How to manage all ingress traffic through single point of control with NetScaler ADC?

Use Case

How to manage all ingress traffic through single point of control so that the critical requests will be prioritized and server overload is protected.

Introduction

Controlling all the ingress traffic at virtual server layer has various advantage over controlling it at service layer. NetScaler Application Level Quality of Experience (AppQoE) feature acts as single point of control to manage all ingress traffic before it gets load balanced at virtual server layer.

AppQoE elevates several existing policy-based security features of the NetScaler appliance into a single integrated feature that takes advantage of a new queuing mechanism, which manages requests to load-balanced web servers and applications at the virtual server level instead of at the service level. This allows NetScaler to handle queuing of all requests to a web site or application as one group before load balancing, instead of as separate streams after load balancing.

Why do you need AppQoE feature for your business? Problems with infrastructure where all the protection features are handled at service level are mentioned below:

- While making the load balancing decision at virtual server level, it will not know the state of protection features that are used at per service level basis and across the multiple services the prioritization and queuing mechanism will differ.
- New client connections will start queuing up at the service level and queue will start growing when services are overloaded and unable to digest more traffic.
- When service goes down whole queue will be flushed and held connections will be terminated.

NetScaler AppQoE feature solves the above problem by using fair queueing mechanism and has following advantages: -

- Single point of control to handle incoming traffic at virtual server level.
- Protection features like DoS (Denial-of-service) protection, priority queuing, sure connect can be handled more efficiently.
    - Sending dynamic responses to the client machine when services are engaged with other requests (SureConnect feature). These built-in responses generated at virtual server level avoids unnecessary Load Balancing processing.
    - Checking the authenticity of client by sending DoS responses against Dos attack makes server more secured (DoS protection). DoS protection at virtual server level gives admission control to NetScaler for better scalability.
    - Prioritizing the incoming request based on the importance of that request (Priority Queuing). It helps to influence the Load Balancing decision and maintains absolute order of priority.

- Better service resource utilization using load balancing decision.
- Queued connection will not get cleaned up if services goes down.

To know more about the how to configure AppQoE for your environment visit How to guide on: - ‘How to protect back-end servers from DOS using AppQoE’.