SAP NetWeaver Server with NetScaler for Load Balancing (SSL offload), Application Firewall and Integrated Caching

This solution guide focuses on deploying Citrix NetScaler with Load balancing (SSL offload), Application Firewall and Integrated caching for SAP NetWeaver server.
# Table of Contents

- **Introduction** 3
  - SAP Web Dispatcher Features 4

- **Topology** 4
  - NetScaler features 5
  - Other considerations and prerequisites 5
  - Summary of Steps 5

- **Solution Description** 6
  - Configuring SSL offload Load Balancing 6
    - Define the load balancing virtual servers (LB vservers) 6
    - Define LBVS server service group binding 7
    - Define Monitors 8
  - Configuring Application Firewall 8
    - Create Signatures 8
    - Application-firewall profile 9
    - Profile’s security checks 10
    - Profile's settings to bind signatures 11
    - Application firewall policy 12
    - Bind the Policy to load balancer 13
    - Monitor logs and tweak the configuration 15
  - **Optimization** 15
    - Configuring Integrated caching 15
    - Define Cache Content group and Cache Policy 17
    - Bind the Policy to load balancer 19
    - Monitor logs and Cache object details 19
  - **Verification** 21
  - **Conclusion** 21
Citrix NetScaler is a world class application delivery controller, with the proven ability to load balance, accelerate, secure and optimize enterprise applications.

SAP NetWeaver AS for ABAP 7.51 Innovation Package offers the foundation for the digital core that is SAP S/4HANA, on-premise edition, and for the standalone custom development of ABAP-based business applications.

Overview of SAP NetWeaver AS for ABAP 7.51 Innovation Package

SAP NetWeaver AS for ABAP 7.51 Innovation package intensifies the support of technology trends like the Internet of Things (IoT), Mobile, Cloud, Big Data and Analytics and offers a foundation for the easy and fast development of simple business applications. The innovations in ABAP together with improvements to SAP HANA-centric application development, SAP Fiori, IoT scenarios support and lifecycle management offer significant benefits.

Why NetScaler for SAP NetWeaver Server?

SSL Offload
NetScaler ADC is best suited for enterprise application delivery as it can do large scale SSL processing with best-in-class SSL performance. NetScaler supports latest ciphers like ECDSA for signature, ECDHE for key exchange with AES-GCM for bulk encryption-decryption. It also supports the latest security features like HTTP Strict Transport Security (HSTS), secure TLS session tickets, OCSP stapling amongst others.

In an SSL offload deployment, NetScaler creates a secure channel with the clients and can optionally have a secure channel with servers (in this case SAP NetWeaver). NetScaler offloads the servers from doing the costly SSL processing and thus allows servers to serve to more clients.

Application Firewall
Citrix® NetScaler AppFirewall™ is a comprehensive ICSA certified web application security solution that blocks known and unknown attacks against web and web services applications. NetScaler AppFirewall enforces a hybrid security model that permits only correct application behaviour and efficiently scans and protects against known application vulnerabilities. It analyses all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modification to applications.

NetScaler AppFirewall technology is included in and integrated with Citrix® NetScaler® MPX and VPX, Platinum Edition, and is available as an optional module that can be added to NetScaler MPX appliances running NetScaler Enterprise Edition. NetScaler AppFirewall is also available as a standalone solution on some NetScaler MPX appliances. The stand-alone NetScaler AppFirewall models can be upgraded via software license to a full NetScaler Application Delivery Controller (ADC).
**Integrated Cache**

The integrated cache provides in-memory storage on the Citrix NetScaler appliance and serves Web content to users without requiring a round trip to an origin server. For static content, the integrated cache requires little initial setup. After you enable the integrated cache feature and perform basic setup (for example, determining the amount of NetScaler appliance memory the cache is permitted to use), the integrated cache uses built-in policies to store and serve specific types of static content, including simple Web pages and image files. You can also configure the integrated cache to store and serve dynamic content that is usually marked as non-cacheable by Web and application servers (for example, database records and stock quotes).

**SAP Web Dispatcher**

It acts a ‘software web switch’, which can reject or accept connections for security purpose and load balances the requests in your SAP system. It is used for HTTPS requests as SSL offload load balancer.

Citrix NetScaler provides similar features which can replace SAP web dispatcher and they are listed below:

<table>
<thead>
<tr>
<th>S.No</th>
<th>SAP Web Dispatcher</th>
<th>Citrix NetScaler</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SSL offload Load Balancing</td>
<td>SSL offload Load Balancing</td>
</tr>
<tr>
<td>2</td>
<td>URL Filtering/URL rewriting</td>
<td>URL Responder/Rewrite</td>
</tr>
<tr>
<td>3</td>
<td>Web caching</td>
<td>Integrated Caching</td>
</tr>
<tr>
<td>4</td>
<td>N/A</td>
<td>Application Firewall</td>
</tr>
</tbody>
</table>


**Topology**

![Topology Diagram]
Configuring NetScaler

Products and version tested

<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP NetWeaver Innovation Package</td>
<td>7.51 SP02</td>
</tr>
<tr>
<td>NetScaler</td>
<td>11.1 and above (Platinum edition)</td>
</tr>
</tbody>
</table>

NetScaler features

The following NetScaler features are discussed in this deployment guide.

- Load balancing
  - SSL offload
- Application Firewall
  - Cookie Consistency check
- Optimization
  - Integrated Caching

Prerequisites and configuration notes

- Make sure you have installed platinum license on the NetScaler appliance.
- Make sure you have enabled, Web access for SAP NetWeaver server by using SAP NetWeaver client, refer below link on how to enable web access (https://blogs.sap.com/2014/02/06/how-to-configure-your-sap-gui-html-for-web-access)
- Configure your DNS settings properly:
  (Note that for the purposes of certificate-based authentication, all addressable hosts that are part of the network setup should have resolvable domain names, not just IP addresses.)

Summary of Steps

1. Create load balancing virtual server (SSL offload).
2. Create a service for local virtual server.
3. Define monitor for service.
4. Create signatures for the application firewall and enable the built-in rules in the web-iis category.
5. Create an application-firewall profile.
6. Configure the profile’s security checks to enable Buffer Overflow, XSS and SQL Injection protections.
7. Configure the profile’s settings to bind signatures and exclude file uploads from inspection, to prevent false positives.
8. Create an application firewall policy with an expression that identifies the traffic flowing to and from the application, and an action that applies the configured profile’s protections to the traffic.
9. Bind the policy to the load balancing virtual server.
10. Monitor logs and tweak the configuration. Deploy relaxation rules to avoid false positives if needed.
11. Optimization (Configure Integrated caching)
12. Define Cache Content group and Cache Policy
13. Bind the Policy to load balance
14. Monitor logs and Cache object details
Solution Description
Configuring SSL offload Load Balancing
A load balancing configuration consists of the definition of load balancing virtual servers (LB vServers), as well as services that are bound to the LB vServers. A service is simply a combination of a server and a protocol. To configure SSL offloading, you must enable SSL processing on the NetScaler appliance and configure an SSL based virtual server that will intercept SSL traffic, decrypt the traffic, and forward it to a service that is bound to the virtual server. SSL offload balancing at NetScaler is depicted in the below diagram.

1. Define the load balancing virtual servers (LB vServers)
Log into the NetScaler GUI. On the Configuration tab, navigate to Traffic Management>Load Balancing>Virtual Servers. For this deployment exercise, we are SSL offloading with one SAP NetWeaver instance. The following load balancing virtual server will be created as part of this configuration:

<table>
<thead>
<tr>
<th>Virtual Server Name</th>
<th>Details</th>
<th>Port</th>
<th>Protocol</th>
<th>Persistence</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_LB_SSL</td>
<td>SSL offload</td>
<td>443</td>
<td>SSL</td>
<td>NA</td>
</tr>
</tbody>
</table>

When defining a new LB vserver, you will be presented with the settings screen.
To enable an SSL-based LB vserver, you should add an SSL certificate and key pair. For this, you may use either a self-signed certificate generated on the NetScaler appliance or a CA (Certificate Authority) signed one. The steps for generating a self-signed certificate on the NetScaler are as follows –
1. Login to your NetScaler appliance via the Configuration Utility.
2. Select Traffic Management > SSL
4. Here, the wizard will lead you through the series of steps for generating the self signed certificate –
   1. Generate the private key
   2. Generate the CSR (Certificate Signing Request)
   3. Generate the Certificate (using the ns-root.cer NetScaler root certificate)
   4. Save the Certificate and Key pair
5. Alternatively, if a certificate and key pair is already available, the same can be added by navigating to SSL>Certificates and clicking on the Add button. For more details refer to http://support.citrix.com/article/CTX109260

2. Define LBVS server service group binding

Now click on the Load Balancing Virtual Server Service Binding tab in the Service and Service Groups section, or alternatively, click on Services in the Traffic Management>Load Balancing subsection and then, click on the Add button.

Every LB service is linked to a server; this can either be a new server or an existing server already defined in the Servers subsection under Load Balancing. Service groups extend this by allowing the creation of a group of services. An LB vserver can use a set of services or a service group.
Here, defines name for the service for SAP NetWeaver server instance, the IP address (or choose from a list in the case of an existing server) for the SAP NetWeaver server instance and the protocol they operate on as per the table below:

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Details</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_HTTP</td>
<td>SAP NetWeaver server</td>
<td>443</td>
<td>HTTP</td>
</tr>
</tbody>
</table>

- Recommended Best Practices: Name your server instances as per their role, not with the IP address
- As there will be multiple items linked to each application (LB vservers, services, policies among others), it is recommended that they be named appropriately for convenience.
3. Define Monitors
After defining services, the following monitors should be defined and bound to the appropriate services –

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Details</th>
<th>Type</th>
<th>Interval</th>
<th>Timeout</th>
<th>Monitor Expression</th>
<th>Receive String</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_HTTP_Mon</td>
<td>SAP NetWeaver Server</td>
<td>HTTP</td>
<td>5</td>
<td>4</td>
<td>GET /sap/bc/gui/sap/its/webgui</td>
<td>SAP NetWeaver server is UP</td>
</tr>
</tbody>
</table>

You should enable Health Monitoring if you would like to have NetScaler poll the server periodically to verify its health – it is recommended that this setting should not be disabled except for diagnostic purposes. If Health Monitoring is disabled, the appliance shows the server UP at all times.

Bind these service groups to the appropriate LB vservers and confirm that they have been bound correctly by checking the same in the LB vserver Basic Settings screen. Add all the SAP NetWeaver servers to be load balanced and bind them to the appropriate load balancing virtual server.

Finally, the LB vservers created will be displayed on the configuration screen to the right in the same screen that is obtained by accessing Traffic Management>Load Balancing>Virtual Servers. This completes essential SSL offload balancing configuration for SAP NetWeaver Server.

Configuring Application Firewall
4. Create Signatures
Make a copy of the application firewall default signatures by clicking on Export under the Action dropdown on the AppFirewall Signatures screen at Security>AppFirewall>Signatures.
Now, add a signature by clicking on Add above, then edit the name and add comments so that the rule is distinguishable. Use the Show/Hide button to select web-iis to isolate all the rules for this Category. By default, the signature rules are disabled. Click the down-arrow on the Action button, and select Enable All Searched Rules to enable all the selected rules. (The following example shows SAP_APPFW_Signs as the signature name)

5. Application-firewall profile
Add a basic application firewall profile for the SAP NetWeaver by navigating to Security> Application Firewall> Profiles and clicking on Add. Use a meaningful name to keep track of the purpose of the profile. Set the profile type to Web Application and Defaults to Basic. (The following example shows SAP_APPFW_profile as the profile name.)
6. Profile’s security checks
Configure the security checks of the newly added profile by clicking on the profile name and clicking on Edit on the profile list page. Enable the Log, Learn, and Stats actions for the Cookie Consistency, SQL Injection and Cross-Site Scripting checks. Enable Log and Stats actions for the Buffer Overflow check. Disable all actions for the rest of the security checks. After analysing the logs enable Block on the above security checks.

As SAP NetWeaver server uses cookies for login access and to make it secure, select Cookie Consistency and click on Action settings to enable Transform action apart from other selected actions and select Encrypt all from drop down of Encrypt server cookies to encrypt both session and persistent cookies, decrypt any encrypted cookies as shown below.
(Note: When encrypting cookies, the application firewall adds the Http Only flag to the cookie. This flag prevents scripts from accessing and parsing the cookie. The flag therefore prevents a script-based virus or trojan from accessing a decrypted cookie and using that information to breach security. This is done regardless of the Flags to Add in Cookies parameter settings, which are handled independently of the Encrypt Server Cookies parameter settings.)

### Cookie Consistency Settings

<table>
<thead>
<tr>
<th>Actions</th>
<th>Log</th>
<th>Stats</th>
<th>Learn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transform</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Transform

- **Encrypt Server Cookies**
  - Encrypt All
- **Proxy Server Cookies**
  - None
- **Flags To Add in Cookies**
  - None

7. **Profile's settings to bind signatures**

Configure the profile's settings. Bind the signatures to the profile and select the check box for Exclude Uploaded Files from Security Checks and select the above created signatures.
8. Application firewall policy

Now, navigate to Security>Application Firewall>Policies> Application Firewall Policies. Create an application firewall policy for the SAP_APPFW profile and bind the policy to the LB vserver.

The following example uses the expression HTTP.REQ.HOSTNAME.EQ("sapwebgui.domain.com") to select the target traffic. (Create a DNS entry pointing to vserver ip with your domain.)
9. Bind the Policy to load balancer
On the policy listing screen, select the newly added policy and click Policy Manager. From the Bind Point options, select Load Balancing Virtual Server. The Virtual Server field now becomes visible. From this field’s drop-down list, select the SAP_LB virtual server that you created earlier. Click Continue to display the Bind Point pane.
In the Select Policy field, click the arrow to display the policy options. Select the SAP_APPFW_pol policy and click Select. Click Bind.

Now, in the Bind Point pane, click Done.
10. Monitor logs and tweak the configuration

In the Application Firewall Policies pane, refresh the page. A Green check mark appears in the Active Column to indicate that the policy is now active.

The SAP web GUI application is now protected by the application firewall. You can monitor the / var/log/ns.log to verify whether any violations are being detected, and fine-tune the security check configuration by adding relaxation rules if needed.

Optimization

11. Configuring Integrated caching

To configure caching, you can use the integrated wizard that makes configuration very straightforward. To initiate the wizard, navigate to Optimization>Integrated Caching as shown in the next screenshot.
Here, you can initiate the Caching Wizard under Getting Started.

**Caching Wizard**

**Specify Content Type**

Specify Content Type*

- Static Content

Select Static Content if requests sent to URL always returns the same content.

The following list contains some examples of static content:
- Style Sheets - /layouts/styles/front.css,
- Scripts - /scripts/helper.js,
- Images - /resources/graphics/thumbnail.gif

[Continue] [Cancel]
12. Define Cache Content group and Cache Policy
The above step requires you to specify the content type, which can be either static (examples given) or dynamic. Helpful hints are provided as shown above to help determine which type of content is relevant for you.

The next step involves defining which content should be cached. The Frequently Used Expressions dropdown helps you define the correct expression; however, if you want the caching policy to apply to all content, you can use ns_true as the expression. (shown in the screenshot below)

The next screen allows you to define when content expires. This can be custom (a defined interval) or heuristic (NetScaler makes the determination based on a percentage of the time since the object was last modified, with a deadline to be set that in used in case the heuristic measurement cannot be made).
The next step involves definition of the caching space to be used on the NetScaler appliance and the minimum size of objects to be cached.
13. **Bind the Policy to load balancer**

Finally, the cache policy should be bound to the relevant vserver. These definitions can be made under Cache Policies as shown in the screen shot below.

![Static Content Caching Wizard](image)

For the SAP NetWeaver deployment, the following settings have been used for caching –
- **Policy Name**: SAP_Cache1_policy
- **Actions**: CACHE
- **Cache Content Group**: SAP_Cache1_policy
- **Undefined-Result Action**: -Global-undefined-result-action (or NOCACHE/RESET)
- **Expression**: SYS.EVAL_CLASSIC_EXPR("ns_true")

**Cache Content Group:**
- **Name**: SAP_Cache1_policy
- **Type**: HTTP
- **Expiry Method**: Heuristic (Recommended)/Custom (if specific settings are required)
- **Default Expiry Times**: As per requirement; set to 233 for test deployment.
- **Parameterization**: Leave values as is (unless Cache selectors are in use; not configured for our test setup)
- **Memory**: Define values as per your system limits
- **Others**: Use default settings. All settings have context-sensitive help available if modification is required.

14. **Monitor logs and Cache object details**

Now check the SAP_Cache1_policy statistics for number of hits to validate caching as displayed in next screen-shot.
To view cache objects, select View Cache Objects under Cache Object to know more details.

The SAP web GUI application is now under integrated caching. You can monitor logs to verify whether all the required details are cached to optimize performance.
Verification
The functioning solution can be verified by navigating to https:// DNS name (sapwebgui)/sap/bc/gui/sap/its/webgui. This will show the SAP NetWeaver Secure Console login screen and logs to check App firewall security and optimization by caching.

Conclusion
Citrix NetScaler enables highly available SAP NetWeaver deployments with its SSL offload balancing capabilities, cookie based application firewall security and caching allowing all the various services provided by SAP to be load balanced and secured.
With NetScaler, enterprises enable high availability for their SAP environments, with extend capabilities for security and optimized access. The policy engine used by NetScaler enables enterprises to deploy any specific use cases that they may require, making the NetScaler solution a flexible and robust one that can meet all enterprise requirements.
To learn more about how NetScaler can bring these benefits to SAP installations or address other application delivery requirements, please visit http://www.citrix.com.

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2016 of $3.42 billion, Citrix solutions are in use at more than 400,000 organizations and by over 100 million users globally. Learn more at www.citrix.com
Copyright © 2017 Citrix Systems, Inc. All rights reserved. Citrix, NetScaler and NetScaler VPX are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.