Thunder Series for SAP Enterprise Portal (Formerly SAP NetWeaver Portal)

Table of Contents

Disclaimer

Introduction

SAP, the global market leader in business resource planning and business management, has multiple applications that are integrated and certified with the A10 Thunder™ ADC product line. SAP applications and services enable companies of all sizes to work together more efficiently and use business insight more effectively.

This document shows how A10 Thunder ADC can be deployed with the SAP Enterprise Portal (formerly known as the SAP NetWeaver Portal). The solution shown in this document is based on the vThunder™ ADC running on an Amazon Web Services (AWS) cloud infrastructure. The solution is also applicable for Thunder and AX Series ADC hardware appliances, other vThunder editions, and the Thunder Hybrid Virtual Appliance (HVA). Since the SAP Enterprise Portal application is based on Application Server (AS) Java, deploying the A10 solution as a server load balancer (SLB) will enhance the performance of the SAP Enterprise Portal cluster. This deployment guide provides detailed configuration steps on how to administer the Thunder ADC with SAP Enterprise Portal systems.

Deployment Guide Prerequisites

This deployment guide was tested with the following:

A10 Networks

- Thunder ADC version 2.7.1 P3 or higher

SAP

- SAP Enterprise (NetWeaver) Portal 7.x
  - ***Note**: This guide uses the NetWeaver name frequently. SAP states that there is no functionality difference with the rebranding from "NetWeaver" to "Enterprise."*

***Note**: For additional deployment options and features that the A10 Thunder ADC can support, please visit the following URL:* http://www.a10networks.com/solutions/enterprise_data_center_solutions.php

Application Specific Deployment Notes

This section of the deployment guide provides implementation and deployment tips on how to expedite deployment of SAP NetWeaver Portal and A10 solutions.

1. The A10 load-balancing solution can be deployed in a single, active/active, active/standby or multi-cluster load balancing mode using an AX Virtual Chassis System (aVCS) with the SAP NetWeaver Portal.
2. SSL Offload using the Thunder ADC is recommended to free up the rigorous SSL processing requirements of the SAP NetWeaver Portal. When an SSL request is initiated, SSL processing requires that every request be decrypted within the initial SSL handshake. A10 SSL security processors are available in most of the Thunder ADCs, which are specially designed to accelerate the repetitive computational processing used to decrypt each SSL request. A10 also offers non-SSL ADC models, which provide the same service for low traffic SSL processing requirements. Refer to A10's ADC datasheets for more information.
3. The SSL traffic (HTTPS) is terminated in the ADC appliance as a reverse proxy. The traffic is then sent to the SAP backend server via unencrypted traffic (HTTP). This configuration allows the reverse proxy to become the defense point for outside attacks.
4. The Web Application Firewall (WAF) feature has been tested within the SAP and A10 solutions. The test was successful and the configuration details of the WAF solution will be included in the WAF section of this guide. Some of the WAF solutions such as credit card scrubbing and SSN scrubbing are features that can be deployed within NetWeaver to intelligently protect Web applications from attacks and vulnerabilities.
5. The ADC Distributed Denial of Service (DDoS) mitigation feature was deployed in the SAP test bed, and Thunder ADC was able to protect the NetWeaver Portal from DDoS attacks. The DDoS feature consumes a low amount of CPU resources and can be enabled as needed. This is highly recommended, especially when the NetWeaver application is deployed within the DMZ.

6. SSL session caching (a.k.a. SSL session ID reuse) is an SSL enhancement that provides better SSL performance, and it is included in this deployment guide as an optional feature.
7. Optimization features such as TCP connection reuse and RAM caching are also available to be deployed within the Thunder ADC device.
8. Within the NetWeaver Portal deployment, we have configured the sample configuration to be deployed to Offload SSL encryption and decryption (HTTPS-to-HTTP).

Accessing the Thunder Series Load Balancer

This section describes how to access the Thunder Series device, which can be accessed either from a command-line interface (CLI) or graphical user interface (GUI):

- CLI – Text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or over the network using either of the following protocols:
  - Secure protocol – SSH version 2
  - Unsecure protocol – Telnet (if enabled)
- GUI – Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using the following protocol:
  - Secure protocol – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

  ***Note**: HTTP requests are redirected to HTTPS by default on the Thunder ADC device.*
  - Default username: "*admin*"
  - Default password: "*a10*"
  - Default IP address of the device: "*172.31.31.31*"

For detailed information about how to access the Thunder Series device, refer to the document "*A10 Thunder Series System Configuration and Administration Guide.pdf.*"

Amazon Web Services Configuration

The A10 and SAP NetWeaver Portal solution has been deployed and tested with vThunder within an Amazon Web Services (AWS) infrastructure. The following important notes should be considered when the A10 solution is deployed within AWS.

Samples shown below represent the configuration required on the primary interface using CLI only. AWS requires that the primary interface be in Dynamic Host Configuration Protocol (DHCP), and it can be utilized as single management IP for management, virtual IP (VIP) and source NAT (SNAT).

The following commands are required:

```
interface ethernet 1
ip address dhcp
```

After the initial login, you will also need to specify the specific TCP ports being used, since port 80 is used for data traffic by default.

The following commands are required for interface ethernet 1:

```
web-service server
web-service port 8080
web-service secure-server
web-service secure-port 8443
```

The following command is required for NAT pool using interface ethernet for SNAT:

```
ip nat pool if SNAT use-if-ip ethernet 1
```

For VIP configuration, the configuration below is required:

```
slb virtual-server v1 use-if-ip ethernet 1
port 80 http
system pbslb bw-list loic
system pbslb over-limit lockup 5 logging 10
```

***Note**: If you are interested in A10 vThunder AWS, you can access the AMI build on AWS Marketplace at:*
https://aws.amazon.com/marketplace/pp/B00HQP4WMO/ref=portal_asin_url

There are different A10 offerings within AWS Marketplace. These range from 10 Mbps, 50 Mbps, 100 Mbps, 200 Mbps, and 500 Mbps. You will also find Buy Your Own License (BYOL) options.

AWS documentation is available at the following links below:

vThunder AWS Installation Guide
https://www.a10networks.com/resources/files/vThunder_AWS_Install_Guide.pdf

vThunder for AWS Product Overview
http://www.a10networks.com/products/vThunder_Amazon_Web_Services.php

Architecture Overview

The network topology in Figure 1a and 1b are sample diagrams of how SAP NetWeaver Portal can be deployed in a regional data center. Other redundancy options can be paired with A10 Thunder ADC and SAP cloud solutions for additional redundancy as a failover site or deployed as a traffic load sharing site using Global Server Load Balancing (GSLB) protocol.

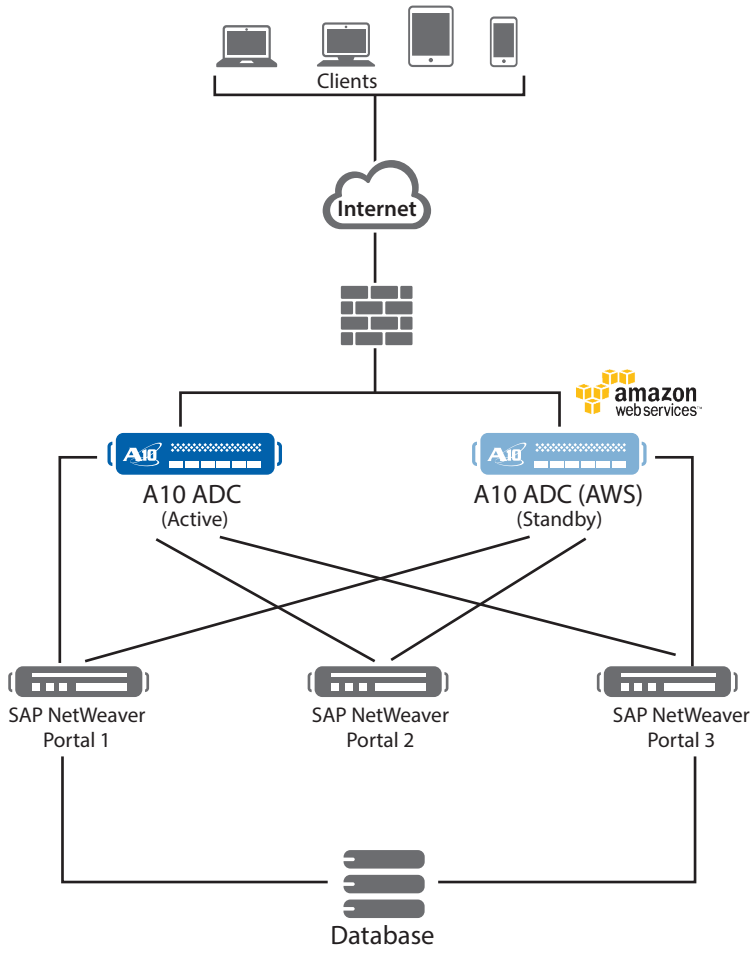

Figure 1a: A10 Thunder ADC with AWS active/standby solution

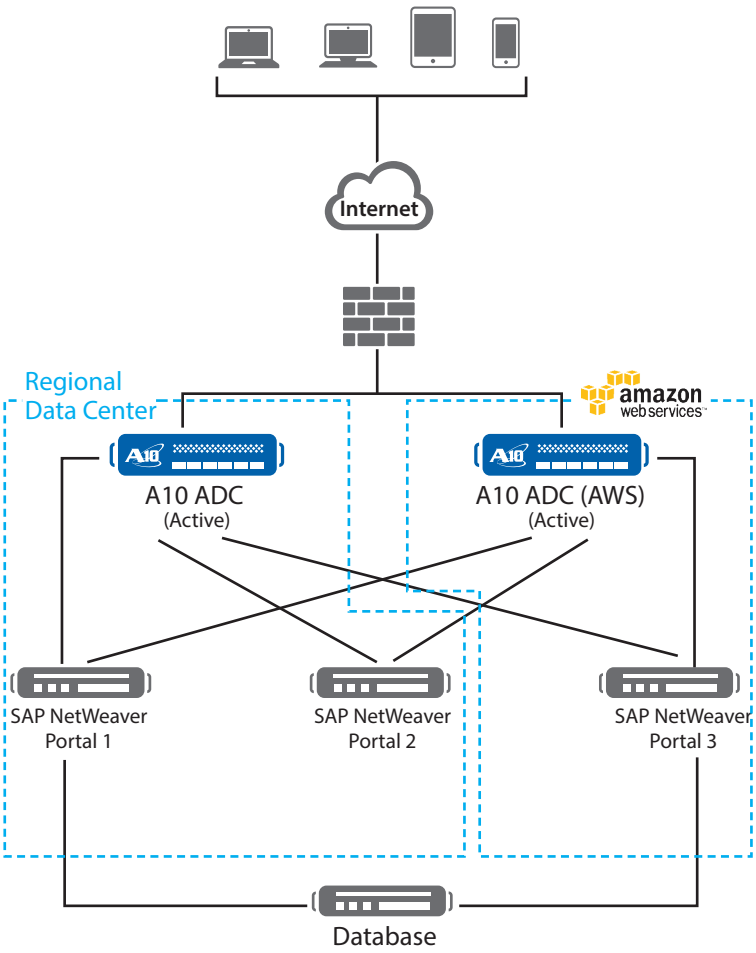

Figure 1b: A10 Thunder ADC and SAP NetWeaver Portal active/active solution with AWS solution

Feature Template Preparation

This section describes how to prepare the Thunder ADC device to enhance SAP NetWeaver Portal components. The templates below will be bound with the HTTPS (50001) Virtual Service once the VIP is created.

- SSL Offload
- Cookie persistence
- TCP Proxy
- Source NAT (Network Address Translation)
- Web Application Firewall (WAF)
- Distributed Denial of Service (DDoS)

SSL Offload

SSL Offload acts as an acceleration feature by removing the burden of processing SSL traffic from the SAP NetWeaver Portal servers. Instead of having NetWeaver Portal servers handling the SSL processing, the Thunder ADC appliance decrypts and encrypts all HTTPS traffic, forwarding the traffic to the server over HTTP (unencrypted).

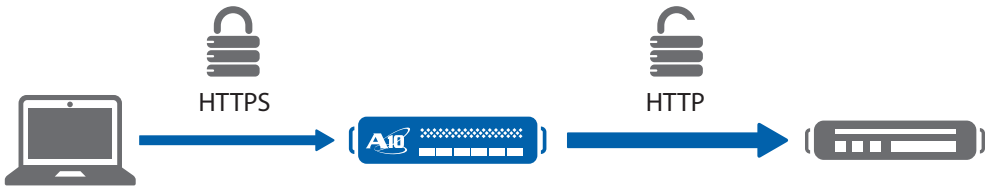

Figure 2: SSL Offload overview

To configure SSL Offload, the following configurations are required:

- Use HTTP for the communication between NetWeaver Portal web servers and Thunder ADC
- Use HTTPS on VIP for the communication between clients and Thunder ADC
- Import existing NetWeaver Portal web server SSL certificate or create self-signed CA on the Thunder ADC device
- Create SSL template and associate VIP with the SSL template

Import or Generate Certificate

1. Navigate to **Config Mode > SLB > SSL Management > Certificate**
2. There are two options to configure when installing an SSL template from the ADC appliance:

   Option 1: Generate a self-signed CA from the Thunder ADC

   Option 2: Import an SSL certificate and key, then export existing CA certificate from NetWeaver Portal web servers and import to Thunder ADC

Option 1: Generate a Self-Signed CA from Thunder ADC

1. Click **Create** to add a new SSL certificate using SSL Management.
2. Enter the File Name of the certificate: "**nwp**"
3. From the Issuer: Select "**Self**" from the dropdown menu, and then enter the following values:
   a. Common Name: "**a10**"
   b. Division: "**a10**"
   c. Organization: "**a10**"
   d. Locality: "**sanjose**"
   e. State or Province: "**ca**"
   f. Country: "**USA**"
   g. Email Address: "**sapadmin@example.com**"
   h. Valid Days: "**730**" (Default)
   i. Key Size (Bits): "**2048**"

   ***Note**: Thunder ADC supports 1028, 2048 and 4096 bit SSL keys. The higher bit SSL key size, the more CPU processing will be required. The Thunder ADC SSL models handle the SSL transaction in hardware.*
4. Click "**OK**" and then click "**Save**" to store your configuration changes.

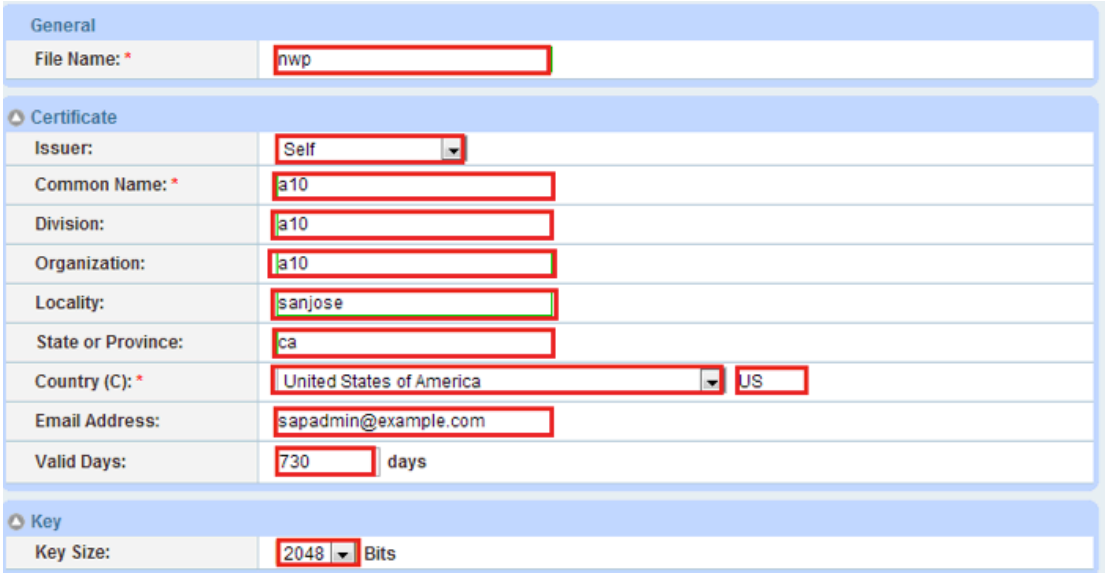

Figure 3: Client SSL certificate creation

Option 2: Import SSL Certificate and Key

1. Click "**Import**" to add a new SSL certificate using SSL Management
2. Enter a name for the certificate ("**nwp**")
3. Select "**Local**" from **Import Certificate from**: (this value will depend on the originating location of the certificate)
4. Enter Certificate Password (if applicable)
5. Enter Certificate Source (if applicable)
6. Click "**OK**" and then click "Save" to store your configuration changes

***Note**: If you are importing a CA-signed certificate for which you used the Thunder Series device to generate the certificate signing request (CSR), you do not need to import the key. The key is automatically generated on the Thunder ADC when you generate the CSR.*

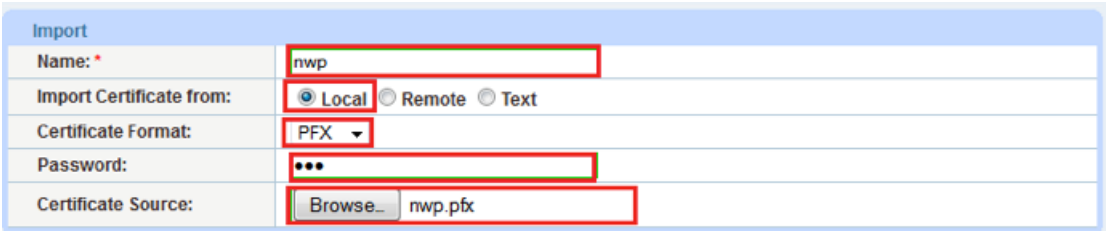

Figure 4: Import SSL certificate

Configure and Apply Client SSL Template

This section describes how to configure a client SSL template and apply it to the VIP.

1. Navigate to **Config Mode > SLB > Template > SSL > Client SSL**
2. Click "**Add**"
3. Enter Name: "**nwpclientssl**"
4. Enter Certificate Name: "**portal**"
5. Enter Key Name: "**portal**"
6. Enter Pass Phrase: "**example**"
7. Enter Confirm Pass Phrase: "**example**"
8. Session Cache Size: "**8000000**" (**optional**)
9. Session Cache Timeout: "**28800**" (**optional**)
10. Session Ticket Lifetime: "**28800**" (**optional**)

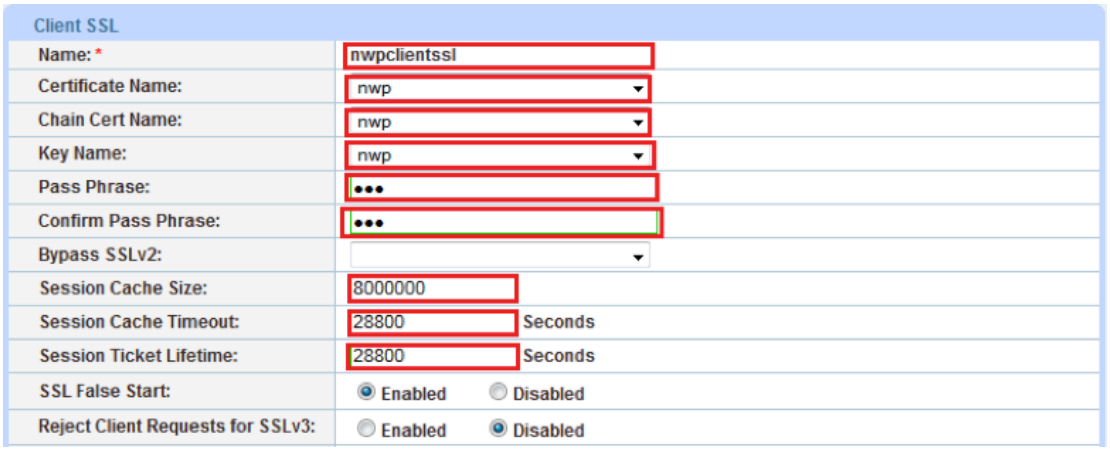

Figure 5: Client SSL

Once the Client SSL template is completed, you must bind the Client SSL to the HTTPS VIP (Port 443), as follows:

1. Navigate to **Config Mode > SLB > Virtual Server**
2. Click on "**Virtual Server name**"
3. **Select** "**443**" and click "**Edit**"
4. Apply the Client SSL template created by clicking the **Client-SSL template** dropdown menu
5. Select "**clientssl**" from the dropdown menu

Figure 6: Client SSL binding

6. Click "**OK**" and then click "**Save**" to store your configuration changes

Cookie Persistence

Cookie persistence enables you to insert a cookie into server responses to clients, in order to direct clients to the same service group, real server or real service port for subsequent requests for this service. The advantage of cookie persistence within the SAP NetWeaver solution is that you can direct all requests to the same SAP NetWeaver backend server that was recently visited, as long as the expiry time has not been exceeded.

Create Cookie Persistence Template

To enable cookie persistence, the template must be created first as follows:

1. Navigate to **Config mode > SLB > Template > Persistent > Cookie Persistence**
2. Click "**Add**" to add a new cookie persistence template
3. Select the Expiration radio button and enter "**86400**" in the **Seconds** field
4. Cookie Name: "**SAPcookie**"
5. Domain: "**example**"
6. Match Type: Select "**Service Group**"
7. Select "**Port**" (select the appropriate match type)
8. Select the **Insert Always** check box

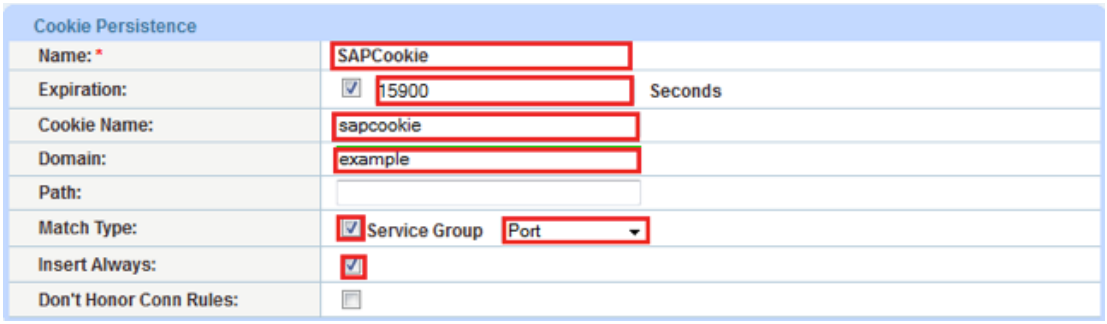

Figure 7: Cookie persistence template

9. Click "**OK**" and then click "**Save**" to store your configuration changes

TCP Proxy

TCP Proxy controls TCP stack settings, such as the TCP idle connection timeout. The TCP idle connection timeout determines how long users can be idle before the Thunder ADC appliance terminates the connection.

1. Navigate to **Config Mode > Template > TCP Proxy**
2. Click "**Add**"
3. Enter TCP Proxy Name: "**sap**"
4. Fin Timeout: **5** seconds
5. Idle Timeout: **28800** seconds (number of seconds that a connection can be idle before the Thunder ADC terminates the connection)
6. Retransmit Retries: **3**
7. SYN Retries: **5**
8. Time Wait: **5** seconds
9. Receive Buffer: **87380** Bytes (maximum number of bytes addressed to the port that the Thunder ADC will buffer)
10. Transmit Buffer: **87380** Bytes (number of bytes sent by the port that the Thunder ADC will buffer)
11. Initial Windows Size: **16324**
12. MSS (Maximum segment size): **1460**
13. Click "**OK**" and then click "**Save**" to store your configuration changes

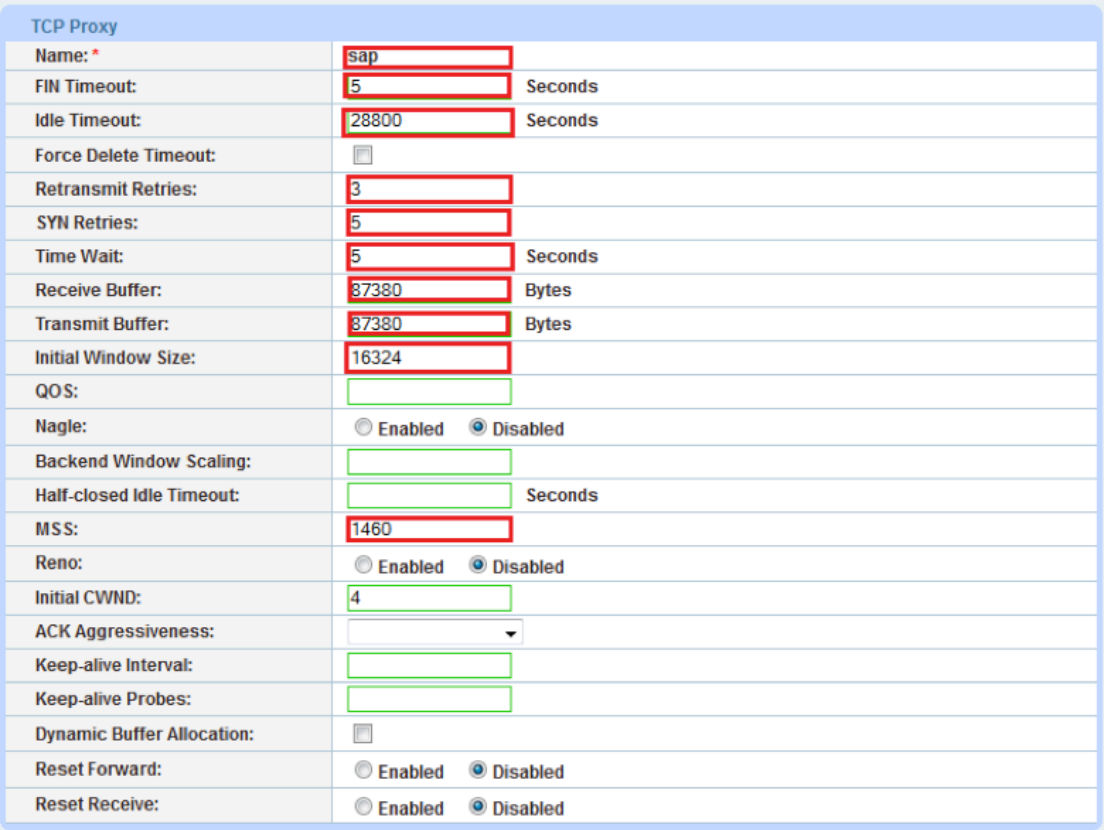

Figure 8: TCP Proxy template

IP Source NAT

This section configures the IP address pool to be used for IP SNAT. When incoming traffic from a client accesses the VIP address (for example: 172.16.1.200), the client requests are "source NAT-ed," which means that Thunder ADC replaces the client's source IP address based on the configured address pool of the source NAT. SNAT is a requirement when your network topology is based on "**one-arm**" deployment and if you have internal clients that reside on the same subnet as the VIP. The SNAT template must be applied in the virtual server port for the NAT to take effect.

Create IP Source NAT Template

1. Navigate to **Config Mode > IP Source NAT > IPv4 Pool**
2. Click "**Add**"
3. Enter IP Source NAT Name: "**SNAT**"
4. Enter Start IP Address:*172.16.1.250* (example)
5. Enter End IP Address: *172.16.1.250* (example)
6. Enter Netmask: *255.255.255.0*

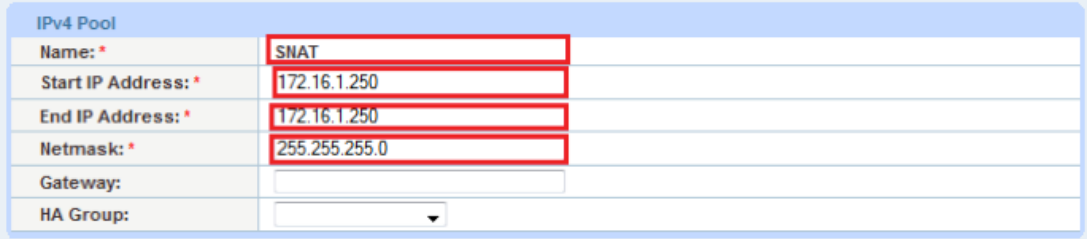

Figure 9: IP SNAT configuration

7. Click "**OK**" and then click "**Save**" to store your configuration changes

***Note**: Apply the SNAT template to the virtual server port. If your SAP NetWeaver environment will consist of many concurrent users, it is advisable to configure multiple SNAT IP addresses. One IP address can be used for up to 64,000 flows. There is also an auto SNAT check option within virtual server port for ease of implementation.*

SLB Configuration

In this section of the deployment guide, SLB servers, service group, virtual services and VIP are configured. Once the SLB components are configured, you will be able to apply all of the preconfigured templates that were created from the previous sections.

Server Configuration

This section demonstrates how to configure the NetWeaver web servers in the Thunder ADC appliance.

1. Navigate to **Config Mode > SLB > Service > Server**
2. Click "**Add**" to add a new server
3. Within the Server section, enter the following required information:
   a. Name: "**nwp1**"
   b. IP Address /Host: 192.0.2.2

   ***Note**: Enter additional servers if needed.*

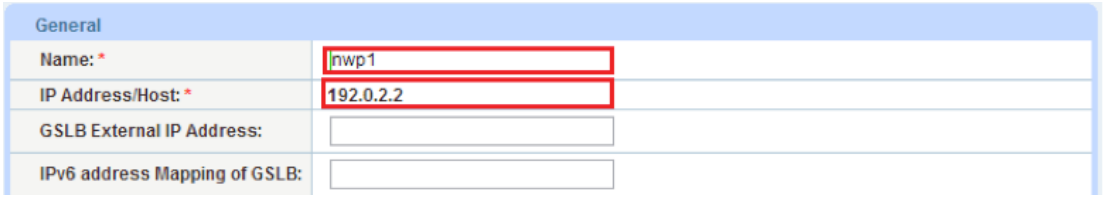

Figure 10: Real server configuration

4. To add ports to the server configuration, navigate to: **Config Mode > SLB > Service > Server > Port**
5. Enter **Port, Protocol** type and then click "**Add**"

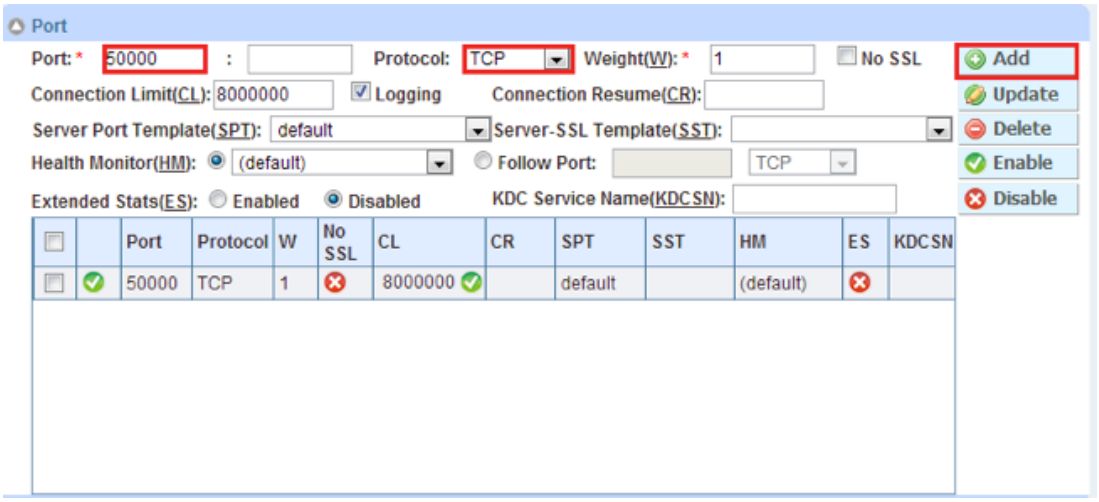

Figure 11: Real server port configuration

6. Click "**OK**" and then click "**Save**" to store your configuration changes

Health Monitor Configuration

The Thunder ADC device can automatically initiate the health status checks of real servers and service ports. This provides clients assurance that all requests are going to functional and available servers. If a server or a port does not respond appropriately to a health check, the server will be temporarily removed from the list of available servers. Once the server is restored and starts responding appropriately to the health checks, the server will be automatically added back to the list of available servers.

1. Navigate to **Config Mode > SLB > Health Monitor > Health Monitor**
2. Health Monitor: Click the dropdown menu and select **Create**
3. Enter the Health Monitor Name: "**nwphc**"
4. Under Method type: Select "**HTTP**"

   ***Note**: By default, Thunder ADC expects the response code 200 (OK) with "HTTP." Please update "URL" or "Expect" section according to your environment.*
5. Click **OK** and then continue with the Service Group configuration

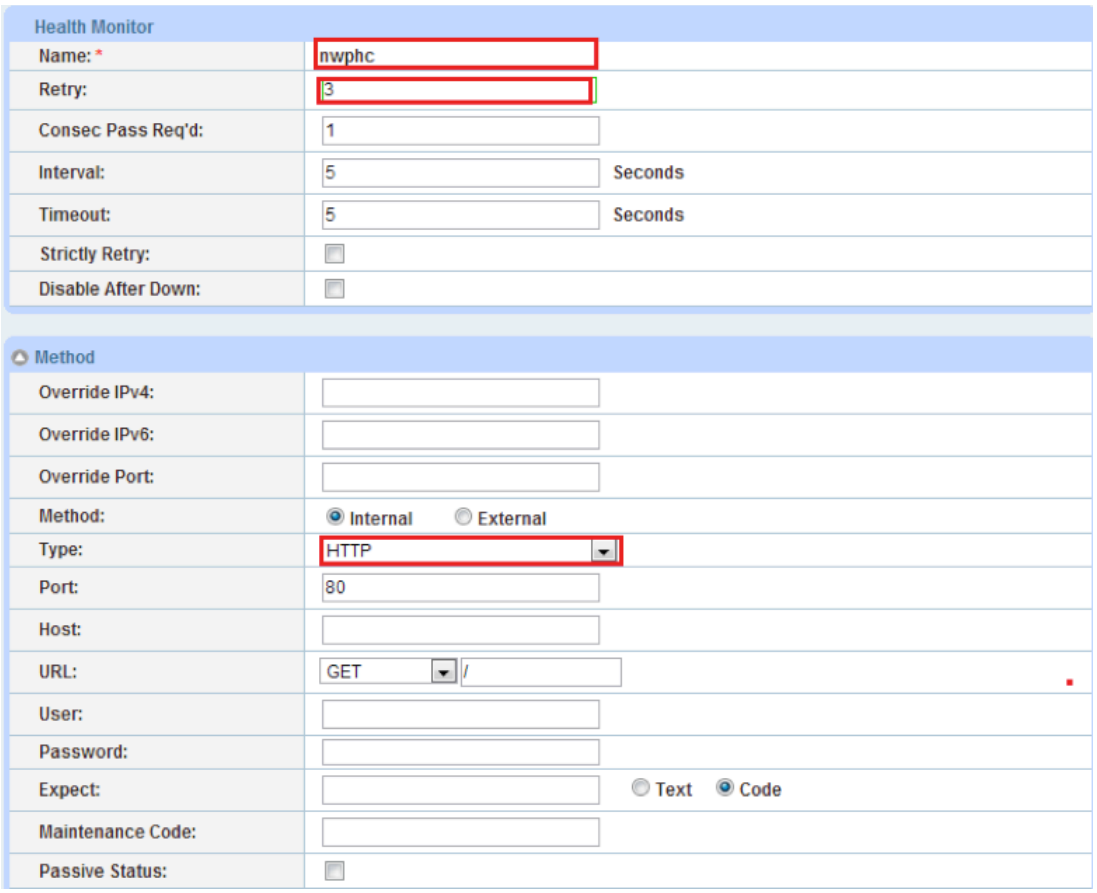

Figure 12: Health Monitor configuration

Service Group Configuration

This section demonstrates how to configure the NetWeaver web servers in a service group. A service group contains a set of real servers from which the Thunder ADC can select to service client requests. A service group supports multiple NetWeaver real servers as one logical server.

1. Navigate to **Config Mode > SLB > Service > Service Group**
2. Click "**Add**" to add a new service group
3. Within the Server Group section, enter the following required information:
   a. Name: "**sg50000**"
   b. Type: Select "**TCP**" from the dropdown menu
   c. Algorithm: Select "**LeastConnection**" from the dropdown menu
   d. Health Monitor: Select "**nwphc**"

The following is another health check that differs from the previously configured server health check. This is an optional server group health check, and you can specify the method type or you can select the default "ping" health check. In this guide, you can either use HTTP or HTTPS depending on the setup configured on the backend servers, either an SSL Offload or full SSL.

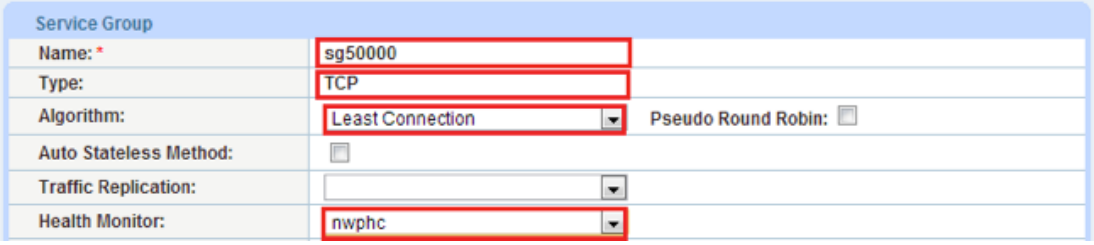

Figure 13: Service Group configuration

4. From the Server section of the window, add one or more servers from the server dropdown list:

   Server: Select "**nwp1**" from the dropdown menu
   Port: Enter "**50000**"

5. Click "**Add**" and enter all available NetWeaver web servers

In Figure 14, the server names **nwp1** and **nwp2** are entered, each with port **50000**.

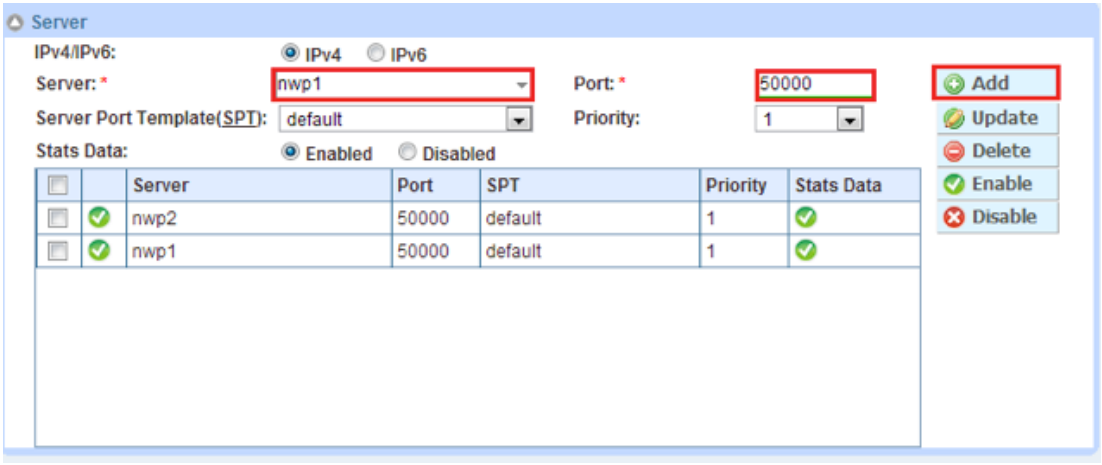

Figure 14: Service Group server configuration

6. Once completed, click "**OK**" and then click "**Save**" to store your configuration changes

***Note**: It is best practice to put each NetWeaver application in a service group. For example, if you have multiple Haiku servers, those servers should be provisioned to be in the same service group.*

Virtual Server

This section demonstrates how to configure the VIP with the Thunder ADC appliance.

1. Navigate to **Config Mode > SLB > Service > Virtual Server**
2. Within the **General** section, enter the following required information:

   a. Name: "**SAPVIP**"

   b. IP Address or CIDR Subnet: *10.0.0.200*

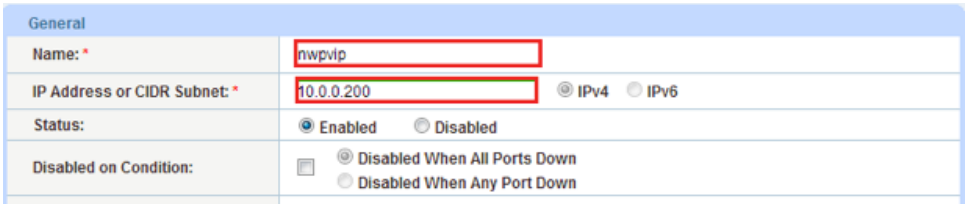

Figure 15: Virtual Server or VIP configuration

3. In the **Port** section:
   a. Click "**Add**"
   b. Enter the Virtual Server Port information
4. Type: From the dropdown menu, select "**HTTPS**"
5. Port: Enter "**50001**"
6. Service Group: From the dropdown menu, select "**sg50000**" to bind the virtual server to the real servers

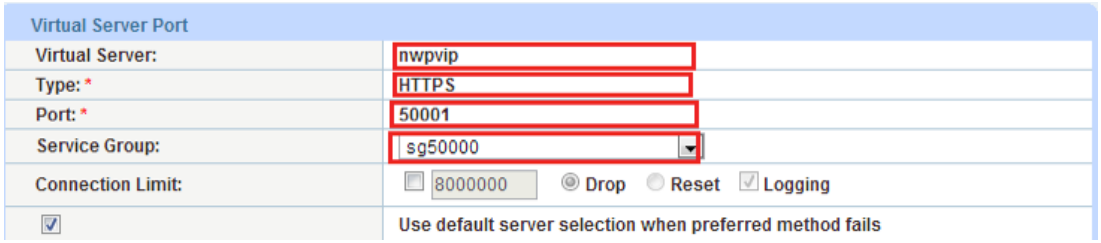

Figure 16: Virtual Server Port configuration

7. Click "**OK**" and then click "**Save**" to store your configuration changes.

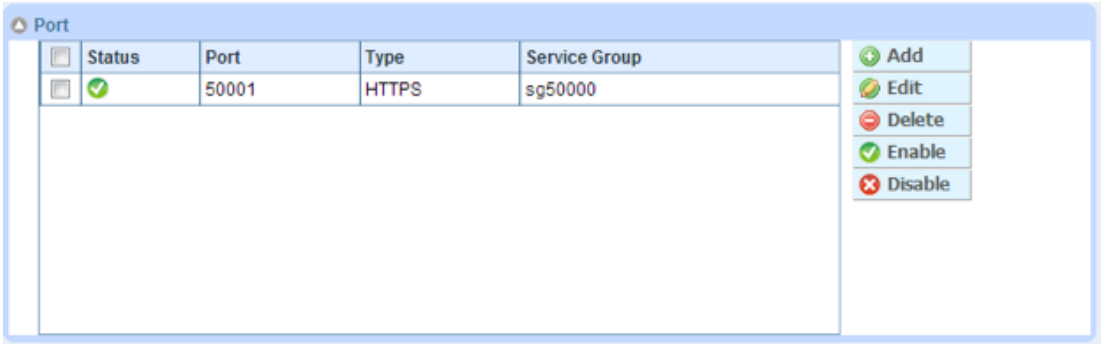

Figure 17: Virtual Port lists

8. Click "**OK**" and then click "**Save**" to store your configuration changes

***Note**: To test and access the SAP NetWeaver Portal with load balancing, use a browser and navigate to the following URL:* https://<FQDN/VIP>:50001/irj/portal

Configuration Templates

Once the templates such as SSL, TCP Proxy and persistence are configured, you can now bind the templates to the port on the VIP to make them operational.

1. Navigate to **Config Mode** > **SLB** > **Virtual Service**
2. Click on the virtual service name

Apply the features by selecting the templates from the applicable dropdown lists.

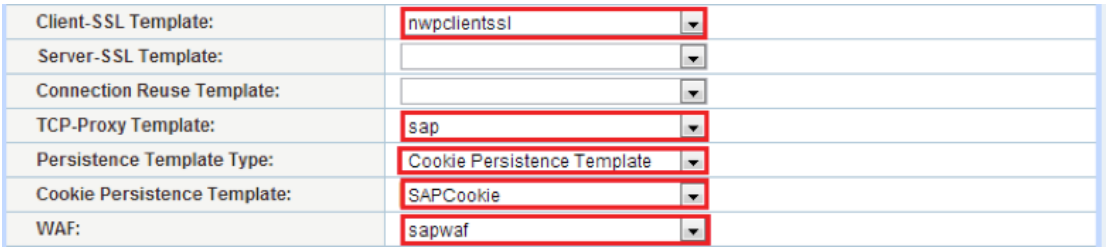

Figure 18: Applying features

3. Click **OK**, then click the **Save** icon at the top of the GUI window to save the configuration

Web Application Firewall (Optional)

This part of the deployment guide will provide additional security protection to the SAP applications using Web Application Firewall (WAF). This feature can be deployed as a pass-through SSL solution using the A10 device as a WAF. To deploy this solution, you need to:

1. Create a WAF template within **Config Mode > Security > WAF > Template**
2. Click "**Add**"
3. Enter Name: "**sapwaf**"
4. Select Deployment Mode as "**Active**"

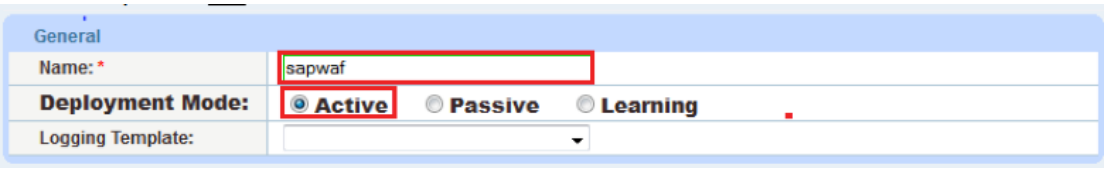

Figure 19: WAF general configuration

This section of the WAF feature is where you specify the location and enable the WAF request protection features. To understand the details of each of the features, refer to the A10 Web Application Firewall Guide. Select the needed protection required for your deployment.

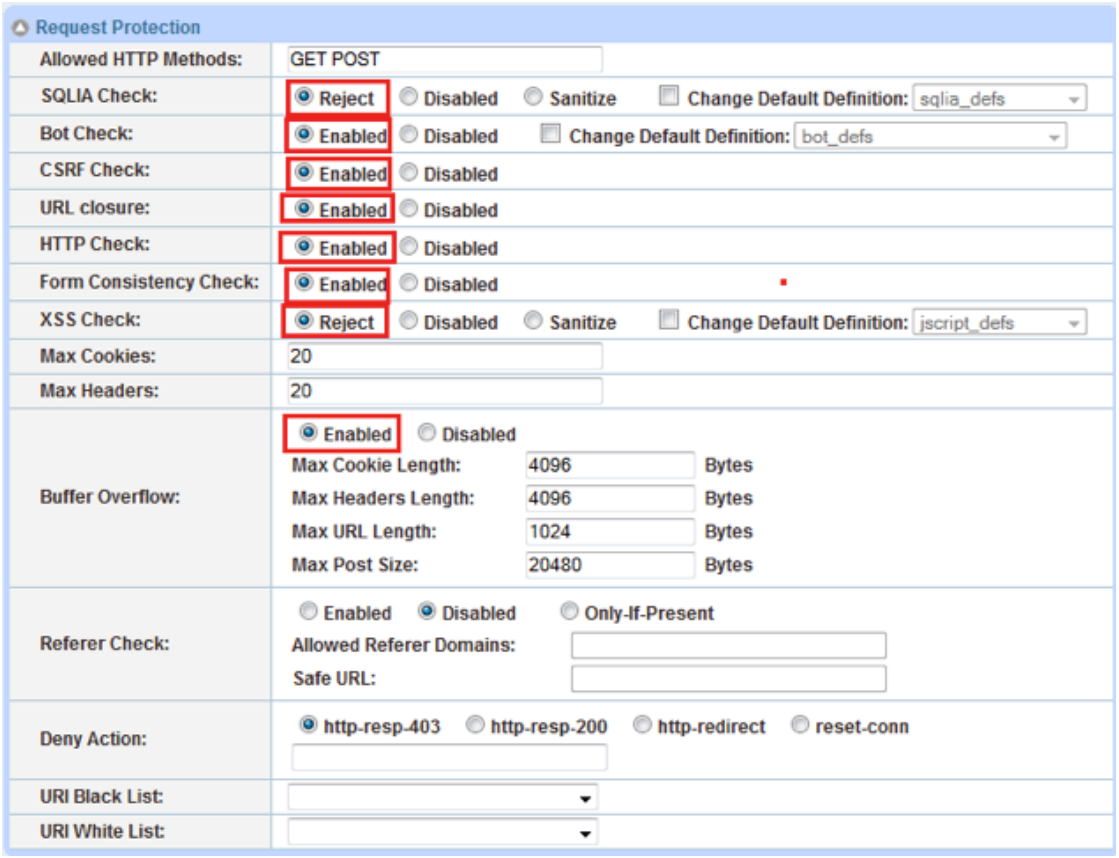

Figure 20: WAF Request Protection configuration

This section will be used to configure the Response Protection required for your deployment.

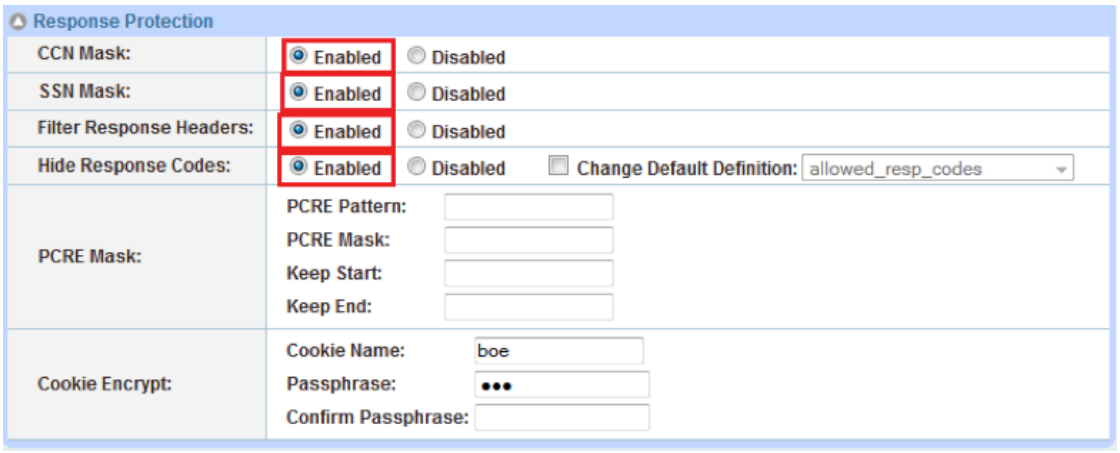

Figure 21: WAF Response Protection configuration

5. Once configured, click **OK** and bind the WAF feature to the HTTPS virtual port for the feature to work

6. Once completed click "**OK**" and click "**Save**" to store the configuration

DDoS Mitigation (Optional)

This section is an additional security feature to protect the SAP application from DDoS attacks. To configure this feature within the A10 Advanced Core Operating System (ACOS®) platform, navigate to **Config Mode** > **Security** > **Network** > **DDoS Protection**.

The DDoS Protection feature is a global configuration, and to enable this feature, you will select the DDoS attacks you would like to drop. In the diagram below, we have selected the DDoS mitigation attack required. Once completed, click "**OK**" and then "**Save**" to store your configuration.

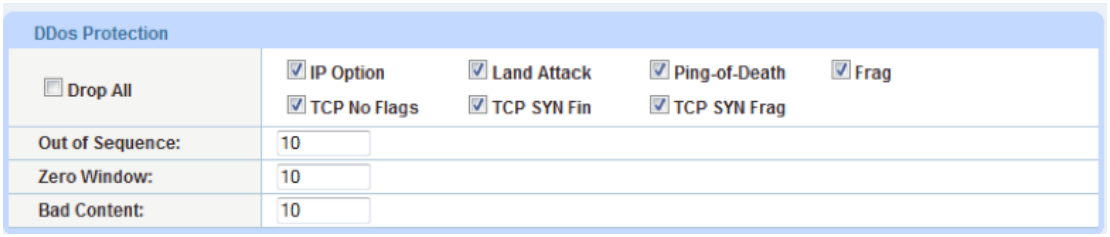

Figure 22: DDoS Protection configuration

In addition, these two command lines are also required to deploy system-wide Policy-Based Server Load Balancing (PBSLB) using a CLI.

```
system pbslb bw-list sap
system pbslb over-limit lockup 5 logging 10
```

The blacklist/whitelist is applied to the system-wide PBSLB within a locking time of 5 minutes and login interface of 10 minutes.

***Note**: The sample BW-List contains group ID 1; however, you don't need to configure the group ID in a PBSLB configuration since a wildcard address is used in the list. To use a specific host or subnet address in the list, please configure the action (reset or drop) for each group ID accordingly.*

Summary and Conclusion

The configuration steps described above show how to set up the Thunder ADC appliance for an SAP Enterprise (NetWeaver) Portal. By using Thunder ADC to load balance Enterprise Portal web application servers, the following benefits are achieved:

- Higher availability if an SAP Enterprise Portal web server fails, meaning there is no direct impact on how users can access the applications
- Reduced application server CPU utilization rates, as Thunder ADC transparently load balances requests across multiple SAP Enterprise Portal applications and web servers
- Greater connection throughput and faster end user responsiveness, by offloading intensive security processing to the Thunder ADC device
- Additional protection against DDoS attacks and an additional level of protection, using the A10 WAF feature

By using Thunder ADC, significant benefits are achieved for all SAP NetWeaver Portal users. For more information about A10 Thunder Series products, please refer to the following URLs:

http://www.a10networks.com/products/thunder-adc.php

http://www.a10networks.com/products/application_delivery_controllers.php

Appendix

Attached is a sample CLI configuration based on the configuration tested above.

```
health monitor nwphc
 method http

slb server nwp1 192.0.2.2
   health-check ping
   port 50000 tcp

slb server nwp2 192.0.2.3
   health-check ping
   port 50000  tcp

slb service-group sg50000 tcp
    method least-connection
    health-check nwphc
    member nwp1:50000
    member nwp2:50000

slb template tcp-proxy sap
   idle-timeout 28800
   receive-buffer 87380
   transmit-buffer 87380
   initial-window-size 16324

slb template cache ramcaching
   policy uri .jpg cache
   policy uri .doc cache
   policy uri .docx cache

slb template waf sapwaf
   bot-check
   http-check
   xss-check reject
   form-consistency-check
```

```
   csrf-check
   ccn-mask
   ssn-mask
   sqlia-check reject

slb template client-ssl nwpclientssl
   cert nwp
   chain-cert nwp
   key nwp pass-phrase encrypted
37O48xvi8uY8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
   session-cache-timeout 28800
   session-cache-size 8000000
   session-ticket-lifetime 28800

slb template persist cookie SAPCookie
   name sapcookie
   domain example
   expire 15900
   insert-always
   match-type service-group

slb virtual-server nwpvip 10.0.0.200
   port 50001  https
      name _10.0.0.200_HTTPS_50001
      source-nat auto
      service-group sg50000
      template tcp-proxy sap
      template waf sapwaf
      template client-ssl nwpclientssl
      template persist cookie SAPCookie
system pbslb bw-list sap
system pbslb over-limit lockup 5 logging 10
monitor buffer-usage 91750
end
```

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
brazil@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.

Part Number: A10-DG-16138-EN-01
July 2014