EnGenius

Technical Paper

IPV6 NAT Proxy Implementation

George Lin | Senior Software Engineer

ABSTRACT—Due to the unlimited number of IPV6 addresses, IPV6 seems to get rid of NAT. Thus, there is no traditional way to execute NAT operation in IPTABLES like IPV4. In this article, it briefly discusses how to implement a simple IPV6 NAT server to redirect packets to remote server for security check as an application for IPV6 NAT.

I - Introduction

NAT(Network Address Translation) is a method of remapping one IP address into another by modifying the IP header of packets while transmitting across routing devices. In IPV4, different devices in the same subnet can be present as a single device in internet by using NAT technique. As becoming a general and essential way in conserving global address space in the face of IPV4 address exhaustion.

And now, the exhaustion problem seems to be impossible in the numerous number of IPV6 address spaces, NAT technique is still valuable and useful for many IPV6 applications. As mentioning one of them below is for security check in web browsing.

II - IPV6 NAT Proxy

In Linux system, the general way to implement an NAT operation is to use IPTABLES. But it only supports IPV4 until the IPV6 NAT proxy is accomplished by the SENAO network. The IPV6 NAT proxy is a kernel module registered in the netfilter. When user triggers the HTTP request for web browsing, the IPV4 and IPV6 packets will flow into the netfilter and the IPV6 NAT proxy will sniffer the IPV6 packet flow. By filtering out the HTTP IPV6 packet, the IPV6 NAT proxy will transfer the packet to a remote server by remapping the destination IPV6 address to IPV6 address of security server (see figure).

The remapping procedure includes calculating the TCP checksum of IPV6 packets while completing network address translation. IPV6 NAT proxy keeps the TCP connection tuple until the security server returns the checking result. Once the security server return the positive result, the original packet will be sent out without the user noticing. Otherwise, the HTTP connection will be dropped by the IPV6 NAT proxy and the user will be blocked for browsing the fraud.

Beside translating to security server, the IPV6 NAT proxy provides options to set different IPV6 address, IPV6 ports, the live time of the tuple and the maximum number of storing tuples for customization.

III - Conclusion

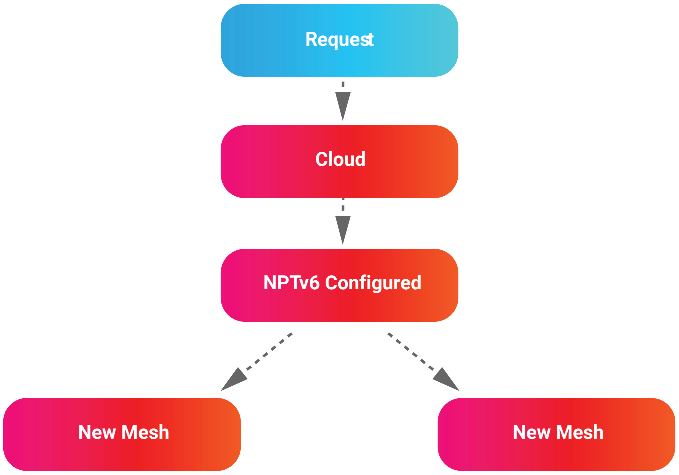
This article describes a simple way to implement an IPV6 NAT server without discussing full-cone NAT, restricted-cone NAT, post-restricted cone NAT and symmetric NAT and invoke the imagination of using NAT in IPV6.

References

1. Network address translation
(https://en.wikipedia.org/wiki/Network_address_translation)

2. Getting the most out of IPV6

(https://blog.paloaltonetworks.com/2015/08/getting-the-most-out-of-ipv6/)



EnGenius Technologies | 1580 Scenic Ave. Costa Mesa, CA 92626

Email: partners@engeniustech.com | Website: engeniustech.com

Version: 1.00 02/2020