How to load balance FTPS servers on a NetScaler ADC?

Use Case

Load balancing secure FTP servers so that availability of application can be increased and load on servers can be balanced.

Introduction

FTP is a bit complicated protocol due to separate control and data connections between the client and the server. There are two modes in which it operates – active and passive and the use of ports at both client and server ends depends on the mode. See https://en.wikipedia.org/wiki/File_Transfer_Protocol#Protocol_overview

NetScaler supports native FTP load balancing along with FTP monitors in both active and passive modes. See http://docs.citrix.com/en-us/netscaler/12/load-balancing/load-balancing-common-protocols/lb-ftp-servers.html

When FTP was originally proposed, securing the data and control channels were not considered necessary, as the network at that time was assumed to consist of trusted systems. Securing the FTP sessions has now become critical because the data is transferred across networks (including Internet) and the data in transit is most of the times sensitive. FTP is often secured with SSL/TLS (FTPS) to satisfy the security requirements.

The problem of FTPS load balancing

After the initial SSL handshake between FTPS client and server, the control channel is encrypted and one can't see the commands within that channel without decrypting it first. Because the data channel is connected to a dynamic port, NAT and Firewall devices generally have a problem with FTPS if the control channel is encrypted, because they cannot determine what port to open for this traffic.

On NetScaler, load balancing of explicit FTPS servers can be done with wildcard port virtual server and adding appropriate listen policies. While wildcard port allows traffic on all ports, listen policy restricts the traffic to defined ports. So, this way you create a single service or virtual server for multiple ports.

Note: in this case you load balance between multiple FTPS servers but do not have visibility into data connections.

Configuration Steps in NetScaler ADC and FTPS Server

Step 1: Configure FTPS Server parameters

IP masquerading to NetScaler VIP is needed when server sends response to clients so that the clients send the request or data connection on the correct IP address.

FTPS server parameters shall be edited for this configuration as follow:

```
pasv_address=10.105.158.13 (this should be NetScaler VIP)

pasv_min_port=2000 (this port range shall be defined in listen policy on NetScaler vserver in step 3)

pasv_max_port=2010
```

Step 2: Add wildcard port ANY type service

Add service with FTPS server IP and * port. Ping-default monitor will get bound to the service which is appropriate for this configuration.

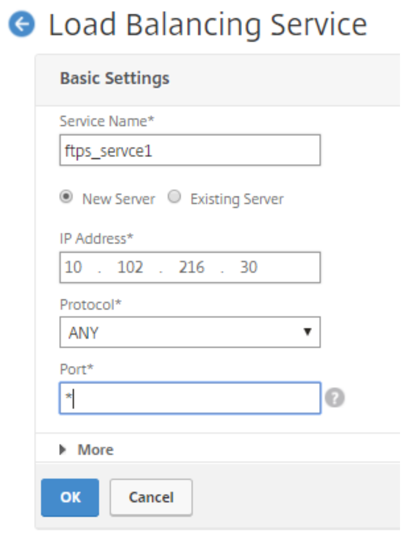
CLI:

At the command prompt, type:

```
add service ftps_service1 10.102.216.30 ANY *
```

GUI:

In the NetScaler GUI, go to Configuration > Traffic Management > Load Balancing -> Services and, add a new Service.



Load Balancing Service

Basic Settings

Service Name*: ftps_servce1

● New Server ○ Existing Server

IP Address*: 10 . 102 . 216 . 30

Protocol*: ANY

Port*: *

Repeat this step for all the FTPS services to be added.

Step 3: Add wildcard port ANY type virtual server

Add virtual server which listens on all ports and set listen policy with destination port numbers as per requirement. Set persistence and load balancing method as per requirement. Bind the service(s) to the virtual server.

CLI:

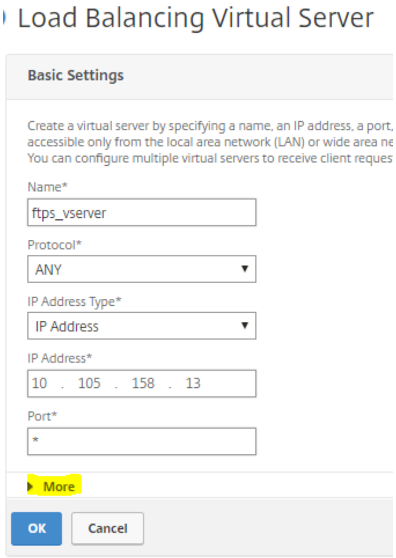
At the command prompt, type:

```
add lb vserver ftps_vserver ANY 10.105.158.13 * -persistenceType SOURCEIP -Listenpolicy
"CLIENT.TCP.DSTPORT.BETWEEN(2000,2010)" -Listenpriority 1

bind lb vserver ftps_vserver ftps_service1
```

GUI:

In the NetScaler GUI, go to Configuration > Traffic Management > Load Balancing -> Virtual Servers and add a virtual server. Click on “More” to open advanced options to add Listen Policy.



Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, accessible only from the local area network (LAN) or wide area ne You can configure multiple virtual servers to receive client reques

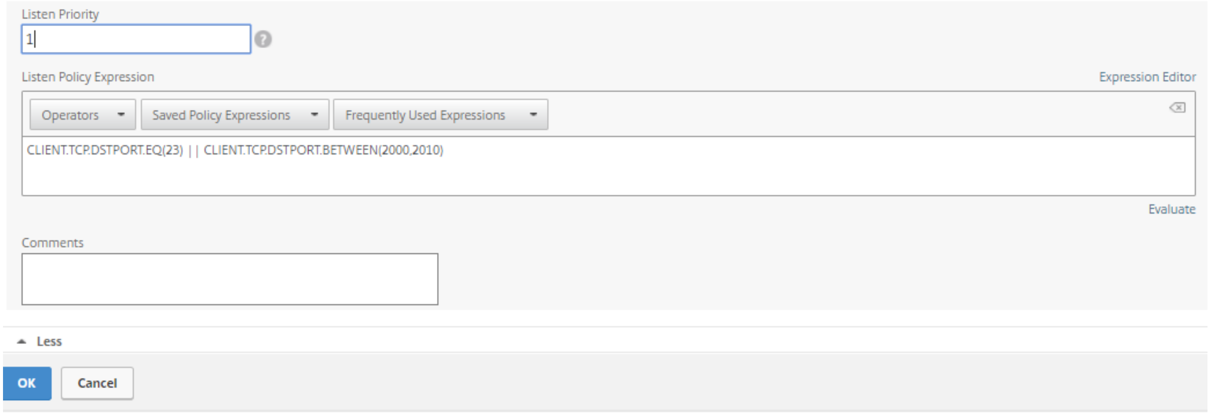
Name*: ftps_vserver

Protocol*: ANY

IP Address Type*: IP Address

IP Address*: 10 . 105 . 158 . 13

Port*: *



Listen Priority: 1

Listen Policy Expression: CLIENT.TCP.DSTPORT.EQ(23) || CLIENT.TCP.DSTPORT.BETWEEN(2000,2010)

Comments:

Note: Ensure to have a single SNIP configured for the vserver because controller and data connections should go to the same FTPS server and should have the same source address. Either configure a single SNIP across NetScaler or set Net Profile on virtual server to use one SNIP for the virtual server.