

STUN (RFC 3489) Vs. STUN (RFC 5389/5780)

October 21, 2013 | By Netmanias (tech@netmanias.com)

What are the differences between NAT types defined in RFC 3489 and RFC 5780?

To understand the differences to be explained below, you must be familiar with the Mapping Behavior and Filtering Behavior of a NAT that we covered last time.

What is STUN?

STUN is a protocol that allows two devices (P2P devices) to discover the presence and types of a NAT between them, and to find out what External IP address and Port are to be replaced by the NAT, for P2P communication between the two devices.

STUN was first defined in RFC 3489 (Standards) back in 2003, and then revised two times once in RFC 5389 (Standards) in 2008 and again in RFC 5780 (Experimental) in 2010.

According to RFC 5389, "classic STUN's algorithm for classification of NAT types (defined in RFC 3489) was found to be faulty, as many NATs (available in the market) did not fit cleanly into the (four) types defined there."

To resolve this problem, classic STUN was modified in RFC 5389 (i.e. to add Attributes to Binding messages). And in RFC 5780, NAT types were re-defined and the algorithm (method) for classification of NAT types was modified.

Both RFC 3489 and 5389 use the same term "STUN", but in two different meanings as follows:

- RFC 3489: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 5389: Session Traversal Utilities for NAT (STUN)

NAT Types Defined in RFC 3489 and 5780

1. Full Cone

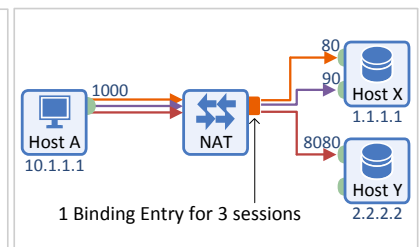
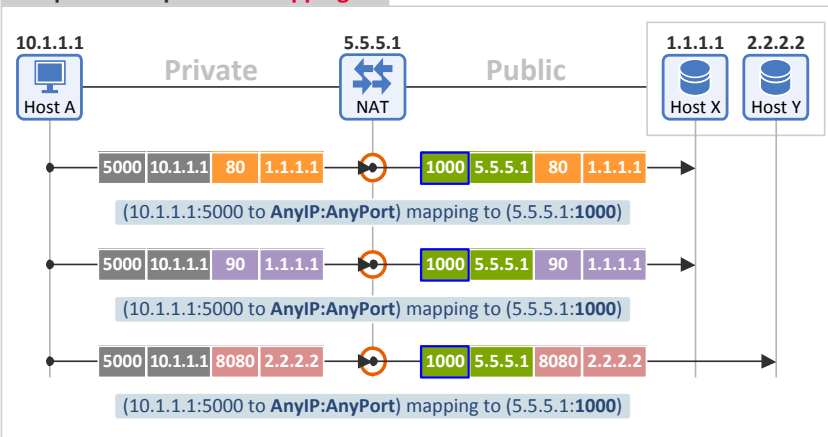
[Mapping Behavior] A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. **[Filtering Behavior]** Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address. (RFC 3489)

A full cone NAT in RFC 3489 corresponds to a NAT that uses Endpoint-Independent Mapping ("EIM") and Endpoint-Independent Filtering ("EIF") in RFC 5780.

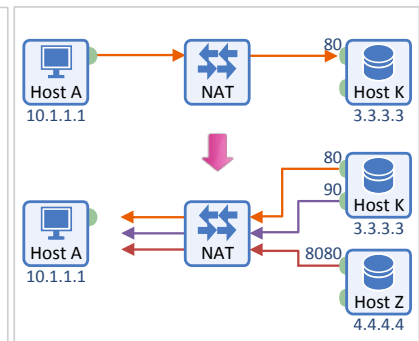
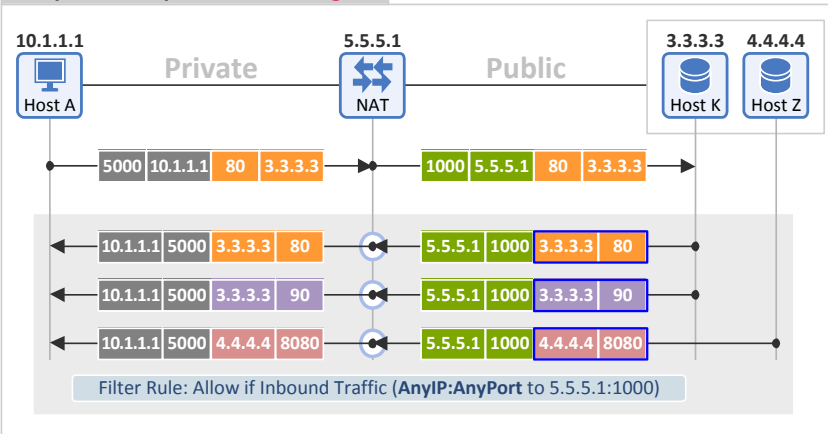
- Mapping Behavior: The NAT translates any outbound packets with the same (1) Source IP and (2) Source Port into the same Port Mapping value (e.g. Translated Port = 1000 in the figure below), regardless of the Destination IP or Destination Port of the packet.
- Filtering Behavior: The NAT checks only the (1) Destination IP and (2) Destination Port of an inbound packet to decide whether to pass the packet or not. Thus, it doesn't care about the Source IP or Source Port values of the External Endpoint.

Full Cone (RFC 3489) = Endpoint-Independent Mapping + Endpoint-Independent Filtering (RFC 5780)

Endpoint-Independent Mapping



Endpoint-Independent Filtering



2. Restricted Cone

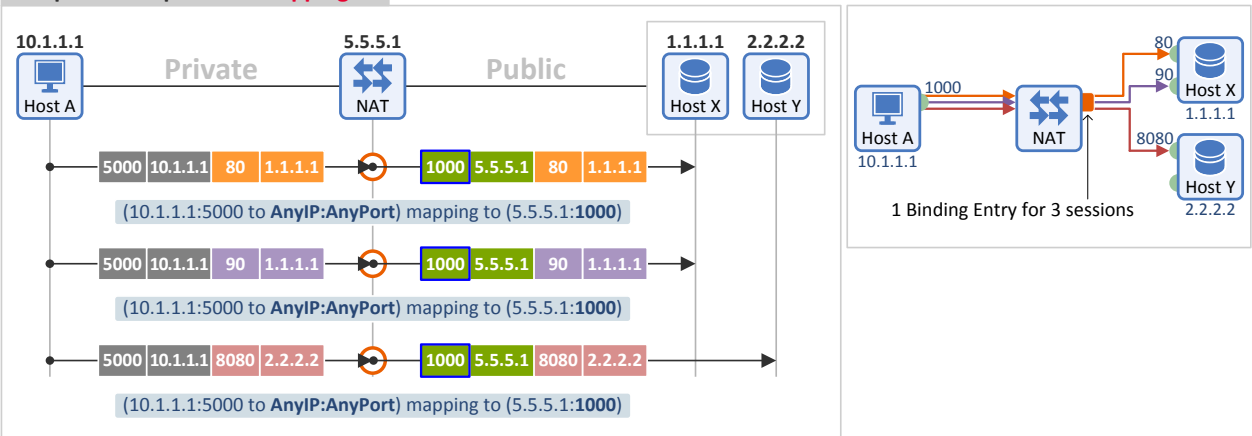
[Mapping Behavior] A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. **[Filtering Behavior]** Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X. (RFC 3489)

A restricted cone NAT corresponds to a NAT that uses EIM and Address-Dependent Filtering ("ADF") in RFC 5780.

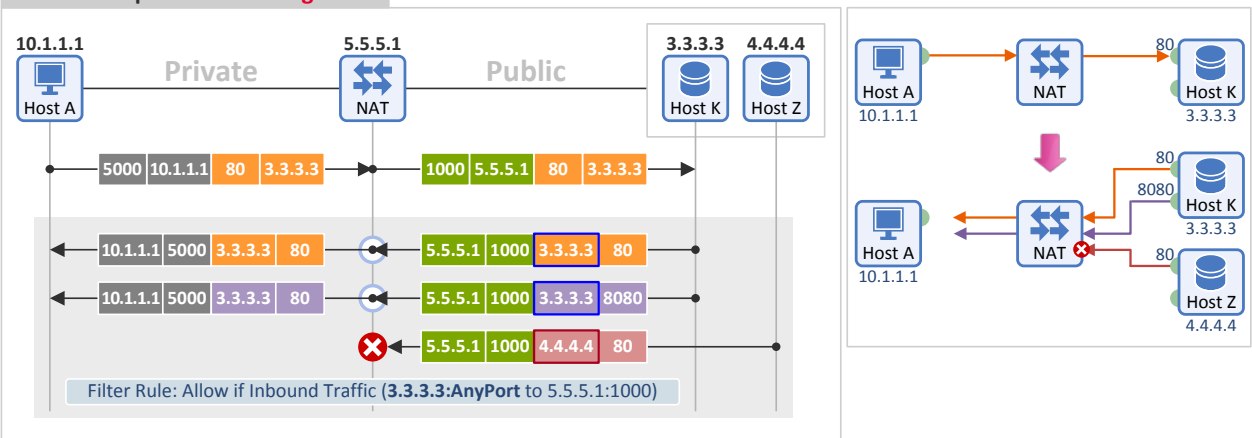
- Mapping Behavior: Same as in a full cone type
- Filtering Behavior: This NAT checks the (1) Destination IP, (2) Destination Port, (3) Source IP AND (4) Source Port of an inbound packet to decide whether to pass the packet or not.

Restricted Cone (RFC 3489) = Endpoint-Independent Mapping + Address-Dependent Filtering (RFC 5780)

Endpoint-Independent Mapping



Address-Dependent Filtering



3. Port Restricted Cone

[Mapping Behavior] A port restricted cone NAT is like a restricted cone NAT, **[Filtering Behavior]** but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P. (RFC 3489)

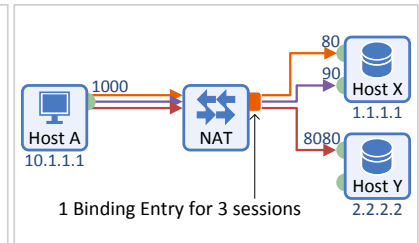
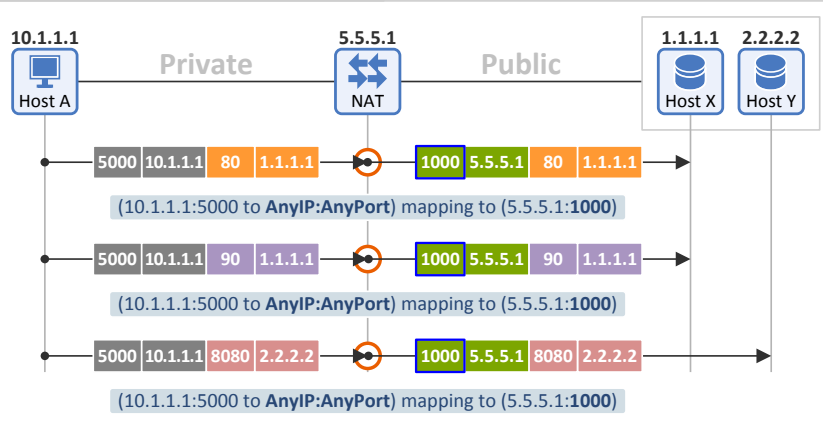
A port restricted cone NAT corresponds to a NAT that uses EIM and Address and Port-Dependent Filtering ("APDF") in RFC 5780.

- Mapping Behavior: Same as in a full cone type

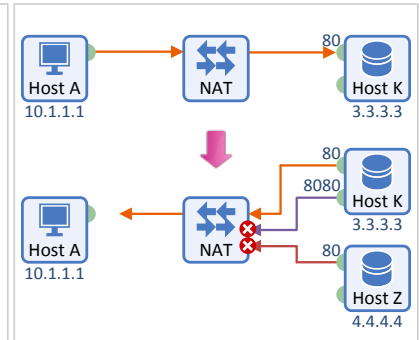
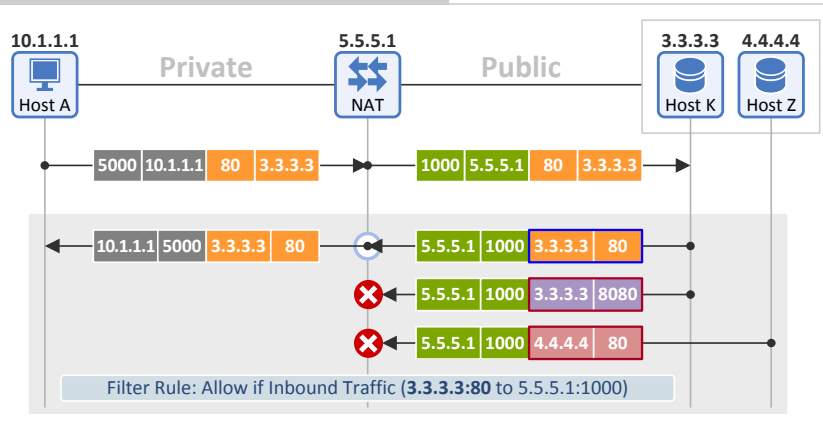
- Filtering Behavior: This NAT checks the (1) Destination IP, (2) Destination Port, (3) Source IP AND (4) Source Port of an inbound packet to decide whether to pass the packet or not.

Port Restricted Cone (RFC 3489) = Endpoint-Independent Mapping + Address and Port-Dependent Filtering (RFC 5780)

Endpoint-Independent Mapping



Address and Port-Dependent Filtering



4. Symmetric

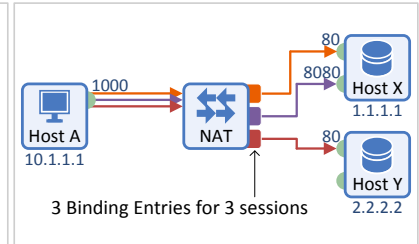
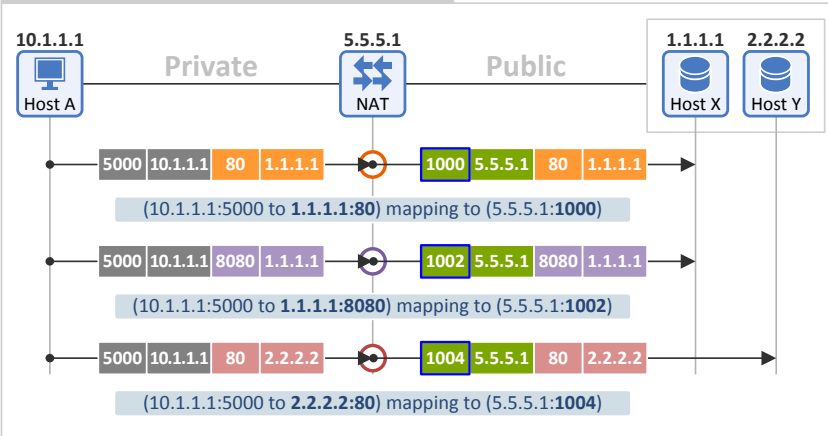
[Mapping Behavior] A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. **[Filtering Behavior]** Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host. (RFC 3489)

A symmetric NAT corresponds to a NAT that uses Address and Port-Dependent Mapping ("APDM") and APDF in RFC 5780.

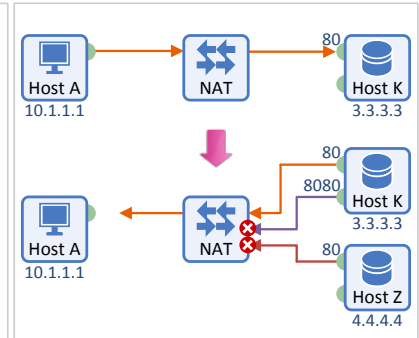
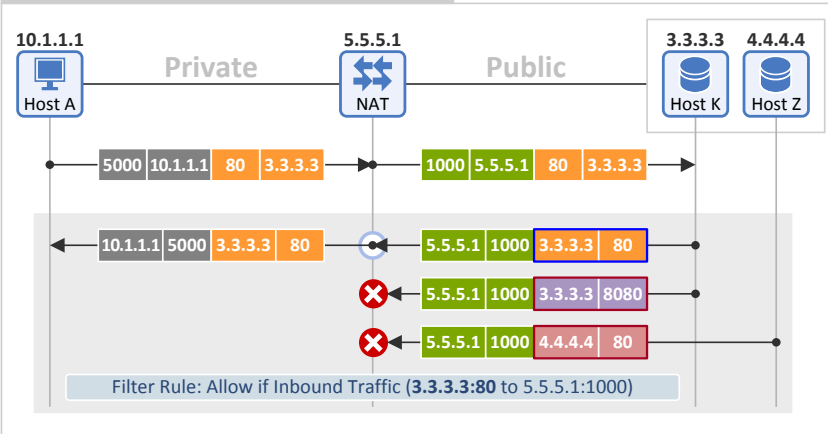
- Mapping Behavior: This NAT uses the same Port Mapping value for only the packets that have the same (1) Source IP, (2) Source Port, (3) Destination IP AND (4) Destination Port.
- Filtering Behavior: Same as in a port restricted cone type

Symmetric (RFC 3489) = Address and Port-Dependent Mapping + Address and Port-Dependent Filtering (RFC 5780)

Address and Port-Dependent **Mapping**



Address and Port-Dependent **Filtering**



Summary

The figure below shows the nine NAT types defined in RFC 5780 and the four NAT types defined in RFC 3489, and how the NAT types in RFC 3489 match their counterparts in RFC 5780.

	RFC 5780 defintion		RFC 3489 definition
NAT Type 1	Endpoint-Independent Mapping	Endpoint-Independent Filtering	Full Cone
NAT Type 2	Endpoint-Independent Mapping	Address-Dependent Filtering	Restricted Cone
NAT Type 3	Endpoint-Independent Mapping	Address and Port-Dependent Filtering	Port Restricted Cone
NAT Type 4	Address-Dependent Mapping	Endpoint-Independent Filtering	
NAT Type 5	Address-Dependent Mapping	Address-Dependent Filtering	
NAT Type 6	Address-Dependent Mapping	Address and Port-Dependent Filtering	
NAT Type 7	Address and Port-Dependent Mapping	Endpoint-Independent Filtering	
NAT Type 8	Address and Port-Dependent Mapping	Address-Dependent Filtering	
NAT Type 9	Address and Port-Dependent Mapping	Address and Port-Dependent Filtering	Symmetric

Netmanias Research and Consulting Scope

		99	00	01	02	03	04	05	06	07	08	09	10	11	12	13
Services	eMBMS/Mobile IPTV															
	CDN/Mobile CDN															
	Transparent Caching															
	BSS/OSS															
	Cable TPS															
	Voice/Video Quality															
	IMS															
	Policy Control/PCRF															
	IPTV/TPS															
Mobile Network	LTE															
	Mobile WiMAX															
	Carrier WiFi															
	LTE Backaul															
Wireline Network	Data Center Migration															
	Carrier Ethernet															
	FTTH															
	Data Center															
	Metro Ethernet															
	MPLS															
	IP Routing															

Visit <http://www.netmanias.com> to view and download more technical documents.

We design the future

We design the future

We design the future

Networks Consulting
 Analyze trends, technologies and market

Report
 Technical documents
 Blog
 One-Shot gallery

Future

Analysis
 Concept Design
 DRM
 POC
 Training

Infrastructure Services

LTE Carrier Ethernet IP/MPLS protocols Wi-Fi CDN Transparent Caching IMS

About NMC Consulting Group (www.netmanias.com)

NMC Consulting Group is an advanced and professional network consulting company, specializing in IP network areas (e.g., FTTH, Metro Ethernet and IP/MPLS), service areas (e.g., IPTV, IMS and CDN), and wireless network areas (e.g., Mobile WiMAX, LTE and Wi-Fi) since 2002.

Copyright © 2002-2013 NMC Consulting Group. All rights reserved.