

How to indicate SharePoint Application servers that SSL Offload is enabled in NetScaler and end client is using HTTPS?

Use Case: How to indicate SharePoint back-end server that the end client is using HTTPS so that the server responds with redirect headers/content which has reference to HTTPS URLs instead of HTTP URLs

Problem Statement:

In SSL Offload configuration in NetScaler, the request/response from NetScaler to server is sent over HTTP and the SharePoint Server uses HTTP URL in its Redirect and HREF links. NetScaler does not convert the HTTP URL to HTTPS URL and this results in end client connecting over HTTP to the NetScaler SSL virtual server.

This issue can be resolved by indicating to the SharePoint server that the end client consuming the SharePoint application is connecting over SSL. The same can be achieved by inserting the below header from NetScaler in request going to SharePoint server.

“Front-End-Https: On”

Following are the steps to enable the Header Insertion at Content Switching (CS) level

How to configure action and policy at content switching virtual server Level:

Instructions:

- 1) Under Configuration tab select **AppExpert > Rewrite > Actions**
- 2) After selecting **Actions** > Click **Add** for a new action and create **SharePoint-Frontend-rewrite-action** like below

← Configure Rewrite Action

Name

Type

Use this action type to insert a header.

Header Name*

Expression

In string expressions, string constants and expressions can be concat

Comments

- Now under Configuration tab select **AppExpert > Rewrite > Policies** and create a New policy like **SharePoint-Frontend-rewrite-policy** and bind policy to the action **SharePoint-Frontend-rewrite-action**.

← Configure Rewrite Policy

Name

Action*
 +

Log Action
 +

Undefined-Result Action*

Expression*

Operators Saved Policy Expressions Frequent

Comments

- Now the above created policy needs to be bound to content switching vserver for all the incoming requests under **Policies** category.

Choose Type

Policies

Choose Policy*

Choose Type*

Content Switching Virtual Server Rewrite Policy Binding X

Search ▾

<input type="checkbox"/>	Priority	Policy Name	Expression	Action	Goto Expression	Invoke
<input type="checkbox"/>	100	Sharepoint-Frontend-rewrite-policy	HTTPREQ_IS_VALID	Sharepoint-Frontend-rewrite-action	END	

CLI commands for the above setup:

```
add rewrite action SharePoint-Frontend-rewrite-action1
insert_http_header Front-End-Https "\"on\""
```

```
add rewrite policy SharePoint-Frontend-rewrite-policy
HTTP.REQ.IS_VALID SharePoint-Frontend-rewrite-action
```

```
bind cs vserver SharePoint-SSL-CSvserver -policyName Sharepoint-
Frontend-rewrite-policy -priority 100 -gotoPriorityExpression END -
type REQUEST
```

5) To check number of policy hits, go to **AppExpert > Rewrite > Policies** and scroll towards right

Rewrite Policies

Show built-in Rewrite Policies Search ▾

Action ▾

	Expression	Action	Undefined-Result Action	Hits
	HTTPREQ_IS_VALID	Rewrite-Action	-Global undefined-result action-	0
policy	HTTPREQ_IS_VALID	Sharepoint_Stylebook-frontend-rewrite-action	-Global undefined-result action-	23
rewrite-policy	HTTPREQHEADER("Accept-Encoding").EXISTS	Sharepoint_Stylebook-Accept-Encoding-rewrite-action	-Global undefined-result action-	129
	HTTPREQ_IS_VALID	Sharepoint-Frontend-rewrite-action	-Global undefined-result action-	35

By following the above instructions, SharePoint servers will know that the end client is using SSL for communication and hence SharePoint servers will respond with HTTPS URL to the client.