

Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 20, 2016

S. Tsuchiya, Ed.
Cisco Systems
October 18, 2015

Benchmarking for CoPP
draft-shishio-bmwg-copp-00

Abstract

Control Plane Policing (CoPP) which is defined as RFC6192 to protect router's control plane from undesired or malicious traffic.

This document provides methodology to confirm implementation of CoPP.

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 This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.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 April 20, 2016.

Copyright Notice

Copyright (c) 2015 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	3
2. Test setup	3
2.1. Topology	3
2.2. Network	4
3. Test procedure	4
3.1. Attack Packet	4
3.1.1. Typical	4
3.1.2. Routing Protocol from trust network1	4
3.1.3. Routing Protocol from untrust network1	4
3.1.4. Control Packet from trust network	4
3.1.5. Control Packet from un-trust network	4
3.1.6. Management Packet from trust network	5
3.1.7. Management Packet from un-trust network	5
3.1.8. undefined packets	5
4. Test Result	5
5. Acknowledgements	5
6. IANA Considerations	5
7. Security Considerations	6
8. References	6
8.1. Normative References	6
8.2. Informative References	6
Author's Address	6

1. Introduction

Control Plane Policing (CoPP) which is defined as RFC6192 to protect router's control plane from undesired or malicious traffic. Some modern router implemented this RFC6192 mechanism as the default. Also some router can support RFC6192 by configuration.

Ethernet based service has been widely deployed for both consumer and business. In some case, service provider has to converge customer network directly without CPE. There is ARP/NDP and broadcast/multicast protocol in the segment, therefore service provider becomes carefully for protection of router's control plane.

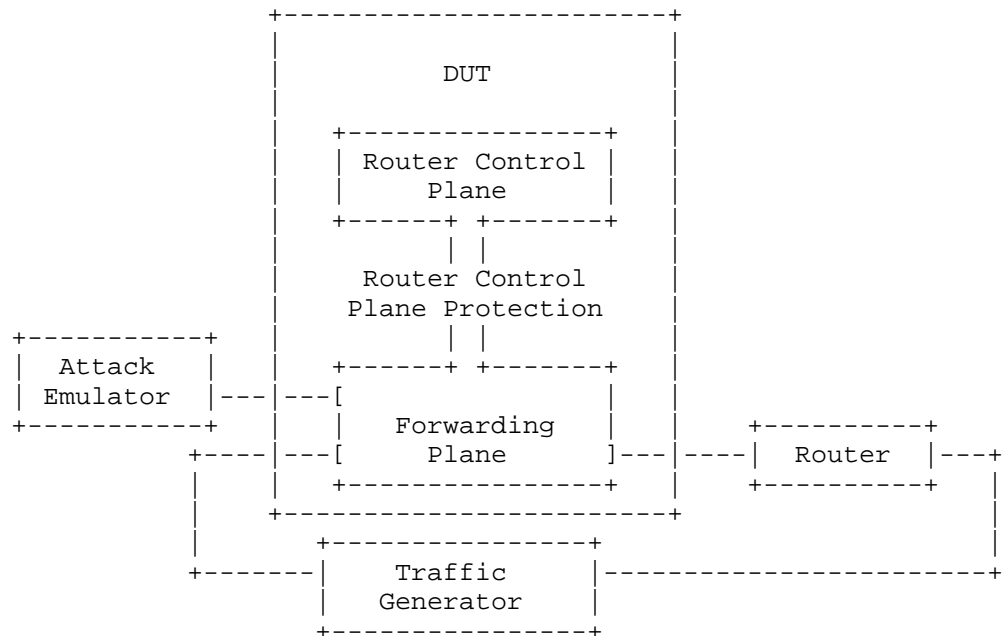
This document provides methodology to confirm implementation of CoPP.

2. Test setup

2.1. Topology

The DUT need to at least 3 interfaces to connect Attack Emulator/Uplink Router/Traffic Generator.

Basic network topology is here



2.2. Network

Configure applicable network parameter on both DUT and uplink router such as IGP/BGP. Send traffic from traffic generator to transit between DUT and Router. If needed configure DUT to protect Control plane. section-3.1 of RFC6192 would be reference.

3. Test procedure

Attack emulator sends packets to DUT to confirm influence of CoPP. section-3.1 of RFC6192 describes example of CoPP. It completely depends on network environment but it can be categorized in the following section.

3.1. Attack Packet

3.1.1. Typical

fragment/ip option/ ICMP ttl exceed

Expect Action: drop/rate-limit

3.1.2. Routing Protocol from trust network1

BGP/OSPF

Expect Action: accept but rate-limit would be preferred

3.1.3. Routing Protocol from untrust network1

BGP/OSPF

Expect Action: drop

3.1.4. Control Packet from trust network

ARP/NDP/ICMP/ICMPv6

Expect Action: accept but rate-limit would be preferred

3.1.5. Control Packet from un-trust network

ARP/NDP/ICMP/ICMPv6

Expect Action: drop

3.1.6. Management Packet from trust network

NTP/SSH/Telnet/Radius/DNS/DHCP

Expect Action: accept/rate-limit

3.1.7. Management Packet from un-trust network

NTP/SSH/Telnet/Radius/DNS/DHCP

Expect Action: drop

3.1.8. undefined packets

IPX/Apple talk

Expect Action: drop

The section will be update more detail(src ip/dst ip and packet type)

Attack duration must be higher than routing protocol hold timer
between DUT and router. Transit packets should be non drop.

4. Test Result

Test Result report needs these information.

Attack	Attack rate[pps/bps]	Attack duration time	Loss of packets on traffic generator
-	-	-	-

5. Acknowledgements

TBD

6. IANA Considerations

No IANA Action is requested at this time.

7. Security Considerations

There is no additional consideration from RFC6192.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

[RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", RFC 6192, DOI 10.17487/RFC6192, March 2011, <<http://www.rfc-editor.org/info/rfc6192>>.

8.2. Informative References

Author's Address

Shishio Tsuchiya (editor)
Cisco Systems
Midtown Tower, 9-7-1, Akasaka
Minato-Ku, Tokyo 107-6227
Japan

Phone: +81 3 6434 6543
Email: shtsuchi@cisco.com

