Network working group
Internet Draft
Category: Standards Track
Expires: August 28, 2011

D. Cheng
Huawei Technologies

February 28, 2011

RADIUS Extensions for NAT Forwarding Port

draft-cheng-behave-nat-fwd-port-radius-ext-00

Status of this Memo

Copyright Notice

Abstract

This memo proposes two new RADIUS attributes with each to carry an Internal Port number and a Configured External Port number, both are associated with a specific NAT device and a specific user, and are configured on a RADIUS server such that when the user requests an Internet connection, the port mapping information can be conveyed to NAS that co-locates with the NAT device via RADIUS protocol, and is used during the NAT operation for IP flows to and from that user. The two attributes also include an IPv4 address or IPv6 address, respectively, as the pinhole internal IP address at the NAT device.

Table of Contents

1. Introduction

In most of the scenarios, the port mapping on a NAT device is dynamically created when the IP packets of an IP connection initiated by a user arrives. For some applications, the port mapping needs to be pre-defined allowing IP packets of applications from outside a NAT device to pass through and "port forwarded" to the correct user located behind the NAT device.

Port Control Protocol or PCP ([I-D.draft-ietf-pcp-base]), provides a mechanism to create pinholes from an external IP address to an internal IP address and port on a NAT device just to achieve the "port forwarding" purpose. PCP is a server-client protocol capable of creating or deleting a pinhole along with a rich set of features on a NAT device in dynamic fashion. In some deployment, all users need is a few, typically just one pre-configured port mapping for applications such

as web cam at home, and the lifetime of such a port mapping remains valid throughout the duration of the customer's Internet service connection time. In such an environment, it is possible to statically configure a port mapping on the RADIUS server for a user and let the RADIUS protocol to propagate the information to the associated NAT device.

In a broadband network, customer information is usually stored on a RADIUS server and at the time when a user initiates an Internet service request, the RADIUS server will populate the user's configuration information to the NAS, which is usually co-located with the BNG, after the connection request is granted. In many cases, the NAT function is also on the BNG, and therefore the port forwarding information can be configured on the RADIUS server as part of the user profile.

This memo proposes two new RADIUS attributes to carry Internal Port number and Configured External Port number, both are associated with a specific NAT device and a specific user, with an IPv4 address or IPv6 address as the pinhole internal address, respectively, and are configured on a RADIUS server such that when the user requests an Internet connection, the port mapping information can be conveyed to the NAS that co-locates with the NAT device via RADIUS protocol, and is used during the NAT operation for IP flows to and from that user.

2. 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 [RFC2119].

3. Operation

Port mapping information for NAT for a user (e.g., a CPE or host) is configured on a RADIUS server, along with other user information such as credentials. The port mapping information that is to be used during the NAT procedure is going to be populated from the RADIUS server to the NAT device using RADIUS protocol.

In Figure-1, a Network Access Server (NAS), co-located with a NAT device on a BNG, operates as a RADIUS client. The NAT device that resides on the BNG performs a single NAT (or firewall) function such as NAT44, NAT64, etc.

When the user sends a service request, the NAS on the BNG sends a RADIUS Access-Request message to the RADIUS server, requesting

authentication. Once the RADIUS server receives the request, it validates the sending client and if the request is approved, the RADIUS server replies with an Access-Accept message including a list of attribute-value pairs that describe the parameters to be used for this connection, including the port forwarding mapping specifically configured for the user.

When the RADIUS Access-Accept message arrived at the BNG, the port mapping information is used to create a pinhole on the NAT, along with the associated pinhole internal IP address, and also the external IP address, when it becomes available, for the specific user. A service granted message is then sent to the user, and after that point, IP packets from application initiated from network side (e.g., web cam) can be "port forwarded" by the NAT on the BNG to the user that is behind the NAT. IP packets belonging to the same flow but on opposite direction also traverse the same pinhole.

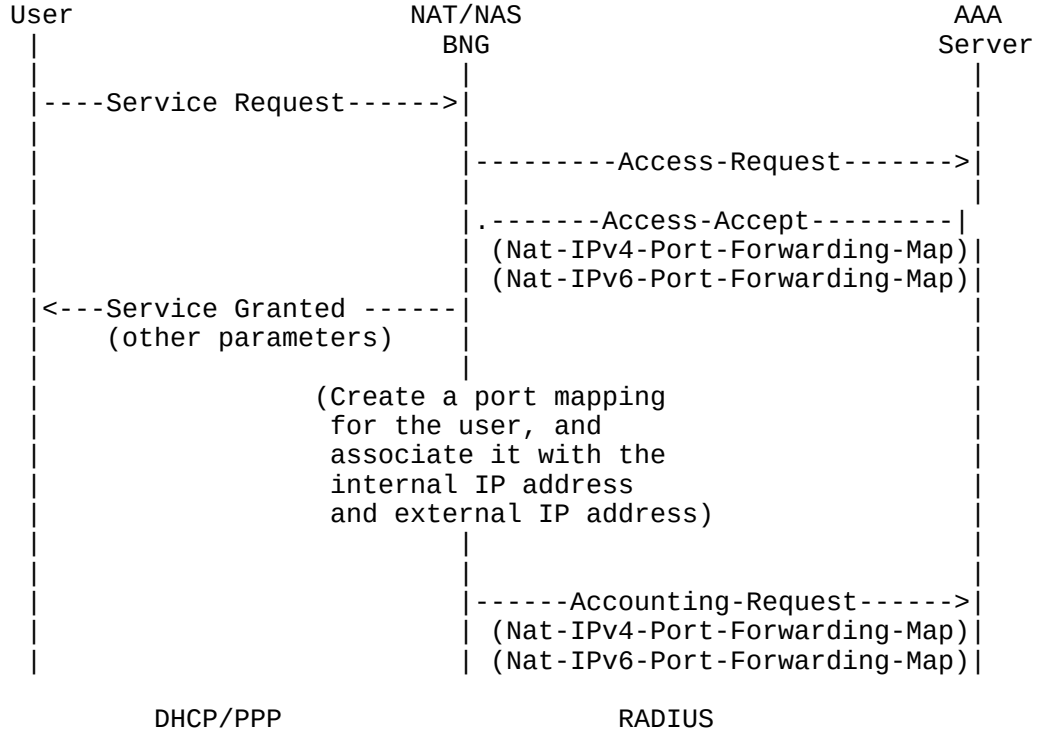

Figure 1: RADIUS Message Flow

When an IP packet travels from behind the NAT outwards (outbound), the NAT must change the source port number, i.e., the internal port to the configured external port, and when an IP packet travels from outside to the inside of the NAT (inbound), the NAT must change the target port number, i.e., the configured external port to the internal port.

Note that the service request that is initiated by a user can be associated with a PPP session or relevant DHCPv4/DHCPv6 message, with the same communication sequence between the RADIUS server and the NAS, and the installation of the port mapping on the NAT. Also, there may be different mechanisms as how an internal IP address and an external IP address (in the context of the NAT) assigned or determined, respectively, on the NAT for a specific user, but the forwarding port mapping information will remain the same as configured on the RADIUS server and is bonded to the specific user with one of its specific IP address.

A port mapping, once created on the NAT, will remain permanently in the duration of the user's Internet connection. When the connection is torn down, the mapping on the NAT must then be removed accordingly.

In the NAT444 scenario, in order to allow an IPv4 packet generated from outside of the BNG reaching the user, a forwarding port mapping is required on the NAT residing on the BNG as described above, but a separate forwarding port mapping is required on the user, typically a CPE, and in addition, the two sets of mapping need to be coordinated, so that an inbound IP packet, i.e., from outside of the BNG destined to the user, will successfully traverse two NATs before arriving at the user. The required mechanism for the NAT444 case is out of the scope of this document.

4. RADIUS Attributes

Two new RADIUS attributes are defined in this document, for IPv4 address and IPv6 address as the NAT pinhole internal address, respectively.

NAT-IPv4-Forwarding-Port-Map Attribute (Figure-2)
NAT-IPv6-Forwarding-Port-Map Attribute (Figure-3)

Description

Both of the two attributes contain a 16-bit Internal Port that identifies the source TCP/UDP port number of an IP packet sent by the user, or the destination port number of an IP packet destined

to the user, and in both cases, the IP packet travels behind the NAT device. Also they contain a 16-bit Configured External Port that identifies the source TCP/UDP port number of an IP packet sent by the user, or the destination port number of an IP packet destined to the user, and in both cases, the IP packet travels outside of the NAT device. In addition, the two attributes contain a 32-bit IPv4 address or 128-bit IPv6 address, respectively, as their respective NAT pinhole's internal IP address. Together, the port pair and IP address determine the port mapping rule for a specific IP flow that traverses a NAT device.

The attribute MAY appear in an Access-Accept packet, and may also appear in an Accounting-Request packet. In either case, the attribute MUST NOT appear more than once in a single packet.

Neither of these attributes MUST NOT appear in any other RADIUS packets.

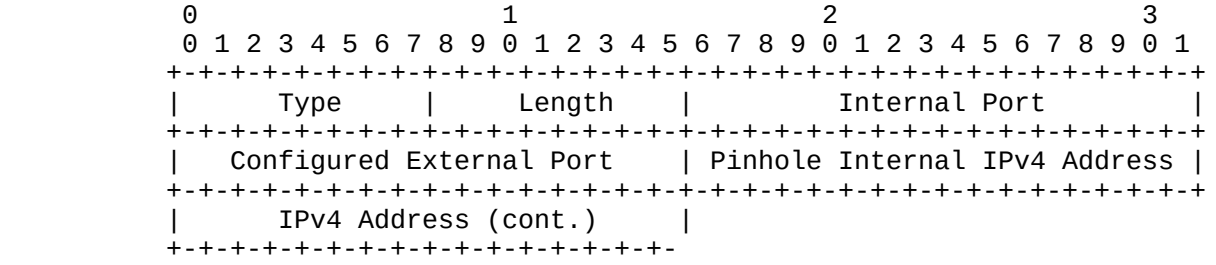

Figure-2 Nat-IPv4-Forwarding-Port-Map Attribute Format

These fields are described below:

Type

Type for NAT-IPv4-Forwarding-Port-Map (value is TBD)

Length

8 octets

Internal Port

Internal port for the pinhole

Configured External Port

External port for the pinhole

Pinhole IPv4 Address

The internal IPv4 address at the pinhole

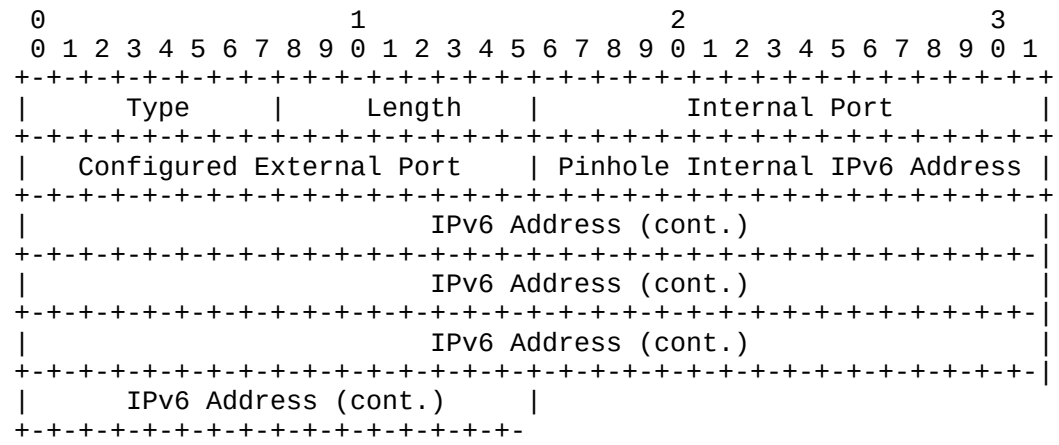

Figure-3 Nat-IPv6-Forwarding-Port-Map Attribute Format

These fields are described below:

Type

Type for NAT-IPv6-Forwarding-Port-Map (value is TBD)

Length

20 octets

Internal Port

Internal port for the pinhole

Configured External Port

External port for the pinhole

Pinhole IPv6 Address

The internal IPv6 address at the pinhole

5. Table of Attributes

The following table provides a guide as the attributes may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	Accounting	#	Attribute
0-1	0-1	0	0	0-1	TBD	NAT-IPv4-Forwarding-Port-Map
0-1	0-1	0	0	0-1	TBD	NAT-IPv6-Forwarding-Port-Map

The meaning of the above table entries is as follows:

0 This attribute MUST NOT be present.

0-1 Zero or one instance of this attribute MAY be present.

6. Security

Security problems of the RADIUS protocol are discussed in [RFC2865].

7. IANA Considerations

This document requires the assignment of new RADIUS attribute numbers for the following attributes:

NAT-IPv4-Forwarding-Port-Map

NAT-IPv6-Forwarding-Port-Map

8. Acknowledgements

Thanks to Dan Wing who provided some useful comments.

9. References

9.1. Normative References

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

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC2865, June 2000.

9.2. Informative References

[I-D.draft-ietf-pcp-base] Wing, D., "Port Control Protocol (PCP), draft-ietf-pcp-base-05, work in progress.

10. Authors' Addresses

Dean Cheng
Huawei Technologies
2330 Central Expressway, CA 95050, USA
Phone:+1 408 330 4754
Email: dean.cheng@huawei.com