Thunder Series for SAP BusinessObjects (BOE)

Table of Contents

Disclaimer

Introduction

SAP, the global market leader in business resource planning and business management, has been integrated and certified with A10 Application Delivery Controller (ADC). SAP applications and services enable companies of all sizes to work together more efficiently and use business insight more effectively.

This document shows how an A10 Thunder Series ADC can be deployed with SAP BusinessObjects Explorer (BOE) as the front end to SAP HANA. The tested solution is based on the virtual edition, vThunder ADC running on Amazon Web Services (AWS) Cloud infrastructure. The solution also works on Thunder and AX Series ADC hardware appliances, other vThunder editions, and the Thunder hybrid virtual appliance (HVA). The deployment guide provides a detailed configuration guide on how to administer the Thunder ADC with SAP BOE systems.

Deployment Guide Prerequisites

The deployment guide was tested based on the following prerequisites.

Thunder ADC Series Requirements

- The A10 Networks Thunder ADC Series must be running version 2.7.1 P3 or higher

SAP Requirements

- SAP BusinessObjects 4.x (Front End to SAP HANA)

***Note**: For additional deployment options and features that the Thunder ADC Series device 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 notes on how to expedite deployment of SAP BusinessObject (front of HANA) and A10 solutions.

1. If the Virtual IP (VIP) is accessed from an external client, the network topology needs to be deployed in routed mode. If the BOE application is accessed internally, the network can be deployed in one-arm mode.
2. In the solutions test, there were two (2) SSL termination options tested; SSL Offload, end-to-end SSL and Pass-through as an optional configuration which is not documented in this guide.
   a. SSL Offload: The SSL traffic is terminated in the ADC as a Reverse Proxy. The traffic is then sent to the SAP backend server via un-encrypted traffic (HTTP). This configuration allows the reverse proxy to become the defense point for outside attacks.
   b. End-to-end SSL: The front end and backend traffic are all in encrypted traffic. There is no clear text transmission on wires any more.
   c. Pass-through SSL (Optional): The A10 ADC is either not used or acts only as network traffic router and utilize A10 features such as ACL, WAF and DDoS. The network connections are not terminated at the ADC but only at the SAP backend Application.
3. 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.
4. The ADC DDoS mitigation feature was deployed in the SAP test bed and the A10 ADC was able to protect the SAP applications from DDoS attacks. The DDoS feature can be enabled whenever is needed and consumes very low CPU usage. Highly recommended for DDoS attack protection.
5. SSL session caching is available in ACOS 2.7.1 P3 and noted in the deployment guide as an optional feature. This feature is an SSL enhancement within ACOS and will provide better SSL performance.
6. SAP applications run on different and unique TCP ports such as SAP Business Objects use port 80, SAP CRM/ DIA use Ports 44300 and 8000 and SAP Portal use port 5000, hence we can use only one VIP address for simple implementation and management.

Accessing the Thunder Series Load Balancer

This section describes how to access the Thunder Series device. The Thunder 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 – Secure Shell (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 device.*

- Default Username: "admin"
- Default password is "a10".
- Default IP Address of the device is "172.31.31.31"

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

Amazon AWS Configuration

The A10 and SAP BusinessObjects solution has been deployed and tested using Amazon AWS infrastructure. The following important notes should be considered when the A10 solution is deployed within AWS.

The configuration samples below are set of configuration required on the primary interface using CLI only. AWS requires that the primary interface has to be in DCHP and can be utilized as single management IP for management, VIP and SNAT.

The following command are required:

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

After the initial login, it is required also to specify specific TCP ports 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 Source NAT:

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

For VIP configuration , this 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
```

Artchitecture Overview

The network topology in Figure 1 is a sample of how SAP BOE is deployed with cloud redundancy between regional data center and cloud solutions using Amazon AWS.

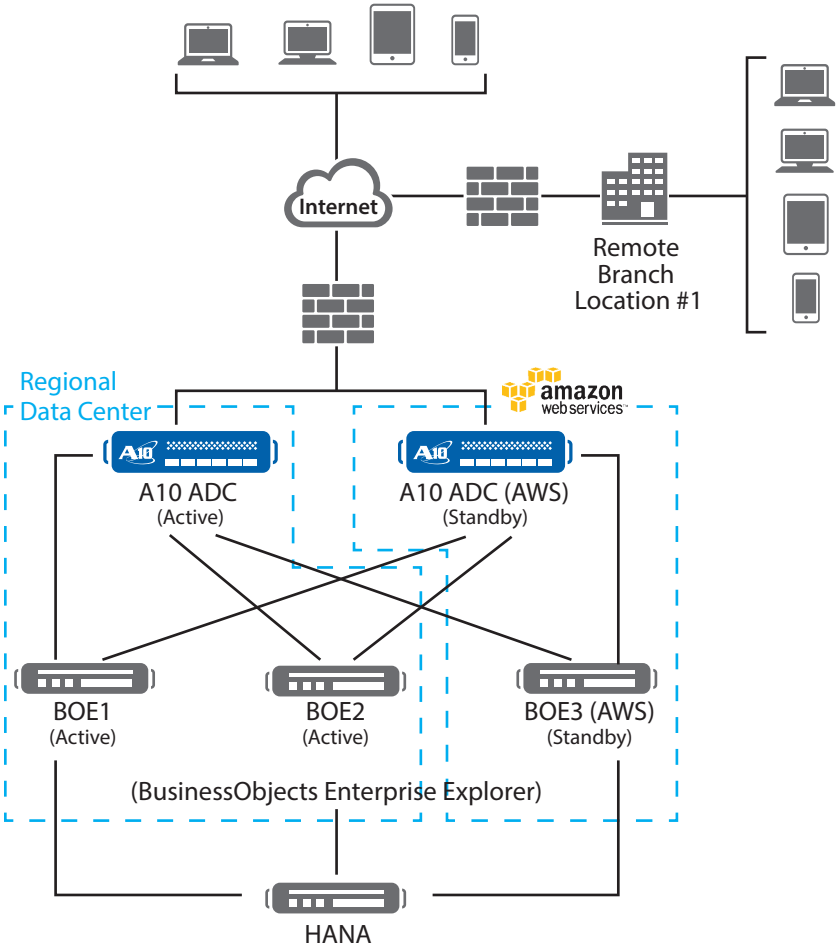

Figure 1: SAP Business Objects Topology

Feature Template Preparation

This section describes how to prepare the Thunder ADC to enhance SAP BOE components. These features provide web application acceleration, optimize BOE web server's performance and increase reliability. These templates below will be bound with the HTTPS (443) Virtual Service once the VIP is created.

- SSL deployment
  - SSL Offload
  - End-to-end SSL
  - Pass-Through SSL
- Cookie Persistence
- TCP Proxy
- 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 BOE servers. Instead of having the BOE servers handling the SSL processing, the Thunder ADC decrypts and encrypts all HTTPS traffic, forwarding the traffic to the Server over HTTP (unsecured).

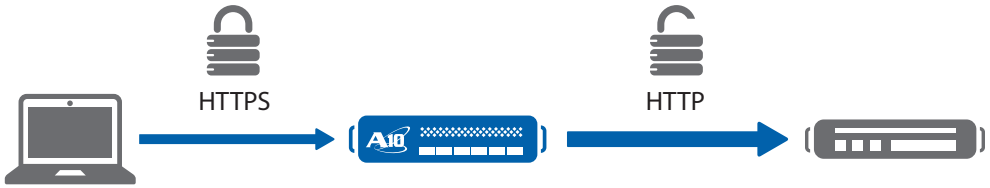

Figure 4: SSL Offload Overview

To configure SSL Offload, the following configurations are required:

- Use HTTP for the communication between BOE web servers and Thunder ADC
- Use HTTPS on Virtual IP for the communication between clients and Thunder ADC
- Import existing BOE web server SSL cert or create self-signed CA on the Thunder ADC
- 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 Series either:
   a. **Option 1**: Generate a Self-Signed CA from the Thunder ADC
   b. **Option 2**: Import an SSL Certificate and Key:
   Export existing CA certificate from BOE web servers and import to Thunder ADC.

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

1. Click **Create** to add a new SSL certificate from the SSL Management
2. Enter the File Name of the certificate: "**WS**"
3. From the Issuer: Select "**Self**" from the from the drop-down menu, and then enter the following values:
   a. Common Name: "**WS**"
   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**: The Thunder ADC supports 1028, 2048, 4096 bit SSL key. 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 "**Save**" configuration.

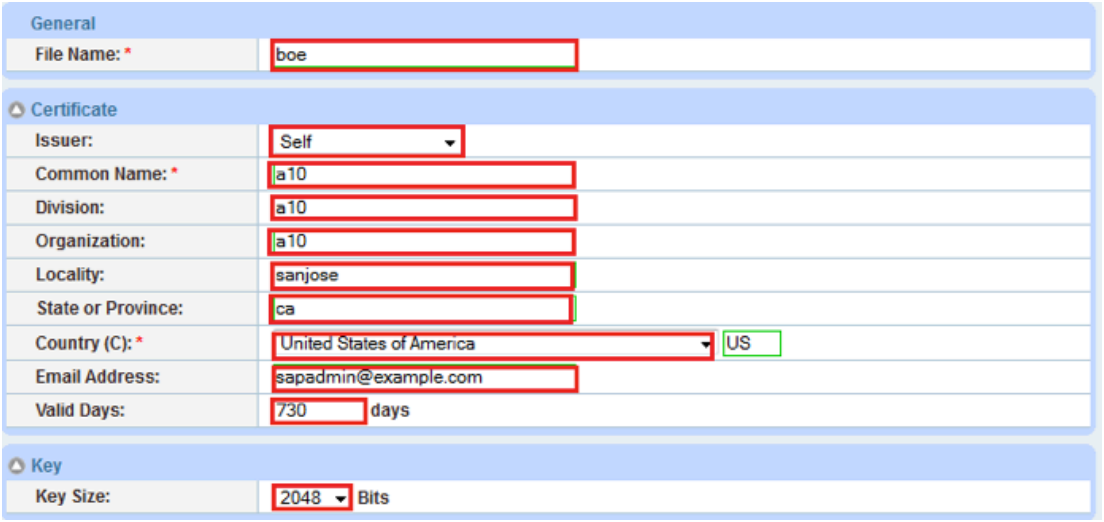

Figure 5: Client SSL Certificate Creation

Option 2: Import SSL Certificate and Key

1. Click "**Import**" to add a new SSL certificate from the SSL Management.
2. Enter a name for the certificate "**boe**".
3. Select "**Local**" from **Import Certificate from**: (depends where the certificate is originating from).
4. Enter Certificate Password (if applicable).
5. Enter Certificate Source (if applicable).
6. Click "**OK**" and "**Save**" your configuration.

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

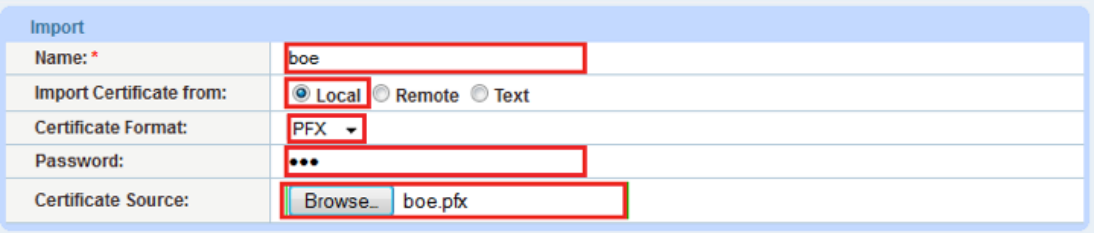

Figure 6: Import SSL Certificate

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: "**clientssl**".
4. Enter Certificate Name: "**boe**".
5. Enter Key Name: "**boe**".
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)**.

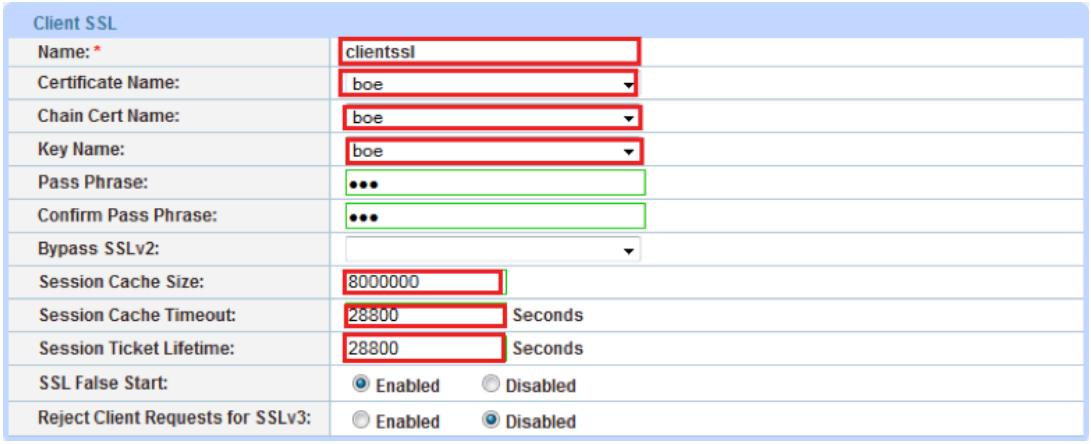

Figure 7: Client SSL

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** drop-down menu.
5. Select "" from the drop-down menu.

Figure 8: Client SSL Binding

6. Click "**OK**" and "**Save**" configuration.

End-to-End SSL

This section of the deployment guide would be the continuation of the SSL Offload feature that was discussed in the previous chapter. The difference is that the end-to-end, or full, SSL feature enables encrypted transaction on back end also which makes end-to-end communication in full encryptions with reverse proxy. To make the SSL Offload to be a Full SSL solution, the back end connection has to be converted from HTTP (80) to HTTPS (443). To deploy the Full SSL solution, a certificate will not be required but you need to bind the Server SSL template to the HTTPS VIP with SSL cipher supported and an optional CA to validate the server certificate.

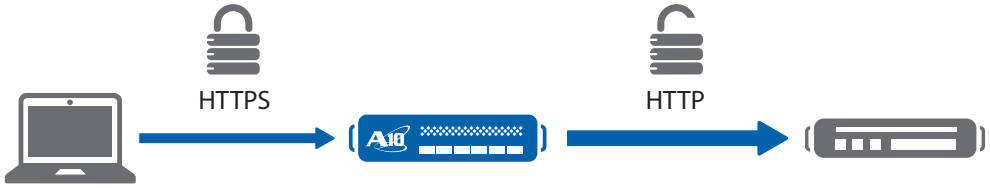

Figure 9: End-to-end SSL Overview

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

1. Navigate to **Config Mode > SLB > Template > SSL > Server SSL**.
2. Click "**Add**".
3. Enter Name: "**serverssl**".

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

Note: To complete the Server SSL template you must create the Server SSL certificate first. You can either import or create a self-signed.

1. Navigate to **Config Mode > SLB > Virtual Server**.
2. Click on "**Virtual Server name**".

Figure 9: SSL Template

Cookie Persistence

Cookie persistence enables you to insert a cookie into server responses to clients, to direct clients to the same service group, real server, or real service port for subsequent request for this service. The advantage of cookie persistence within the BOE solution is to direct all requests to the same BOE 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.

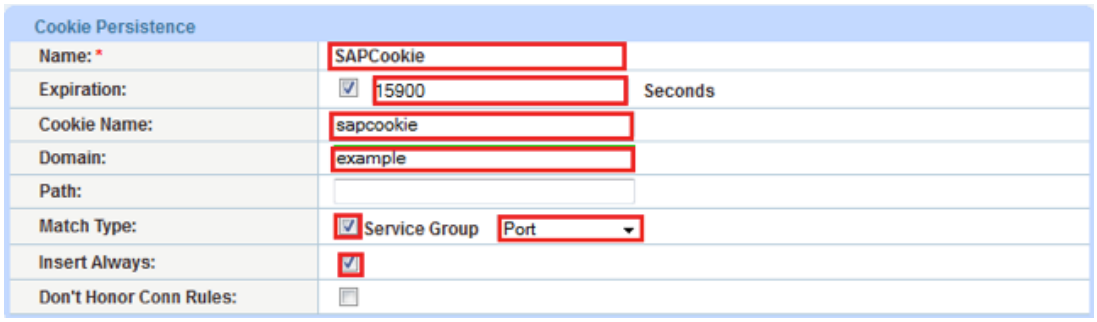

Figure 10: Cookie Persistence Template

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 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 (This is the number of seconds that a connection can be idle before the Thunder Series terminates the connection).
6. Retransmit Retries: 3.
7. SYN Retries: 5.
8. Time Wait: 5 Seconds.
9. Receive Buffer: 87380 Bytes (Max 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.

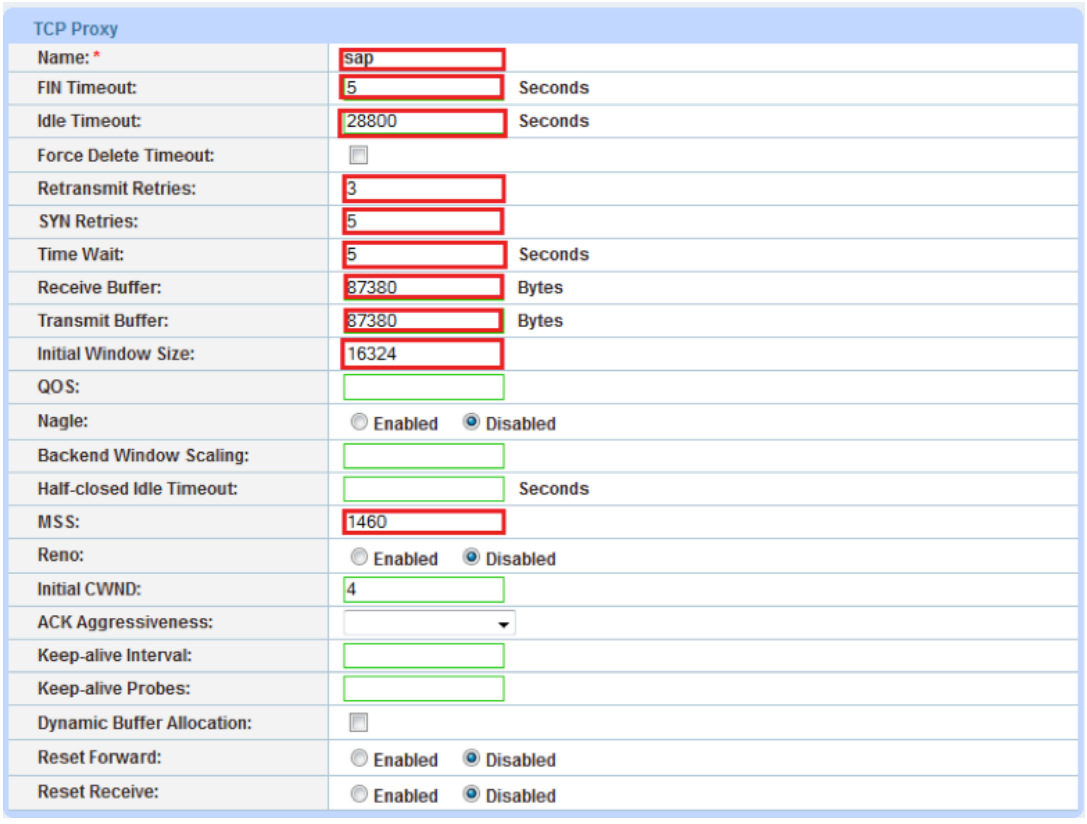

Figure 11: TCP Proxy Template

IP Source NAT

This section configures the IP Address pool to be used for IP Source Network Address Translation (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 must be required 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 Source NAT 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*.

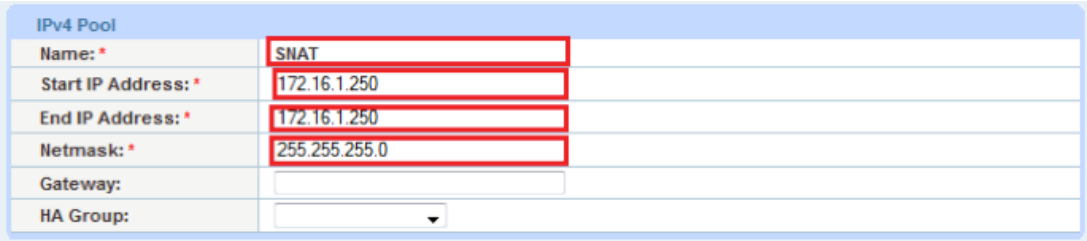

Figure 12: IP Source NAT Configuration

7. Click "**OK**" and "**Save**" configuration.

***Note**: Apply the SNAT template to the Virtual Server Port. If the SAP BOE 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.*

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 we will be able to apply all the pre-configured templates that were created from the previous sections.

Server Configuration

This section demonstrates how to configure the Business Object web servers in the Thunder ADC.

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: "**boe1**"
   b. IP address /Host: *172.16.1.10*

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

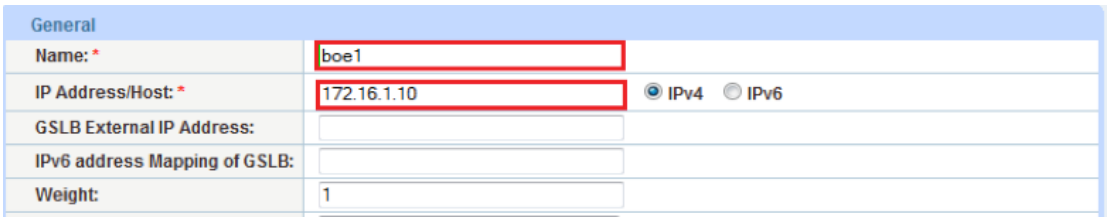

Figure 13: Real Server Configuration

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

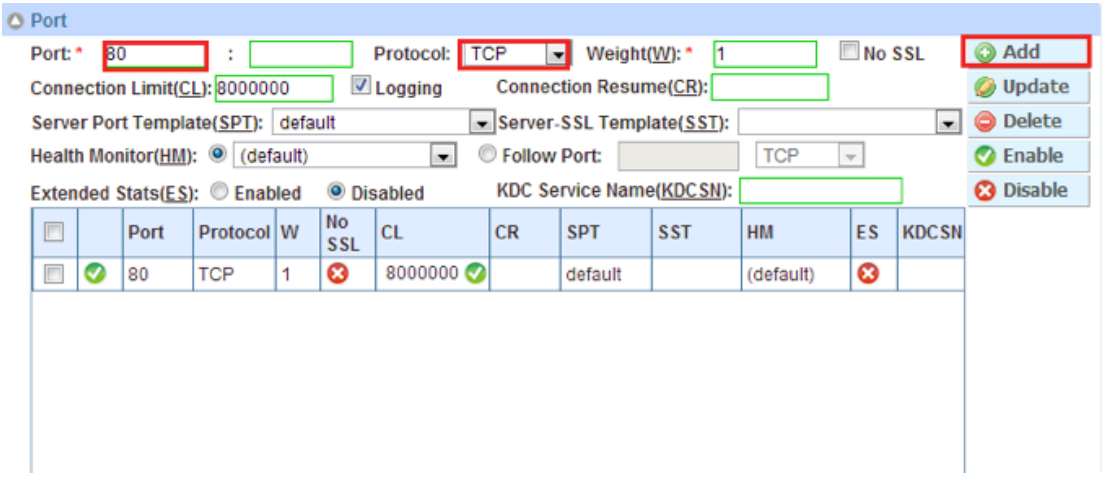

Figure 14: Real Server Port Configuration

6. Click "**OK**" and "**Save**" configuration.

Health Monitor Configuration

The Thunder ADC can automatically initiate the health status checks of real servers and service ports. This provides clients assurance that all requests go 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 drop-down menu and select **Create**.
3. Enter the Health Monitor Name, "**saphc**".
4. Under Method type, select "**HTTP**".

***Note**: By default, Thunder ADC expects response code 200 (OK) with "HTTP". method. Please update "URL" or "Expect" section according to your environment.*

5. Click **OK** and then continue with the Service Group configuration.

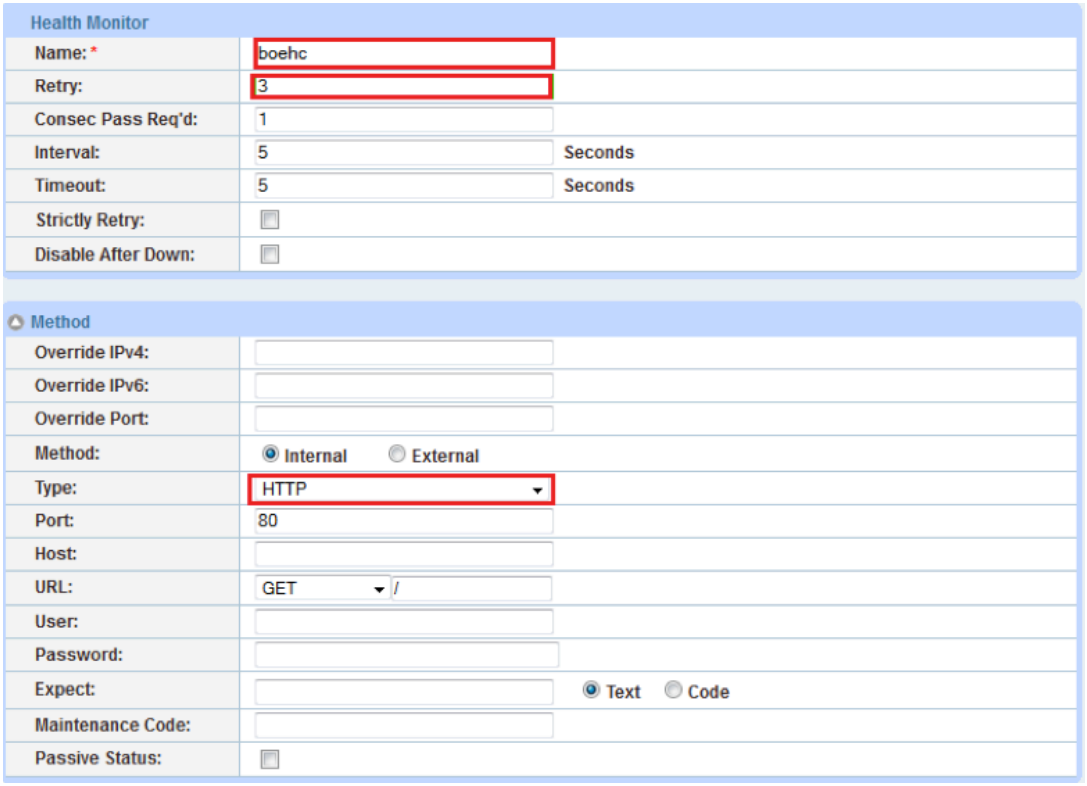

Figure 15: Health Monitor Configuration

Service Group Configuration

This section demonstrates how to configure the BOE 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 BOE 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: "**boeservers**".
   b. Type: Select "**TCP**" from the drop-down menu.
   c. Algorithm: "**LeastConnection**" from the drop-down menu.
   d. Health Monitor: Select "**sgboehc**"

***Note**: This is another health check other than the server health check that was previously configured. This is an optional server group health check and you can specific 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 back end servers either a SSL Offload or Full SSL.*

Figure 16: Service Group Configuration

4. From the Server section of the window, add one or more servers from the server drop-down list:
   Server: Select "**boe1**" from the drop-down menu.
   Port: Enter "**80**".
5. Click "**Add**" and enter all the available BOE web servers.

In **Figure 17**, the server names **boe1** and **boe2** are entered, each with port **80**.

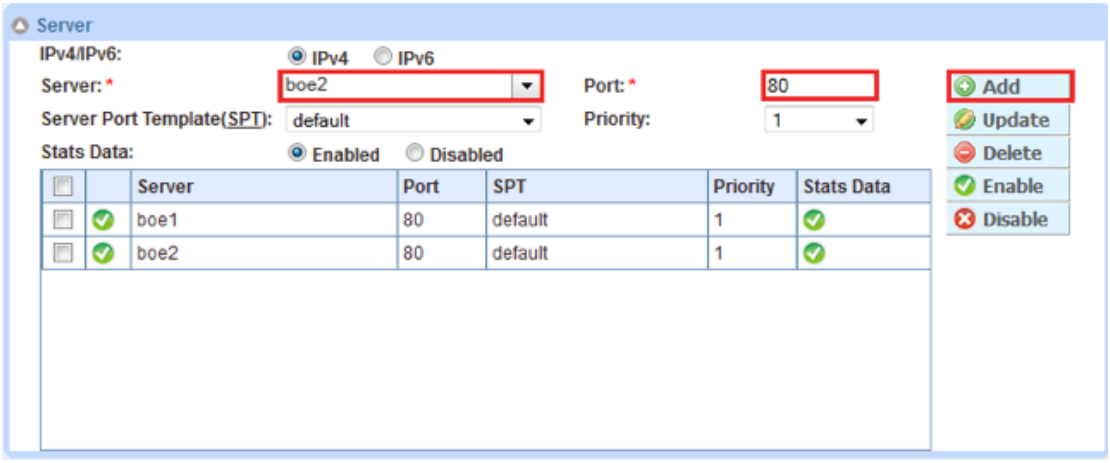

Figure 17: Service Group Server Configuration

6. Once completed click "**OK**" and "**Save**" configuration.

***Note**: It is best practice that each BOE application must be 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.

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: *172.16.1.200*.

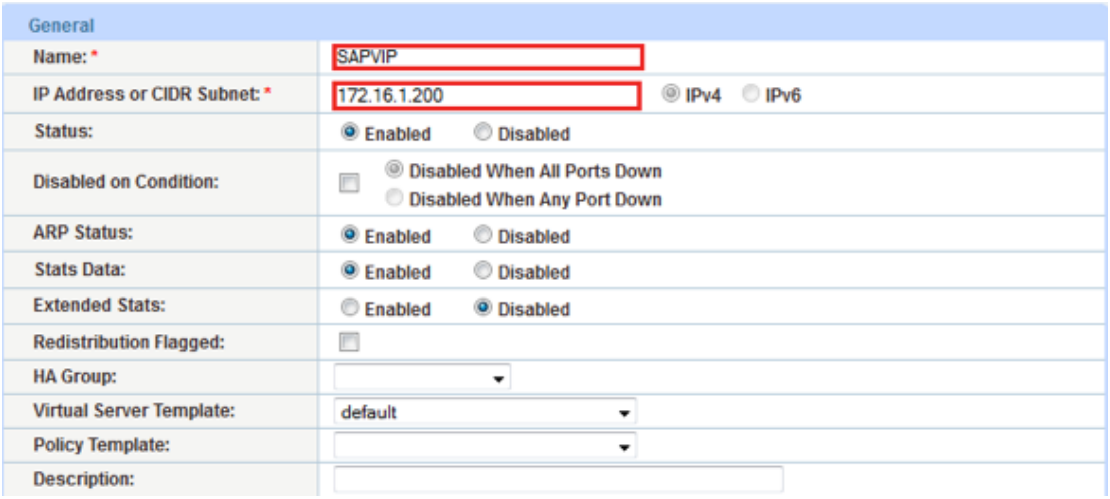

Figure 18: Virtual Server or VIP Configuration

3. In the **Port** section:
   a. Click "**Add**".
   b. Enter the Virtual Server Port information.
   c. Type: From the drop down menu select "**HTTPS**"
   d. Port: "**443**"
   e. Service Group: From the drop down menu select: "**sgboe**" to bind the virtual server to the real servers.

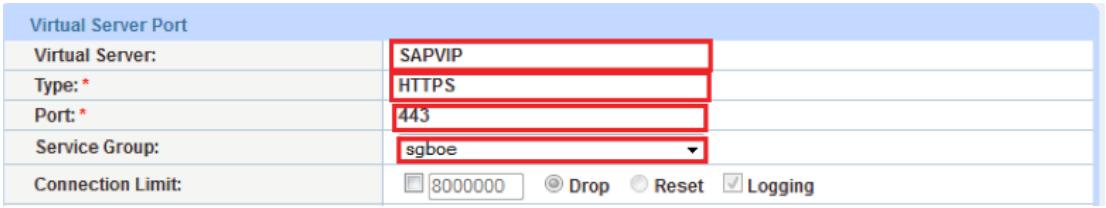

Figure 19: Virtual Server Port Configuration

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

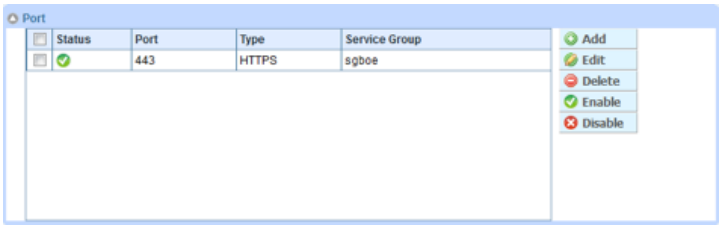

Figure 20: Virtual Port Lists

5. Click "**OK**" and "**Save**" configuration.

Configuration Templates

Once the templates such as SSL, TCP Proxy and Persistence templates are configured, you can now bound 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 drop-down lists.

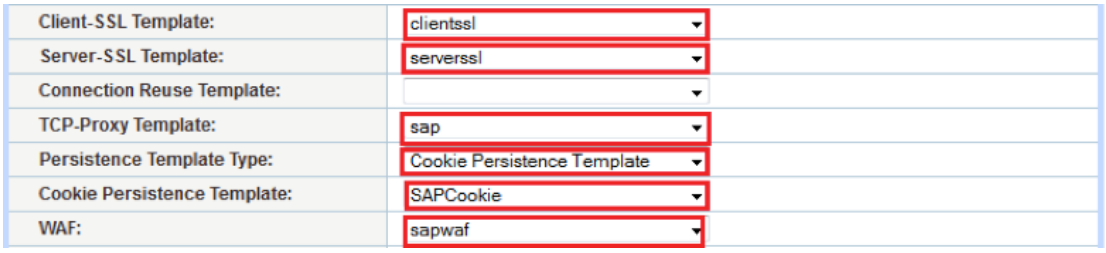

Figure 21: Applying features

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

aFleX Redirect (Optional)

As an added feature to the SAP deployment, it is necessary to add port 80 with an aFleX to redirect script within the "SAPVIP" Virtual Port Lists for SAP clients that are not familiar with the HTTPS URL requirements to get redirected to the correct BOE portal URL address. This feature can be achieved using an aFleX script called "redirect1". This aFleX is pre-canned so no scripting required.

To achieve this feature, add port 80 from the Virtual Port Lists and from the virtual service configurations on port 80, select the option aFleX and select "redirect1".

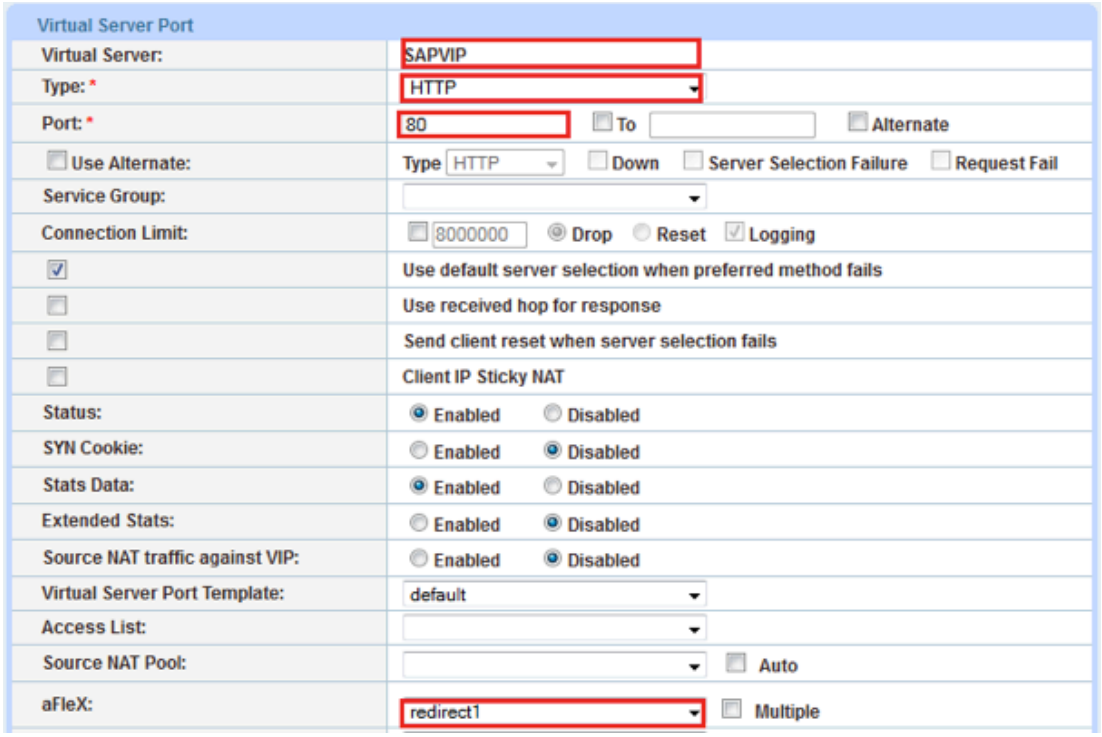

Figure 22: Port 80 redirect feature

Sample Redirect Script:

```
when HTTP_REQUEST {
HTTP::redirect https://[HTTP::host][HTTP::uri]
}
```

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 solution. To deploy this solution, you need to create a WAF template within Config Mode > Security > WAF > Template. Click add.

1. Enter Name: "sapwaf"
2. Select Deployment Mode as "Active"

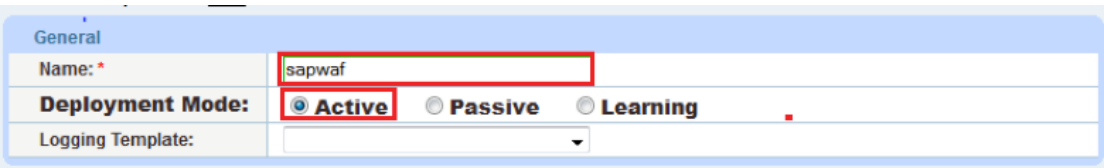

Figure 23: WAF General Configuration

3. This section of the WAF feature is the location to enable the WAF request protection features. To understand the details of each of the features, refer to the A10 Systems and Configuration Guide. Select the needed protection required for your deployment.

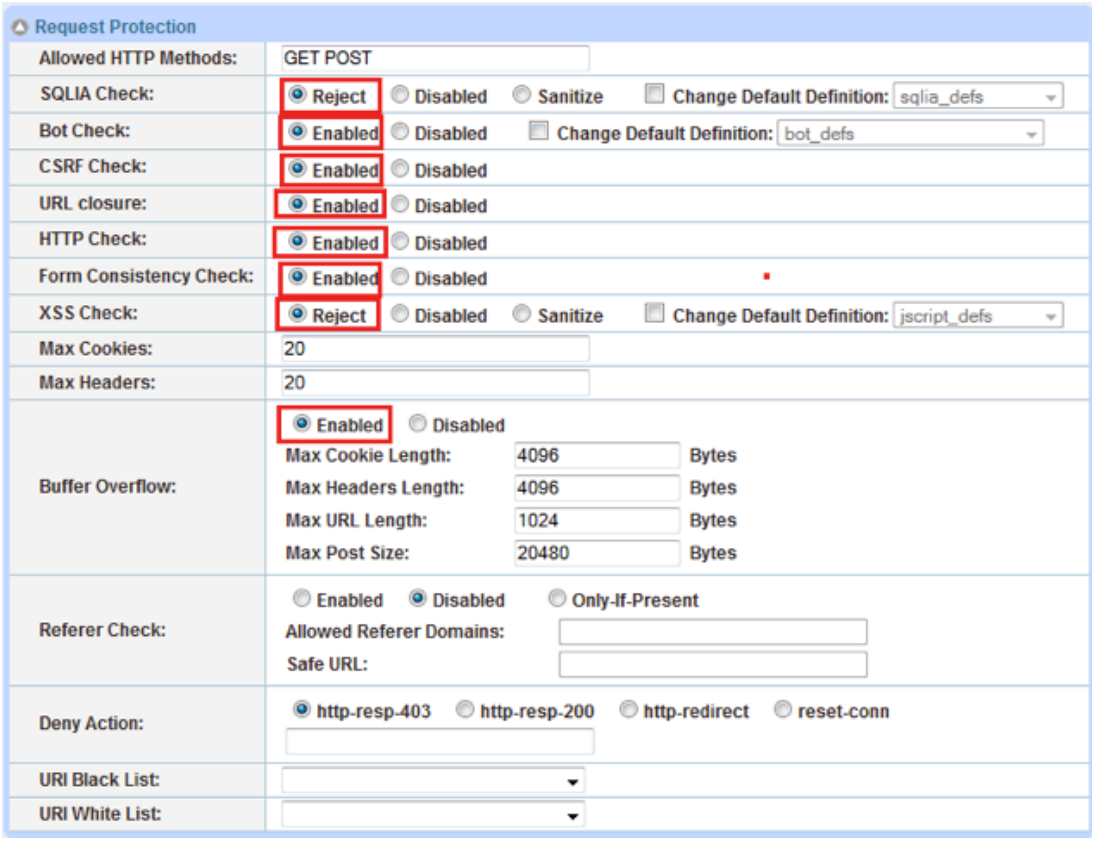

Figure 24: WAF Request Protection Configuration

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

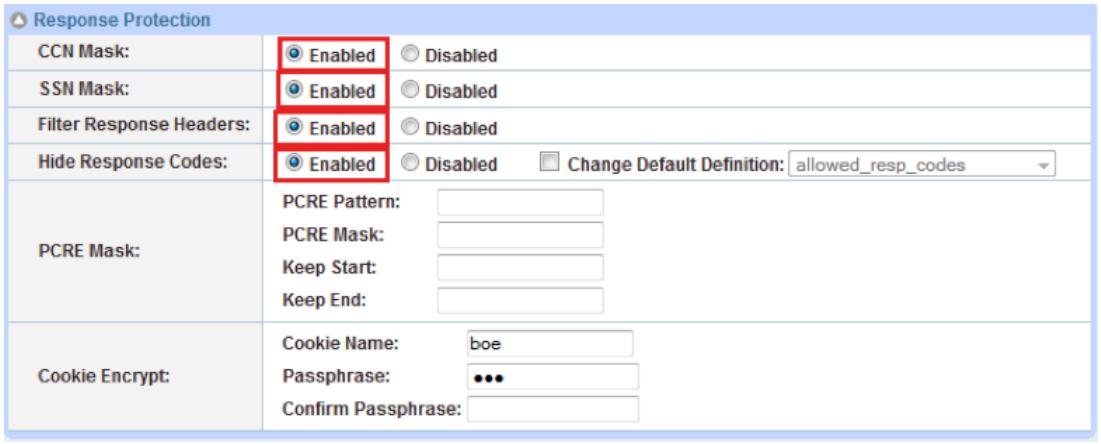

Figure 25: WAF Response Protection Configuration

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

Figure 26: WAF Template Configuration

5. Once completed click "OK" and "Save" configuration

DDOS Mitigation (Optional)

This section is an additional security feature to protect SAP application from DDoS attacks. To configure this feature within the ACOS solution, navigate to Config Mode > Security > Network > DDoS Protection.

The DDoS Protection feature is a global configuration and to enable this feature, select the necessary DDoS attacks you would like to drop. In the diagram below, we have selected the DDoS mitigation attack required.

1. Once completed click "**OK**" and "**Save**" configuration.

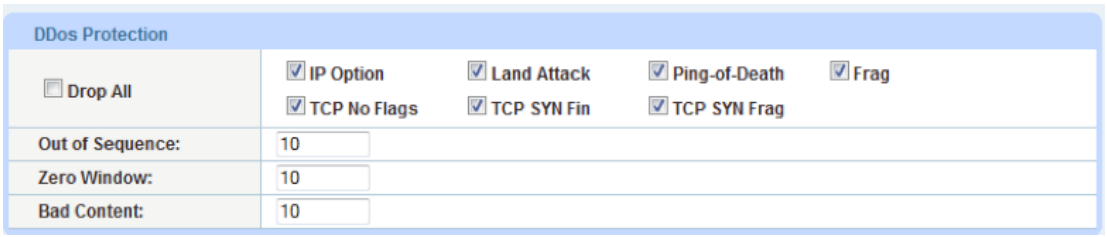

Figure 27: DDoS Protection Configuration

In addition, these two command lines are also required to deploy system-wide PBSLB using CLI.

system pbslb bw-list sap

system pbslb over-limit lockup 5 logging 10

The Black/White list is applied to the system wide PBSLB within a locking time of 5 minutes and loggin interface of 10 minutes.

***Note**: The sample BW-List contains group ID 1; however, you don't need to configure the group ID in aPBSLB 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

In summary, the configuration steps described above show how to set up the Thunder ADC for SAP BusinessObjects Explorer (BOE) in front of HANA. By using the Thunder ADC to load balance BOE web application servers, the following benefits are achieved:

- Higher availability when if an SAP BOE 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 BOE applications and web servers
- Greater connection throughput and faster end user responsiveness by off-loading intensive security processing to the Thunder ADC.
- Additional protection against DDoS attacks and an additional level of protection with the A10 WAF feature.

By using Thunder ADC, significant benefits are achieved for all SAP BusinessObjects 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

Thunder ADC CLI sample configurations:

```
ip nat pool SNAT 10.0.1.145 10.0.1.145 netmask /24
health monitor sgboehc
 method http
slb template server-ssl serverssl
slb server boe2 10.0.1.245
   port 80  tcp
slb server boe1 10.0.1.244
   health-check ping
   port 80  tcp
slb service-group sgboe tcp
    health-check ping
    member boe1:80
    member boe2:80
slb template tcp-proxy sap
   idle-timeout 28800
   receive-buffer 873801
   transmit-buffer 87380
   mss 1460
   initial-window-size 16324
slb template waf sapwaf
   ccn-mask
   ssn-mask
   cookie-encrypt “boe” secret-encrypted
XcB3Vki0oTA8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
slb template client-ssl clientssl
   cert boe
   chain-cert boe
   key boe pass-phrase encrypted
37O48xvi8uY8EIy41dsA5zwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
   session-cache-timeout 28800
   session-cache-size 8000000
   session-ticket-lifetime 28800
slb template persist cookie SAPCookie
   name sapcookie
   domain sap
   expire 15900
   insert-always
   match-type service-group
slb template persist source-ip PortalSIP
   match-type server
slb virtual-server SAPVIP 172.16.1.200
   port 443  https
      source-nat pool SNAT
      service-group sgboe
```

```
    use-rcv-hop-for-resp
    template tcp-proxy sap
    template waf sapwaf
    template client-ssl clientssl
    template server-ssl serverssl
    template persist cookie SAPCookie
port 80  http
    aflex redirect1
```

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

Part Number: A10-DG-16132-EN-01
May 2014

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.