How to protect your App infrastructure from layer7 DoS attacks?

Use Case

How to protect your App infrastructure from layer7 DoS attacks?

Introduction

Internet hackers often try to bring down a website by sending a surge of GET/POST requests or other HTTP-level requests. There are several freely available tools to launch such attacks as well and it is a constant concern to the business. NetScaler provides Layer 7 Denial of Service (DoS) Protection using AppQoE feature which provides an effective way to prevent such attacks from impacting the Web Application.

When NetScaler appliance detects an attack, it responds to the incoming requests with a Java or HTML script containing DoS challenge to filter out illegitimate client requests. In the HTTP challenge-response generation and validation process, AppQoE uses cookies to validate the client's response and verifies the authenticity of the incoming requests.

How to configure L7 DoS protection feature on NetScaler appliance:

1. Enable AppQoE feature on NetScaler

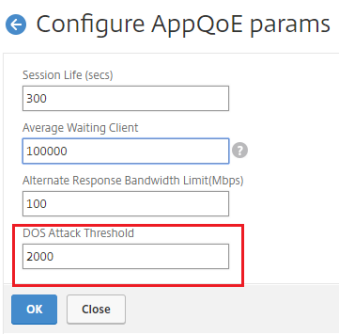
At the command prompt, type the following commands:

- enable ns feature appqoe
- show ns feature

From configuration utility interface, perform following steps:

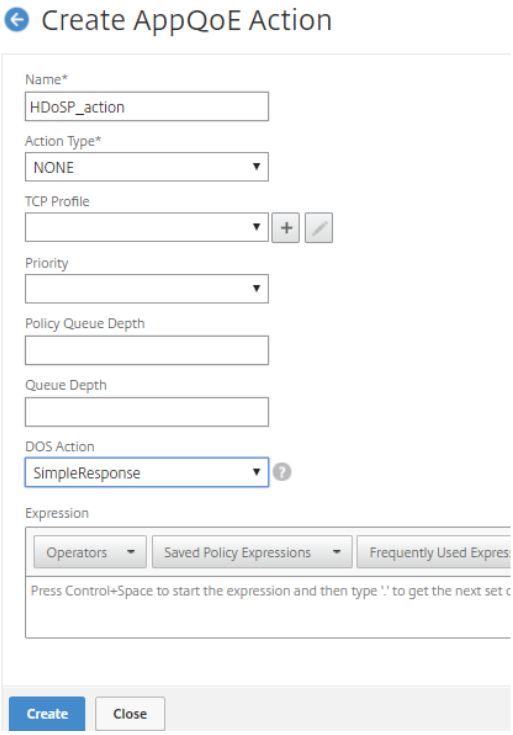
- Navigate to System > Settings.
- In the details pane, click Configure Advanced Features.
- In the Configure Advanced Features dialog box, select the AppQoE check box.
- Click OK.

2. Configure AppQoE parameters.



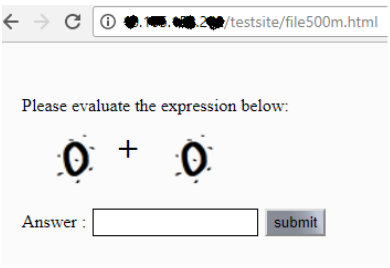
DOS Attack Threshold field describes the number of connections that must be waiting in queue before the ADC responds with DoS protection measures.

3. Configure AppQoE action.



Description for AppQoE action fields;

- Action Type (NONE) – No alternate response is provided for Action Type-NONE.
- DOS Action (SimpleResponse | HICResponse) – When DOS attack threshold is reached, DOS action will be triggered. For authenticity of the incoming requests, NetScaler ADC will send HTTP challenges to client machine. A client machine capable of computing the original value is considered genuine.
    - In SimpleResponse, challenge is sent to client machine in the form of cookies and genuine client machine will respond back to the cookies without human intervention. (e.g. NetScaler will send 4+3=? Challenge in _DOSH body cookie where client machine computes the value for this cookie and respond back with the final value).
    - In HICResponse, NetScaler will send the challenge in the form of image where human intervention is required to solve the challenge. (e.g. NetScaler will send 2+6= ? challenge to client machine where human will calculate the value and submit it for authenticity). For more details, refer following screenshot:



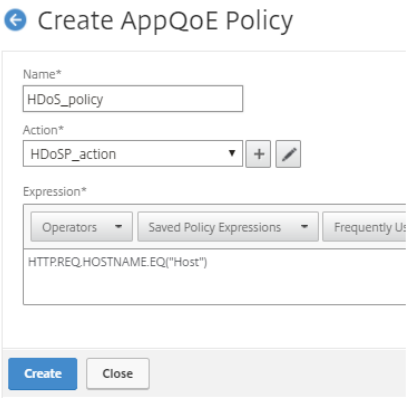
Note: The expression that you can see in above screenshot is NetScaler generated number used for validation which is client specific and does not change for 2

minutes. We do not call it as CAPTCHA implementation because NetScaler has its own implementation for generating dynamic number.

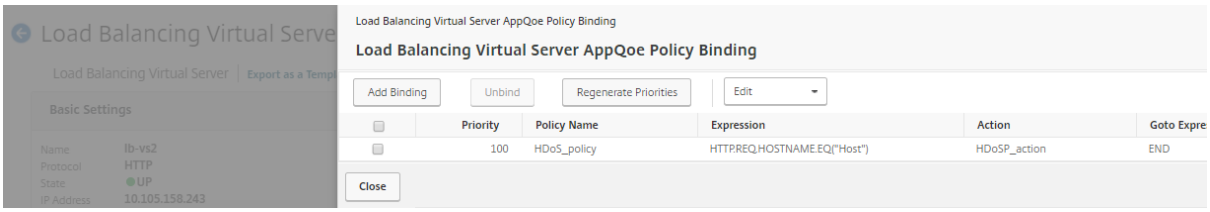
- For SimpleResponse or HICResponse DoS action option, you can add an optional second-level check in expression box.

From above screenshot, we can say that DoS protection AppQoE feature will be enabled only for top 10 URLs which are mentioned in the ANALYTICS.STREAM method. You can certainly configure the policy expression to look at larger set of URLs or the entire URL set.

4. Configure AppQoE policy and bind AppQoE action to it.



5. Bind AppQoE policy to Load balancing virtual server to protect application infrastructure.



Citrix NetScaler AppQoE feature in a nutshell helps the customers to protect their applications from DoS attack by configuring NetScaler with HDoS protection feature. Application infrastructure security is taken care by NetScaler AppQoE enabled layer 7 DoS protection.