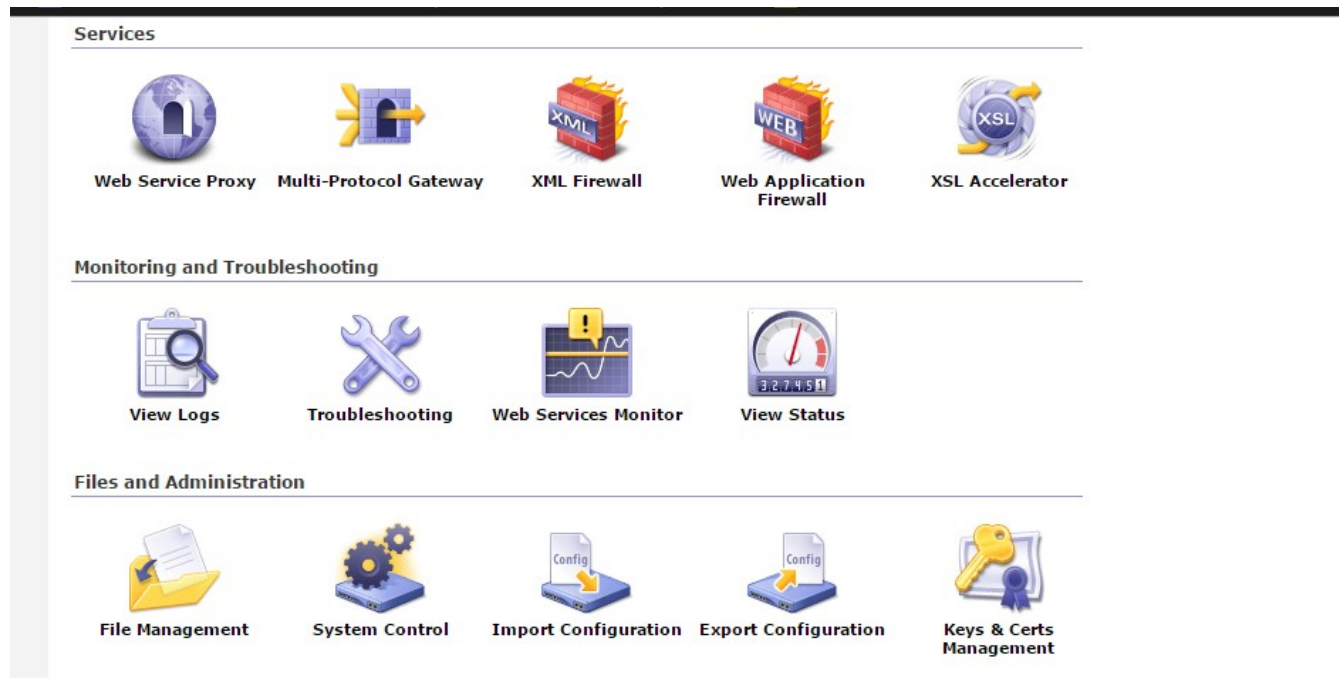


Sign-Verify Service :

Login to your domain and click on **Multi-Protocol Gateway**



Give the name to MPG.And click on “+” for MPG Policy.

Apply Cancel [Help](#)

General Configuration

Multi-Protocol Gateway Name <input type="text" value="Sign-Verify"/> *	XML Manager default + ... *
Summary <input type="text"/>	Multi-Protocol Gateway Policy (none) + ... *
Type <input type="radio"/> dynamic-backends <input checked="" type="radio"/> static-backend *	URL Rewrite Policy (none) + ...

Back side settings	Front side settings
Default Backend URL <input type="text"/> *	Front Side Protocol (empty) <input type="text"/> Add + ... *
<input type="button" value="MQ Helper"/> <input type="button" value="WebSphere JMS Helper"/> <input type="button" value="IMSCoconnect Helper"/>	

User Agent settings

Give the policy **name** and create a **new rule** with Rule direction “**Client to Server**”

The screenshot displays the 'Configure Multi-Protocol Gateway Style Policy' interface in a Google Chrome browser window. The address bar shows the URL: <https://172.17.12.93:9090/configure/StylePolicyEditor/?skipNav=true&policyNameSelect=&service=M>.

Policy:

Policy Name: *

Rule:

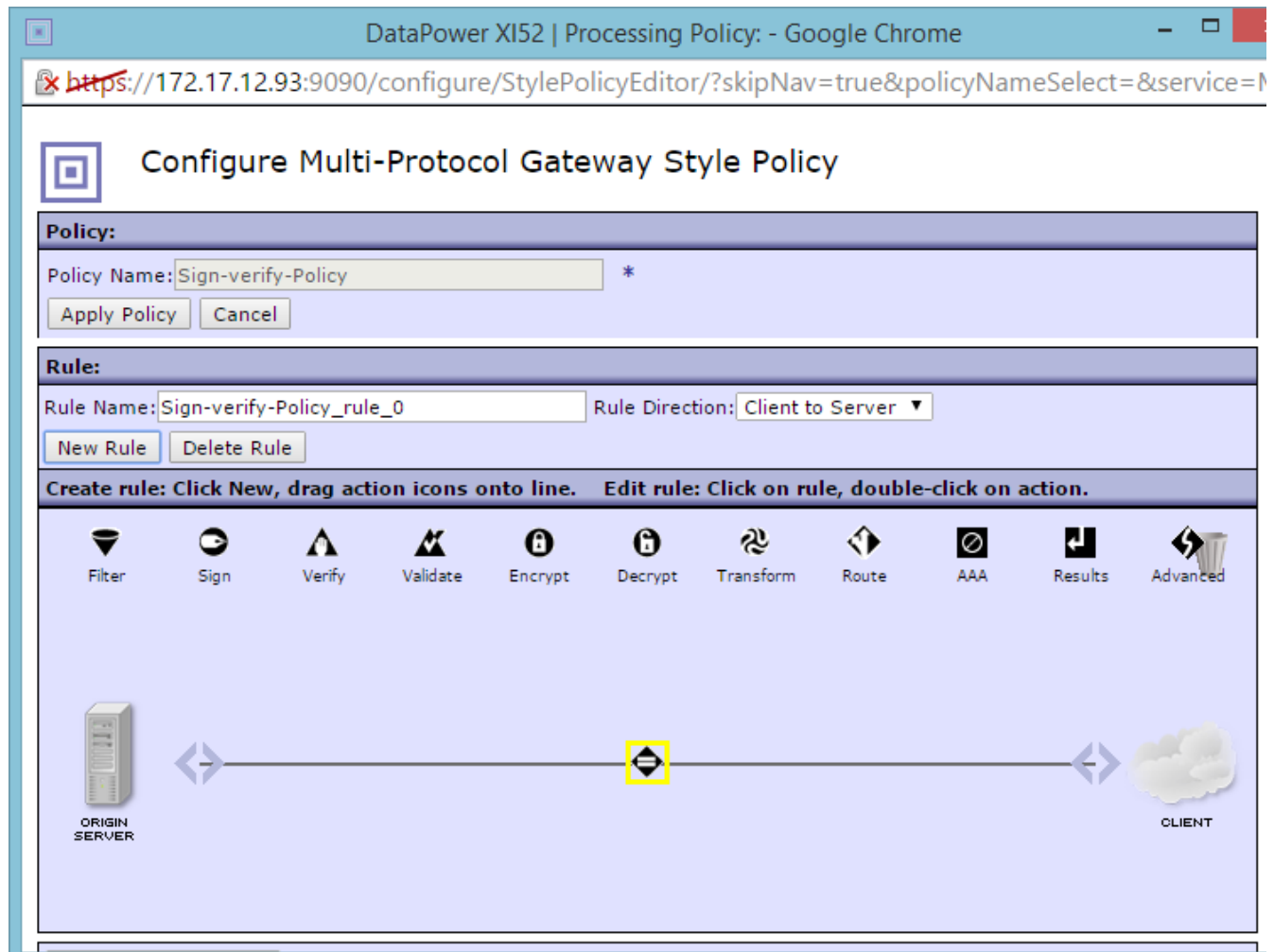
Rule Name: Rule Direction: Both Directions ▼

Create rule: Click New, drag action icons onto line. Edit rule: Click on action. click on action.

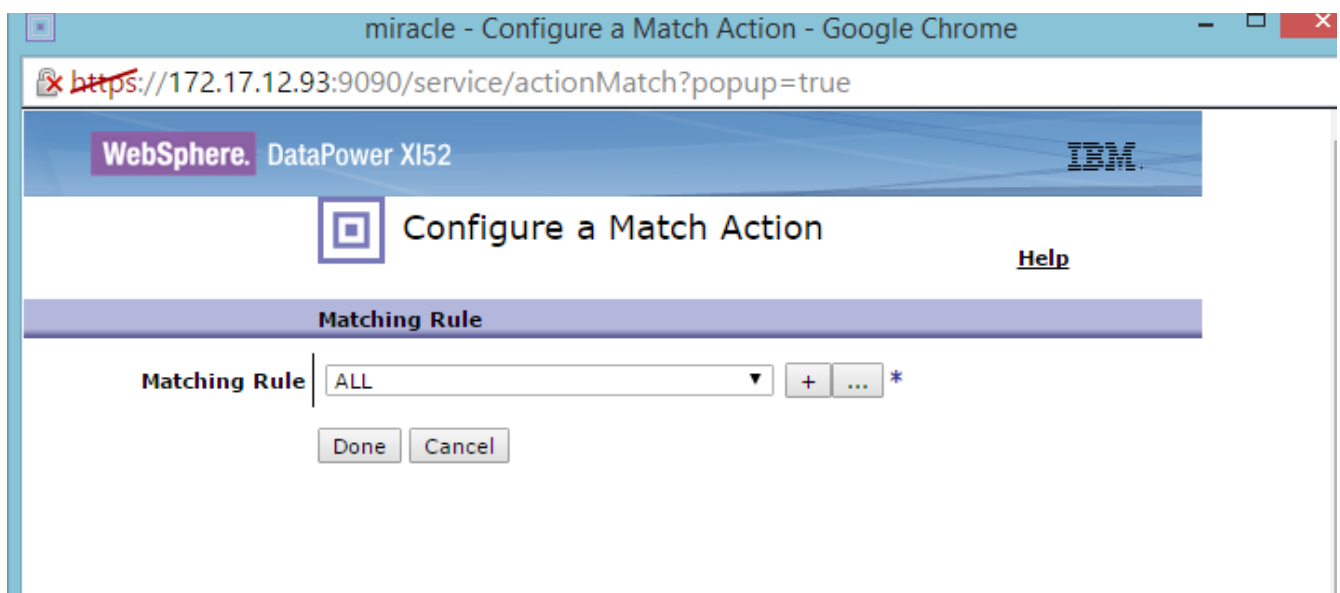
Filter Sign Verify Validate Encrypt Decrypt Transform Route AAA Results Advanced

ORIGIN SERVER ↔ CLIENT

Double click on the icon and configure it



Click the dropdown and select **ALL** and click **Done**



Then Drag and drop the Result action onto the rule

DataPower XI52 | Processing Policy: - Google Chrome

<https://172.17.12.93:9090/configure/StylePolicyEditor/?skipNav=true&policyNameSelect=&service=>

Configure Multi-Protocol Gateway Style Policy

Policy:

Policy Name: *

Rule:

Rule Name: Rule Direction:

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action.

Filter Sign Verify Validate Encrypt Decrypt Transform Route AAA Results Advanced

ORIGIN SERVER CLIENT

Drag and Drop Sign action onto the rule and double click on it.



Configure Multi-Protocol Gateway Style Policy

Policy:

Policy Name: *

Rule:

Rule Name:

Rule Direction:

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action.



Filter



Sign



Verify



Validate



Encrypt



Decrypt



Transform



Route



AAA



Results



Advanced




ORIGIN
SERVER



CLIENT

Give the crypto certificate a name .
Select the sscert as public key certificate

 <https://172.17.12.93:9090/configure/CryptoCertificate?skipNav=true&newObjPopup=true&newObj>

Configure Crypto Certificate

This configuration has been added and not yet saved.

Main

Crypto Certificate

Name

Administrative State

File Name

Password

Password Alias


☐ on ☐ off

(none)
SSL_Key_Pair_Reverse-privkey.pem
SSL_Key_Pair_Reverse-sscert.pem
SSL_Key_Pair_forward-privkey.pem
SSL_Key_Pair_forward-sscert.pem
Sign-Verify-Key1-privkey.pem
Sign-Verify-Key1-sscert.pem
cert1.cer
cert2.cer
encrypt-Decrypt-key-privkey.pem
encrypt-Decrypt-key-sscert.pem
key1-privkey.pem
key1-sscert.pem
key2-privkey.pem
key2-sscert.pem
key3-privkey.pem
key3-sscert.pem
key4-privkey.pem
key4-sscert.pem
key4-sscert.pem.txt
(none)

*

[Help](#)

Click Apply.

 <https://172.17.12.93:9090/configure/CryptoCertificate?skipNav=true&newObjPopup=true&newObjPopu>

Configure Crypto Certificate

This configuration has been added and not yet saved.

Main

Crypto Certificate

[Help](#)

Name *

Administrative State ☒ enabled ☐ disabled

File Name *

Password

Password Alias

 ~~https://~~172.17.12.93:9090/configure/CryptoKey/key1?skipNav=true&editObjPopup=true&editObjPopu



Configure Crypto Key

Main

Crypto Key:key1 [up]

[Export](#) | [View Log](#) | [View Status](#) | [Help](#)
[Convert Crypto Key Object](#)

Administrative State

☒ enabled ☐ disabled

File Name

cert:/// ▼

Sign-Verify-Key1-privkey.pem ▼ *

Password

Password Alias

☐ on ☒ off

Sign

Envelope Method

- ☐ Enveloped Method
- ☐ Enveloping Method
- ☐ SOAPSec Method
- ☒ WSSec Method *
- ☐ Advanced

Message Type

- ☒ SOAP Message
- ☐ SOAP With Attachments
- ☐ Raw XML Document, including SAML for Enveloped
- ☐ Selected Elements (Field-Level)
- ☐ Advanced *

Asynchronous

☐ on ☒ off

Use Asymmetric Key

☒ on ☐ off ☐ Save

Signing algorithm

rsa ☐ Save

Key

sign-verify-key12 ☒ Save

Certificate

sign-verify-cert ☒ Save

WS-Security Version

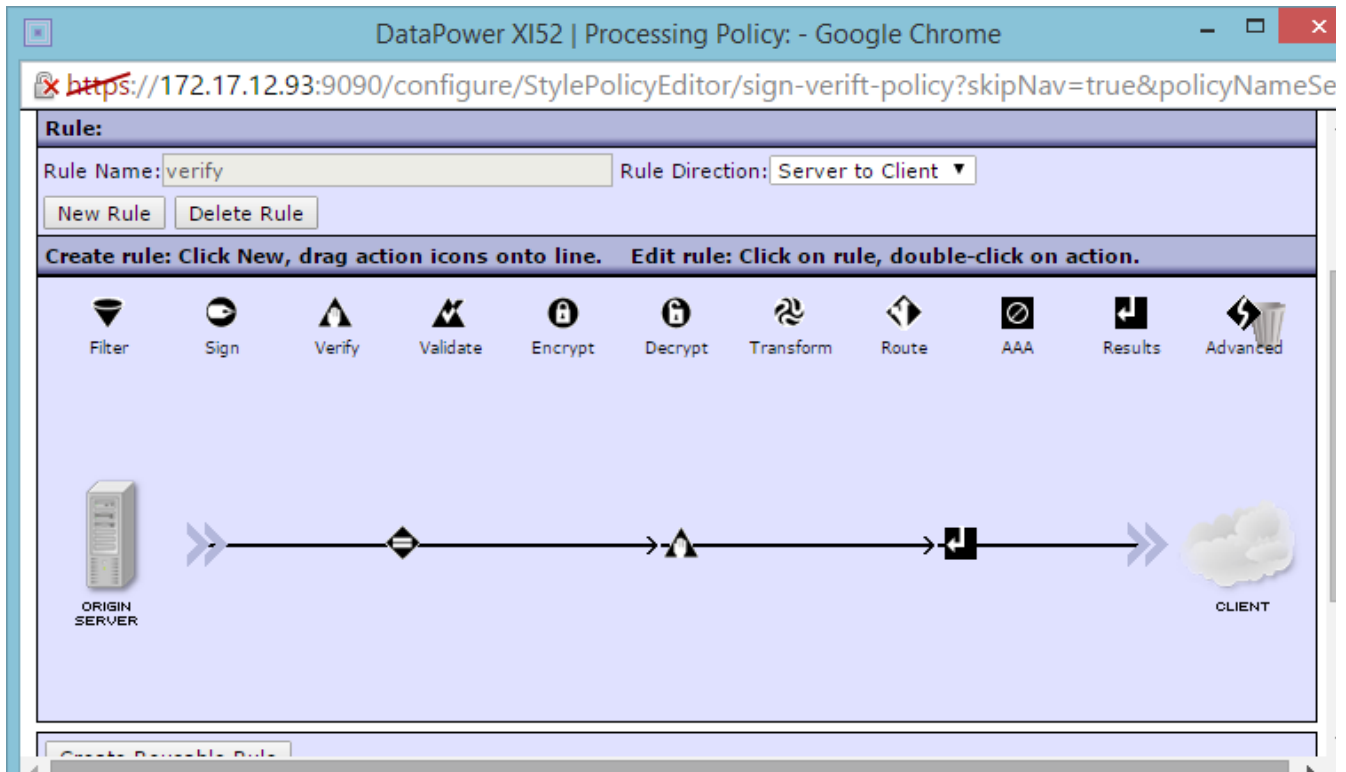
1.0 ☐ Save

Output

Output

(auto) (auto)

Create a **new rule** and configure it.
Then add **Result** action and then **Verify** action.
Let the rule direction be “**Server to Client**”.



Double click on verify to configure it.

Click on validation credential and upload the certificate.

WebSphere. DataPower XI52

IBM

Configure Verify Action

[Help](#)

Basic

Advanced

Input

Input

INPUT

INPUT ▼

*

Options

Verify

Asynchronous

on

off

Signature Verification Type

RSA/DSA Signatures ▼

☐ Save

Optional Signer Certificate

☐ Save

Validation Credential

cert1 ▼

+

...

☒ Save

Output

Output

OUTPUT ▼

Delete

Done












Cancel




Click on Apply policy after configuring both sign and verify






Rule:

Rule Name: Rule Direction:

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action.

 Filter
  Sign
  Verify
  Validate
  Encrypt
  Decrypt
  Transform
  Route
  AAA
  Results
  Advanced

 ORIGIN SERVER
 
 CLIENT

Configured Rules				
Order	Rule Name	Direction	Actions	
↑↓	sign	Client to Server	  	delete rule
↑↓	verify	Server to Client	 	delete rule

Create new Front side Protocol. Select HTTP Front Side Handler

Multi-Protocol Gateway Name

Sign-Verify *

Summary

Type

☐ dynamic-backends

☒ static-backend *

XML Manager

default ▾ + ... *

Multi-Protocol Gateway Policy

(none) ▾ + ... *

URL Rewrite Policy

(none) ▾ + ...

Back side settings

Default Backend URL

 *

MQ Helper

WebSphere JMS Helper

IMSConnect Helper

User Agent settings

Match	Property
Note: To edit the User Agent, please access via the XML Manager above.	

SSL Client Crypto Profile

(none) ▾ + ...

Front side settings

Front Side Protocol

(empty)

 ▾ Add + ...

 *

Create a New:

FTP Poller Front Side Handler

NFS Poller Front Side Handler

SFTP Poller Front Side Handler

FTP Server Front Side Handler

HTTP Front Side Handler

HTTPS Front Side Handler

IMS Callout Front Side Handler

IMS Connect Handler

WebSphere JMS Front Side Handler

MQTTE Front Side Handler


MQ Front Side Handler

SFTP Server Front Side Handler

Stateless Raw XML Handler

Stateful Raw XML Handler

Give the name and port number and select GET method and click Apply

 ~~https://~~172.17.12.93:9090/configure/HTTPSourceProtocolHandler/sign-verify-hand

Comments	<input type="text"/>
Local IP Address	<input type="text" value="0.0.0.0"/> <input type="button" value="Select Alias"/> *
Port Number	<input type="text" value="7329"/> *
HTTP Version to Client	<input type="text" value="HTTP 1.1"/> ▼
Allowed Methods and Versions	<div><input checked="" type="checkbox"/> HTTP 1.0 <input checked="" type="checkbox"/> HTTP 1.1 <input checked="" type="checkbox"/> POST method <input checked="" type="checkbox"/> GET method <input checked="" type="checkbox"/> PUT method <input type="checkbox"/> HEAD method <input type="checkbox"/> OPTIONS <input type="checkbox"/> TRACE method <input type="checkbox"/> DELETE method <input checked="" type="checkbox"/> URL with Query Strings <input checked="" type="checkbox"/> URL with Fragment Identifiers <input type="checkbox"/> URL with .. <input type="checkbox"/> URL with cmd.exe</div>
Persistent Connections	<input checked="" type="radio"/> on <input type="radio"/> off
Maximum Persistent Reuse	<input type="text" value="0"/>

Give the Backend URL and click Apply and then Save Config.

Multi-Protocol Gateway Name <input type="text" value="Sign-Verify"/> *	XML Manager <input type="text" value="default"/> + ... *
Summary <input type="text"/>	Multi-Protocol Gateway Policy <input type="text" value="(none)"/> + ... *
Type <input type="radio"/> dynamic-backends <input checked="" type="radio"/> static-backend *	URL Rewrite Policy <input type="text" value="(none)"/> + ...

Back side settings	Front side settings				
Default Backend URL <input type="text" value="http://172.17.12.93:21045"/> *	Front Side Protocol <input type="text" value="sign-verify-handler"/> ✕ <input type="text" value="sign-verify-handler"/> Add + ... *				
<input type="button" value="MQ Helper"/> <input type="button" value="WebSphere JMS Helper"/> <input type="button" value="IMSCONNECT Helper"/>					
User Agent settings					
<table border="1"><thead><tr><th>Match</th><th>Property</th></tr></thead><tbody><tr><td colspan="2">Note: To edit the User Agent, please access via the XML Manager above.</td></tr></tbody></table>	Match	Property	Note: To edit the User Agent, please access via the XML Manager above.		
Match	Property				
Note: To edit the User Agent, please access via the XML Manager above.					
SSL Client Crypto Profile <input type="text" value="(none)"/> + ...					
Response Type <input type="radio"/> JSON <input type="radio"/> Non-XML <input type="radio"/> Pass through <input checked="" type="radio"/> SOAP <small>SOAP 1.1</small>	Request Type <input type="radio"/> JSON <input type="radio"/> Non-XML <input type="radio"/> Pass through <input checked="" type="radio"/> SOAP <small>SOAP 1.1</small>				

Later test the service in SOAP UI

