IPv6 Operations
Internet-Draft
Intended status: Informational
Expires: January 16, 2014

M. Gysi
G. Leclanche
Swisscom
E. Vyncke, Ed.
Cisco Systems
R. Anfinsen
Altibox

July 15, 2013

Balanced Security for IPv6 CPE
draft-v6ops-vyncke-balanced-ipv6-security-01.txt

Abstract

This document describes how an IPv6 residential Customer Premise Equipment (CPE) can have a balanced security policy that allows for a mostly end-to-end connectivity while keeping the major threats outside of the home. It is based on an actual IPv6 deployment by Swisscom and proposes to allow all packets inbound/outbound EXCEPT for some layer-4 ports where attacks and vulnerabilities (such as weak passwords) are well-known.

Table of Contents

1. Introduction

Internet access in residential IPv4 deployments generally consist of a single IPv4 address provided by the service provider for each home. Residential CPE then translates the single address into multiple private IPv4 addresses allowing more than one device in the home, but at the cost of losing end-to-end reachability. IPv6 allows all devices to have a unique, global, IP address, restoring end-to-end reachability directly between any device. Such reachability is very powerful for ubiquitous global connectivity, and is often heralded as one of the significant advantages to IPv6 over IPv4. Despite this, concern about exposure to inbound packets from the IPv6 Internet (which would otherwise be dropped by the address translation function if they had been sent from the IPv4 Internet) remain. This document describes firewall functionality for an IPv6 CPE which departs from the "simple security" model described in [RFC6092] . The intention is to provide an example of a security model which allows most traffic, including incoming unsolicited packets and connections, to traverse the CPE unless the CPE identifies the traffic as potentially harmful based on a set of rules. This model has been deployed successfully in Switzerland by Swisscom without any known security incident.

This document is applicable to off-the-shelves CPE as well to managed Service Provider CPE or for mobile Service Providers (where it can be centrally implemented).

2. Threats

For a typical residential network connected to the Internet over a broadband connection, the threats can be classified into:

- o denial of service by packet flooding: overwhelming either the access bandwidth or the bandwidth of a slower link in the residential network (like a slow home automation network) or the CPU power of a slow IPv6 host (like networked thermostat or any other sensor type nodes);

- o denial of service by Neighbor Discovery cache exhaustion [RFC6583]: the outside attacker floods the inside prefix(es) with packets with a random destination address forcing the CPE to exhaust its memory and its CPU in useless Neighbor Solicitations;

- o denial of service by service requests: like sending print jobs from the Internet to an ink jet printer until the ink cartridge is empty or like filing some file server with junk data;

- o unauthorized use of services: like accessing a webcam or a file server which are open to anonymous access within the residential network but should not be accessed from outside of the home network or accessing to remote desktop or SSH with weak password protection;

- o exploiting a vulnerability in the host in order to get access to data or to execute some arbitrary code in the attacked host such as several against old versions of Windows;

- o trojanized host (belonging to a Botnet) can communicate via a covert channel to its master and launch attacks to Internet targets.

3. Overview

The basic goal is to provide a pre-defined security policy which aims to block known harmful traffic and allow the rest, restoring as much of end-to-end communication as possible. This pre-defined policy can be centrally updated and could also be a member of a security policy menu for the subscriber.

3.1. Rules for Balanced Security Policy

These are an example set of generic rules to be applied. Each would normally be configurable, either by the user directly or on behalf of the user by a subscription service.

If we name all nodes on the residential side of the CPE as 'inside' and all nodes on the Internet as 'outside', and any packet sent from

outside to inside as being 'inbound' and 'outbound' in the other direction, then the behavior of the CPE is described by a small set or rules:

1. Rule RejectBogon: apply ingress filtering in both directions per [RFC3704] and [RFC2827] for example with unicast reverse path forwarding (uRPF) checks (anti-spoofing) for all inbound and outbound traffic (implicitly blocking link-local and ULA in the same shot), this is basically the Section 2.1 Basic Sanitation and Section 3.1 Stateless Filters of [RFC6092];

2. Rule ProtectWeakServices: drop all inbound and outbound packets whose layer-4 destination is part of a limited set (see Section 3.2), the intent is to protect against the most common unauthorized access and avoid propagation of worms (even if the latter is questionable in IPv6); an advanced residential user should be able to modify this pre-defined list;

3. Rule Openess: allow all unsolicited inbound packets with rate limiting the initial packet of a new connection (such as TCP SYN, SCTP INIT or DCCP-request not applicable to UDP) to provide very basic protection against SYN port and address scanning attacks. All transport protocols and all non-deprecated extension headers are accepted. This a the major deviation from REC-11, REC-17 and REC-33 of [RFC6092].

4. All requirements of [RFC6092] except REC-11, REC-18 and REC-33 must be supported.

3.2. Rules example for Layer-4 Protection as Used by Swisscom

The rule ProtectWeakService can be implemented by using the following suggestions as implemented by Swisscom in 2013:

Transport	Port	Description
tcp	22	Secure Shell (SSH)
tcp	23	Telnet
tcp	80	HTTP
tcp	3389	Microsoft Remote Desktop Protocol
tcp	5900	VNC remote desktop protocol

Table 1: Drop Inbound

Transport	Port	Description

tcp-udp	88	Kerberos
tcp	111	SUN Remote Procedure Call
tcp	135	MS Remote Procedure Call
tcp	139	NetBIOS Session Service
tcp	445	Microsoft SMB Domain Server
tcp	513	Remote Login
tcp	514	Remote Shell
tcp	548	Apple Filing Protocol over TCP
tcp	631	Internet Printing Protocol
udp	1900	Simple Service Discovery Protocol
tcp	2869	Simple Service Discovery Protocol
udp	3702	Web Services Dynamic Discovery
udp	5353	Multicast DNS
udp	5355	Link-Lcl Mcast Name Resolution

Table 2: Drop Inbound and Outbound

This list should evolve with the time as new protocols and new threats appear, [DSHIELD] is used by Swisscom to keep those filters up to date. Another source of information could be the appendix A of [TR124]. The above proposal does not block GRE tunnels ([RFC2473]) so this is a deviation from [RFC6092].

Note: the authors believe that with this set the usual residential subscriber, the proverbial grand-ma, is protected. Of course, technical susbcribers should be able to open other applications (identified by their TCP or UDP ports) through their CPE through some kind of user interface or even select a completely different security policy such as the open or 'closed' policies defined by [RFC6092].

4. IANA Considerations

There are no extra IANA consideration for this document.

5. Security Considerations

The authors of the documents believe and the Swisscom deployment shows that the following attack are mostly stopped:

o Unauthorized access because vulnerable ports are blocked

This proposal cannot help with the following attacks:

o Flooding of the CPE access link;

o Malware which is fetched by inside hosts on a hostile web site (which is in 2012 the majority of infection sources).

6. Acknowledgements

The authors would like to thank several people who initiated the discussion on the ipv6-ops@lists.cluenet.de mailing list, notably: Tore Anderson, Lorenzo Colitti, Merike Kaeo, Simon Leinen, Eduard Metz, Martin Millnert, Benedikt Stockebrand.

7. Informative References

[DSHIELD] DShield, "Port report: DShield", , <https://secure.dshield.org/portreport.html?sort=records>.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC6092] Woodyatt, J., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, January 2011.

[RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, March 2012.

[TR124] Broadband Forum, "Functional Requirements for Broadband Residential Gateway Devices", December 2006, <http://www.broadband-forum.org/technical/download/TR-124.pdf>.

Authors' Addresses

Martin Gysi
Swisscom
Switzerland

Email: Martin.Gysi@swisscom.com

Guillaume Leclanche
Swisscom
Switzerland

Email: Guillaume.Leclanche@swisscom.com

Eric Vyncke (editor)
Cisco Systems
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 2 778 4677
Email: evyncke@cisco.com

Ragnar Anfinsen
Altibox
Norway

Email: Ragnar.Anfinsen@altibox.no