How to use Port Control Protocol in NetScaler?

Introduction

In today's networks NAT device plays an important role providing IPv4 preservation, IPv6 migration and security and thus the chances of packet translation happening in an end to end communication is quite high. In order to have control over these NAT devices, Port Control Protocol was developed(RFC – 6887). Port Control Protocol commonly referred as PCP enables applications and equipment to read/write explicit mappings between an external IP address, protocol and port, and an internal IP address, protocol and port. These explicit mappings allows inbound communication to reach the hosts behind a NAT or firewall.

Why PCP?

With DHCP the internal IP address varies often and thus the external IP address/ port also changes frequently. While hosting a service on a server behind firewall or NAT, this frequently changing external IP address/port posts a challenge. Below are the list of problems faced commonly in a NAT environment.

Problems

- Hosting of web services in private network lead to Dynamic DNS issues(change in NAT IP during reallocation of IP)
- Need to Monitor/Access Home Gateway(HG) devices from outside/office
    1. No control over NAT and Firewall
    2. Have to raise a request to Service provider for Static mapping
- Internet of Things (Rapid growth of HG)
    1. Keep alive messages takes bandwidth consumption
    2. Battery consumption on mobile devices

Solution

PCP comes to rescue here by providing the below mentioned support to overcome the above mentioned problems.

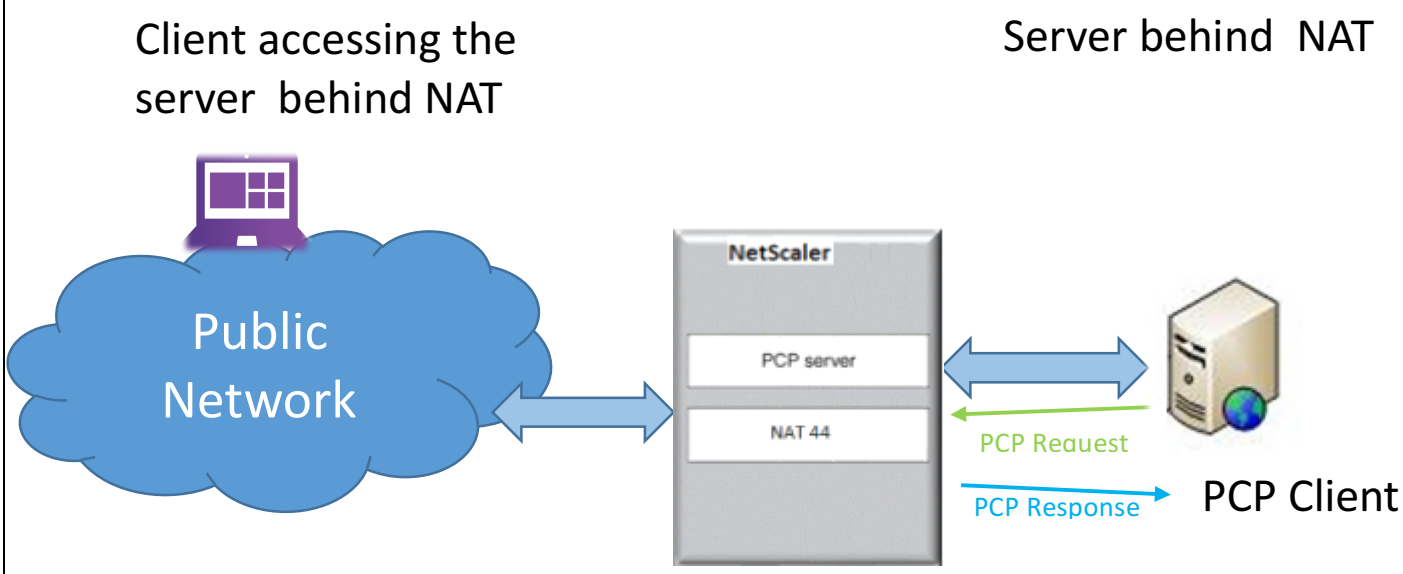
- PCP clients can get updated mappings from NAT device using PCP
- Give controls to applications/devices at HG
    1. Whenever it wants to act as service, it can request its upstream devices

2. Applications decide when the session at upstream devices should terminate

Primary Uses cases for DDNS with PCP

PCP Communication

Port Control Protocol (PCP) keeps device (PCP client) and NAT/CGN server (PCP server) dynamically aware about the change in both internal and external IP address and port number. Netscaler should be able to receive PCP request from any client and provide appropriate response for them.



PCP works in a client server model over UDP and uses various OPCODEs are used for performing PCP operations. In NetScaler PCP server can be used with NAT44, NAT64 and DS-Lite.

To configure PCP on NetScaler,

Using Command Prompt:

```
> add pcp server <pcp_server_name> ip <port>
```

- Creates register service for ip and port with ns_pcp_handler as service handler

```
> add pcp profile <pcp_profile_name>
-announceMulticount <Positive_integer>
-mapping [ENABLED | DISABLED]
-maxMapLife <secs>
```

-minMapLife <secs>

-peer [ENABLED | DISABLED]

-thirdParty[ENABLED | DISABLED]

announceMulticount – the number of to be sent to PCP clients

mapping – knob to enable/disable mapping

maxMapLife , minMapLife – maximum and minimum life time of mapping in secs

peer – knob to enable/disable peer

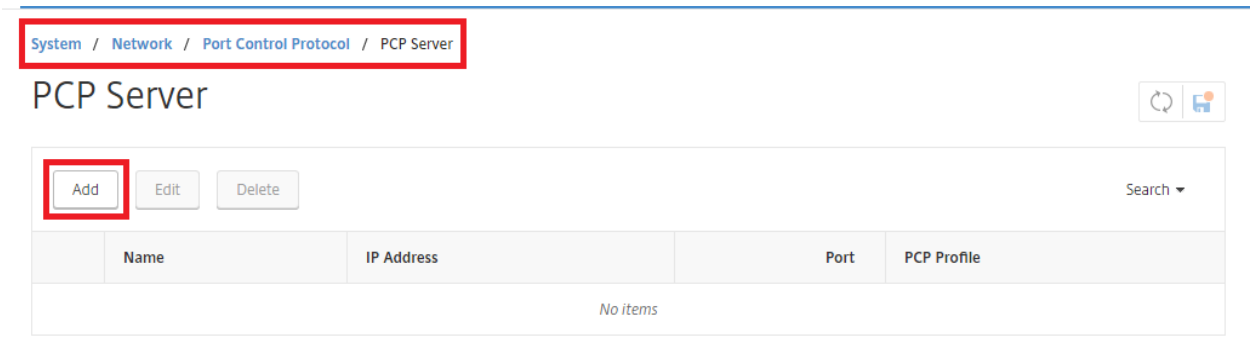
thirdParty – PCP client can send PCP messages on behalf of third party clients

> bind pcp server to LSN groups

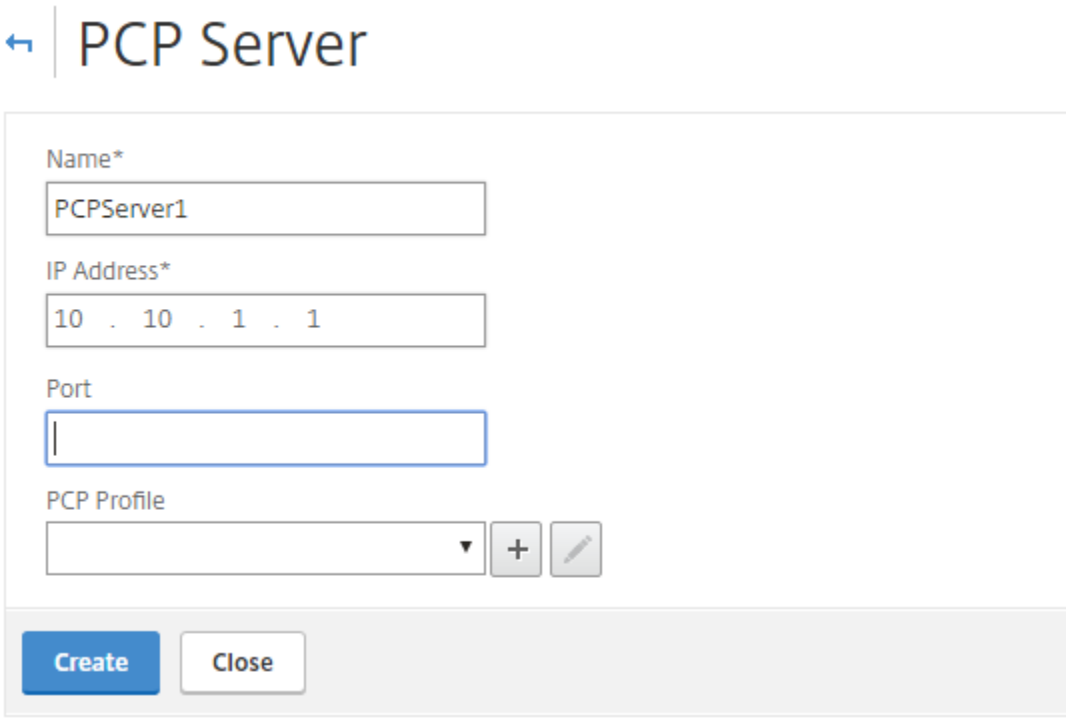
- Whenever we bind PCP server to LSN group it inherits the properties of LSN group.

Using Configuration Utility:

Navigate to System -> Network -> Port Control Protocol

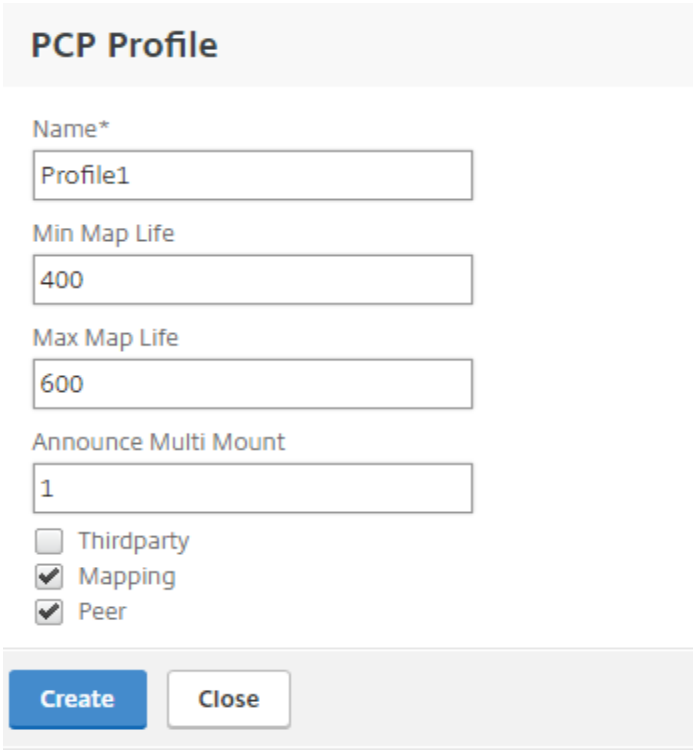


Click “Add” to create a PCP server.



Enter the PCP Server parameters and click “Create”

If there is no PCP Profile added, it can be created as shown by adding PCP paramaters.



This feature is supported only in NetScaler 11.1 release onwards.