ADDING TRANSFORMATION ACTION IN XML FIREWALL
(LOOPBACK)

1.Logging into WebGUI

2. Click on XML Firewall

3. Click on existing XML Firewall

Debug Probe is enabled, which impacts performance. Change Troubleshooting settings.

Configure XML Firewall

XML Firewall Name	Op-State	Logs	Req-Type	Local Address	Port	Resp-Type	Remote Address	Port
dynamic	up	🔍	XML	0.0.0.0	2169	XML		
first	up	🔍	Pass through	0.0.0.0	7271	Pass through		
loopback	up	🔍	Pass through	0.0.0.0	2172	Pass through		
Sample	up	🔍	Pass through	0.0.0.0	7272	Pass through		
Sample_firewall	down	🔍	XML	0.0.0.0	2141	XML	172.17.4.71	4547

Add Wizard   Add Advanced

4. Click on editing policy button

The running configuration of the domain contains unsaved changes. Review changes.
Debug Probe is enabled, which impacts performance. Change Troubleshooting settings.

Configure XML Firewall

General   Advanced   Stylesheet Params   Headers   Monitors   XML Threat Protection

Apply   Cancel   Delete   Clone | Export | View Log | View Status | Show Probe | Validate
                                                                 Conformance | Help
XML Firewall Service status: [up]

General Configuration

Firewall Name
simple *

Comments

Firewall Type
Loopback ▼ *

XML Manager
default ▼ [+] [...] *

Processing Policy
simple ▼ [+] [...] *

URL Rewrite Policy
(none) ▼ [+] [...]

Back End

With a loopback proxy back end type, there is no back end
server; the device is responding to the client.

Front End

Local address
0.0.0.0   Select Alias *

Port Number
2175 *

With this type, there is no back end server which needs
credentials from the device.

Reverse (Server) Crypto Profile
(none) ▼ [+] [...]

5. Drag and drop 'Transform Action' on 'Client to Server' policy.

6. Now double click on 'Tranform Action'.

7. Now click on upload button in Transform file

8. Now click on choose file and select '.xsl' file from the directory

9. Now click on continue

Status:
- local:///Sample.xsl has been uploaded successfully.

Continue
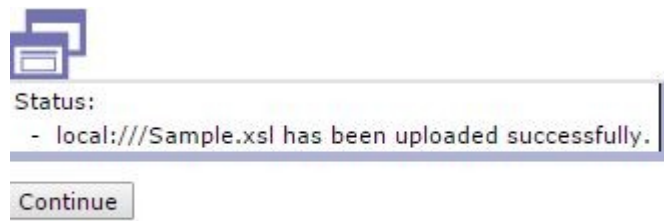
10. Select output as 'PIPE' and click on 'Done'.

Configure Transform with XSLT style sheet Action
Help

Basic   Advanced

Input

Input | (auto) | (auto) ▼ | *

Options

Transform with XSLT style sheet

Use Document Processing Instructions
○ Transform binary
○ Transform with a processing control file, if specified
○ Transform with embedded processing instructions, if available
● Transform with XSLT style sheet

Transform File | local:/// ▼
Sample.xsl ▼ | Upload... | Fetch... | Edit... | View... | Var Builder | *

URL Rewrite Policy | (none) ▼ | + | ...

Asynchronous | ○ on ● off

Output

Output | PIPE | PIPE ▼

Delete   Done   Cancel

11

11.　　Now click on 'Apply Policy'

Configure XML Firewall Style Policy

Policy:

Policy Name: simple   *

[Apply Policy] [Cancel]
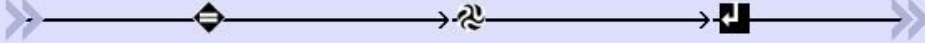
Export | View Log | View Status | Close Window |

Rule:

Rule Name: simple_request   Rule Direction: Client to Server ▼

[New Rule] [Delete Rule]

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

CLIENT

ORIGIN SERVER

[Create Reusable Rule]

		Configured Rules			
Order	**Rule Name**	**Direction**	**Actions**		
⬆⬇	simple_request	Client to Server	⬦　♻　⮐		delete rule

12.

12. Now click on 'Apply' and save config. Click on show probe.

Configure XML Firewall

General Advanced Stylesheet Params Headers Monitors XML Threat Protection

Apply Cancel Delete

XML Firewall Service status: [up]

General Configuration

Firewall Name
simple *

Comments
an example XML Firewall Service

Firewall Type
Loopback *

XML Manager
default + ... *

Processing Policy
simple + ... *

URL Rewrite Policy
(none) + ...

Back End

With a loopback proxy back end type, there is no back end server; the device is responding to the client.

With this type, there is no back end server which needs credentials from the device.

With this type, the response type is always "unprocessed".

Front End

Local address
0.0.0.0 Select Alias *

Port Number
2175 *

Reverse (Server) Crypto Profile
(none) + ...

Request Type
Pass through

13.   Now click 'Enable Probe' and Click on 'Send Message' to Test

WebSphere. DataPower XI52 IBM.

Refresh Flush Enable Probe Export Capture View Log Send Message Close

view   trans#   type   inbound-url   outbound-url   rule   client-ip

(no transaction recorded)

14. Test Service

Request

URL:

http://172.17.12.93:2175

| MQ Helper | WebSphere JMS Helper | IMSConnect Helper |

*

Request Headers:

Header Name	Value	
		Add

Request Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<Test>
<payload>Test Message</payload>
</Test>
```

Make Call

Response

Response Code:
200

Response Headers:

Response Body:

```
<Test
   xmlns:dpm="http://www.datapower.com/schemas/management"
   xmlns:dpfunc="http://www.datapower.com/extensions/functions"
>
   <payload>Test Message</payload>
</Test>
```