

How to protect back-end servers from DoS attack using NetScaler AppQoE feature?

Use Case

How to protect back-end servers from DoS (Denial-of-Service) attack using NetScaler AppQoE feature.

Introduction

Application level Quality of Experience (AppQoE) helps control allocation of resources based on prioritization along with DoS protection for back-end resources. Using the AppQoE you can accomplish following benefits: -

- Prioritization of incoming request,
- Maintain priority order across multiple connections,
- DoS protection at application layer by sending DoS challenges with JavaScript to validate client,
- Providing alternate or build-in response to keep client busy,
- Serve the content from custom response file on NetScaler.

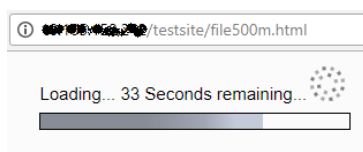
AppQoE Parameters details:

Description for AppQoE action fields;

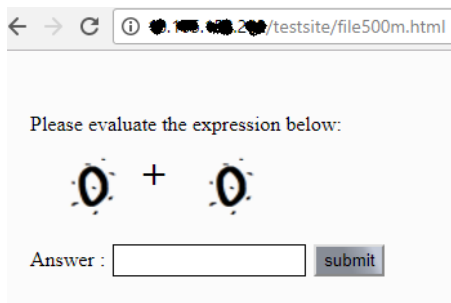
- Action Type – NetScaler ADC will perform any one of the following responder action:
 - I. ACS – Serves the content from Alternate Content Server specified in 'Alternate Content Server Name' (e.g. ex_server1) once 'Maximum connections' (e.g. 500) or 'Delay' threshold is reached. ACS action type will provide temporary web page till requested resources are not available. See below screenshot for alternate web page;



- II. NS – Built-in NetScaler ADC response provided when 'Maximum connections' or 'Delay' threshold is reached. NS action type will provide built-in temporary web page till requested resources are not available. See below screenshot for alternate web page;



- III. NONE – No alternate content is provided; new connections will wait till back-end resources are ready to serve new content. It is mandate to select Priority field for Action Type as NONE.
- Priority – specifies the order in which waiting requests are to be fulfilled when resources are available. It has various options such as HIGH, MEDIUM, LOW or LOWEST. If priority is not configured, default priority choice set to LOWEST.
- Policy Queue Depth – When the policy queue size (number of requests queued for the policy binding this action is attached to) increases to the specified threshold, subsequent requests are dropped to the lowest priority level.
- Queue Depth – Threshold value for specified priority (HIGH | MEDIUM | LOW). After reaching threshold value subsequent request assigned to LOWEST priority queue.
- 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:



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

Custom File

DOS Action

HICResponse

Expression

Operators Saved Policy Expressions Frequently Used Expressions

ANALYTICS.STREAM("Top_URL").IS_TOP_FREQUENTS(10)

- IV. TCP profile – It is, an option field, collection of TCP settings that can be bound to AppQoE policy. Static TCP profiles are bound at load balancing virtual server level but for few use cases (for e.g. Telco 3G /4G users) we need to configure TCP settings dynamically. In such scenarios, we can configure TCP profile and bind it to AppQoE policy. For TCP profile configuration, click on: - <https://support.citrix.com/article/CTX130962>

How to configure AppQoE feature on NetScaler appliance:

1. Enable AppQoE feature on NetScaler

At the command prompt, type the following commands:

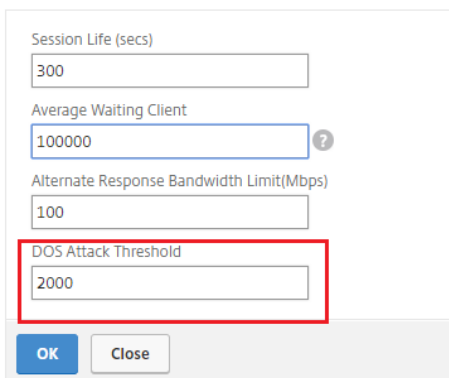
- enable ns feature appqoe
- show ns feature

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.

← Configure AppQoE params



The screenshot shows a configuration dialog box titled "Configure AppQoE params". It contains four input fields: "Session Life (secs)" with a value of 300, "Average Waiting Client" with a value of 100000, "Alternate Response Bandwidth Limit(Mbps)" with a value of 100, and "DOS Attack Threshold" with a value of 2000. The "DOS Attack Threshold" field is highlighted with a red rectangular border. At the bottom of the dialog, there are two buttons: "OK" and "Close".

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

3. Configure AppQoE action.

← Create AppQoE Action

Name*
HDOSP_appqoe_action

Action Type*
ACS

TCP Profile
nstcp_default_profile

Priority
▼

Policy Queue Depth
100

Queue Depth
500

Maximum Connections
500

Delay (microseconds)
▼

Alternate Content Server Name*
ex_server1

Alternate Content Path*
/html/defaultresponse.html

Custom File
▼

DOS Action
HICResponse

Expression
Operators Saved Policy Expressions Frequently Used Expressions

Press Control-Space to start the expression and then type ':' to get the next set of options

These fields are not available for Action Type: NONE

These fields will be visible only for Action Type: ACS

Action Type values can be: ACS, NS or NONE.

DOS Action values can be: NONE, SimpleResponse or HICResponse

For Action Type (NS | ACS), its mandate to set either Maximum connections or Delay field.

Expression box will only be present for DOS Action (SimpleResponse | HICResponse).

Option to set Alternate Content Server Name and Alternate Content Path will only be available for Action Type – ACS.

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

← Create AppQoE Policy

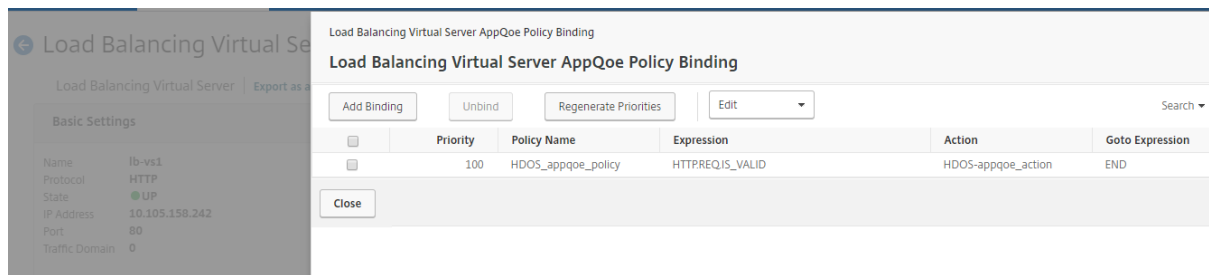
Name*
HDOSP_appqoe_policy

Action*
HDOS-appqoe_action

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
HTTP.REQ.IS_VALID

Create Close

5. Bind AppQoE policy to Load balancing virtual server.



The screenshot displays the NetScaler GUI for configuring AppQoE policy binding on a Load Balancing Virtual Server. The main window is titled "Load Balancing Virtual Server AppQoE Policy Binding". On the left, a sidebar shows "Basic Settings" for the virtual server "lb-vs1", including details like Protocol (HTTP), State (UP), IP Address (10.105.158.242), Port (80), and Traffic Domain (0). The main area contains a table of bindings with the following data:

Priority	Policy Name	Expression	Action	Goto Expression
100	HDOS_appqoe_policy	HTTPREQIS_VALID	HDOS-appqoe_action	END

Buttons for "Add Binding", "Unbind", "Regenerate Priorities", and "Edit" are visible at the top of the table. A "Close" button is located at the bottom left of the main configuration area.

So, NetScaler AppQoE feature provides various advantages like priority queuing, SureConnect and DoS protection to protect the back-end resources against the attack.