Penno, "Analysis of Potential Solutions for Revealing a Host Identifier (HOST_ID) in Shared Address Deployments", RFC 6967, June 2013.

Authors' Addresses

Li Xue
Huawei
NO.156 Beiqing Rd. Z-park, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan,
Beijing, HaiDian District 100095
China

Email: xueli@huawei.com

Behcet Sarikaya
Huawei
5340 Legacy Dr.
Plano, TX 75024

Email: sarikaya@ieee.org