K9038: The order of precedence for local traffic object listeners

https://my.f5.com/manage/s/article/K9038
Published Date: **Sep 22, 2015 UTC** Updated Date: **Mar 15, 2023 UTC**

Topic

When you create local traffic objects that process network traffic on the BIG-IP system, such as virtual servers, network address translations (NATs), and secure network address translations (SNATs), the BIG-IP system creates appropriate listeners for the objects that you define. A local traffic object with a destination listener processes requests that match a destination host or network IP address that is defined on the BIG-IP system.

A local traffic object with a source listener processes requests that originate from a host, or group of hosts, defined on the BIG-IP system. A local traffic object with source and destination listener processes requests that match a source and destination host or network IP address that is defined on the BIG-IP system.

SNAT matching behavior on virtual server or NAT traffic

SNAT objects can still match traffic after the traffic has already matched a virtual server or destination address of a NAT (displayed as NAT address in the Configuration utility). Therefore, they can translate the source address upon egress to the server side unless that traffic is already subjected to SNATs that are applied to the virtual server.

For example, when the BIG-IP system receives a new connection from source IP address 192.168.20.1 to destination IP address 192.168.10.1, the virtual server or NAT listener on 192.168.10.1 accepts the connection and, upon egress to the server side the SNAT listener 192.168.20.0/24, processes the connection and translates the source address to the translation address that is configured on the SNAT object.

If there is a source address translation configured on the virtual server, this address is used instead rather than the SNAT object. Continuing with the example, the system translates 192.168.20.1 to the translation address of 172.16.20.1. As a result of this behavior, you can configure a single SNAT object to translate traffic from all virtual servers destined to the next hop on the server side, as opposed to configuring the source address translation property on every virtual server. In this circumstance, when you want to bypass the SNAT for a specific virtual server (which has a pool configured) and allow the client address on the server side, you can disable the associated pool **Allow SNAT** setting. For more information about this behavior, and SNAT features, refer to K7820: Overview of SNAT features.

Description

The following rules apply when determining the order of precedence applied to local traffic objects.

Multiple destination listeners

These local traffic objects create listeners for new connection requests matching the destination host or network IP address:

- Virtual servers (Destination address)
- NATs (NAT address)

Connections matching both a virtual server and a NAT

When a new connection request matches both a virtual server and a NAT, the virtual server listener always has precedence, unless the NAT object has a more specific address. When the NAT object address is more specific than the virtual server address, the system ignores the specificity of the virtual server address.

For example, when the BIG-IP system receives a new connection request for destination IP address 192.168.10.1, the virtual server listener 192.168.10.1 has a higher precedence than NAT listener 192.168.10.1. If the virtual server listener is a network address such as 192.0.0.0/8, then the NAT listener 192.168.10.1 takes precedence.

Note: There is a change in behavior for virtual server and NAT precedence for CGNAT/BIG-IP AFM in which, if listener IP address for both virtual server and NAT match, the NAT takes precedence. For more information, refer to K67779110: Traffic not passing through forwarding virtual server after upgrading to BIG-IP AFM V15.1.0.

Connections matching multiple virtual servers

When a new connection request matches multiple virtual servers, the BIG-IP system places a higher precedence on the virtual server listener with a more specific IP address/netmask.

For example, when the BIG-IP system receives a new connection request for destination IP address 192.168.10.1 and service port 80, the virtual server listener 192.0.0.0/8:any has a higher precedence than the virtual server listener 0.0.0.0/0:80.

Multiple source listeners

These local traffic objects create listeners for new connection requests matching the source host or network IP address:

- NATs (Origin address)
- SNATs (Origin)
- Virtual servers (Destination address)

It is important to understand the following regarding NATs and SNATs and virtual servers:

NATs and SNATs

- NATs can use only host IP addresses for the source address match.
- SNATs can use both host and network IP addresses for the source address match.
- NATs and SNATs cannot share the same origin host IP address.

NATs and virtual servers

- BIG-IP LTM does not track NAT connections. A NAT (origin address) and a virtual server cannot shared the same IP address.

Connection matching both NATs and SNATs

When a new connection request matches both a NAT and SNAT, the BIG-IP system places a higher precedence on the NAT listener.

For example, when the BIG-IP system receives a new connection request from source IP address 192.168.10.1, the NAT listener 192.168.10.1 has a higher precedence than SNAT listener 192.168.10.0/24.

Connection matching multiple SNATs

When a new connection request matches multiple SNATs, the BIG-IP system places a higher precedence the SNAT listener with a more specific IP address/netmask.

For example, when the BIG-IP system receives a new connection request from source IP address 192.168.10.1, the SNAT listener 192.168.10.0/24 has a higher precedence than the SNAT listener 192.168.0.0/16.

Connection matching NATs and virtual servers

- NAT and virtual server (without a SNAT pool)

  If a request originating from the NAT's origin IP address also matches a virtual server **without a SNAT pool**, the virtual server will process the connection and apply the **NAT** translation address to the outgoing packet.

- NAT and virtual server (configured with a SNAT pool)

  If a request originating from the NAT's origin IP address also matches a virtual server **with a defined SNAT pool**, the virtual server will process the connection and apply the **SNAT pool** translation address to the outgoing packet.

For more information, including examples of each use case, refer to K9039: A virtual server with a SNAT pool takes precedence over matching the NAT

Multiple source and destination listeners

Beginning in BIG-IP 11.3.0, the only local traffic object that can create a listener for new connection requests matching the source and destination host or network IP address is the following:

- Virtual servers (Source address/Destination address)

Connection matching multiple virtual servers

When a new connection request matches multiple virtual servers, the BIG-IP system places a higher precedence on the virtual server listener with a more specific IP destination address/netmask.

For example, when the BIG-IP system receives a new connection request from source IP address 192.168.20.1 to destination IP address 192.168.10.1, the virtual server listener destination 192.168.10.1 and source 192.168.20.0/24 has a higher precedence than virtual server listener destination 192.168.10.0/24 and source 192.168.20.1.

Related Content

- K6459: Order of precedence for virtual server matching (9.x - 11.2.1)
- K14800: Order of precedence for virtual server matching (11.3.0 and later)