Table of Contents

1. Application Firewall

1.1 Introduction:

The Citrix Application Firewall appliance (also available as a feature on a Citrix® NetScaler® appliance) prevents security breaches, data loss, and possible unauthorized modifications to Web sites that access sensitive business or customer information. It does so by filtering both requests and responses, examining them for evidence of malicious activity and blocking those that exhibit it. Your site is protected not only from common types of attacks, but also from new, as yet unknown attacks.

In addition to protecting Web servers and Web sites from unauthorized access and misuse by hackers and malicious programs, the Application Firewall provides protection against security vulnerabilities in legacy CGI code or scripts, Web server software, and the underlying operating system.Most types of attacks against Web servers and Web sites are launched to accomplish either Obtaining private information or Obtaining unauthorized access and control.

Many types of attacks can be used to obtain private information from or make unauthorized use of your Web servers. These attacks include:

Buffer overflow attacks: Sending an extremely long URL, cookie, or other bit of information to a Web server in hopes of causing it or the underlying operating system to hang, crash, or behave in some manner useful to the attacker.

Cookie security attacks: Sending a modified cookie to a Web server, usually in hopes of obtaining access to unauthorized content by using falsified credentials.

Forceful browsing: Accessing URLs on a Web site directly, without navigating to the URLs via hyperlinks on the home page or other common start URLs on the Web site. Forceful browsing is normally used to gain access to unauthorized information, but can also include a buffer overflow attack and be used to compromise your server.

Web form security attacks: Sending inappropriate content to your Web site in a Web form. Inappropriate content can include modified hidden fields, HTML or code in a field intended for alphanumeric data only, an overly long string in a field that accepts only a short string, an alphanumeric string in a field that accepts only an integer, and a wide variety of other data that your Web site does not expect to receive in that Web form.

In addition to standard Web form security attacks, two specialized types of attacks on Web form security deserve special mention:

SQL injection attacks: Sending an active SQL command or commands in a Web form or as part of a URL, with the goal of causing an SQL database to execute the command or commands.

Cross-site scripting attacks: Using a URL or a script on a Web page to violate the same-origin policy, which forbids any script from obtaining properties from or modifying any content on a different Web site

Unknown Types of Attacks: The greatest threat against Web sites and applications does not come from known attacks. It comes from new and unknown attacks, attacks for which the Application Firewall may not yet have a specific check. For this reason, the Application Firewall does not have to rely only upon specific signatures and checks. It can compare requests and responses to a profile of the normal use of a protected Web site. You help create this profile by

providing certain information to the Application Firewall. The Application Firewall then generates the rest of this profile by using its learning feature. Thereafter, if a request or response falls outside of the profile for that Web site or application, either the threat in the request or response is neutralized, or the request or response is blocked.

This combination of signatures, specific checks, and a learned profile is called a hybrid security model.

1.2 Appfirewall checks in StoreFront template.

Here is a list of AppFirewall checks performed in StoreFront template to protect API requests in the XML format.

1.2.1 XML Schema validation:

The XML schema validation feature provides special defenses against attacks cotaining invalid XML requests. It examines the POST bodies of XML requests that are coming from API provided by StoreFront application using provided schema files. If the Application Firewall detects any user request not abiding the schema format, then it learn this request and logs the request.

2. Deploying Application Firewall Template (StoreFront)

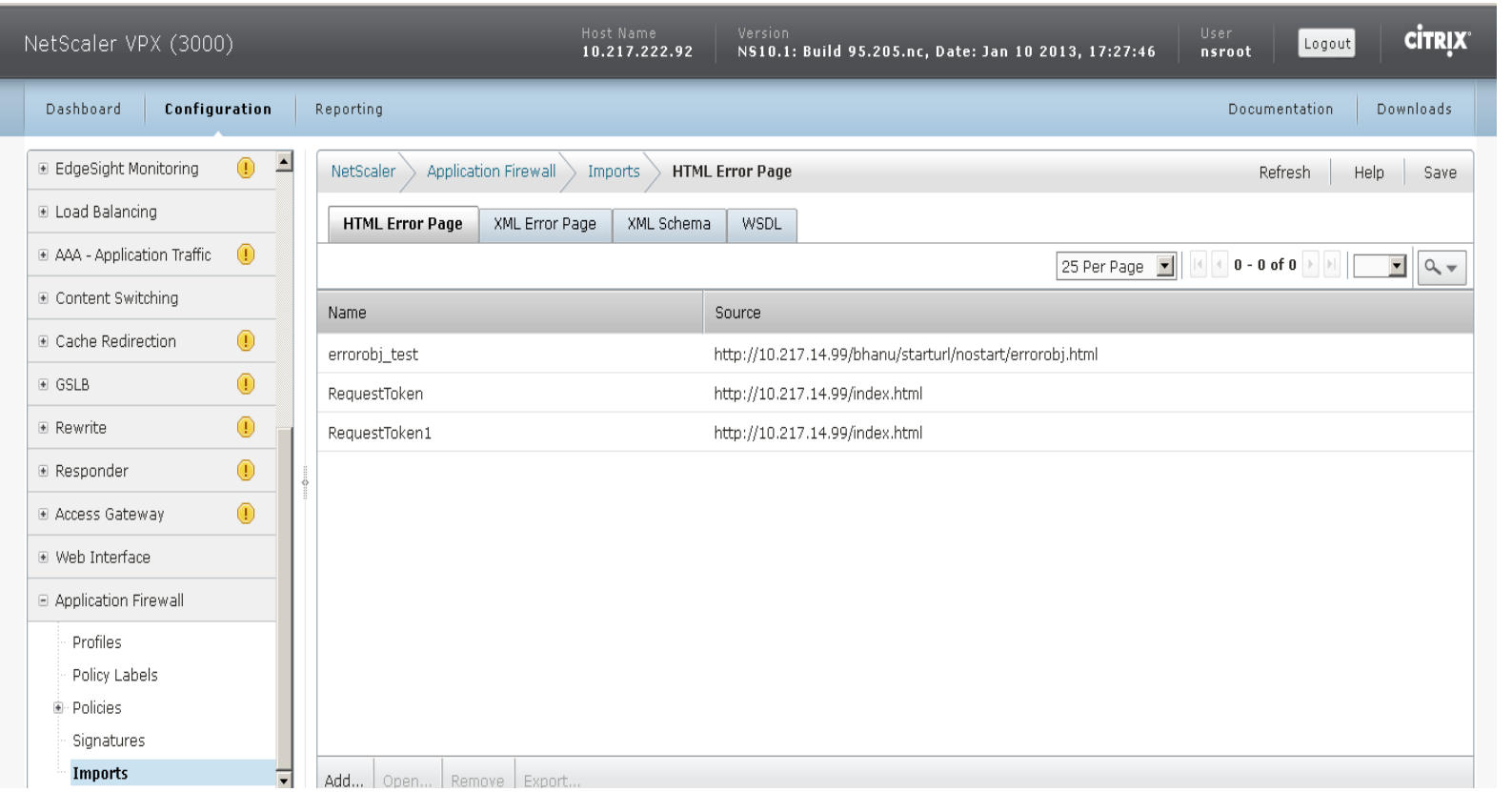
2.1 Pre-requisites :

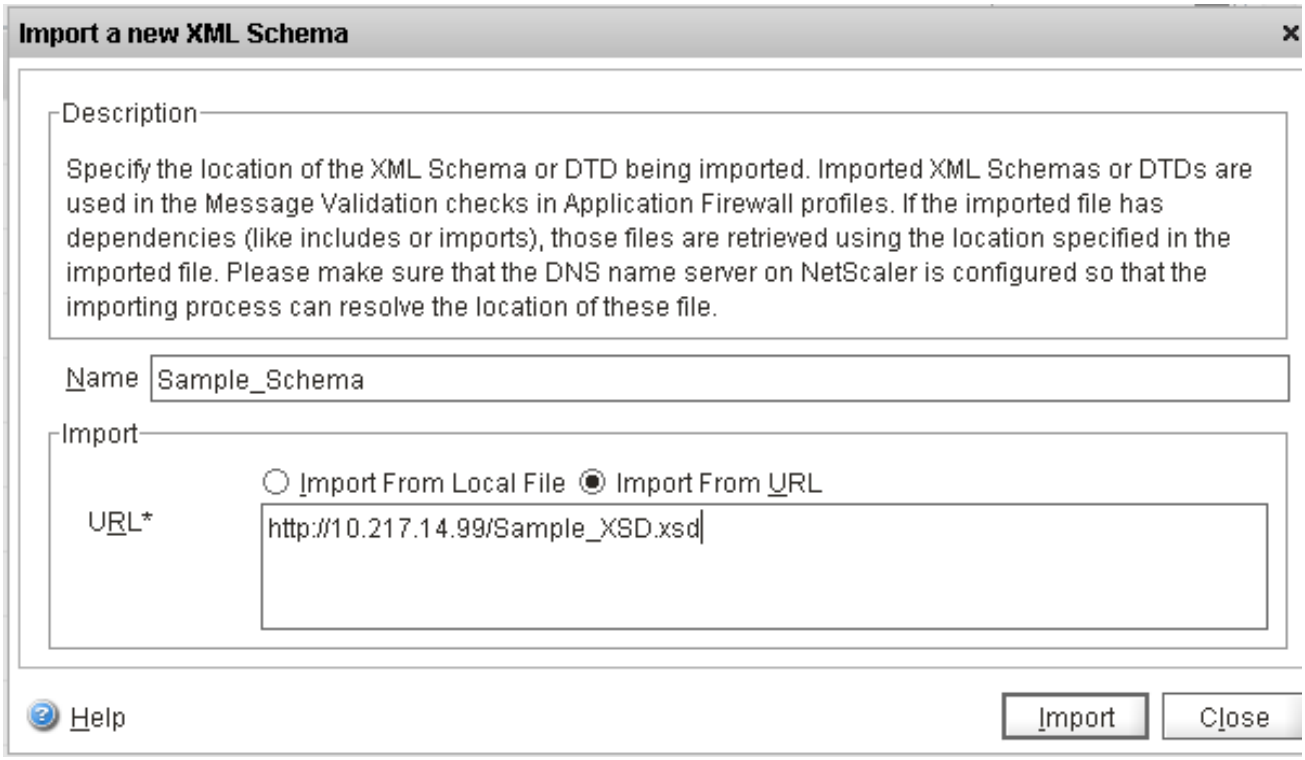
Before using StoreFront template for application firewall support, user need to do certain setup on netscaler box.

1) Download all the schema files available on publically shared location (Amazon S3 server, links below). Before importing StoreFront template user need to import these schema files one by one on the netscaler box as shown in below figures.
2) User has to give the respective names only as mentioned in the commands below to the schema files since the same name is used in the StoreFront template. There are total 22 schema files that user has to import before importing template.
3) Please make sure all the import commands are passed before proceeding with the App Exprt template deployement step.
4) Commands:

1) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/Accounts
2) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/Discovery
3) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/RefreshToken
4) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/RequestToken
5) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/CommonSchema
6) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/LaunchParams
7) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/RequestTokenResponse
8) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/ServiceRecord
9) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/SessionState
10) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/ClaimsPrincipal
11) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/DestroyToken

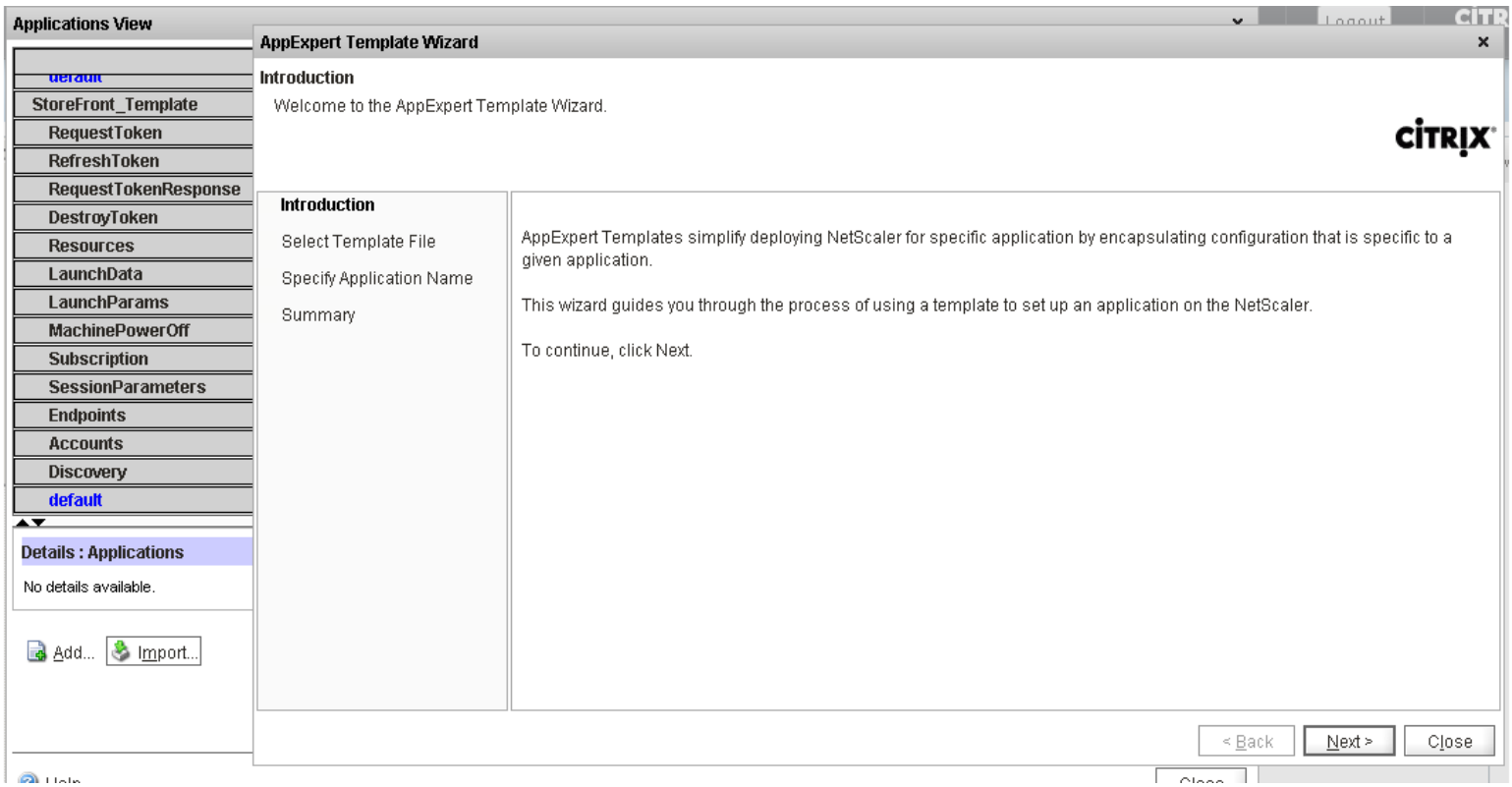
12) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/Endpoints
13) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/MachinePowerOff
14) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/Resources
15) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/SessionParameters
16) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/Subscriptions
17) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/DestroyTokenResponse
18) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/LaunchData
19) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/MachinePowerOffParams
20) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/RequestTokenChoices
21) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/SessionResult
22) import appfw xmlschema https://s3.amazonaws.com/AppC_Schema/SubscriptionsExport

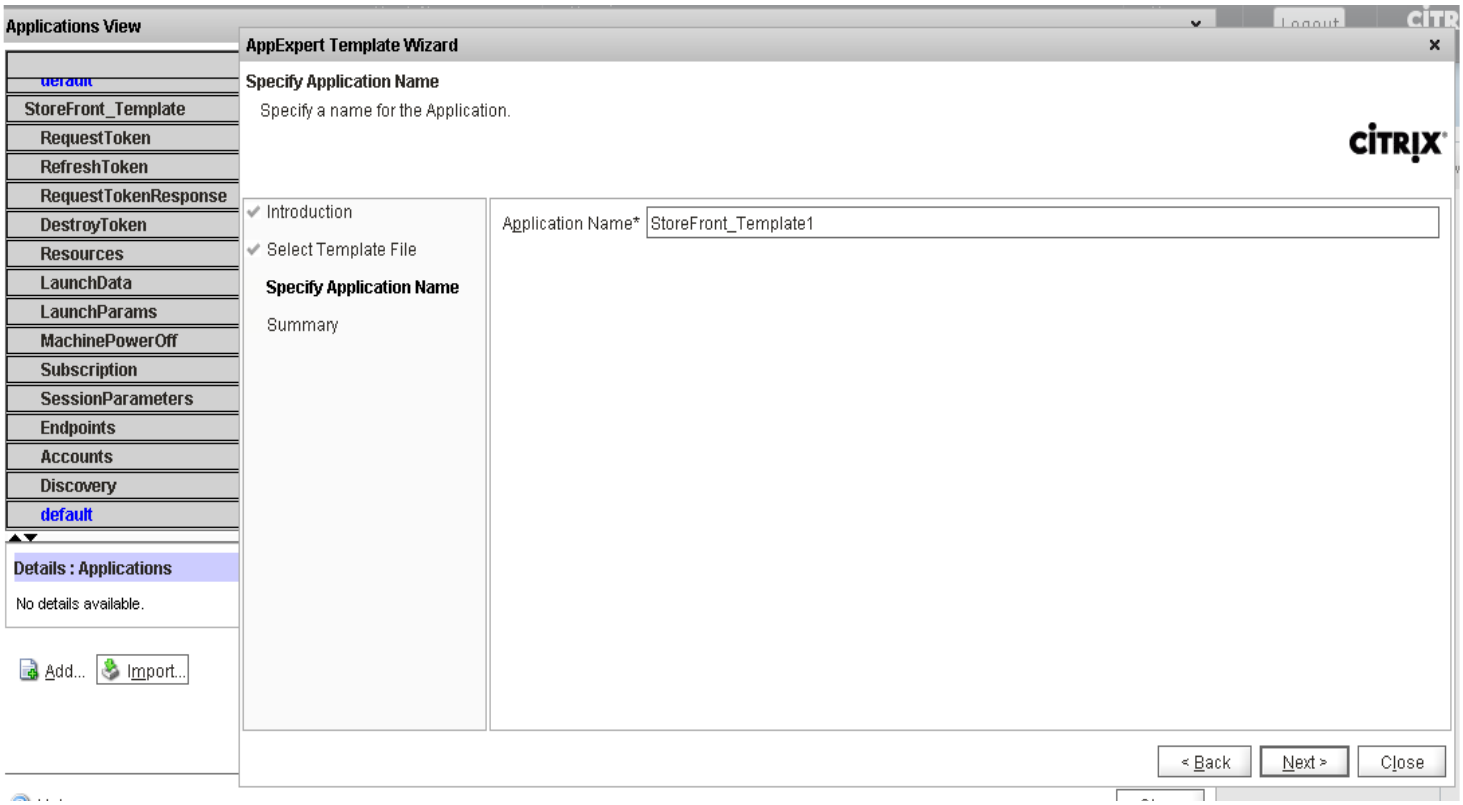


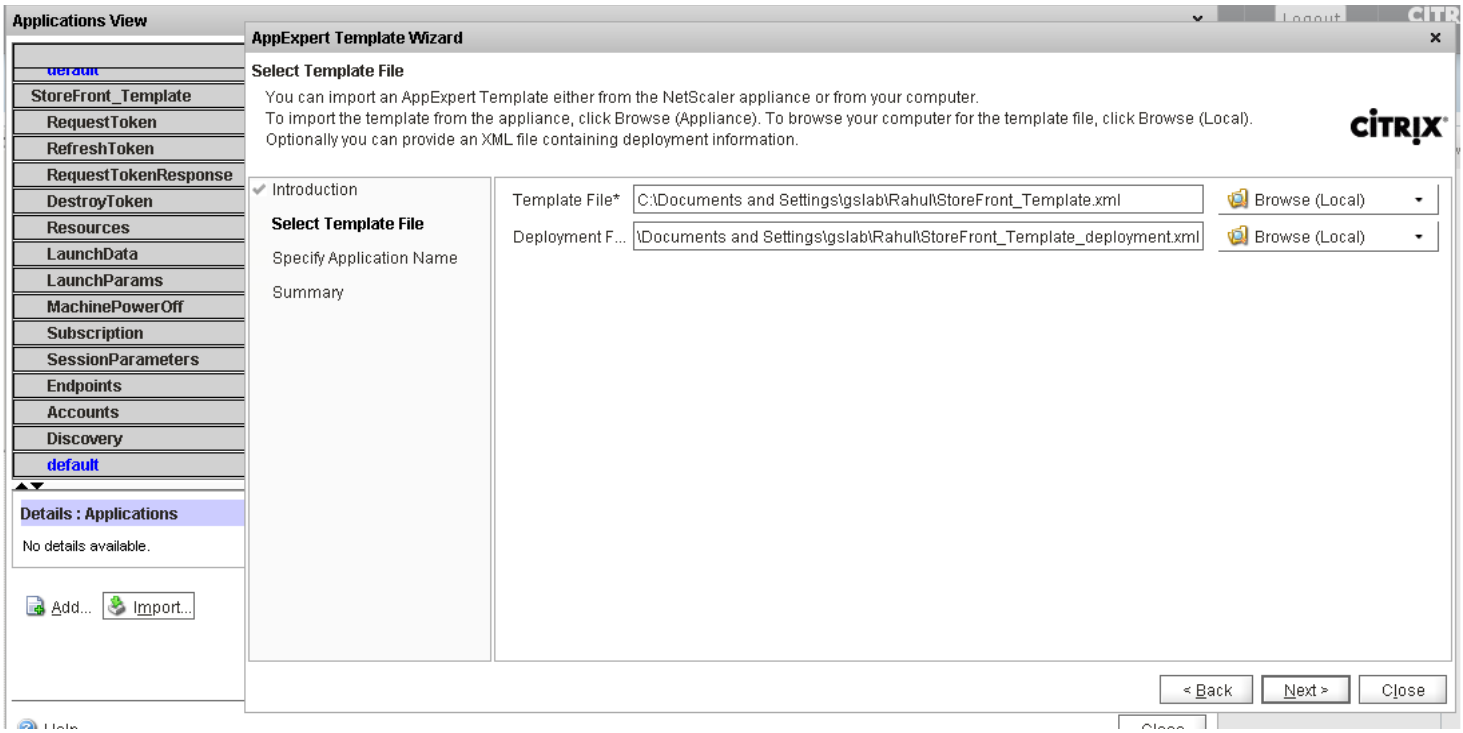


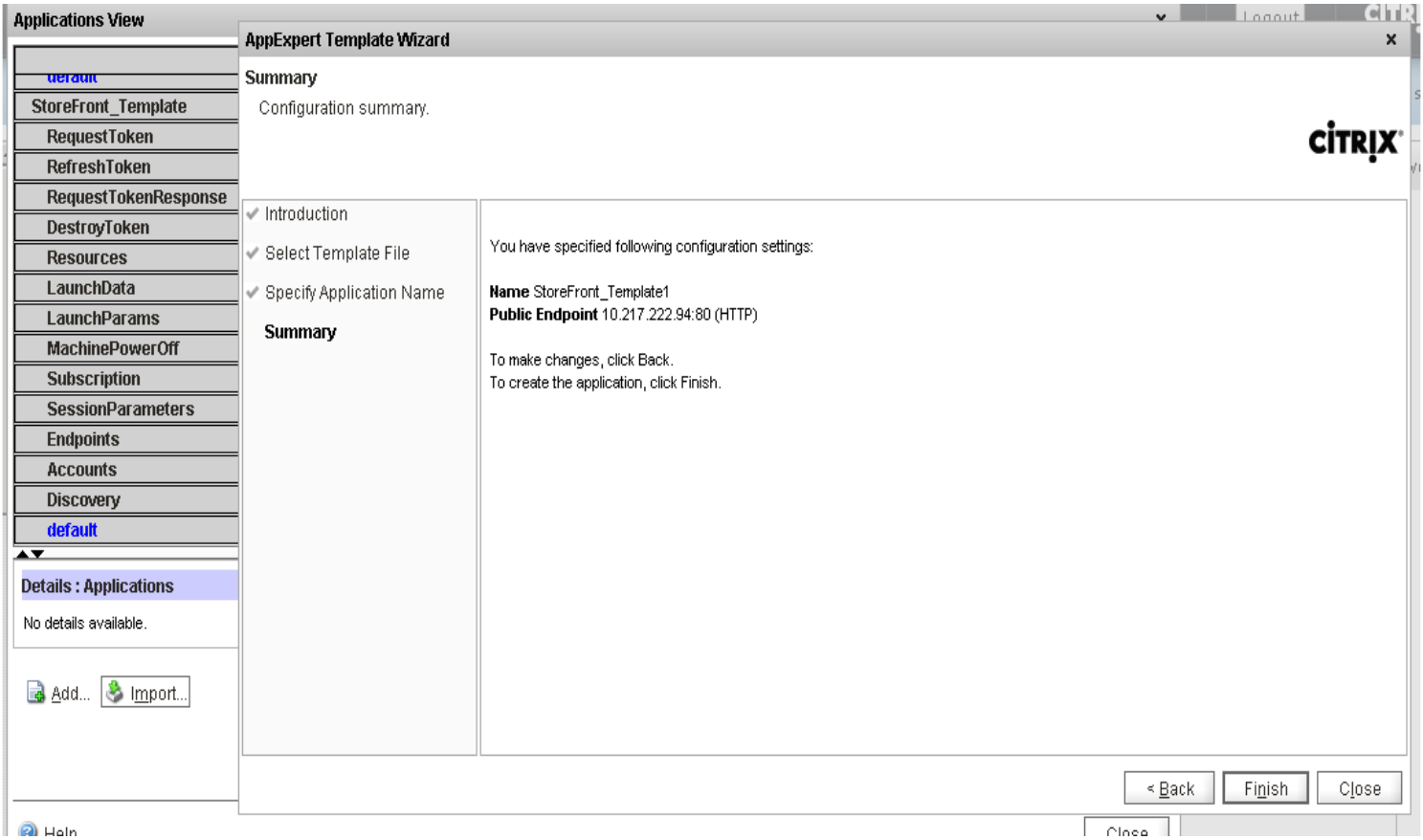
2.2 Deployment:

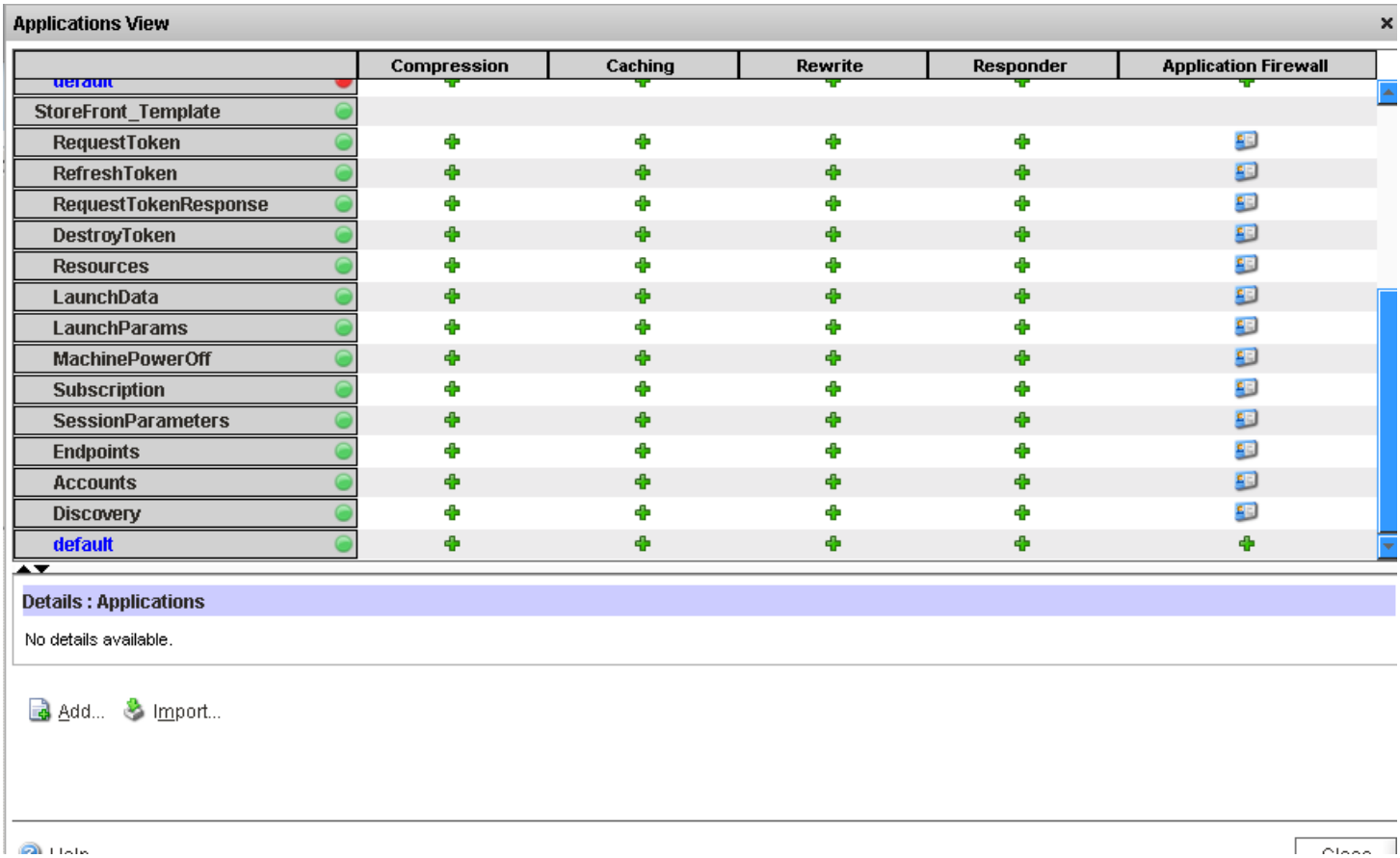
1) Deployment require 2 xml files.
    a. StoreFrontTemplate.xml
    b. StoreFrontTemplate_Deployment.xml (optional)
2. Following screen shot depict the functionality to import StoreFront Template.


Applications View
AppExpert Template Wizard
Introduction
Welcome to the AppExpert Template Wizard.
CITRIX
Introduction
Select Template File
Specify Application Name
Summary
AppExpert Templates simplify deploying NetScaler for specific application by encapsulating configuration that is specific to a given application.
This wizard guides you through the process of using a template to set up an application on the NetScaler.
To continue, click Next.
StoreFront_Template
RequestToken
RefreshToken
RequestTokenResponse
DestroyToken
Resources
LaunchData
LaunchParams
MachinePowerOff
Subscription
SessionParameters
Endpoints
Accounts
Discovery
default
Details : Applications
No details available.
Add...
Import...
< Back
Next >
Close


Applications View
AppExpert Template Wizard
Specify Application Name
Specify a name for the Application.
CITRIX
Introduction
Select Template File
Specify Application Name
Summary
Application Name*
StoreFront_Template1
StoreFront_Template
RequestToken
RefreshToken
RequestTokenResponse
DestroyToken
Resources
LaunchData
LaunchParams
MachinePowerOff
Subscription
SessionParameters
Endpoints
Accounts
Discovery
default
Details : Applications
No details available.
Add...
Import...
< Back
Next >
Close

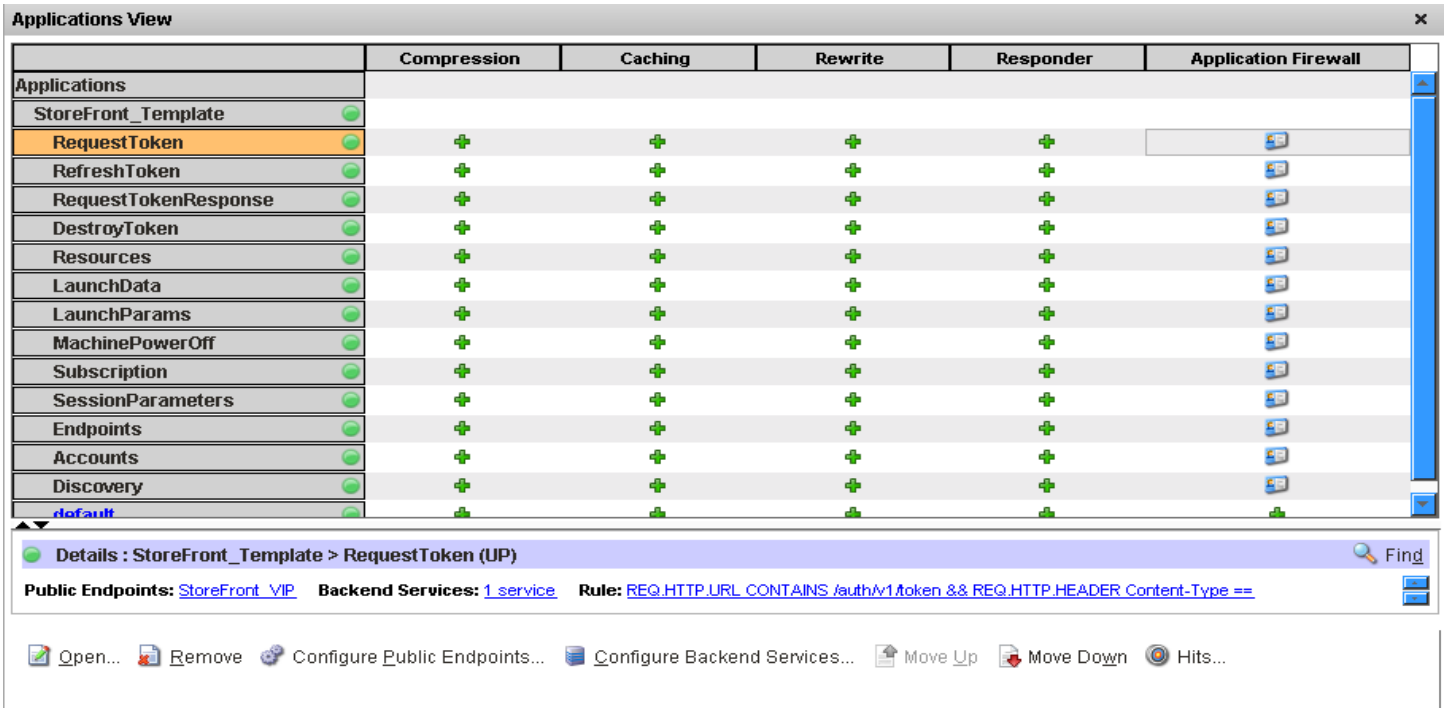

Applications View
AppExpert Template Wizard
Select Template File
You can import an AppExpert Template either from the NetScaler appliance or from your computer.
To import the template from the appliance, click Browse (Appliance). To browse your computer for the template file, click Browse (Local).
Optionally you can provide an XML file containing deployment information.
CITRIX
Introduction
Select Template File
Specify Application Name
Summary
Template File*
C:\Documents and Settings\gslab\Rahul\StoreFront_Template.xml
Browse (Local)
Deployment F...
\Documents and Settings\gslab\Rahul\StoreFront_Template_deployment.xml
Browse (Local)
StoreFront_Template
RequestToken
RefreshToken
RequestTokenResponse
DestroyToken
Resources
LaunchData
LaunchParams
MachinePowerOff
Subscription
SessionParameters
Endpoints
Accounts
Discovery
default
Details : Applications
No details available.
Add...
Import...
< Back
Next >
Close


Applications View
AppExpert Template Wizard
Summary
Configuration summary.
CITRIX
Introduction
Select Template File
Specify Application Name
Summary
You have specified following configuration settings:
Name StoreFront_Template1
Public Endpoint 10.217.222.94:80 (HTTP)
To make changes, click Back.
To create the application, click Finish.
StoreFront_Template
RequestToken
RefreshToken
RequestTokenResponse
DestroyToken
Resources
LaunchData
LaunchParams
MachinePowerOff
Subscription
SessionParameters
Endpoints
Accounts
Discovery
default
Details : Applications
No details available.
Add...
Import...
< Back
Finish
Close



2.3 Modifying AppFw for StoreFront Application Units through Wizard.

2.3.1 Following figure highlights one of the application unit (RequestToken) to which we can modify application firewall checks.



2.3.2 User can modify it by clicking on under application firewall column.After clicking on it will show pop-up window as shown below.

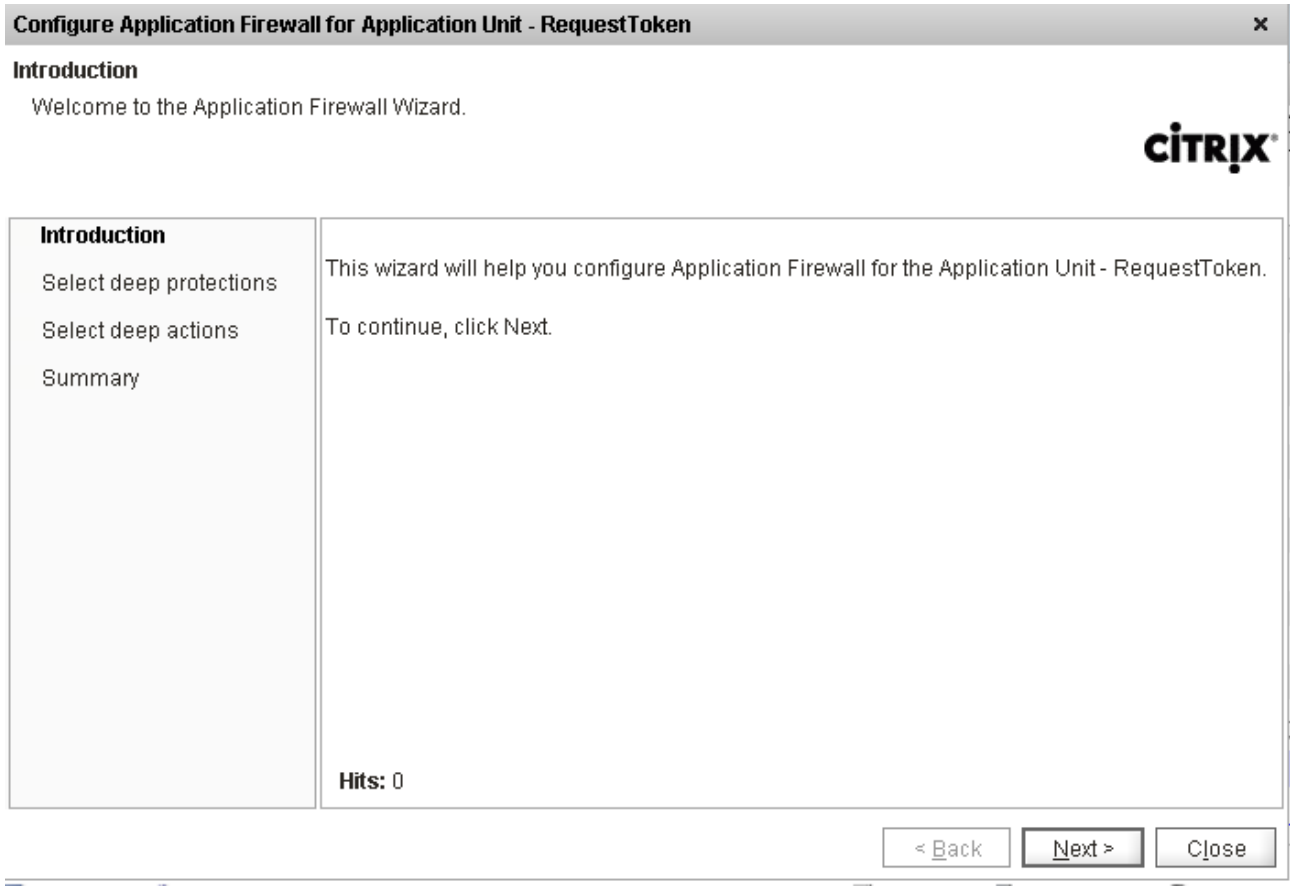


Figure 2.3.2

2.3.3 After clicking on next button it will redirect user to enable/disable the protection security checks which can be applied for selected application unit.

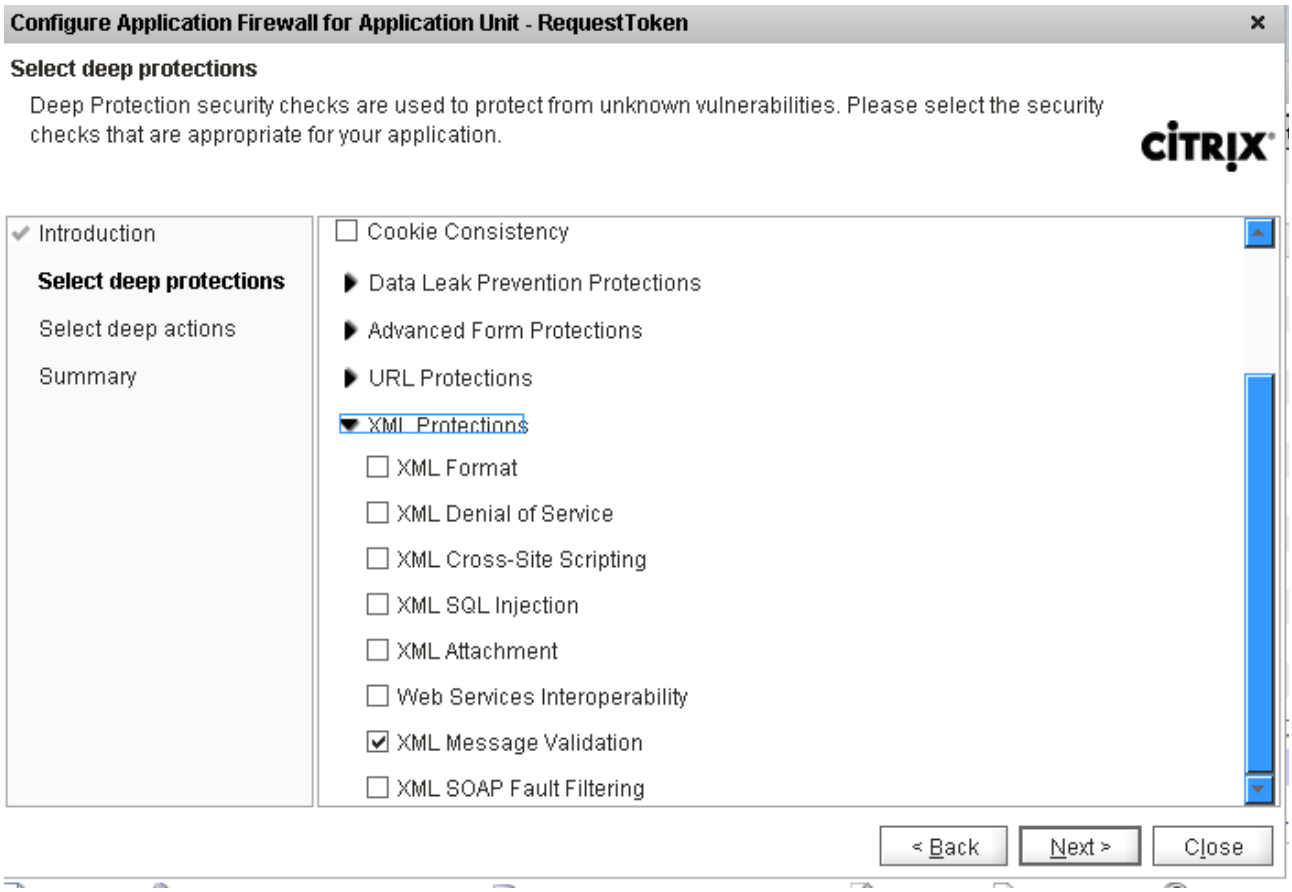


Figure 2.3.3

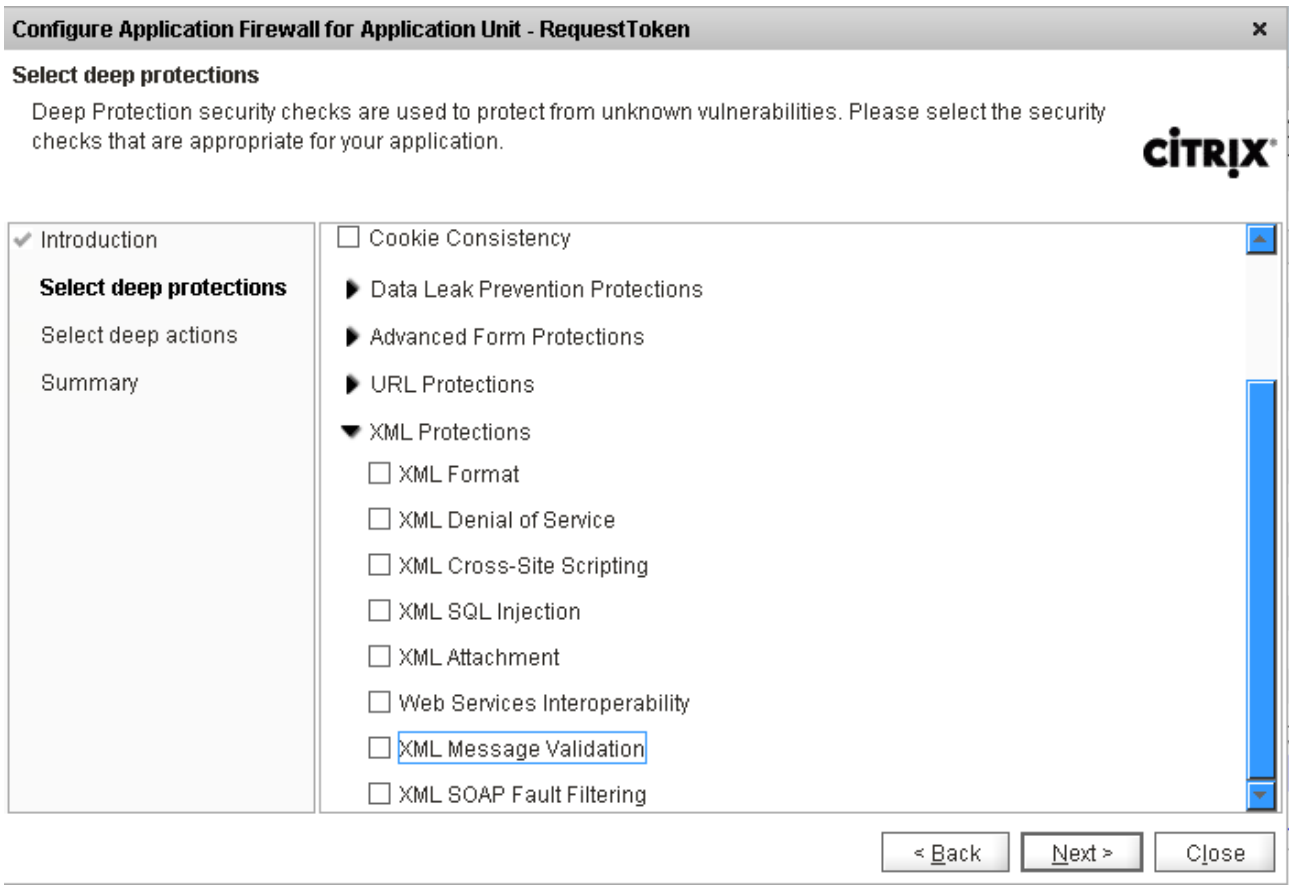


Figure 2.3.4

2.3.4 User can click on the next button to save newly configured settings.

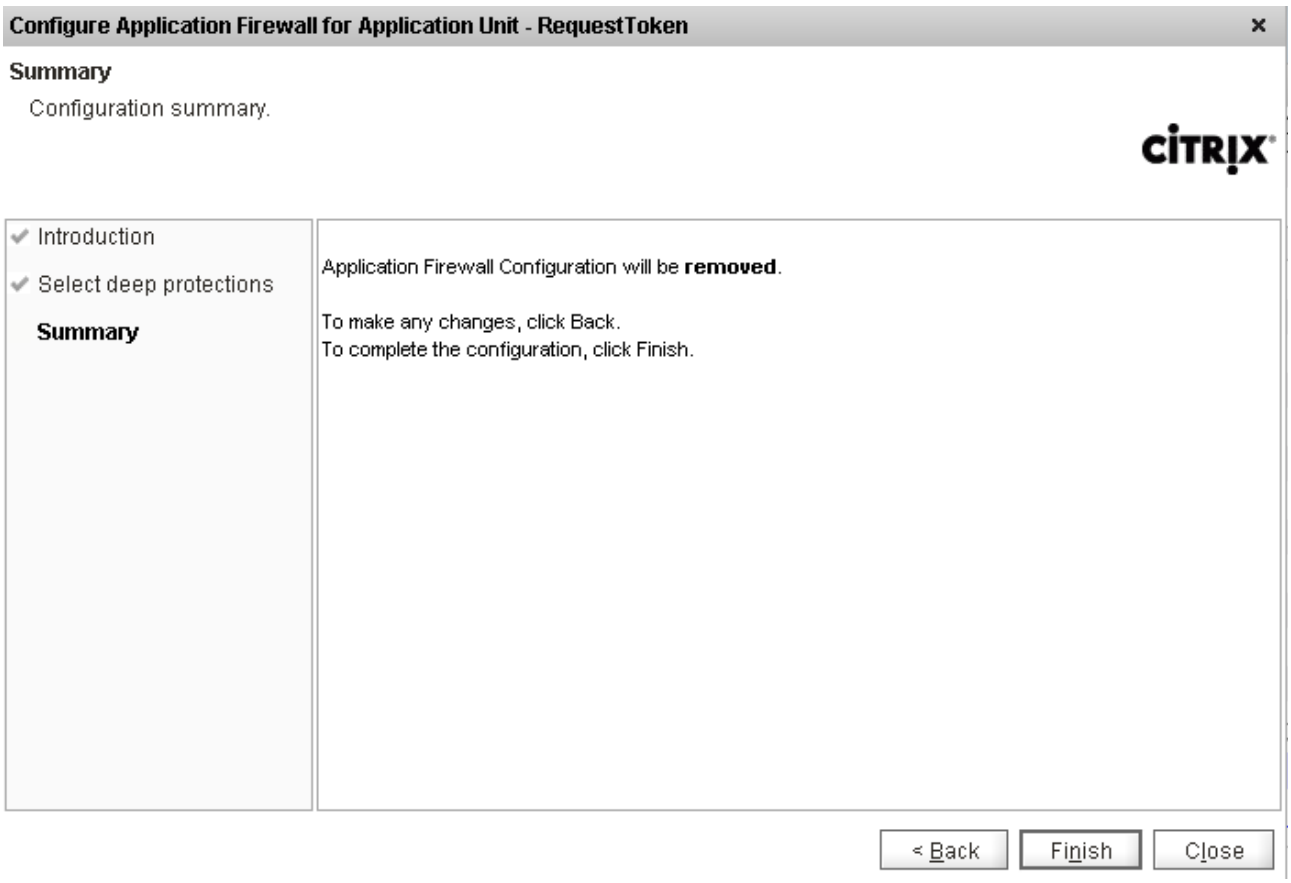


Figure 2.3.5

2.3.5 After clicking on finish button settings will get saved and pop-up for exit will appear.

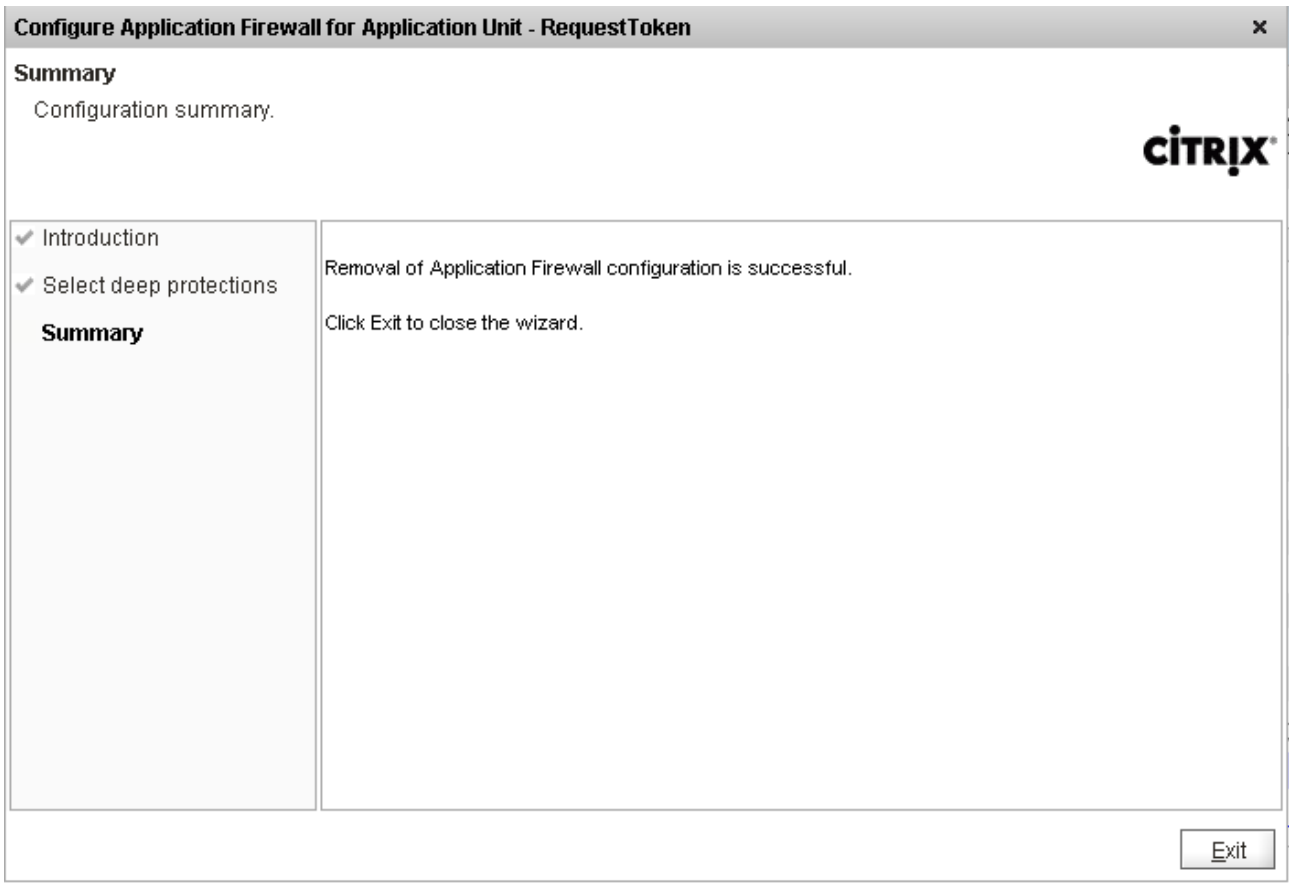


Figure 2.3.6

2.3.6 After clicking on exit button it will redirect user to configuration summary window.

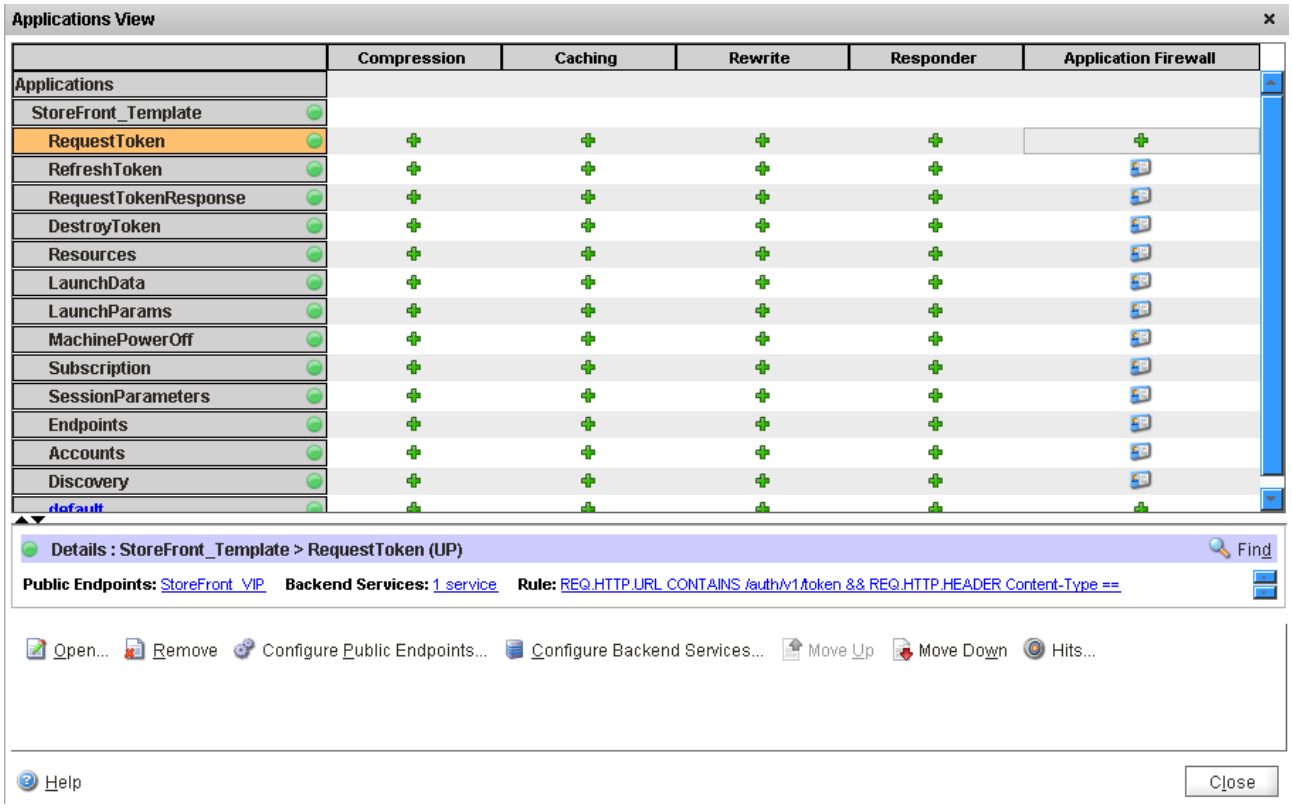


Figure 2.3.7