

Rewrite for Citrix ADC

Mani Shankar Kumar

Sr. System Engineer, Gilead Sciences Inc.

I. WHAT IS REWRITE

Rewrite refers to the rewriting of some information in the Citrix ADC appliance's requests or responses. Rewriting can assist in providing access to the requested content while avoiding exposing unnecessary details about the actual configuration of the Web site. The following are a few examples of when the rewrite feature comes in useful.

- The Citrix ADC can rewrite all the http:// links in a response body to make it look more secure.
- The insecure links in the response must be converted into secure links during the SSL offload deployment. Using the rewrite option, you can rewrite all http://links to https:// to ensure that Citrix ADC's outgoing responses to the client contain secured links.
- If a website must display an error page, a custom error page can be displayed instead of the default 404 Error page. For example, if you show the Web site's home page or site map instead of an error page, the visitor stays on the site rather than leaving.
- You can use the Rewrite option to launch a new Web site while keeping the old URL.
- If a site's topic has a complicated URL, you can rewrite it with a simple, easy-to-remember URL (also known as a "cool URL").
- You can append the default page name to a website's URL. For example, if the default page of a company's Web site is http://www.xyz.com/index.php, you can rewrite the URL to 'xyz.com/index.php' when a user types 'xyz.com' in the browser's address bar. Citrix ADC can modify the headers and body of HTTP requests and responses when the rewrite feature is enabled.
- You can use protocol-aware Citrix ADC policy expressions in the rewrite policies you configure to rewrite HTTP requests and responses. The virtual servers that handle HTTP requests and responses must be HTTP or SSL compliant. You can perform the following actions in HTTP traffic:
 - Modify the URL of a request
 - Add, modify or delete headers
 - Add, replace, or delete any specific string within the body or headers.

Consider the payload as a raw stream of bytes when rewriting TCP payloads. Each virtual server that manages TCP connections must be of the TCP or SSL TCP type. TCP rewrite refers to the rewriting of TCP payloads that are not HTTP data. Any part of the TCP payload can be added, modified, or deleted in TCP traffic.

II. HOW REWRITE WORKS

A rewrite policy is made up of a rule and an action. The rule specifies the traffic to which the rewrite is applied, and the action specifies the action taken by the Citrix ADC. Multiple rewrite policies can be defined. Set the bind point and priority for each policy.

A bind point is a point in the traffic flow where the Citrix ADC examines the traffic to determine whether it can be rewritten. A policy can be bound to a specific load balancing or content switching virtual server, or it can be made global if you want the policy to apply to all traffic handled by the Citrix ADC.

These policies are known as global policies. The Citrix ADC has some default policies in addition to user-defined policies. A default policy cannot be changed or deleted.

Citrix ADC evaluates policies in the following order:

- Global policies
- Policies bound to specific virtual servers
- Default policies

It should be noted that Citrix ADC can only apply a rewrite policy when it is bound to a point.

Citrix ADC implements the rewrite feature as follows:

- The Citrix ADC appliance looks for global policies first, then at individual bind points.
- When multiple policies are bound to the same bind point, the Citrix ADC evaluates them in the order of their priority. The highest priority policy is evaluated first. Following the evaluation of each policy,
 - If the policy is TRUE (the traffic matches the rule), the action associated with the policy is added to a list of actions to be performed. When the characteristics specified in the

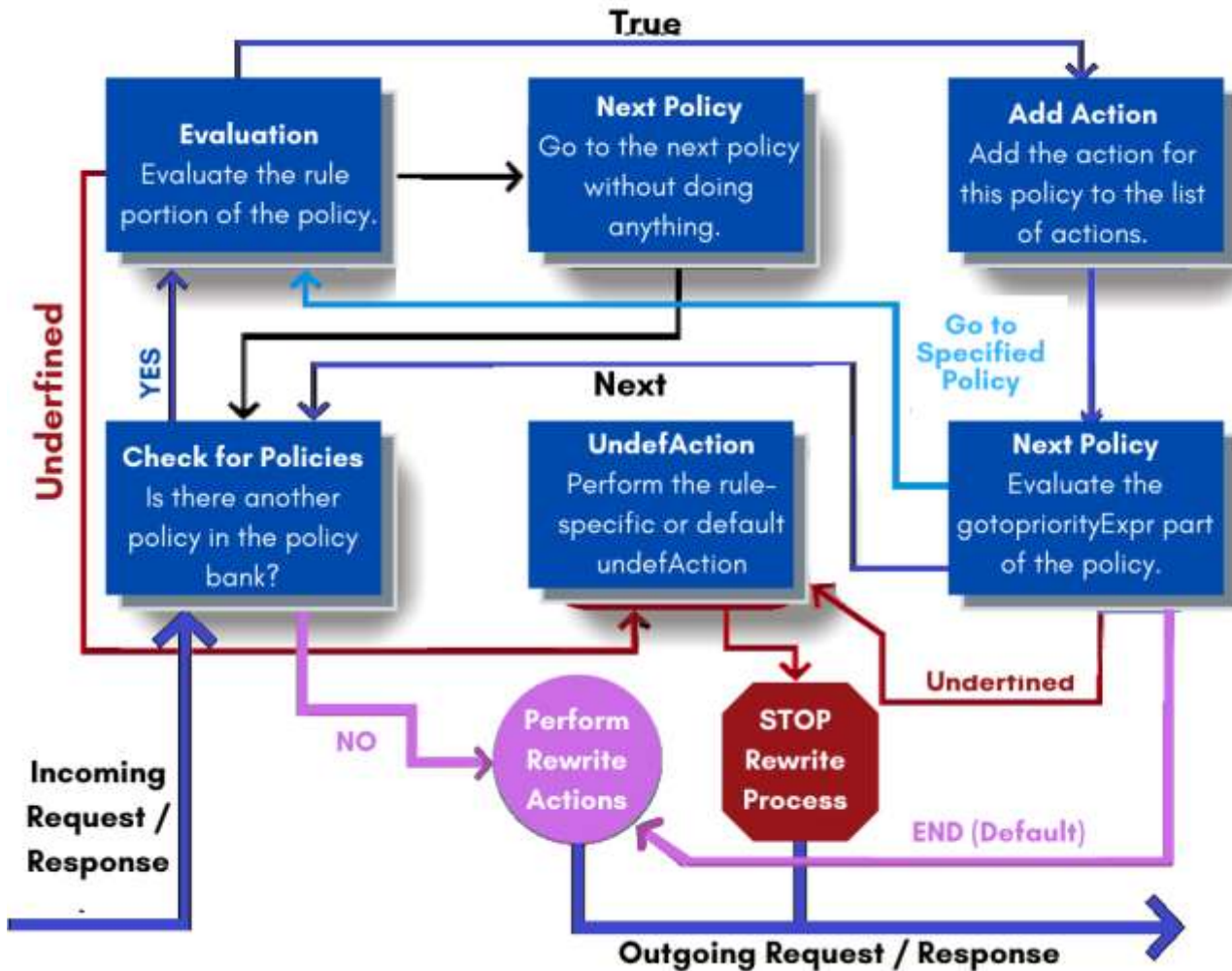
policy rule match the characteristics of the request or response being evaluated, a match occurs.

In addition to the action, you can specify the policy that should be evaluated after the current policy is evaluated for any policy. This is known as the 'Go to Expression' policy. If a Go to Expression (gotoPriorityExpr) policy is specified for any policy, the Citrix ADC evaluates the Go to Expression policy and ignores the policy with the next highest priority.

To indicate the Go to Expression policy, you can specify the policy's priority; you cannot use the policy's name. Set the Go to Expression to 'END' if you want the Citrix ADC to stop evaluating other policies after evaluating a specific policy.

After all policies have been evaluated, or when a policy's Go to Expression is set to END, the Citrix ADC begins performing the actions on the list of actions.

The diagram below represents how Citrix ADC processes a request or response when the rewrite feature is enabled.



Rewrite

As rewrite actions, specify the actions to be taken on the Citrix ADC appliance, such as adding, replacing, or deleting text within the body, or adding, modifying, or deleting

headers, or any changes in the TCP payload. See Configuring a Rewrite Action for more information on rewrite actions.

The table below describes the actions that the Citrix ADC can take when a policy evaluates to TRUE.

Action Result

Insert The rewrite action specified for the policy is carried out.
 NOREWRITE The request or response is not rewritten. Citrix ADC forwards the traffic without rewriting any part of the message.

RESET The connection is aborted at the TCP level.

DROP The message is dropped.

Custom Action

You can create the action according to the requirement.

To use the

Rewrite feature, take the following steps:

- Enable the feature on the Citrix ADC.
- Define rewrite actions.
- Define rewrite policies.
- Bind the policies to a bind point to bring a policy into effect.

Binding a Rewrite Policy

You must bind a rewrite policy after creating it in order for it to take effect. If you want to apply your policy to all traffic that passes through your Citrix ADC, you can bind it to Global, or you can bind it to a specific virtual server or bind point to direct only that virtual server or bind point's incoming traffic to that policy.

If an incoming request matches a rewrite policy, the policy's associated action is performed. Rewrite policies for evaluating HTTP requests and responses can be bound to HTTP or SSL virtual servers, or to the REQ OVERRIDE, REQ DEFAULT, RES OVERRIDE, and RES DEFAULT bind points. TCP rewrite policies can only be bound to virtual servers of type TCP or SSL TCP, or to the bind points OTHERTCP REQ OVERRIDE, OTHERTCP REQ DEFAULT, OTHERTCP RES OVERRIDE, and OTHERTCP RES DEFAULT.

Note: The term OTHERTCP refers to all TCP or SSL TCP requests and responses that you want to treat as a raw stream of

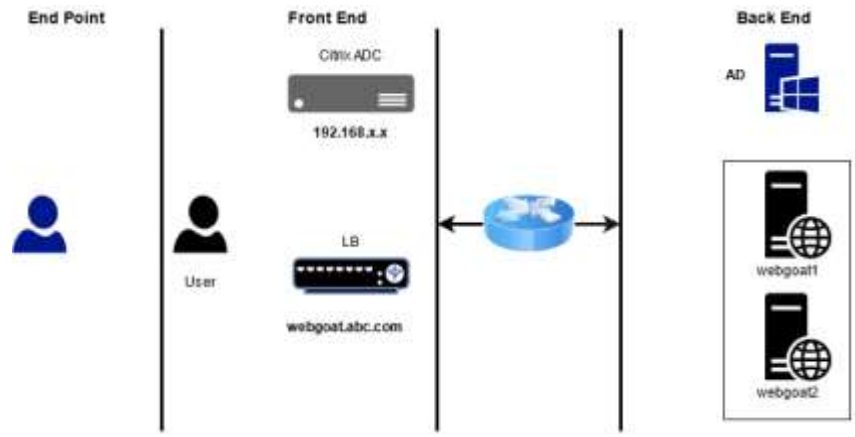
bytes regardless of the protocols that the TCP packets encapsulate in the context of the Citrix ADC appliance. You assign a priority to a policy when you bind it. The order in which the policies you define are evaluated is determined by the priority. The priority can be set to any positive integer. Policy priorities in the Citrix ADC operating system work in reverse order - the higher the number, the lower the priority.

For example, if you have three policies with priorities of 10, 100, and 1000, the policy with priority 10 is applied first, followed by the policy with priority 100, and finally the policy with priority 1000. The rewrite feature, unlike most other features in the Citrix ADC operating system, continues to evaluate and implement policies after a request matches a policy.

The effect of a specific action policy on a request or response, on the other hand, will frequently differ depending on whether it is performed before or after another action. Priority is essential for achieving the desired results. By setting priorities with intervals of 50 or 100 between each policy when you bind it, you can leave yourself plenty of room to add other policies in any order and still have them evaluate in the order you want. If you do this, you will be able to add new policies at any time without having to re-assign the priority of an existing policy. When you bind a rewrite policy, you can also assign a goto expression (gotoPriorityExpression) to the policy. A goto expression can be any positive integer that corresponds to the priority assigned to a different policy that is higher in priority than the policy containing the goto expression. If a goto expression is assigned to a policy and a request or response matches the policy, the Citrix ADC will immediately go to the policy whose priority matches the goto expression. It will not evaluate any policies that have priority numbers that are lower than the current policy but higher than the priority number of the goto expression.

Rewrite

Lab Environment Overview: To demonstrate the Citrix ADC rewrite policy, I created a lab environment in which I performed the necessary steps to configure the Citrix ADC rewrite policy.



SERVER LIST:

FQDN	IP Address	Description
ad.abc.com	192.168.x.x	Domain Controller
adc.abc.com	192.168.x.101	Citrix ADC
webgoat.abc.com	172.21.10.x1	Web Server lb vsrv rbg (Load Balancer)

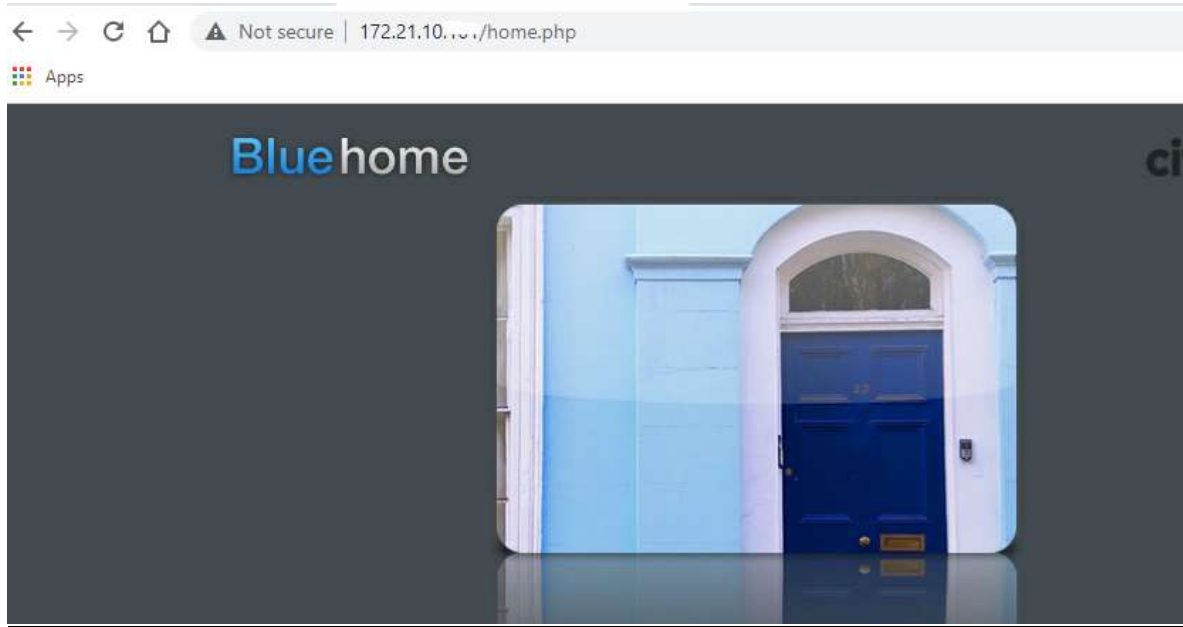
In This environment we have two web application node for WebGoat website. We already configured load balancing on Citrix ADC for web Application Webgoat1 and webgoat2 and our load balancer FQDN is webgoat.abc.com and Load Balancer IP 172.21.10.x1

Step-1: View the default page ("/") on website

Open a web browser and find <http://172.21.10.X1/> (open your website)



Step-2: open <http://172.21.10.X1/home.php> page



Note: we want to set home.php page as landing page for user

Step-3: Connect to Primary ADC:

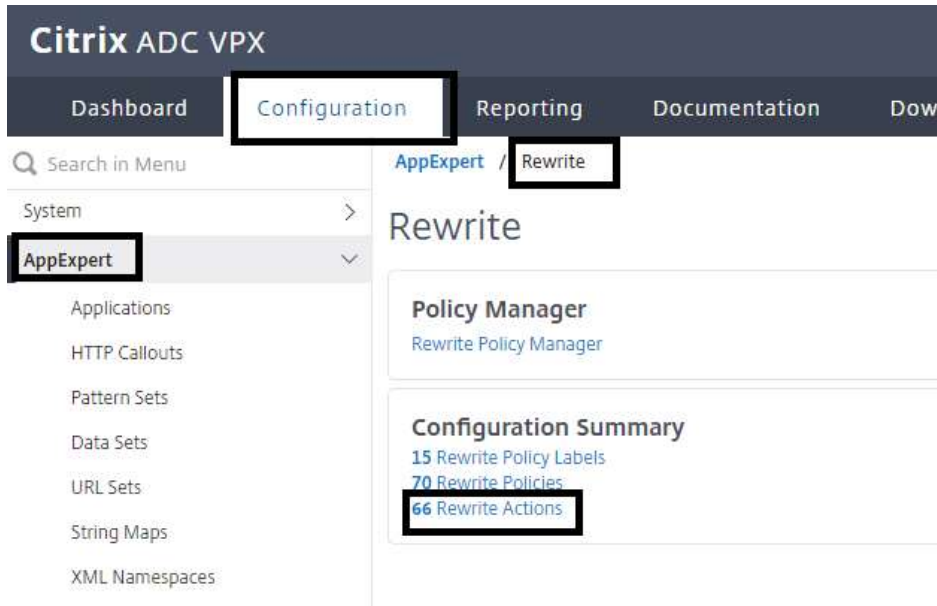
Open Google Chrome and connect to Primary ADC using NSIP <https://192.168.30.x>.

Log on using the credentials:

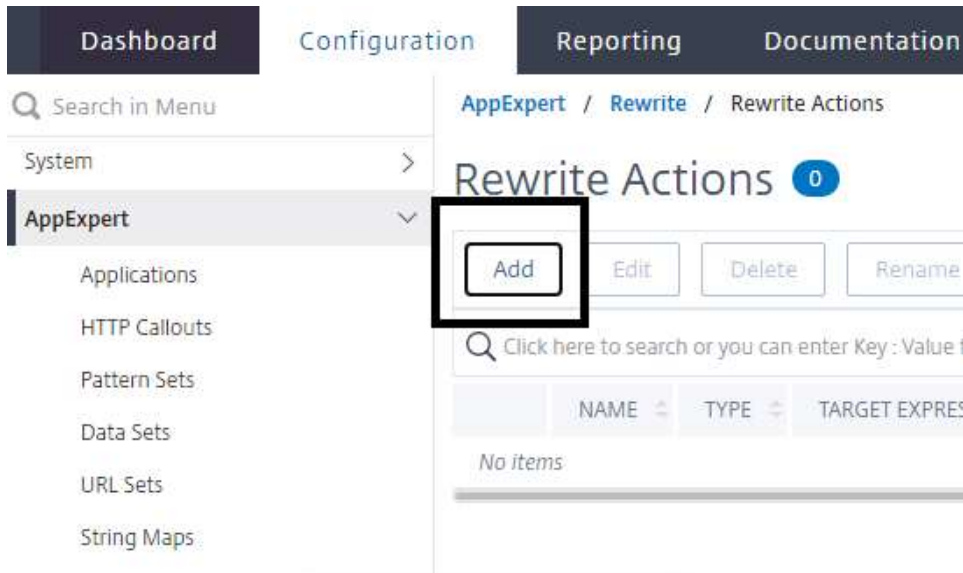


Step-4: Create a Rewrite action that will replace the URL path to "/home.php":

- Browse to AppExpert > Rewrite > Actions.



- Click Add.



- Enter rw_act_sendtohome in the Name field.
- Select REPLACE in the Type field. This designates the type of rewrite action to perform.
- Configure the target expression: This identifies the element of the request to replace

HTTP.REQ.URL.PATH

- Configure the value expression, which identifies what to replace the target with:

"/home.php"

Create Rewrite Action

Name*
rw_act_sendtohome

Type*
REPLACE

Use this action type to replace specified text reference with custom text in request/response.

Expression to choose target location *

Select Select Select

HTTP.REQ.URL.PATH

Expression to Replace with

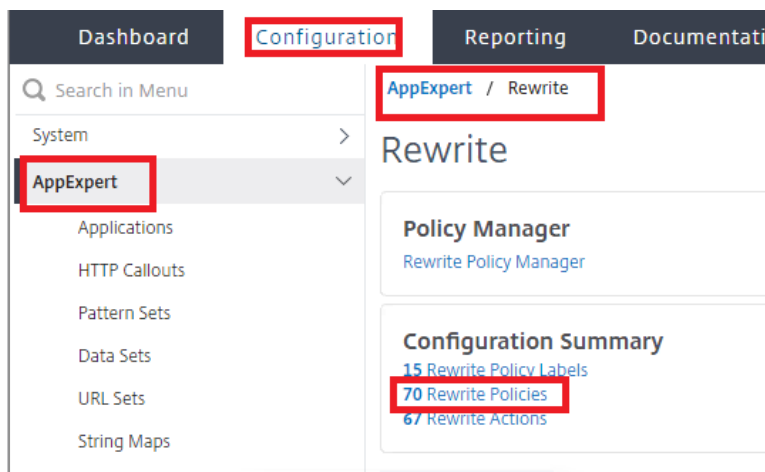
Select Select Select

"/home.php"

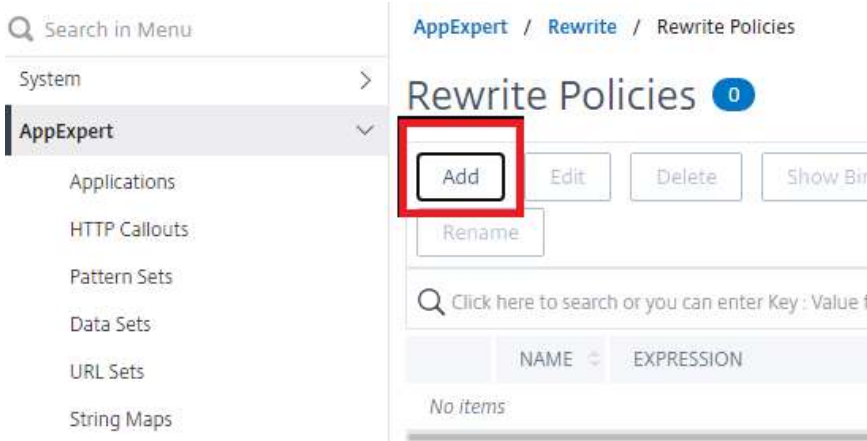
- Click **Create**

Step-5: Create a rewrite policy to replace the original URL only when users access the default path ("/").

- Browse to **AppExpert > Rewrite > Policies**.



- Click **Add**.



- Enter **rw_pol_sendtohome** in the Name field.
- Select **rw_act_sendtohome** in the Action field that we created previous step.

Configure the expression for the policy so it only applies when default path ("/") is requested by users:

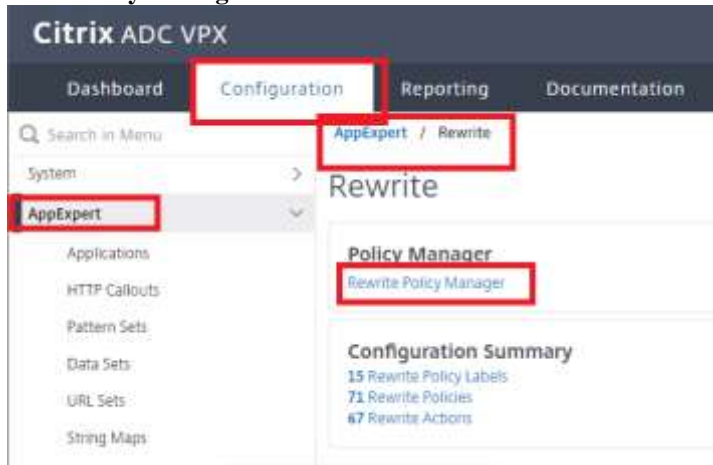
HTTP.REQ.URL.PATH.EQ("/")

← Create Rewrite Policy

- Click **Create**

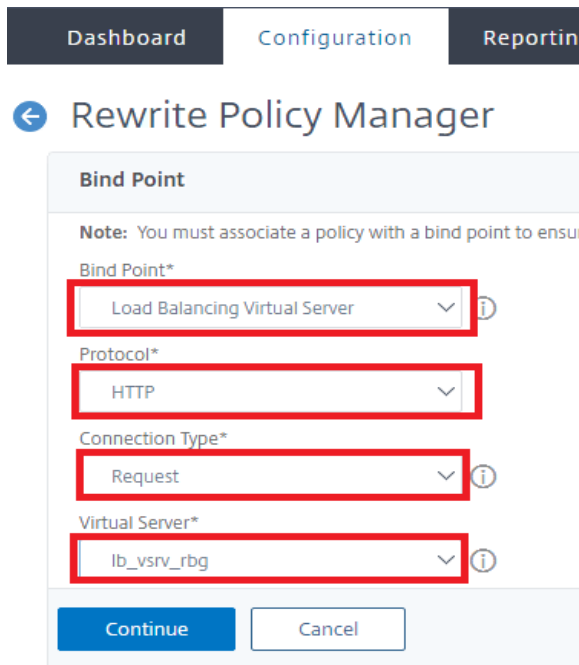
Step-6: Bind the rewrite policy to web server

Click **Policy Manager**.



Select the bind point for **lb_vsrv_rbg** for HTTP Request-time traffic:

- Select **Load Balancing Virtual Server** from the Bind Point field.
- Select **HTTP** from the Protocol field.
- Select **REQUEST** from the Connection Type field.
- Select **lb_vsrv_rbg** from the Virtual Server field.



- Click **Continue**

Bind the policy to this bind point:

- Click **Click to Select** under **Select Policy**.

← Rewrite Policy Manager

Bind Point

Bind Point **Load Balancing Virtual Server**
Virtual Server **lb_vsrv_rbg**

Policy Binding

Select Policy*

Click to select > Add

Binding Details

Priority*

100

GoTo Expression*

- Select **rw_pol_sendtohome** and click **Select**.

Rewrite Policies 1

Select Add Edit Delete Show Bindings Statistics

Rename

Q Click here to search or you can enter Key : Value format

	NAME	EXPRESSION
🔍	rw_pol_sendtohome	HTTP.REQ.URL.PATH.EQ("/")

Total 1 25 Per Pag

- Priority should automatically show 100, otherwise enter that value.
- Select **Next** in the GoTo Expression.

Policy Binding

Policy Binding

Select Policy*

rw_pol_sendtohome > Add Edit

► More

Binding Details

Priority*
100 ⓘ

Goto Expression*
NEXT ⓘ

Invoke LabelType*
None ▾

Bind Close

- Click **Bind**.

Dashboard Configuration Reporting Documentation

Rewrite Policy Manager

Bind Point

Bind Point: Load Balancing Virtual Server
Virtual Server: lb_vsrv_rbg

Add Binding Unbind Regenerate Priorities Bind NOPOLICY-REWRITE

Click here to search or you can enter

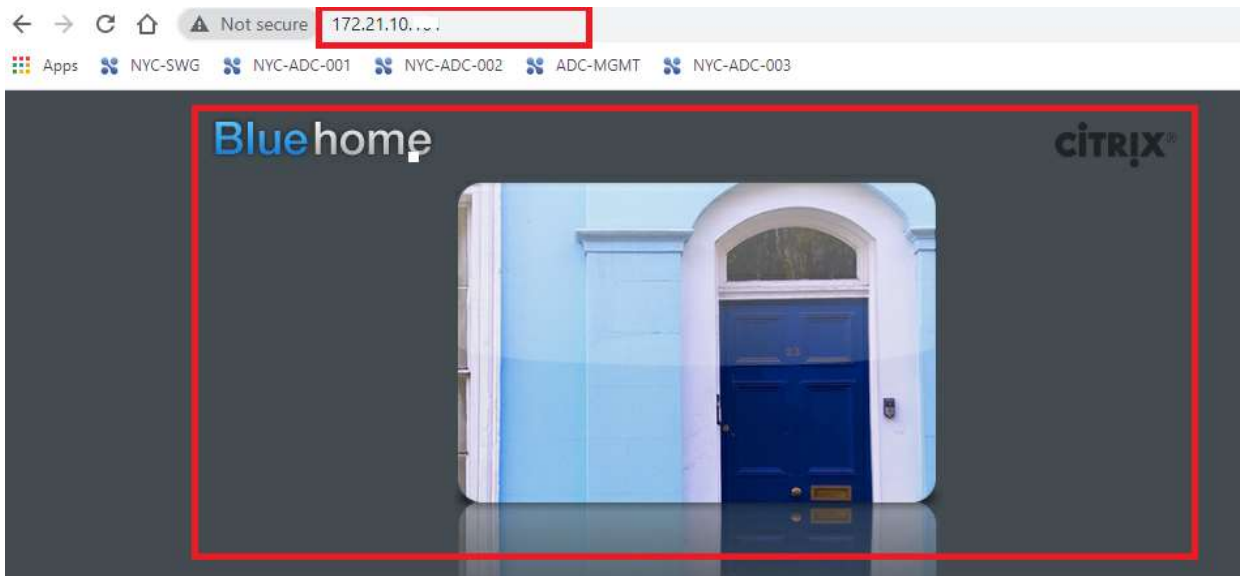
	PRIORITY	POLICY NAME	EXPRESSION
<input type="checkbox"/>	100	rw_pol_sendtohome	HTTPREQ.URL.PATH.EQ("/")

Done

- Click **Done**.

Step-6: Verifying the rewrite policy

Browse to <http://172.21.10.X1/>



Verify that content for /home.php is displayed

Client make a request for ("/") page but Citrix ADC modifies the request sent to the server and fetches "/home.php".