Abstract

This document specifies the behavior of a PCP Proxy element, for instance embedded in Customer Premise routers.

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 September 8, 2011.

Copyright Notice

Copyright (c) 2011 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. PCP Server Discovery and Provisioning .................... 3
3. Control of the Firewall ................................. 4
4. PCP Proxy Interface .................................... 4
5. PCP Proxy Without NAT in the CP Router ................. 4
6. PCP Proxy With NAT Embedded in the CP Router .......... 4
   6.1. Change of the WAN IP Address ..................... 5
7. Simple PCP Proxy ........................................ 5
   7.1. Simple PCP Proxy Behaviour ....................... 5
   7.2. Unsupported PCP Options ........................... 6
   7.3. Unsupported PCP OpCodes ......................... 6
   7.4. PCP Message Truncation ............................ 7
   7.5. Secure Transport Mode ............................. 7
8. Smart Proxy .............................................. 7
9. IANA Considerations .................................... 7
10. Security Considerations ................................ 7
11. References ............................................. 8
   11.1. Normative References ............................... 8
   11.2. Informative References ............................ 8
Authors’ Addresses .......................................... 8
1. Introduction

PCP [I-D.ietf-pcp-base] discusses the implementation of NAT control features that rely upon Carrier Grade NAT (CGN) devices such as DS-Lite AFTR [I-D.ietf-softwire-dual-stack-lite].

The Customer Premise router, the B4 is DS-Lite, is in charge to enforce some security controls on PCP requests so implements a PCP Proxy function, i.e., it acts as a PCP server receiving PCP requests on internal interfaces, and as a PCP client forwarding accepted PCP requests on an external interface to a CGN PCP server which answers by PCP responses the Proxy sends back to PCP clients on Internal hosts.

The Proxy can be simple, i.e., implement as transparent/minimal processing as possible, or it can be smart, i.e., handle multiple CGN PCP servers, cache requests/responses, etc. A smart Proxy can be associated with UPnP IGD [I-D.bpw-pcp-upnp-igd-interworking] or/and NAT-PMP [I-D.bpw-pcp-nat-pmp-interworking] Interworking Function.

```
+-------------+
| PCP Client  |
|-----+---+---|
|     | PCP Proxy | PCP Server |
|     |-----+---+---|
|     | PCP Client |     |
|-----+---+---+---+
```

Figure 1: Reference Architecture

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].

2. PCP Server Discovery and Provisioning

The PCP Proxy MUST implement one of the discovery methods listed in [I-D.ietf-pcp-base] (e.g., DHCP [I-D.bpw-pcp-dhcp]).

The address of the PCP Proxy is provisioned to local PCP Clients as their default PCP Server: If the PCP DHCP option is supported by an internal PCP Client, it will retrieve from its CP router the IP address to use when issuing its PCP requests (i.e., the address of the PCP Proxy); otherwise internal PCP Clients will assume their
default router being the PCP Server.

The PCP Proxy MUST use 44323 to listen to incoming PCP requests from internal PCP Clients. If a distinct port is used and unless this port is configure by some means, PCP communications will fail.

3. Control of the Firewall

A security policy to accept PCP messages from the provisioned PCP Server are to be enabled on the CP router. This policy can be for instance triggered by DHCP configuration or by outbound PCP requests issued from the PCP Proxy to the provisioned PCP Server.

In order to accept inbound and outbound traffic associated with PCP mappings instantiated in the upstream PCP Server, appropriate security policies are to be configured on the firewall.

4. PCP Proxy Interface

A PCP Proxy should be bound to a LAN interface.

The PCP Proxy SHOULD NOT accept requests coming from the WAN interfaces of the CP router.

5. PCP Proxy Without NAT in the CP Router

When no NAT is embedded in the CP router, the port number included in received PCP messages (from the PCP Server or PCP Client(s)) are not altered by the PCP Proxy.

6. PCP Proxy With NAT Embedded in the CP Router

When the PCP Proxy is co-located with a NAT function in the CP router, it MUST update the content of received mapping messages with the port number belonging to the external interface of the CP router (i.e., after the NAT operation) and not as initially positioned by the PCP Client. For the reverse path, PCP response messages are intercepted by the PCP Proxy to replace the target port number to what has been initially positioned by the PCP Client. A NAT state is required to be maintained by the PCP Proxy (or NAT) for this purpose.

The PCP Proxy MUST update the requested lifetime value of the PCP request to be at least equal to the validity timer of the corresponding NAT binding in the CP router. If the PCP Server.
Because the PCP Server may grant a lifetime smaller or larger than the requested lifetime, the PCP Proxy should update the local state to avoid the NAT binding lifetime be smaller than the one assigned by the terminating PCP Server (as positioned in the assigned-lifetime field).

6.1. Change of the WAN IP Address

When a new IP address is assigned to the WAN interface, the mappings instructed by internal PCP Clients are to be updated in the PCP Server. Two solutions may be considered:
1. If a mapping table is stored locally, the PCP Proxy proceeds to update all the mappings on behalf of the PCP Client. This option is transparent for the PCP Clients.
2. Or an advertisement mechanism is implemented locally to force PCP Client refresh their mappings.

7. Simple PCP Proxy

A simple PCP Proxy performs minimal modifications to PCP requests and responses, in particular it does not change the Epoch value in responses. So it does not handle more than one PCP server.

7.1. Simple PCP Proxy Behaviour

Unless THIRD_PARTY option is present, the Target IP Address is assumed to be equal to the source IP address of a received PCP request.

A PCP Proxy can be configured to accept or to reject PCP requests including THIRD_PARTY option enclosing an IP address distinct than the source IP address of the request.

When third-party mappings are not allowed, the detailed behavior at the reception of a PCP request on an internal interface is as follows:

- apply security controls.
- if the request is rejected, build a fake error response and send it back to the PCP client.
- if the request is accepted, adjust it and forward it on a fresh UDP socket connected to the PCP server. Wait for the response during a reasonable delay. If a NAT is co-located with the PCP Proxy, the Target Port Number MUST be updated as specified in Section 6.
o when the response is received from the PCP server, adjust it back and forward it to the source PCP client. The PCP Proxy MUST enforce request validation rules to check whether a request has been issued to that PCP Server.
o on a hard error on the UDP socket, build a fake ICMP error and send it to the source PCP client.

The reasonable delay minimum value is 20 seconds, request retransmission is handled by PCP clients.

For each pending request, the proxy MUST maintain in a data record:

- the request payload
- the interface where the request was received
- the source IP address of the request
- the source UDP port of the request
- the UDP socket connected to the PCP server
- an expire timeout

Receiving interfaces can be implemented by a set of servicing sockets, each socket bound to an address of an internal interface. Interface, source address and port are used to send back packets to the source PCP client. The request payload is used to generate fake ICMP. Responses are received on the UDP socket.

There is no (not yet) standardized way to build a fake error response, in particular no way to determine which Epoch value to put into it. This is why it is better to build a fake ICMP error than a fake error response with NETWORK_FAILURE on a socket hard error.

### 7.2. Unsupported PCP Options

The simple PCP Proxy MUST ignore any unknown PCP Option received in PCP messages and proxy these PCP messages following the procedure specified above.

### 7.3. Unsupported PCP OpCodes

When the PCP Proxy is not co-located with a NAT, the simple PCP Proxy MUST proceed to the security validation operations when handling received unknown PCP OpCodes.

When the PCP Proxy is co-located with a NAT, unknown PCP OpCode may enclose the target port number. Proxying an Unknown PCP Opcode without updating the content of message may lead to failures. For this reason, a PCP Client behind a NAT to detect the presence of a NAT in the path and to position its target port accordingly.
7.4. PCP Message Truncation

The PCP Proxy MUST NOT truncate PCP messages below the packet size limit specified in [I-D.ietf-pcp-base].

7.5. Secure Transport Mode

A simple PCP Proxy is not supposed to manage PCP communications with different transport modes in each communication side (e.g., DTLS in one side and UDP in the other one).

Simple PCP Proxy is supposed to use UDP in both communication legs as this is the default transport protocol used in [I-D.ietf-pcp-base].

8. Smart Proxy

When a simple PCP Proxy uses as global variables only the CGN PCP server IP address, a set of servicing sockets and a list of pending request handlers, a smart PCP Proxy implements more services.

[To be elaborated further: - multiple PCP servers - Epoch handling [I-D.boucadair-pcp-failure] - request/response caching - retransmission - keeping the full state]

9. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

10. Security Considerations

The security controls are applied on PCP requests and are about:

- authorized target addresses, in particular in case of a third party.
- authorized internal and external ports (note the external port is in general assigned by the CGN PCP server).

Requests for a third party are not allowed by default.

11. References
11.1. Normative References

[I-D.bpw-pcp-dhcp]
Boucadair, M., Penno, R., and D. Wing, "DHCP and DHCPv6 Options for Port Control Protocol (PCP)",
draft-bpw-pcp-dhcp-03 (work in progress), March 2011.

[I-D.ietf-pcp-base]
Wing, D., Cheshire, S., Boucadair, M., Penno, R., and F. Dupont, "Port Control Protocol (PCP)",
draft-ietf-pcp-base-06 (work in progress), February 2011.


11.2. Informative References

[I-D.boucadair-pcp-failure]
draft-boucadair-pcp-failure-00 (work in progress), January 2011.

[I-D.bpw-pcp-nat-pmp-interworking]

[I-D.bpw-pcp-upnp-igd-interworking]
Boucadair, M., Penno, R., Wing, D., and F. Dupont,
"Universal Plug and Play (UPnP) Internet Gateway Device (IGD)-Port Control Protocol (PCP) Interworking Function",
draft-bpw-pcp-upnp-igd-interworking-02 (work in progress), February 2011.

[I-D.ietf-softwire-dual-stack-lite]
Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion",
draft-ietf-softwire-dual-stack-lite-07 (work in progress), March 2011.
Authors’ Addresses

Mohamed Boucadair
France Telecom
Rennes  35000
France

Email: mohamed.boucadair@orange-ftgroup.com

Reinaldo Penno
Juniper Networks
1194 N Mathilda Avenue
Sunnyvale, California  94089
USA

Email: rpenno@juniper.net

Dan Wing
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California  95134
USA

Email: dwing@cisco.com

Francis Dupont
Internet Systems Consortium

Email: fdupont@isc.org