Deployment Guide

Microsoft SharePoint 2013

DG_SP2013_022015

TABLE OF CONTENTS

1 INTRODUCTION

This deployment guide contains detailed procedure to configure A10 Thunder Series Unified Application Service Gateways or AX Series Application Delivery Controllers (ADCs), powered by Advanced Core Operating System (ACOS), to support Microsoft SharePoint 2013.

Microsoft SharePoint is a web application platform, providing intranet portals, content and document management, collaboration, social networks, enterprise search, and business intelligence. Microsoft has been ranked as one of the leaders in the Enterprise Contents Management (ECM) market with SharePoint 2010. SharePoint 2013 has improved its flexibility, scalability and reliability with many of new features and enhancements. SharePoint 2013 is also optimized to support any work style and environment including cloud-based solution.

SharePoint is highly scalable tool and can be deployed with multi-server and multi-layer architecture in order to serve thousands of client access and requests with HTTP and HTTPS protocol. The UASG™ and AX ADC environment with its ACOS has been designed especially for high load applications such as SharePoint, providing better application performance, high resiliency, offloading security processing.

2 PREREQUISITES AND ASSUMPTIONS

This deployment guide has the following prerequisites and assumptions (based on tested configuration).

UASG™ and AX ADC (ACOS device) environment:

- ACOS device should be running ACOS version 2.7.1 or higher. (Tested with 2.7.1-P2)
- SharePoint 2013 has been tested with both A10 hardware and virtual appliances.
- ACOS devices have been tested with Routed mode and One-arm mode configurations.

SharePoint 2013 environment:

- All Microsoft SharePoint 2013 Server components are running on Windows Server 2012 Standard Operating System (64-bit).
- Microsoft SharePoint Server 2013 is installed on application farm with multiple application servers.
- Microsoft SQL Server 2012 SP1 is installed as Database Server.
- For more details of the SharePoint 2013 installation, please refer to appropriate SharePoint documentation:
  http://technet.microsoft.com/EN-US/library/cc303424.aspx

Client environment:

- Windows 7 Operating System (64-bit and 32-bit) are used for Client OS
- Tested client browsers
  - Microsoft Internet Explorer Version 8, 9 and 10
  - Google Chrome Version 28
  - Mozilla Firefox Version 4.0.1

It's important that you make sure that the SharePoint 2013 servers and the SQL database are properly installed and functioning, before installing the ACOS load balancer.

3 DEPLOYMENT OVERVIEW

3.1 SHAREPOINT CONFIGURATION SCENARIOS

SharePoint 2013 uses the server farm model with a multi-tier structure, which offers more scalability and flexibility. A server farm consists of web servers, application servers and database servers. Each group of servers can be called Tier, for example web-tier, application-tier and database-tier.

It's beneficial to have the ACOS device in front of SharePoint web servers as a reverse proxy, which can reduce web server loads and provide higher availability in case of web server failure. In addition, the following application acceleration features, available on the ACOS device, can free server resources and improve the overall performance of SharePoint 2013 environments.

- RAM Caching
- HTTP Compression
- Connection Reuse
- SSL Offload

3.2 TOPOLOGY DIAGRAM

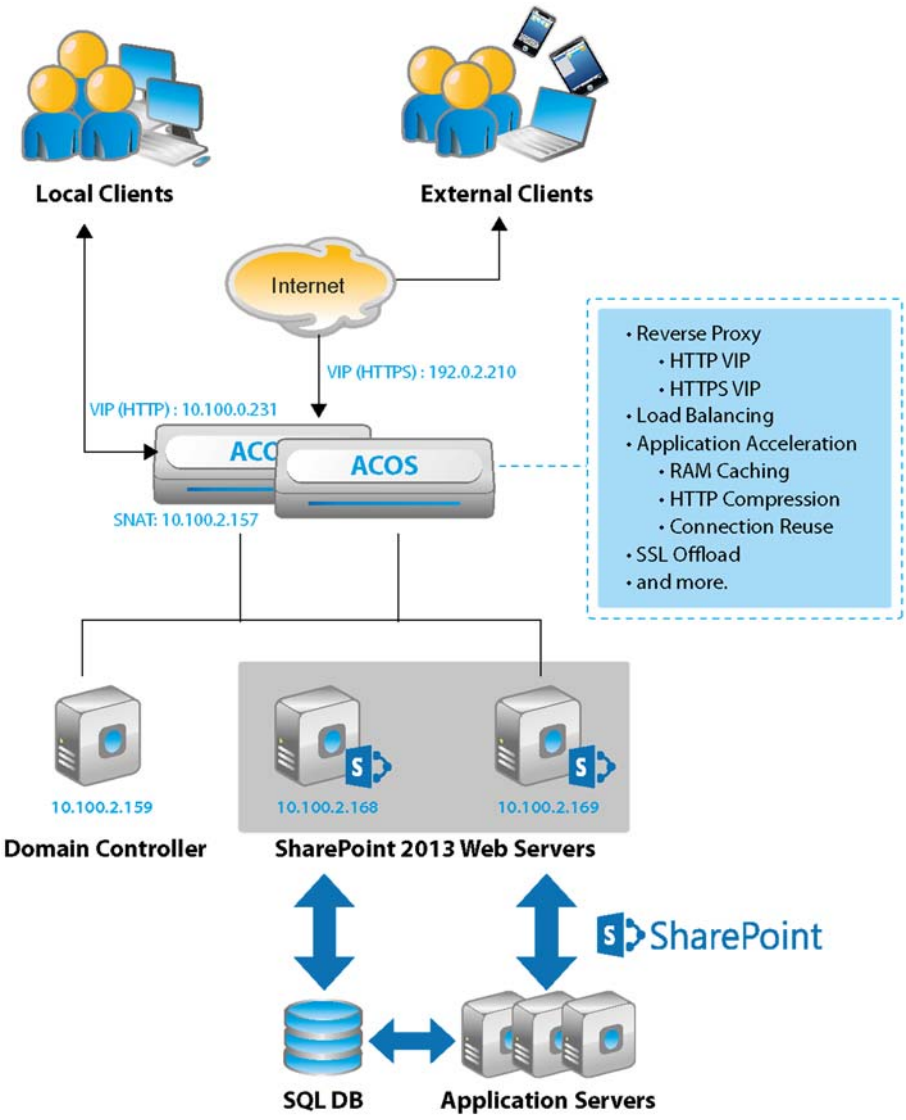


Figure 1: Topology Diagram for SharePoint 2013 with ACOS

3.3 ACOS DEVICE DEPLOYMENT CONSIDERATION

This deployment guide provides the following scenarios including application acceleration features.

3.3.1 CONFIGURE THE ACOS DEVICE FOR SHAREPOINT USING HTTP

This scenario is a basic deployment using HTTP protocol communication and can be used for internal users. ACOS devices are placed in front of SharePoint 2013 web servers and function as a virtual server (VIP) and reverse proxy, offering load balancing, application acceleration, and high availability.

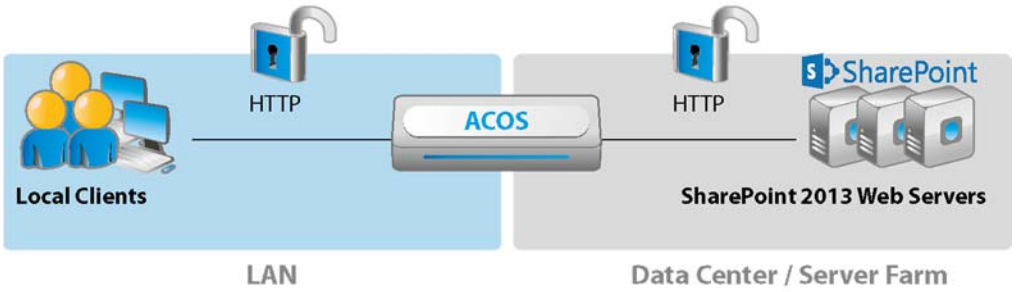


Figure 2: ACOS with HTTP VIP for SharePoint 2013

3.3.2 CONFIGURE THE ACOS DEVICE FOR SHAREPOINT USING HTTPS

This scenario provides secured communication with encrypted traffic using SSL. Typically, there are two options for SSL deployment; SSL offload and SSL bridging. In both options, the ACOS device uses an HTTPS VIP which provides secured communication between clients and ACOS devices. With the SSL bridging option, communication between ACOS device and SharePoint web servers also needs to be encrypted. This can offer end-to-end SSL encrypted communication, which is more secure but adds more load on the SharePoint 2013 web servers for SSL transactions (for example, key exchange, encryption, decryption etc.).

In this example, the SSL offload option is used for simulating external users access through Internet or WAN. This option offers secured communications over the Internet/WAN and also improves server efficiency by offloading SSL transaction on the SharePoint 2013 web server.

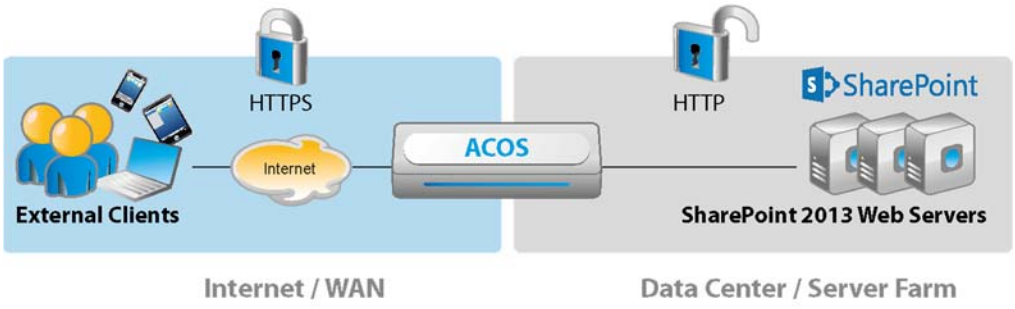


Figure 3: ACOS with HTTPS VIP for SharePoint 2013

3.4 CHANGES IN SHAREPOINT 2013

There are numerous changes added into SharePoint 2013 from SharePoint 2010. However, basic functionalities and architecture are inherited from SharePoint 2010. Therefore, most ACOS device configurations for SharePoint 2010 can be applicable to SharePoint 2013 deployments. This section explains the following features on SharePoint 2013 which might require configuration changes on the ACOS device.

3.4.1 DISTRIBUTED CACHE SERVICE

This feature stores each user login token in the distributed Cache Service and shares the authentication information among all the SharePoint 2013 web servers. Therefore, SharePoint 2013 does not require load balancers affinity (also known as session persistence) anymore.

For more details of the Distributed Cache Service, refer to SharePoint documentation: http://technet.microsoft.com/en-us/library/jj219758.aspx.

3.4.2 REQUEST MANAGEMENT

This feature helps the farm to manage incoming requests by evaluating logic rules in order to determine which action to take, and which server(s) should handle the requests. This is effective for medium to large size SharePoint 2013 farms, along with load balancer appliances such as the ACOS device. With this feature, it is recommended to use the "Least Connections" load balancing algorithm on the ACOS device.

For more details on Request Management, refer to SharePoint documentation: http://social.technet.microsoft.com/wiki/contents/articles/16177.request-management-in-sharepoint-2013.aspx

4 ACCESSING THE ACOS DEVICE

This section describes how to access the ACOS device. The ACOS device 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 ACOS device.*
- Access information:
  - Default Username: admin
  - Default password: a10
  - Default IP Address of the device: 172.31.31.31

For more information on how to access the ACOS device, refer to document "*System Configuration and Administration Guide*"

5 CONFIGURING THE ACOS DEVICE FOR SHAREPOINT 2013 USING HTTP

This section describes how to configure the ACOS device to load balance SharePoint web servers using the HTTP protocol, which is a scenario for internal users. This includes the application acceleration features in addition to normal real server and virtual server configuration.

5.1 CONFIGURATION STEPS

This section describes configuration steps for SharePoint 2013 using HTTP protocol. Following are the high level configuration steps in this example:

- Real server configuration
  - Health Monitor
  - Real Servers
- Service group configuration
- Virtual server configuration
  - IP Source NAT
  - RAM Caching
  - HTTP Compression
  - Connection Reuse
  - HTTP Virtual Server (VIP)

5.2 SERVER CONFIGURATION

5.2.1 HEALTH MONITOR CONFIGURATION

The ACOS device can regularly check the health of real servers and service ports. Health checks are used to assure that all the requests from clients are directed only to functional and available servers. If a real server or service does not respond appropriately to a health check, the server is removed from the list of available servers until it responds to the health checks appropriately. At this point, the server is automatically added back to the list of available servers.

You can use default health monitor (ping) and/or customized health monitors. The configuration in this guide uses default and custom HTTP health monitors.

The example below describes how to create a Health Monitor sending HTTP GET request and expecting HTTP 401 response.

1. Navigate to **Config Mode > SLB > Health Monitor > Health Monitor**.
2. Click **Add** to create a new health monitor.

3. In the **Health Monitor** box, enter **Name** "HM-HTTP".
4. In the **Method** box, enter the following information:
   - **Type**: HTTP
   - **Port**: 80
   - **Host**: sp
   - **URL**: GET and /
   - **Expect**: 401
5. Click **OK**. The health monitor appears in the health monitor table.

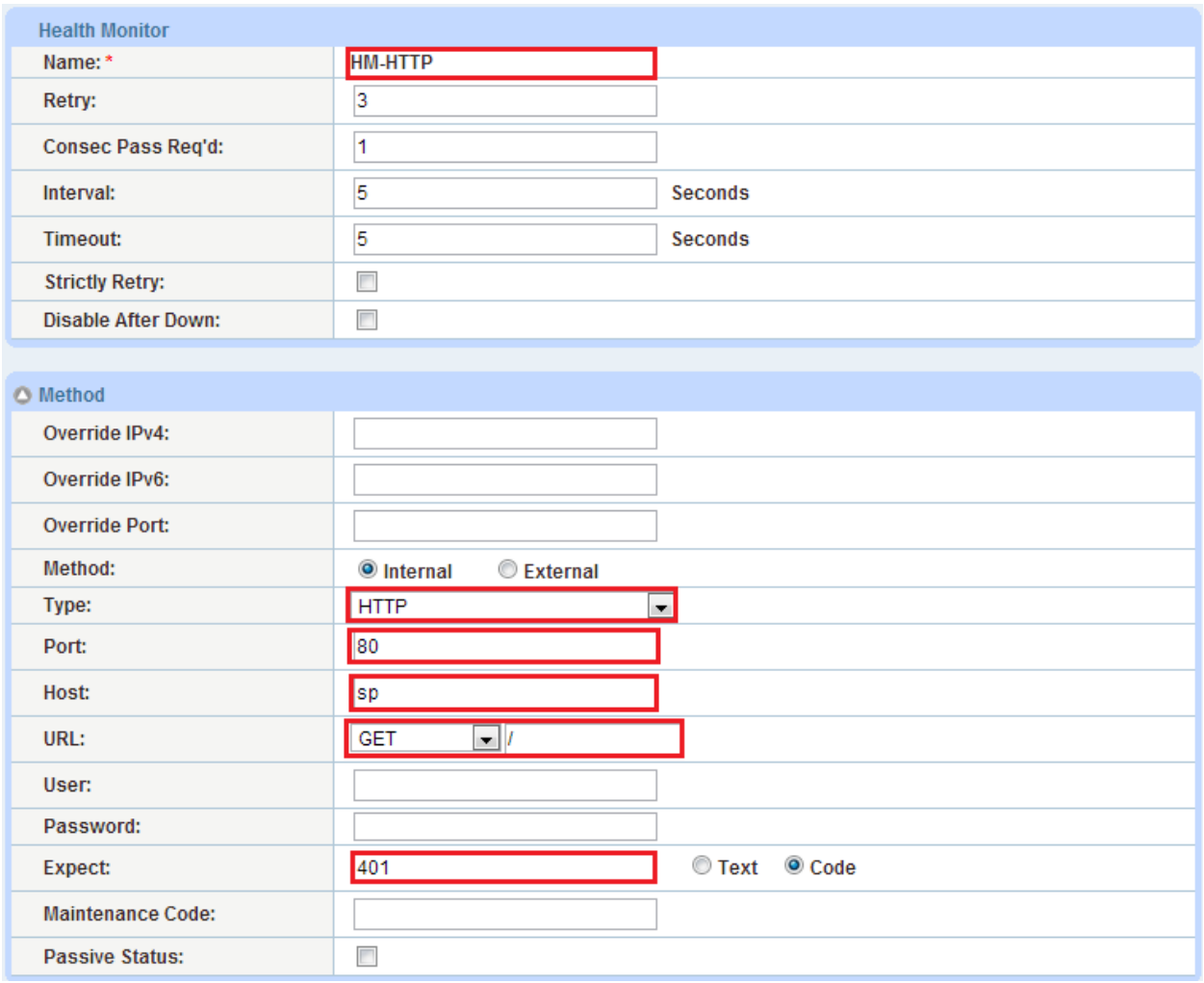


Figure 4: Health Monitor configuration

5.2.2 REAL SERVER CONFIGURATION

This section describes how to configure SharePoint web servers as real servers on the ACOS device. You need to configure a separate server for each SharePoint web server. In this example, both default health monitor and customer health monitor are applied to the real server configuration.

1. Navigate to **Config Mode > SLB > Service > Server**.
2. Click **Add** to add a new server.
3. In the **General** box, configure the information of real server. In this example, use the following information.
   - **Name**: SRV-SharePoint1
   - **IP address / Host**: 10.100.2.168
   - **Health Monitor**: leave the "default" health monitor selected
   - Configure other options as needed.

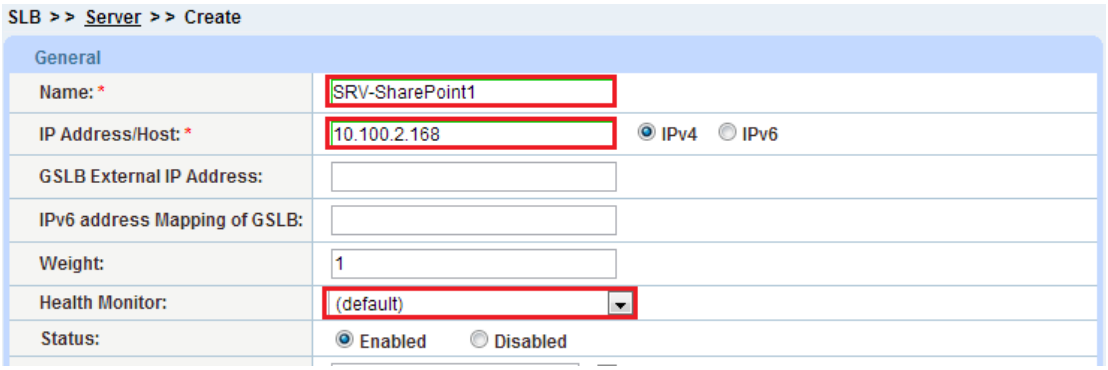


Figure 5: Real Server - General configuration

4. In the Port box, enter the number of the service port and other settings for the real server. In this example, use the following information.
   - **Port**: 80
   - **Protocol**: TCP
   - **Health Monitor (HM)**: Select "HM-HTTP" (configured in the previous section) from drop-down menu.
   - Click **Add**.

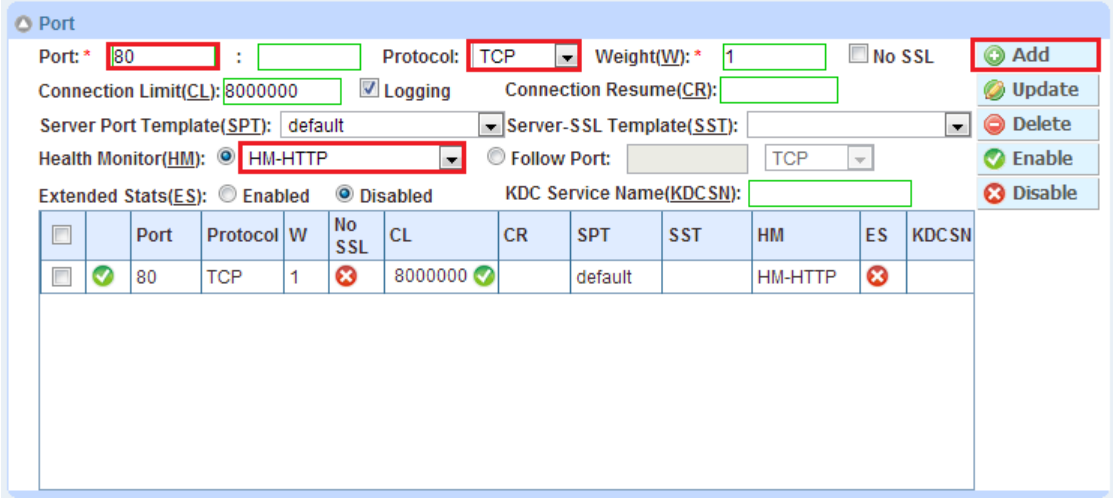


Figure 6: Real Server - Port configuration

5. Repeat the above steps (2-4) for each of the SharePoint web servers.
6. Click **OK**, and then click **Save** to store your configuration changes.

5.3 SERVICE GROUP CONFIGURATION

A service group contains a set of real servers that provide the same service, and makes one logical server, from which the ACOS device can select to service client requests. This example uses a service group that contains SharePoint 2013 web servers and the applicable service port 80.

1. Navigate to **Config Mode > SLB > Service > Service Group**.
2. Click **Add** to add a new service group.
3. In the **Server Group** box, enter the following information:
   - **Name**: SG-SharePoint
   - **Type**: Select "TCP" from the drop-down menu.
   - **Algorithm**: Select "Least Connection" from the drop-down menu.
   - **Health Monitor**: Select "HM-HTTP" from the drop-down menu.

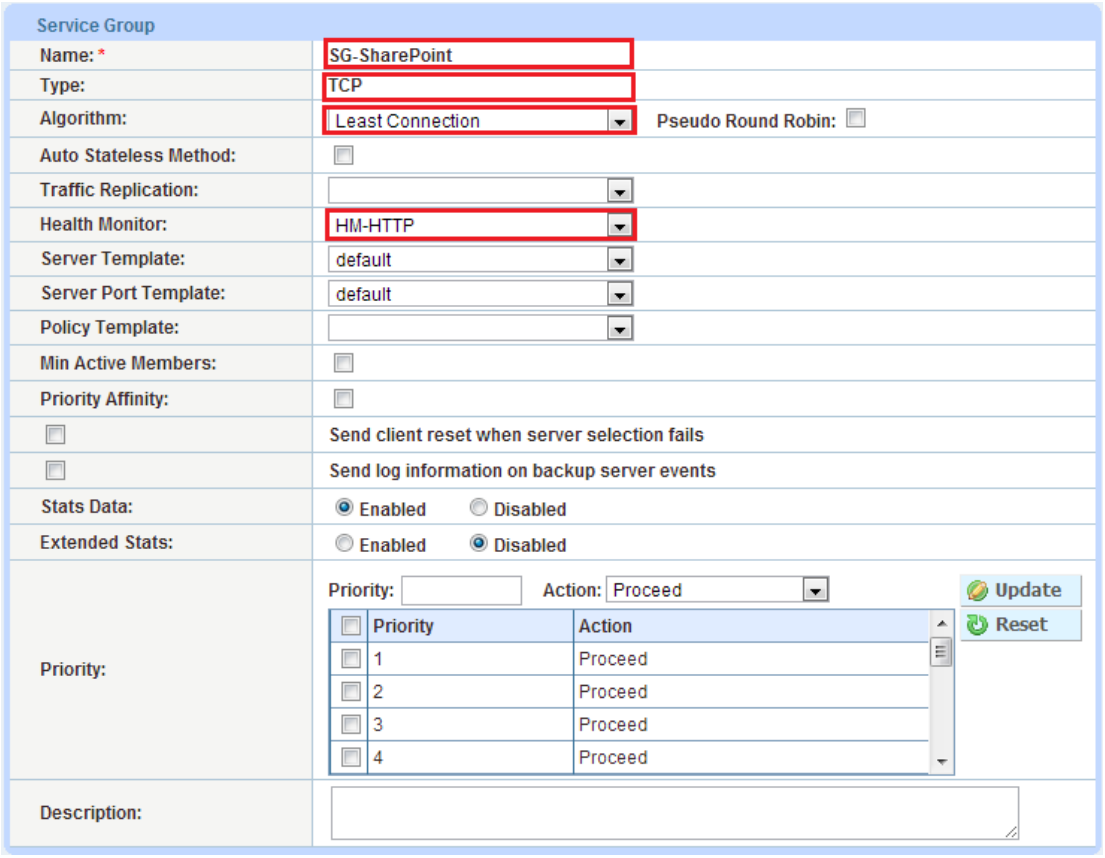


Figure 7: Service group configuration

4. In the **Server** box, add real servers with specifying the service port fop each SharePoint web server.

   - **Server**: Select "SRV-SharePoint1" from drop-down menu.
   - **Port**: 80
   - Click **Add**.
   - Repeat this step for each real server.

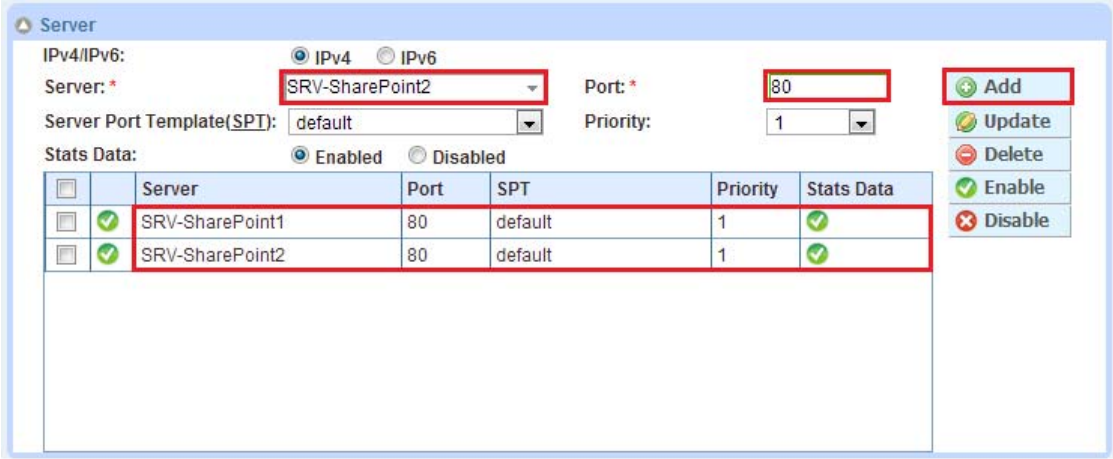


Figure 8: Service group servers list

5. Click **OK,** and then click **Save** to store your configuration changes.

5.4 VIRTUAL SERVER CONFIGURATION

5.4.1 IP SOURCE NAT CONFIGURATION

This step configures the IP address pool to use for IP Source Network Address Translation (SNAT). When traffic from clients hit the Virtual Server (VIP), the ACOS device replaces the source IP address of the clients' request with an IP address from the SNAT pool.

1. Navigate to **Config Mode > IP Source NAT > IPv4 Pool**.
2. Click **Add**.
3. In the **IPv4 Pool** box, enter the following values:
   - **Name**: SNAT1
   - **Start IP Address**: 10.100.2.157
   - **End IP Address**: 10.100.2.157
   - **Netmask**: 255.255.255.0

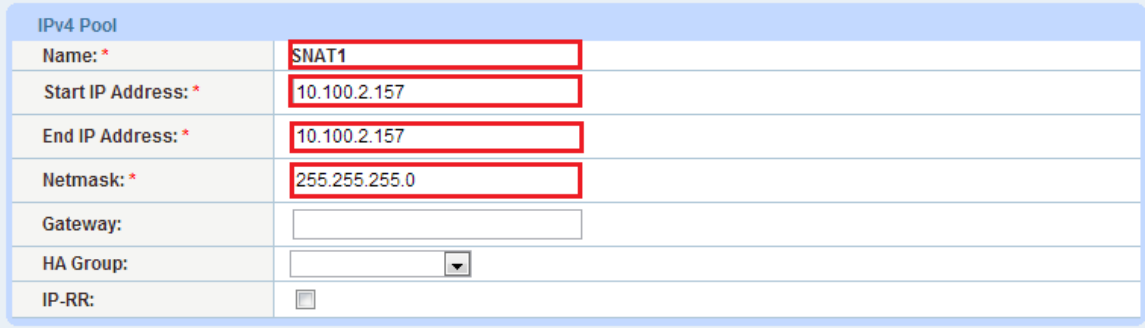


Figure 9: SNAT configuration

4. Click **OK**, then click **Save** to save the configuration.

5.4.2 RAM CACHING TEMPLATE CONFIGURATION

RAM Caching is a high-performance, in-memory Web cache that by default caches HTTP responses (RFC 2616 compliant). It can results in significant reduction in the load of the SharePoint web server and also latency and bandwidth utilization in the server farm.

1. Navigate to **Config Mode > SLB > Template > Application > RAM Caching**.
2. Click **Add**.
3. In the **RAM Caching** box, enter or select the following values:
   - **Name**: RC-SharePoint
   - **Replacement Policy**: Least Frequently Used (default)
   - All other values: Use default value in this example.

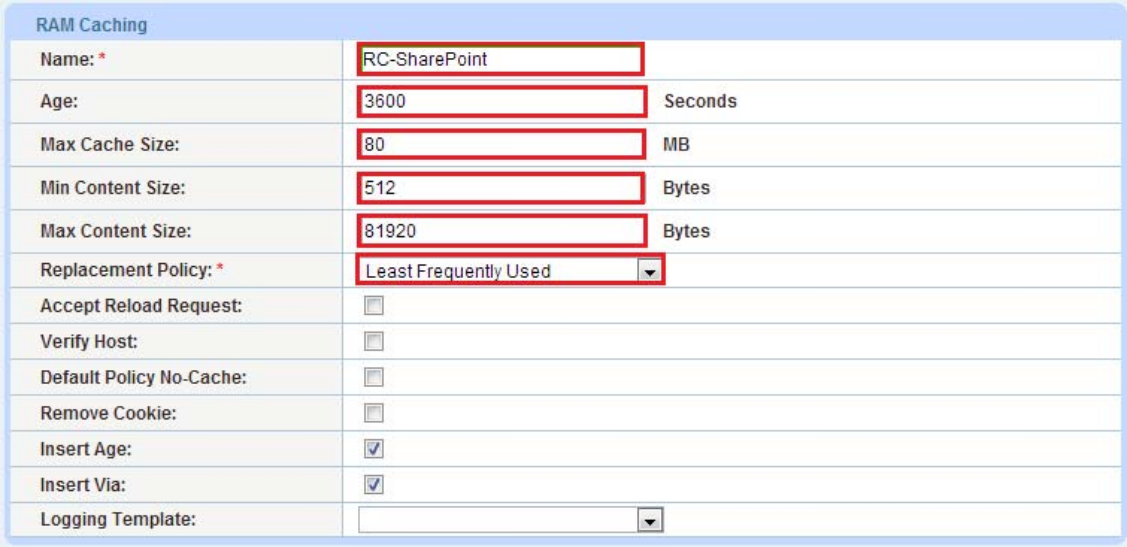


Figure 10: RAM Caching configuration

4. Click **OK**, then click **Save** to save the configuration.

5.4.3 HTTP TEMPLATE CONFIGURATION FOR HTTP COMPRESSION

HTTP templates have many options, including options to modify the HTTP header information, and URL based switching and more. You can use these options per your deployment requirement. In this example, it describes how to configure HTTP compression feature on the HTTP template.

1. Navigate to **Config Mode > SLB > Template > Application > HTTP**.
2. Click **Add**.
3. In the **HTTP** box, enter the **Name** "HTTP-Template-SharePoint".

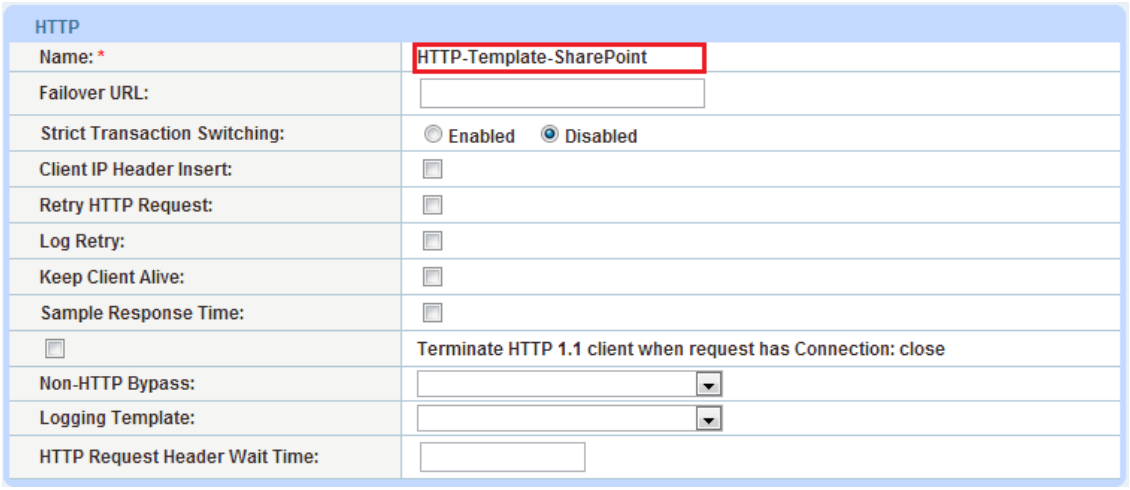


Figure 11: HTTP Template configuration

4. Click and expand the **Compression** box.

5. Select "Enabled" radio button on the **Compression** and choose **Level** "1(least compression, fastest)" (default)

6. (Optional) Add the **Content Type** to be specifically compressed. In this example, use "pdf", "pptx", and "doc" and click **Add** for each.

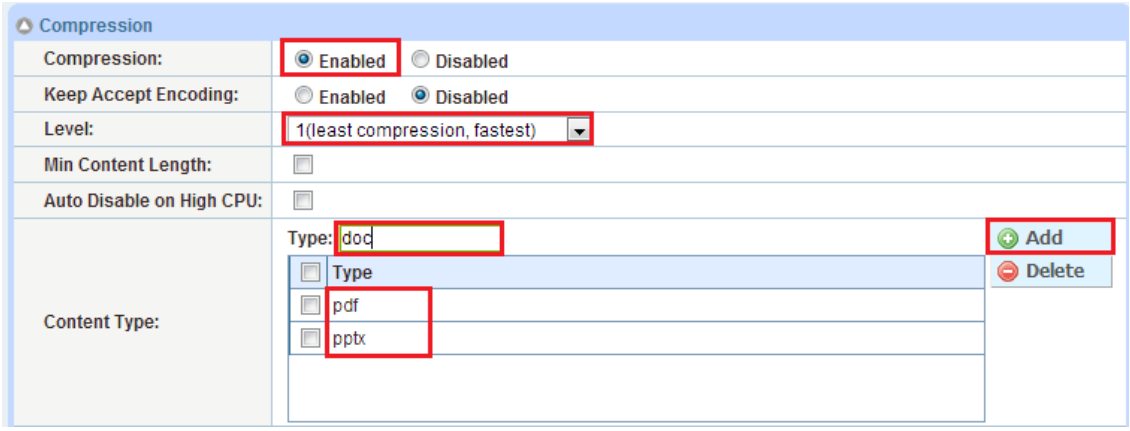


Figure 12: HTTP Compression configuration

7. Click **OK**, then click **Save** to save the configuration.

5.4.4 TCP CONNECTION REUSE

Connection Reuse reduces the overhead associated with setting up TCP connections (3-way handshake), by establishing persistent TCP connections with SharePoint web servers and then multiplexing client TCP requests over those connections. This feature offers a significant benefit as it eliminates the need of opening new connections for every single client connection.

***Note**: You must have SNAT when you use Connection Reuse feature*

1. Navigate to **Config Mode > SLB > Template > Connection Reuse**.
2. Click **Add**.
3. In the **Connection Reuse** box, enter the **Name** "CR-Share-Point".

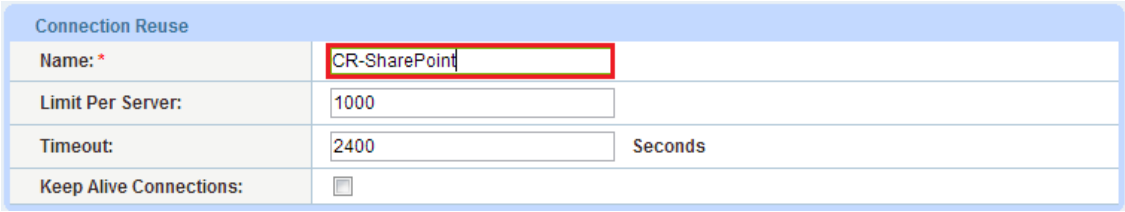


Figure 13: Connection Reuse configuration

4. Click **OK**, then click **Save** to save the configuration.

5.4.5 HTTP VIRTUAL SERVER (VIP) CONFIGURATION

The virtual server is also called VIP (Virtual IP) where the client will send SharePoint access requests to. The VIP consists of service groups and protocol port numbers, which are also bound with multiple feature templates configured in the previous sections.

In this example, SharePoint 2013 VIP is configured with HTTP (port 80) for internal users.

1. Navigate to **Config Mode > SLB > Service > Virtual Service**.
2. Click **Add** to add a new virtual server.
3. In the **General** box, enter the name of the Virtual IP (VIP) and its IP address:
   - **Name**: VIP-SharePoint
   - **IP Address**: 10.100.0.231

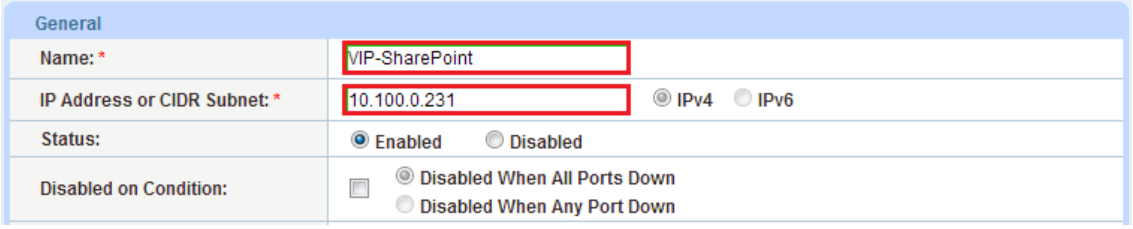


Figure 14: HTTP VIP - General configuration

4. In the **Port** box, click **Add**. The **SLB >> Virtual Server >> *VIP-SharePoint* >> Port >> Create** screen appears.

5. In the **Virtual Server Port** box, enter the following information

   - **Type**: Select "HTTP" from the drop-down menu.
   - **Port**: 80
   - **Service Group**: Select "SG-SharePoint" from the drop-down menu.

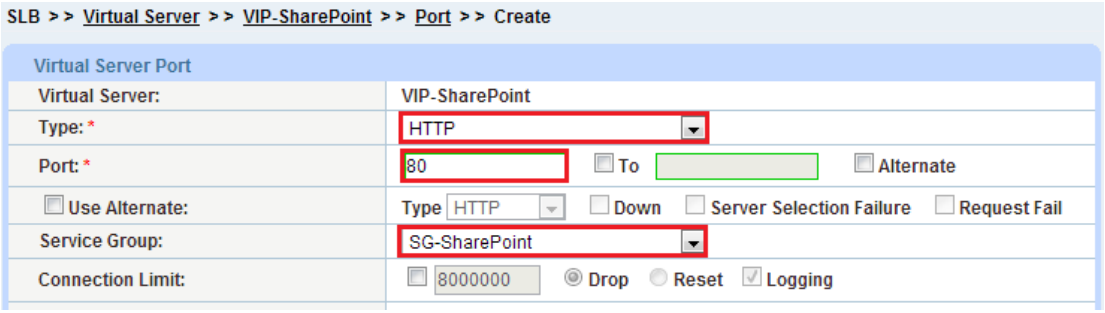


Figure 15: HTTP VIP - Virtual Port configuration

6. In the **Virtual Server Port** box, apply the following feature templates:

   - **Source NAT Pool**: SNAT1
   - **HTTP Template**: HTTP-Template-SharePoint
   - **RAM Caching Template**: RC-SharePoint
   - **Connection Reuse Template**: CR-SharePoint

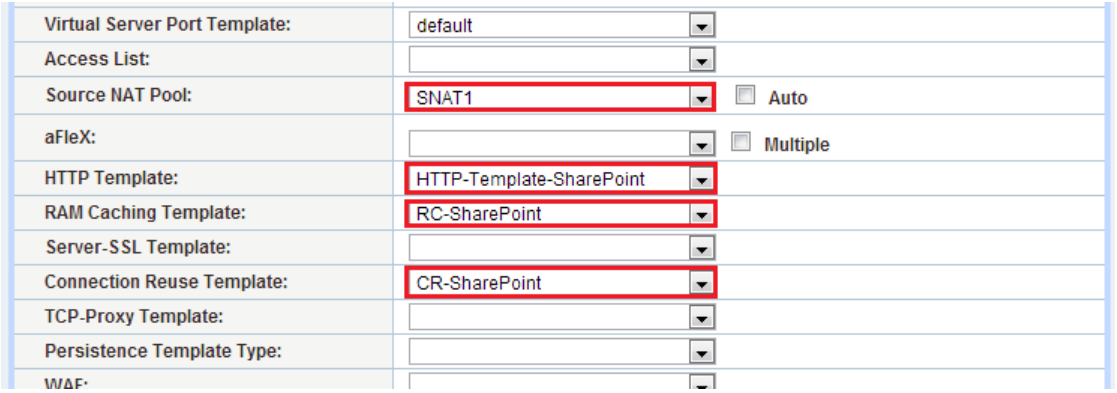


Figure 16: HTTP VIP - applying templates

7. Click **OK**. The virtual server port appears in the list of the **Port** box.

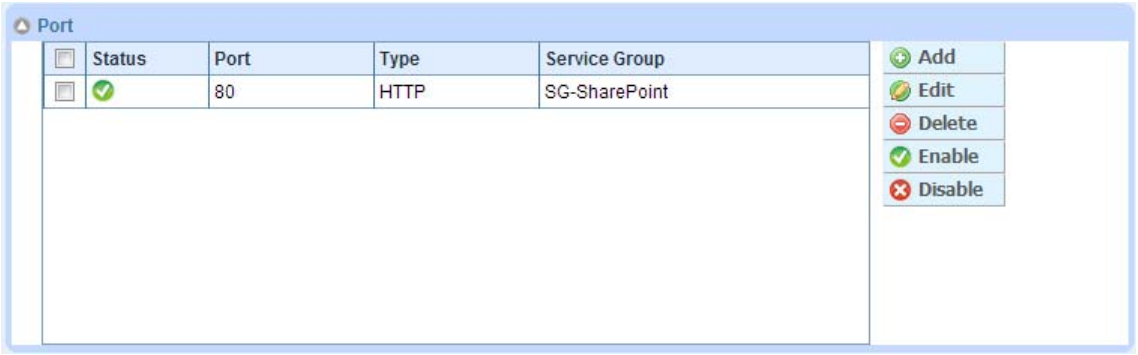


Figure 17: HTTP VIP - Virtual Port list

8. Click **OK**, then click **Save** to save the configuration.

5.5 DEPLOYMENT VALIDATION

To validate that the HTTP VIP configuration is functioning correctly, do the following.

1. Open a web browser and navigate to the SharePoint 2013 using appropriate URL and login to the SharePoint 2013. For example, http://sp.example.com or http://sp.

2. Make sure that you can successfully access and open the SharePoint 2013 site using the HTTP protocol

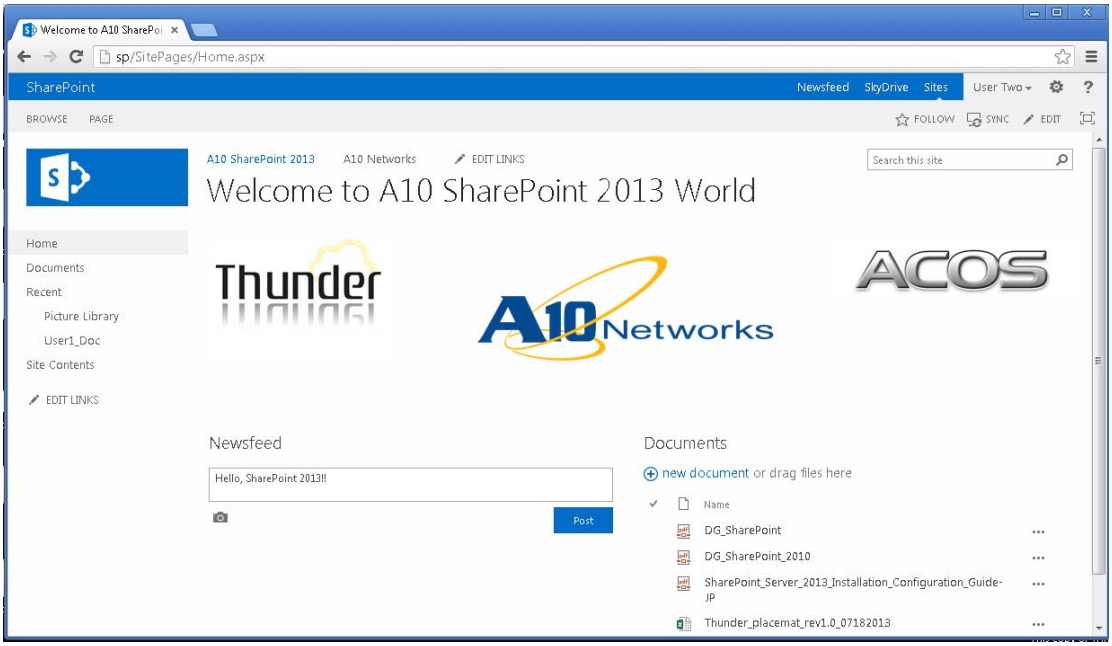


Figure 18: Connection to SharePoint 2013 through HTTP VIP

3. On the ACOS device, navigate to **Monitor Mode > SLB > Service > Virtual Server**.

4. Check virtual server status (In this example, VIP-SharePoint-EXT/192.0.2.210) showing green , and also statistics on the HTTPS virtual port (HTTPS/443) are increased

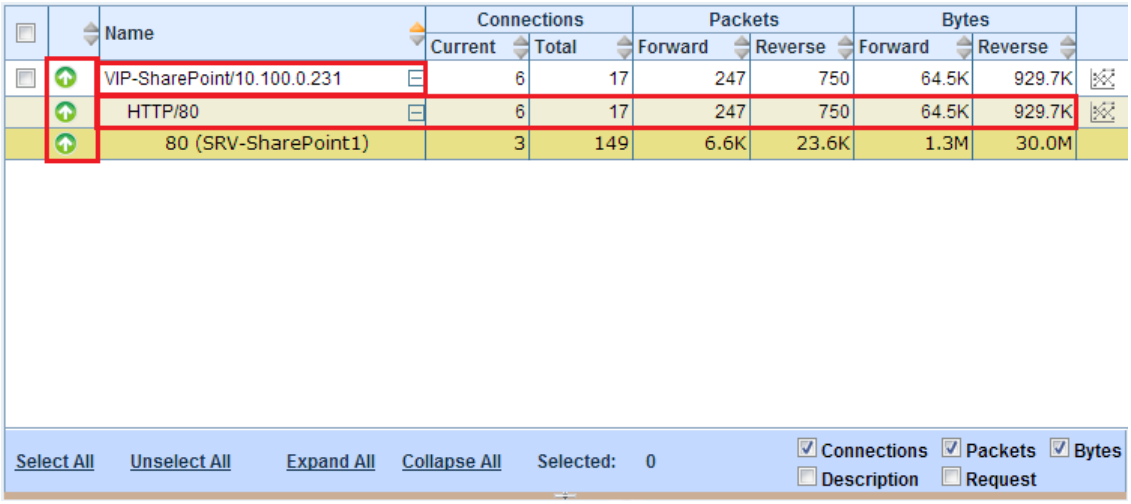


Figure 19: VIP status and Virtual Port statistics view

6 CONFIGURING THE ACOS DEVICE FOR SHAREPOINT 2013 USING HTTPS

This section describes how to configure the ACOS device to load balance SharePoint web servers using HTTPS (SSL) to securely encrypt communication from the client to the ACOS device. With this configuration, there are two options for SSL deployments—SSL offload and SSL bridging. Utilizing SSL for encryption on the load balancer reduces web server CPU utilization and simplifies management with a single place to manage site certificates.

6.1 CONFIGURATION STEPS

To configure the ACOS device to load balance SharePoint web servers over SSL, you can use most of the steps described in section 5.2 Server Configuration and 5.3 Service Group Configuration.

In this example, a new virtual server (VIP) for HTTPS is created, that uses existing real servers and service group configurations. On the virtual server configuration, service type HTTPS is used, which requires additional configuration steps regarding SSL certificate and template.

6.2 SSL PREPARATION

Before configuring the virtual server, the following additional steps also are required:

- SSL certificate configuration
- SSL client template configuration
- Rewriting redirect URL using aFleX (optional)

6.2.1 SSL CERTIFICATE CONFIGURATION

You can import or create SSL certificates for SSL communication. In this example, a certificate and key are created.

1. Navigate to **Config Mode > SLB > SSL Management > Certificate**.
2. Click **Create** to add a new SSL certificate.
3. Enter the following information and values to issue a self-signed certificate:
   - **File Name**: SP2013-CERT
   - **Issuer**: Self

- **Common Name**: sharepoint.example.com
- **Division**: EXAMPLE
- **Organization**: EXAMPLE
- **Country**: United State of America
- **Valid Days**: 730 (Default)
- **Key Size**: 2048

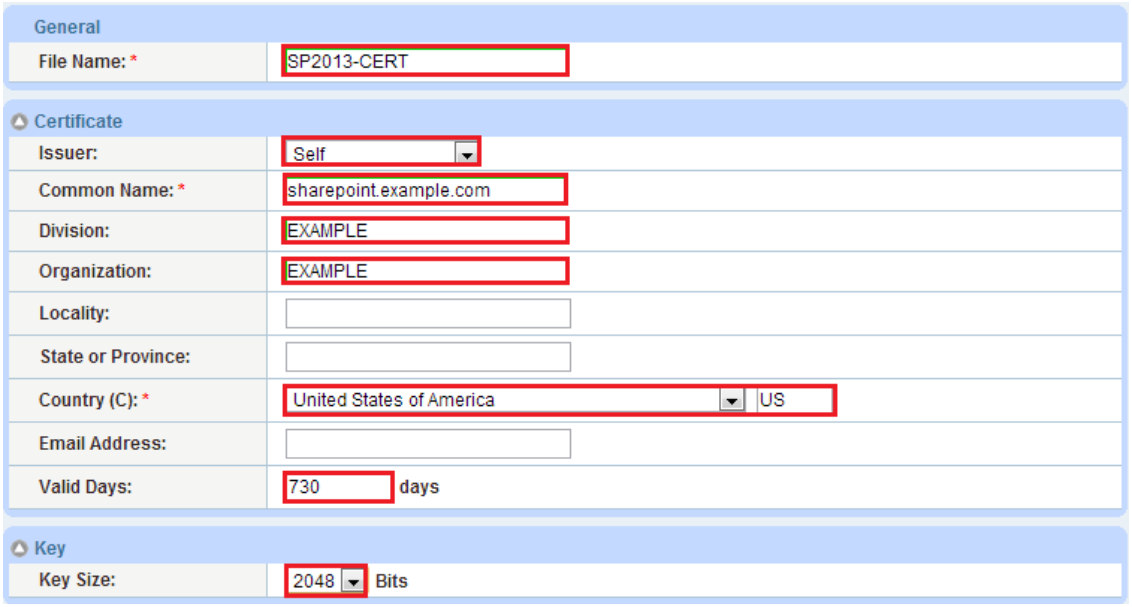


Figure 20: SSL Certificate creation

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

6.2.2 SSL CLIENT TEMPLATE CONFIGURATION

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** to create a Client SSL template.
3. Enter the following information
   - **Name**: SP2013-SSL

- **Certificate Name**: SP2013-CERT
- **Key Name**: SP2013-CERT

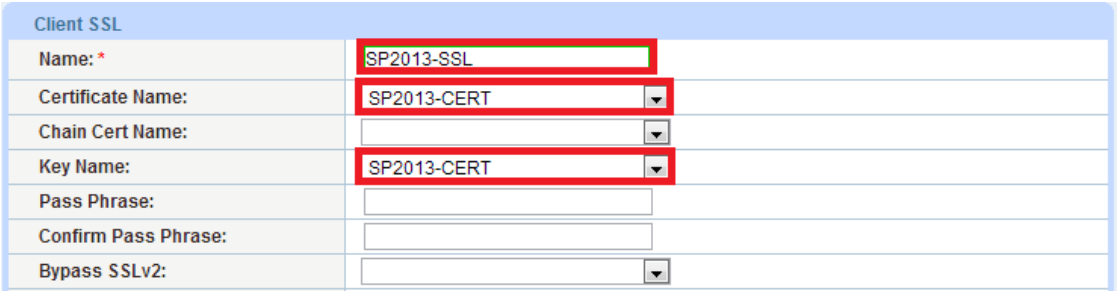


Figure 21: SSL Client Template configuration

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

6.3 VIRTUAL SERVER (VIP) CONFIGURATION

6.3.1 REWRITING REDIRECT URL IN HTTP RESPONSE USING AFLEX (OPTIONAL)

In some cases of SSL offload topology, SharePoint 2013 web servers may return HTTP Redirect (code 302) messages, including a redirect URL (absolute link) with HTTP protocol. Therefore, you may need to rewrite the redirect URL with HTTPS on the ACOS device. This section describes how to transparently rewrite the redirect HTTP URL in the HTTP response payload with the HTTP URL by using ACOS aFleX scripting.

1. Navigate to **Config Mode > SLB > aFleX**.
2. Click **Add**.
3. Enter the **Name**: REWRITE-TO-HTTPS

4. In the **Definition** field, enter the following script.

```
when HTTP_RESPONSE {
 # check Content-Type to avoid unnecessary collects
  if { [HTTP::header "Content-Type"] contains "text" } {
    HTTP::collect
  }
}


when HTTP_RESPONSE_DATA {
  set clen [HTTP::payload length]
  regsub -all "http://" [HTTP::payload] "https://" newdata
  HTTP::payload replace 0 $clen $newdata
  HTTP::release
}
```

***Note**: This script is also available as a part of predefined aFleX script "http_payload_replace"*

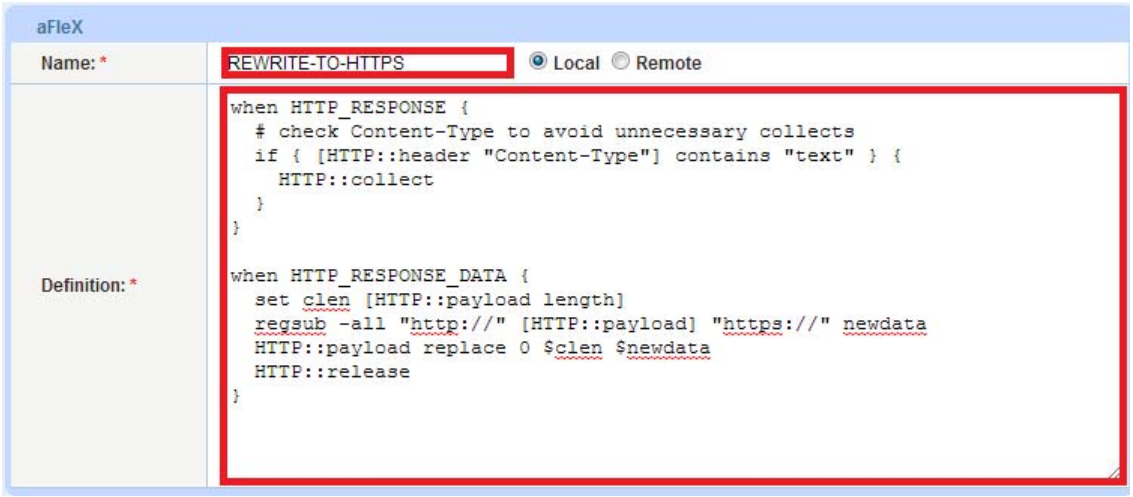


Figure 22: aFleX script

5. Click **OK**, then click **Save** to save the configuration.

6.3.2 HTTPS VIRTUAL SERVER (VIP) CONFIGURATION

This section describes how to create an HTTPS VIP for SSL offload on the ACOS device. You can also apply all the feature templates configured in the previous sections to this HTTPS VIP.

In this example, a new SharePoint 2013 VIP is configured with HTTPS (port 443) for external users via Internet or WAN. SharePoint 2013 web servers are running services on HTTP (port 80).

1. Navigate to **Config Mode > SLB > Service > Virtual Service**.
2. Click **Add** to add a new virtual server.
3. In the **General** box, enter the name of the Virtual IP (VIP) and its IP address:
   - **Name**: VIP-SharePoint-Ext
   - **IP Address**: 192.0.2.210

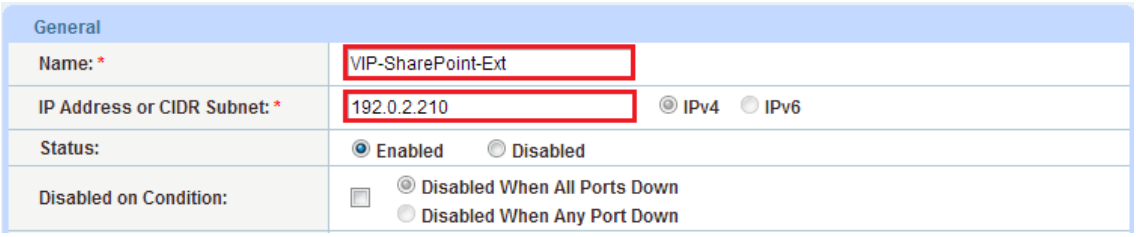


Figure 23: HTTPS VIP - General configuration

4. In the **Port** box, click **Add**. The **SLB > Virtual Server > *VIP-SharePoint* > Port > Create** screen appears.
5. In the **Virtual Server Port** box, enter the following information
   - **Type**: Select "HTTPS" from the drop-down menu.
   - **Port**: 443
   - **Service Group**: Select "SG-SharePoint" from the drop-down menu.

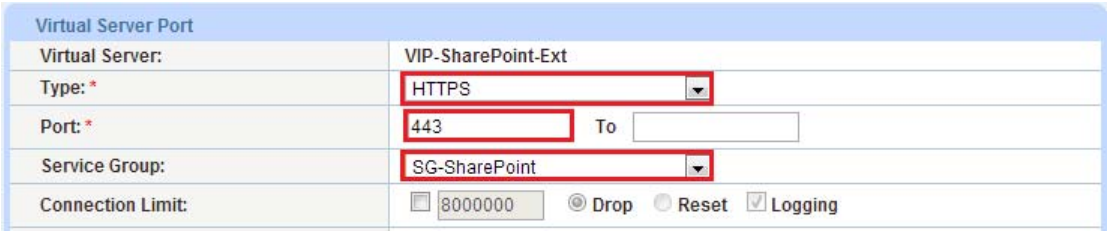


Figure 24: HTTPS VIP - Virtual Port configuration

6. In the **Virtual Server Port** box, apply the following feature templates and aFleX script:

   - **Source NAT Pool**: SNAT1
   - **aFleX**: REWRITE-TO-HTTPS
   - **HTTP Template**: HTTP-Template-SharePoint
   - **RAM Caching Template**: RC-SharePoint
   - **Connection Reuse Template**: CR-SharePoint

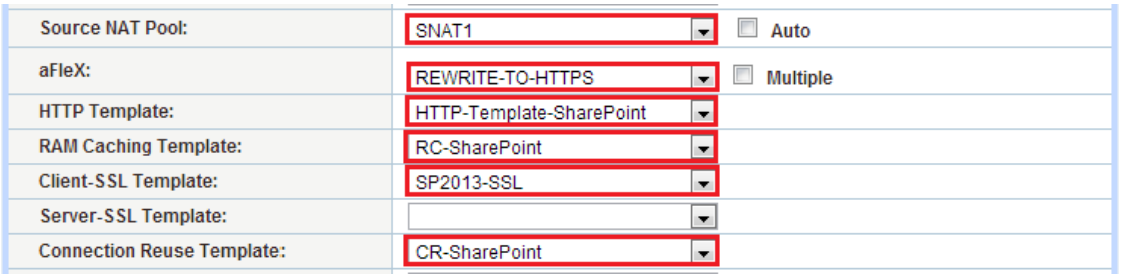


Figure 25: HTTPS VIP - applying templates

7. Click **OK**. The virtual server port appears in the list of the **Port** box.

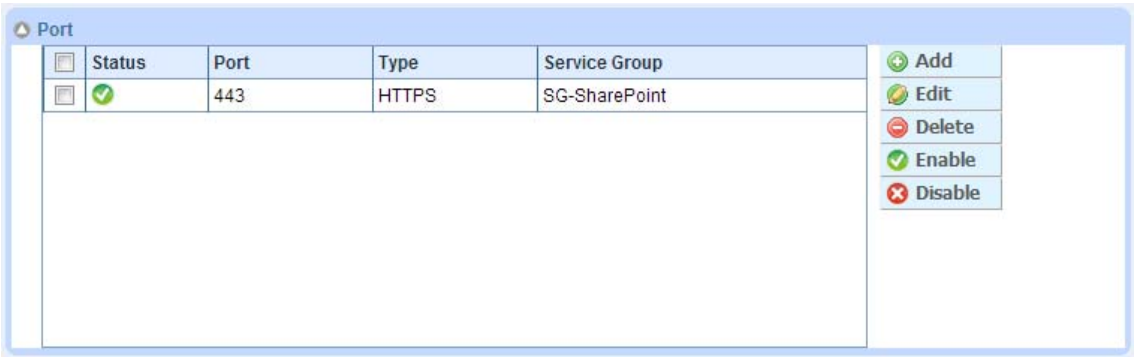


Figure 26: HTTPS VIP - Virtual Port list

8. Click **OK**, then click **Save** to save the configuration.

6.3.3 REDIRECTING CLIENT ACCESS FROM HTTP TO HTTPS (OPTIONAL)

This section describes how to redirect SharePoint access requests for HTTP (port 80) to HTTPS (port 443) using ACOS aFleX scripts. This is one of the most common methods used for HTTPS VIP service and ACOS has a preconfigured aFleX script called "redirect1".

In this example, a new virtual port with HTTP (port 80) is created on the VIP-SharePoint-Ext and the aFleX script redirect1 is applied on to it.

1. Navigate to **Config Mode > SLB > Service > Virtual Service**.
2. Select "VIP-SharePoint-Ext" from the virtual server list.
3. In the **Port** box, click **Add** to add a new virtual port.
4. In the **Virtual Server Port** box, enter the following information
   - **Type**: Select "HTTP" from the drop-down menu.
   - **Port**: 80
   - **Service Group**: Select "SG-SharePoint" from the drop-down menu.
   - **aFleX**: Select "redirect1" from the drop-down menu.

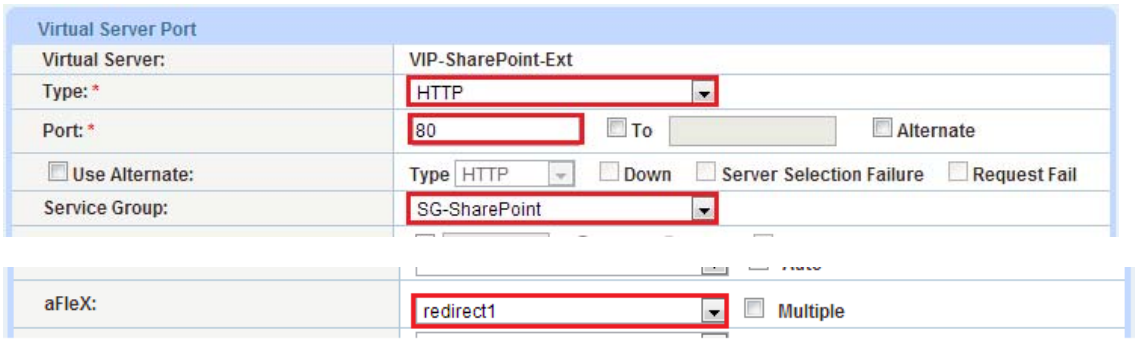


Figure 27: HTTPS VIP - HTTP redirect configuration

5. Click **OK**. The virtual server port appears in the list of the **Port** box.

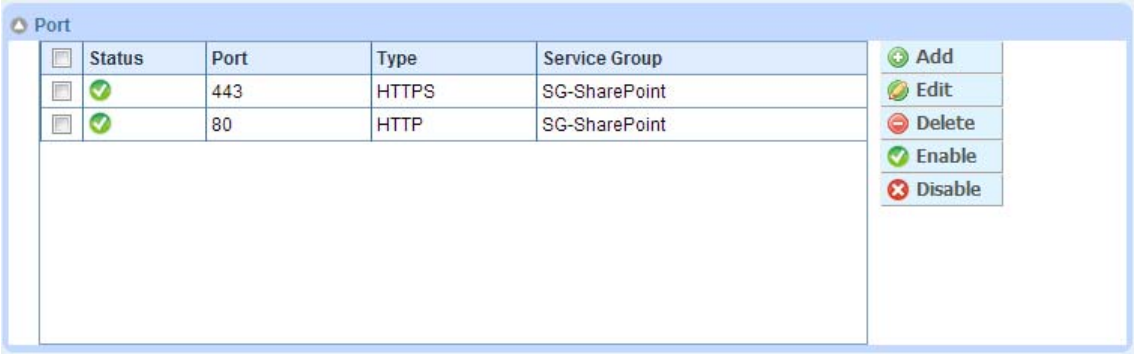


Figure 28: HTTPS VIP - Virtual Port list with port 443 and 80

6. Click **OK**, then click **Save** to save the configuration.

6.4 DEPLOYMENT VALIDATION

To validate that the HTTPS VIP configuration is functioning correctly, do the following.

1. Open a web browser on an external client device
2. Access SharePoint 2013 using appropriate URL and login to the SharePoint 2013 site.
   - Using HTTPS - in this example, https://sharepoint (or https://sharepoint.example.com)
   - Using HTTP - in this example, http://sharepoint (or http://sharepoint.example.com)
3. Make sure that you can successfully access and open SharePoint 2013 site with HTTPS protocol

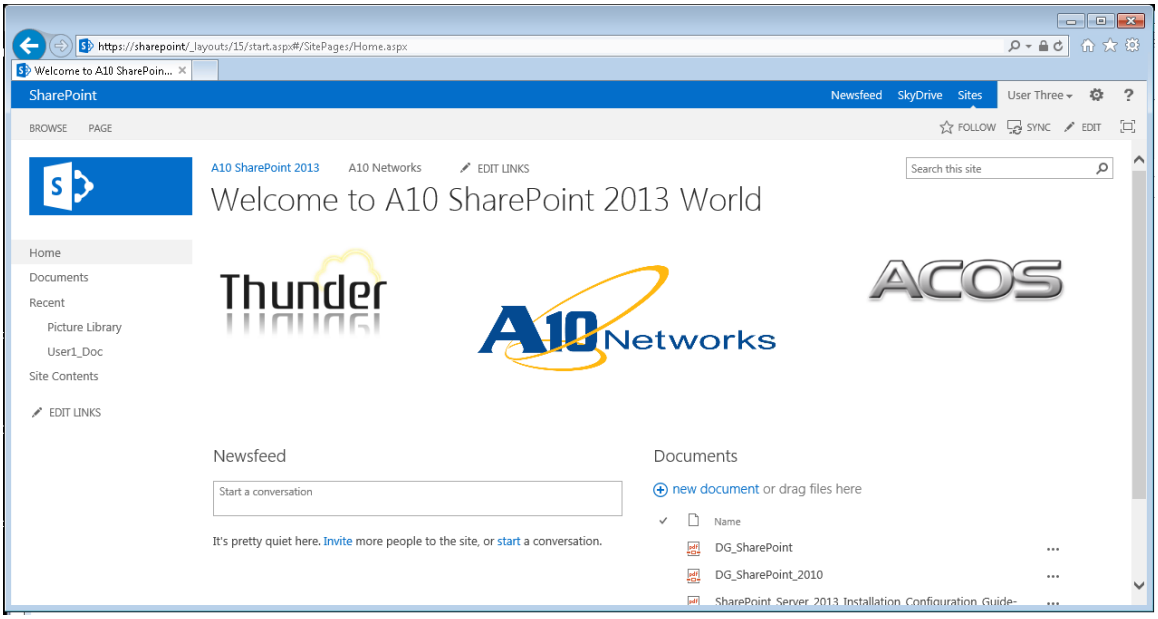
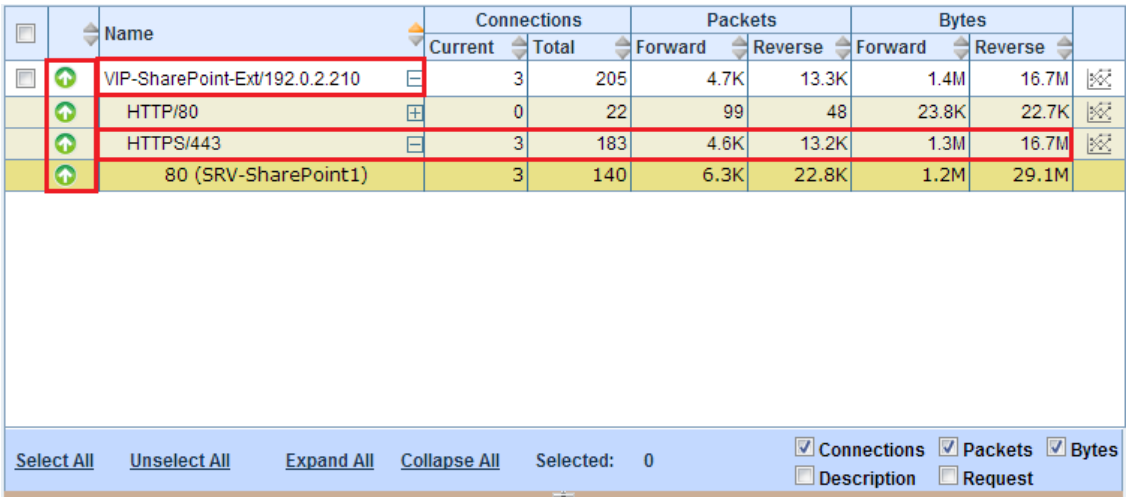


Figure 29: Connection to SharePoint 2013 through HTTPS VIP

4. On the ACOS device, navigate to **Monitor Mode > SLB > Service > Virtual Server**.

5. Check virtual server status (In this example, VIP-SharePoint-EXT/192.0.2.210) showing green , and also statistics on the HTTPS virtual port (HTTPS/443) are increased



Name	Connections		Packets		Bytes	
	Current	Total	Forward	Reverse	Forward	Reverse
VIP-SharePoint-Ext/192.0.2.210	3	205	4.7K	13.3K	1.4M	16.7M
HTTP/80	0	22	99	48	23.8K	22.7K
HTTPS/443	3	183	4.6K	13.2K	1.3M	16.7M
80 (SRV-SharePoint1)	3	140	6.3K	22.8K	1.2M	29.1M

Select All Unselect All Expand All Collapse All Selected: 0
Connections Packets Bytes
Description Request

Figure 30: VIP status and Virtual Port statistics view

7 OPTIONAL SECURITY FEATURES

The ACOS device adds another security layer for load balanced servers and applications. Adding to an in-depth defense strategy, key protections are architected into the ACOS device.

A10 provides high-performance detection and prevention against distributed denial-of-service (DDoS) and protocol attacks that can cripple servers and take down applications. Since the ACOS device is placed between the routers and data center resources, it is ideally positioned to detect and stop attacks directed at any data center server or application. Using specialized ASICs in select models, ACOS device can continue to inspect, stop, and redirect all application traffic at network speeds.

1. To install a standard set of DDoS mitigation features, navigate to Config Mode > Security > Network > DDoS Protection.

2. Select all the checkboxes of the DDoS Protection features you would like to activate.

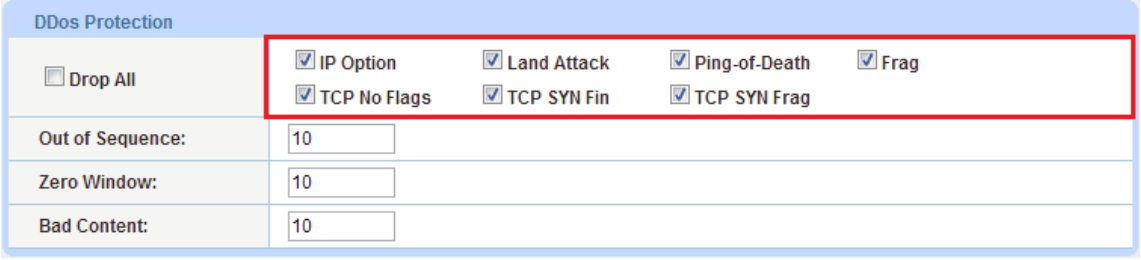


Figure 31: DDoS protection configuration

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

For other DDoS features and Security features such as Web Application Firewall, refer to A10 Thunder series and AX series documentation from the link below (login required).

https://www.a10networks.com/support-axseries/techlibrary.php

8 SUMMARY AND CONCLUSION

The deployment guide describes how to set up the ACOS devices for Microsoft SharePoint 2013. By using the ACOS devices to load balance SharePoint web servers, the following key advantages can be achieved:

- Higher scalability
  - ♦ Multiple SharePoint web servers can be pooled together without any change on user's access method.

- New SharePoint web servers can be easily added at any time without affecting existing service for the users.

- Higher availability
  - SharePoint web servers' availability is periodically verified using health monitor. In case of server failure, user traffic is redirected to other available servers without any interruption.

- Higher performance
  - All the client traffic is seamlessly distributed across all available SharePoint web servers using the preferred load balancing algorithm.
  - Utilizing application acceleration features frees SharePoint web server resources for other operations.

- Additional features at no additional cost
  - Security features such as DDoS protection, Web Application Firewall and other useful features are included in ACOS; ready to use without additional cost

By using the A10 Thunder Series Unified Application Service Gateway or AX Series Application Delivery Controller, significant benefits are achieved for all Microsoft SharePoint 2013 users. For more information about A10 Thunder Series and AX Series products, please refer to the following URLs:

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

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

http://a10networks.com/resources/solutionsheets.php

http://a10networks.com/resources/casestudies.php

9 APPENDIX - SAMPLE CLI CONFIGURATION

CLI Configuration

```
hostname ACOS
ip nat pool SNAT1 10.100.2.157 10.100.2.157 netmask /24
health monitor HM-HTTP
 method http expect response-code 401 host sp
slb server SRV-SharePoint1 10.100.2.168
   port 80  tcp
       health-check HM-HTTP
slb server SRV-SharePoint2 10.100.2.169
   port 80  tcp
       health-check HM-HTTP
slb service-group SG-SharePoint tcp
    health-check HM-HTTP
    member SRV-SharePoint1:80
    member SRV-SharePoint2:80
slb template connection-reuse CR-SharePoint
slb template cache RC-SharePoint
slb template http HTTP-Template-SharePoint
   compression enable
   compression content-type pdf
   compression content-type pptx
   compression content-type doc
slb template client-ssl SP2013-SSL
   cert SP2013-CERT
   key SP2013-CERT
```

```
slb virtual-server VIP-SharePoint 10.100.0.231
   port 80  http
      source-nat pool SNAT1
      service-group SG-SharePoint
      template http HTTP-Template-SharePoint
      template cache RC-SharePoint
      template connection-reuse CR-SharePoint
slb virtual-server VIP-SharePoint-Ext 192.0.2.210
   port 80  http
      service-group SG-SharePoint
      aflex redirect1
   port 443  https
      source-nat pool SNAT1
      service-group SG-SharePoint
      template http HTTP-Template-SharePoint
      template cache RC-SharePoint
      template client-ssl SP2013-SSL
      template connection-reuse CR-SharePoint
      aflex REWRITE-TO-HTTPS
```

aFleX scripts

```
aFleX script: REWRITE-TO-HTTPS
when HTTP_RESPONSE {
  # check Content-Type to avoid unnecessary collects
  if { [HTTP::header "Content-Type"] contains "text" } {
    HTTP::collect
  }
```

```
}
when HTTP_RESPONSE_DATA {
  set clen [HTTP::payload length]
  regsub -all "http://" [HTTP::payload] "https://" newdata
  HTTP::payload replace 0 $clen $newdata
  HTTP::release
}
aFleX script: redirect1
# redirect HTTP request to https URL
when HTTP_REQUEST {
  HTTP::redirect https://[HTTP::host][HTTP::uri]
}
```