DEPLOYMENT GUIDE

HOW TO DEPLOY MICROSOFT SHAREPOINT 2016 WITH A10 THUNDER ADC

OVERVIEW

Microsoft SharePoint Server 2016 is a collaboration platform that organizations of all sizes can use to improve the efficiency of business processes. SharePoint Server 2016 sites provide environments that administrators can configure to provide personalized access to documents and other information. Integrated search features enable users to quickly and efficiently find content regardless of the physical location of data.

A10 Networks Thunder® ADC line of Application Delivery Controllers provides intelligent load balancing, security, acceleration and optimization for Microsoft SharePoint 2016 deployments.

Adding Thunder ADC to your Microsoft SharePoint deployments provides the following benefits:

- **High Scalability** – Thunder ADC allows organizations to effectively scale their SharePoint services for a very large number of employees by load balancing traffic among multiple SharePoint front-end servers.
- **High Availability** – SharePoint services are guaranteed even if a SharePoint front-end server goes offline.
- **High Performance** – Thunder ADC can improve SharePoint server performance though features such as SSL offload and HTTP compression.
- **Better Security** – Thunder ADC can mitigate distributed denial of service (DDoS) attacks. In addition, it can provide an authentication proxy service and web application firewall (WAF). No additional licenses are required for those security features.
- **Simplified Deployment** – A10 Networks AppCentric Templates (ACT) allow organizations to configure and deploy SharePoint effortlessly. They also provide visibility into SharePoint services and login activities.

The purpose of this guide is to provide a step-by-step process for deploying SharePoint 2016 with Thunder ADC using AppCentric Templates (ACT). Refer to Appendix A for the equivalent CLI-based configuration.

For additional deployment guides for Microsoft applications, such as Skype for Business and Exchange, please refer to https://www.a10networks.com/resources/deployment-guides.

TABLE OF CONTENTS

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

DEPLOYMENT PREREQUISITES

This SharePoint 2016 deployment with Thunder ADC has the following prerequisites (based on tested configuration, Appendix A):

- Thunder ADC must be running A10 Networks Advanced Core Operating System (ACOS®) version 4.1.1-P5 or higher.
- The AppCentric Templates (ACT) version is act-1020-17 (see Appendix B for details).
- The solution was deployed with a single vThunder ADC device. Two devices are required for high availability.
- The solution can be deployed in the same way using either virtual (vThunder) or physical Thunder ADC appliances.

For system requirements to deploy SharePoint 2016 servers, see:
https://technet.microsoft.com/en-us/library/cc262749(v=office.16).aspx

DEPLOYMENT TOPOLOGY

SharePoint 2016 introduces MinRole, a new farm topology based on a set of predefined server roles. When configuring your SharePoint farm, you now select the role of a server when you create a new farm or join a server to an existing farm. SharePoint will automatically configure the services on each server based on the server's role.

For details about the new MinRole server roles in SharePoint 2016, refer to Microsoft's website:
https://technet.microsoft.com/en-us/library/mt346114(v=office.16).aspx

Additionally in SharePoint 2016, Central Administration is no longer provisioned on all servers by default. Instead, Central Administration is now provisioned only on the first server in a farm by default when using the SharePoint Products Configuration Wizard. In this deployment, we follow this default setting and Central Administration was provisioned on a single SharePoint application server.

The diagram below provides an architectural overview of how SharePoint 2016 can be optimized with Thunder ADC.

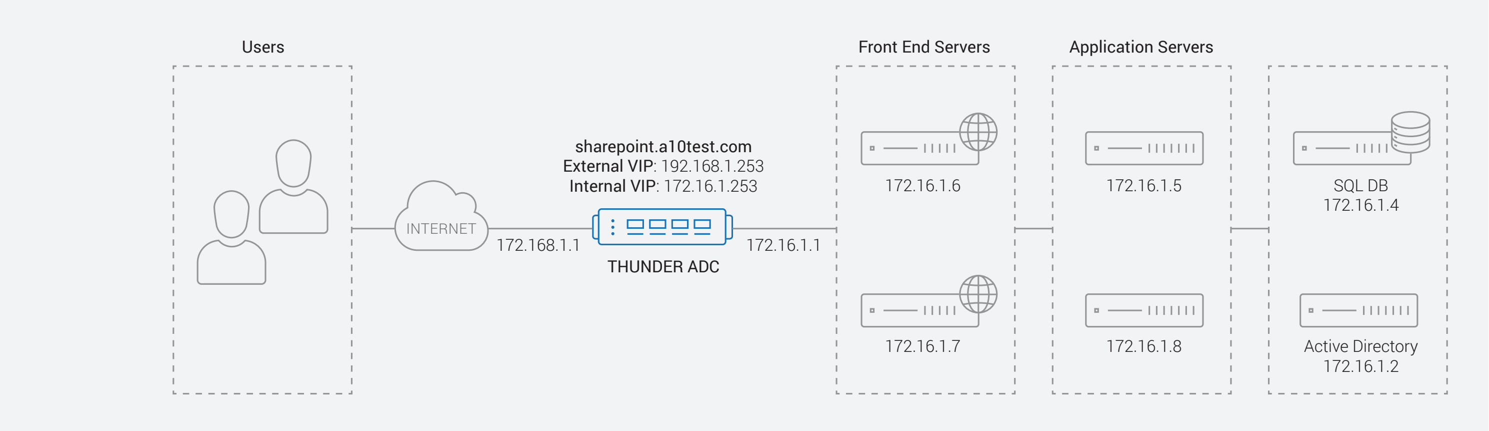


Figure 1: Lab topology

In this deployment, the Thunder ADC will be deployed with the following features:

- Separate virtual IPs for internal and external client access
- Load balancing using least-connection method
- SSL offload
- HTTP-to-HTTPS redirection
- HTTP Strict Transport Security (HSTS)
- Higher preference for Perfect Forward Secrecy (PFS) cipher suites

- IP Source NAT with client-IP insertion
- HTTP health monitoring
- HTTP compression
- DDoS mitigation
- Authentication Proxy

Separate virtual IPs for internal and external client access: In this deployment, we configure two SharePoint HTTPS virtual servers on the Thunder ADC – one for internal client and the other for external clients. The internal clients will access the SharePoint web site at virtual IP (VIP) 172.16.1.253, and the external clients will access it at the VIP 192.168.1.253.

Load balancing using least-connection method: The Thunder ADC will load balance traffic by selecting the SharePoint server that has the least current client connections on it.

SSL Offload: SSL offload acts as an acceleration feature by removing the burden of processing SSL traffic from the SharePoint servers. Instead of having the SharePoint servers handle SSL processing, Thunder ADC decrypts all HTTPS traffic, forwarding the traffic to the server over HTTP. The Thunder ADC can also re- encrypt the traffic sent to the SharePoint servers if required.

To use SSL Offload, you need to either import an SSL Certificate or you can generate a self-signed certificate on Thunder ADC.

HTTP-to-HTTPS redirection: With this option, the Thunder ADC will securely redirect a client connection using HTTP to an HTTPS URL.

HTTP Strict Transport Security (HSTS): HSTS allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol [1]. The Thunder ADC will communicate HSTS policy to the client by inserting an HTTPS response header field named “Strict-Transport-Security.”

Higher preference for Perfect Forward Secrecy (PFS) cipher suites: Forward secrecy (FS) is a property of secure communication protocols in which a compromise of long-term keys does not compromise past session keys. Forward secrecy protects past sessions against future compromises of secret keys or passwords[2]. The Thunder ADC will give preference to PFS ciphers for HTTPS communication with the clients.

IP Source NAT with client-IP insertion: Source NAT (SNAT) is required when your network topology is based on a “one-arm” deployment and if you have internal clients that reside on the same subnet as the VIP. When IP source NAT is enabled on the Thunder ADC, the request received by the real server does not have the client’s IP address. With the client-ip insertion option enabled, the Thunder ADC device will insert the client’s IP address into the X-ClientIP header before sending the request to a real server.

HTTP health monitoring: 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.

HTTP compression: Compression reduces the amount of bandwidth required to send content to clients. The content types (e.g. pdf, ppt) that should be compressed can be specified while enabling the option.

DDoS mitigation: In this deployment, the Thunder ADC will be configured to defend against common DDoS attacks.

Authentication Proxy: In this deployment, the Thunder ADC will be configured to authenticate the clients, thereby providing enhanced security and visibility by acting as authentication proxy.

[1] https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

[2] https://en.wikipedia.org/wiki/Forward_secrecy

ACCESSING THUNDER ADC

This section describes how to access Thunder ADC from a command line interface (CLI), Graphical user interface (GUI) or AppCentric Templates (ACT):

- **CLI** – The CLI is a 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** – This is a web-based interface in which you click buttons, menus and other graphical icons to access the configuration or management pages. From these pages, you can 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)
- **AppCentric Templates (ACT)** - A10 ACOS GUI plug-in module that enhances the user experience to deploy, monitor and troubleshoot applications in a frictionless manner. Obtain the latest ACT file and import it into the Thunder ADC. Refer to Appendix B for details on how to acquire and import the file. AppCentric Templates can be accessed by opening the GUI by entering the management IP in the browser's address bar (e.g. https://172.31.31.31/) and navigating to **System > App Template**.

***NOTE**: HTTP requests are redirected to HTTPS by default on Thunder ADC.*

Default Access Information:

- Default Username: "admin"
- Default password: "a10"
- Default IP address of the device: "172.31.31.31"

***NOTE**: For detailed information on how to access the Thunder ADC device, refer to the System Configuration and Administration Guide.*

THUNDER ADC SHAREPOINT CONFIGURATION USING APPCENTRIC TEMPLATES

APPCENTRIC TEMPLATES (ACT) OVERVIEW

ACT is a wizard-based configuration tool that enables organizations to apply best practices for deploying and securing their SharePoint 2016 solution with minimal effort. A10 highly recommends the use of this configuration tool for the deployment and management of SharePoint 2016, since these templates were developed with a focus on best practices. For that reason, most of the subsequent points can be easily configured via AppCentric Templates.

Refer to Appendix B for details on how to acquire and import the ACT file.

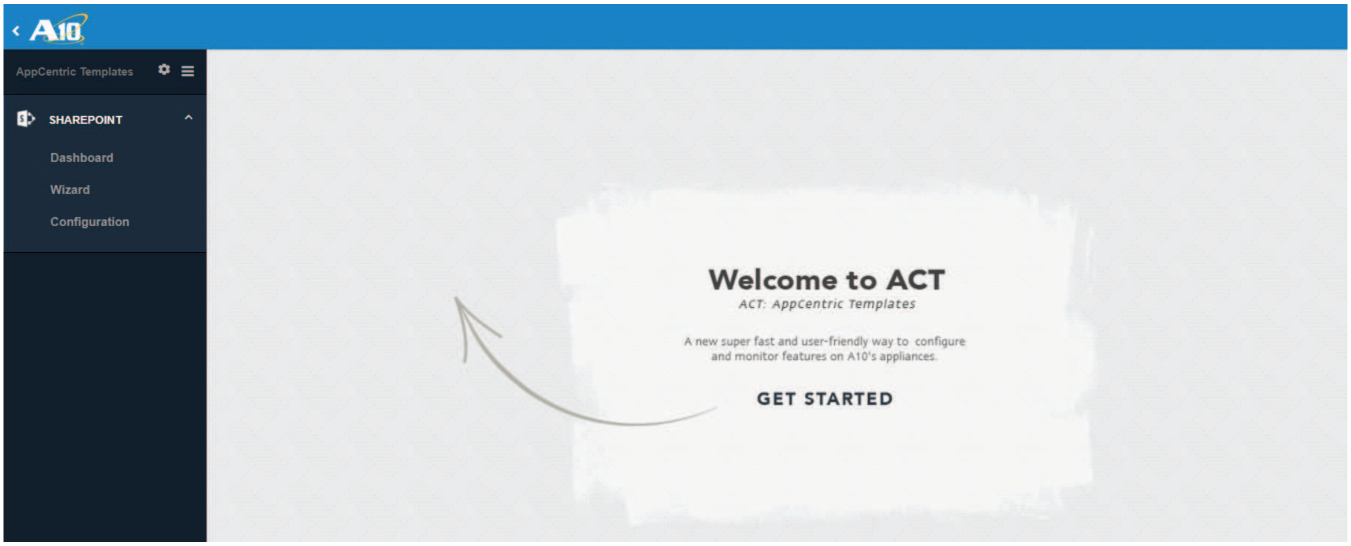
CONFIGURATION USING ACT

To access ACT, first log into Thunder ADC using the web GUI:

- IP address: management IP address
- Default username: “admin”
- Default password: “a10”

Go to System > App Templates

If prompted to specify username and password, specify your regular admin credentials:



Welcome to ACT

ACT: AppCentric Templates

A new super fast and user-friendly way to configure and monitor features on A10's appliances.

Figure 2: Accessing ACT

Once you’ve logged in to ACT, select “SHAREPOINT” from the AppCentric Templates menu.

There are three main sections in the AppCentric Template:

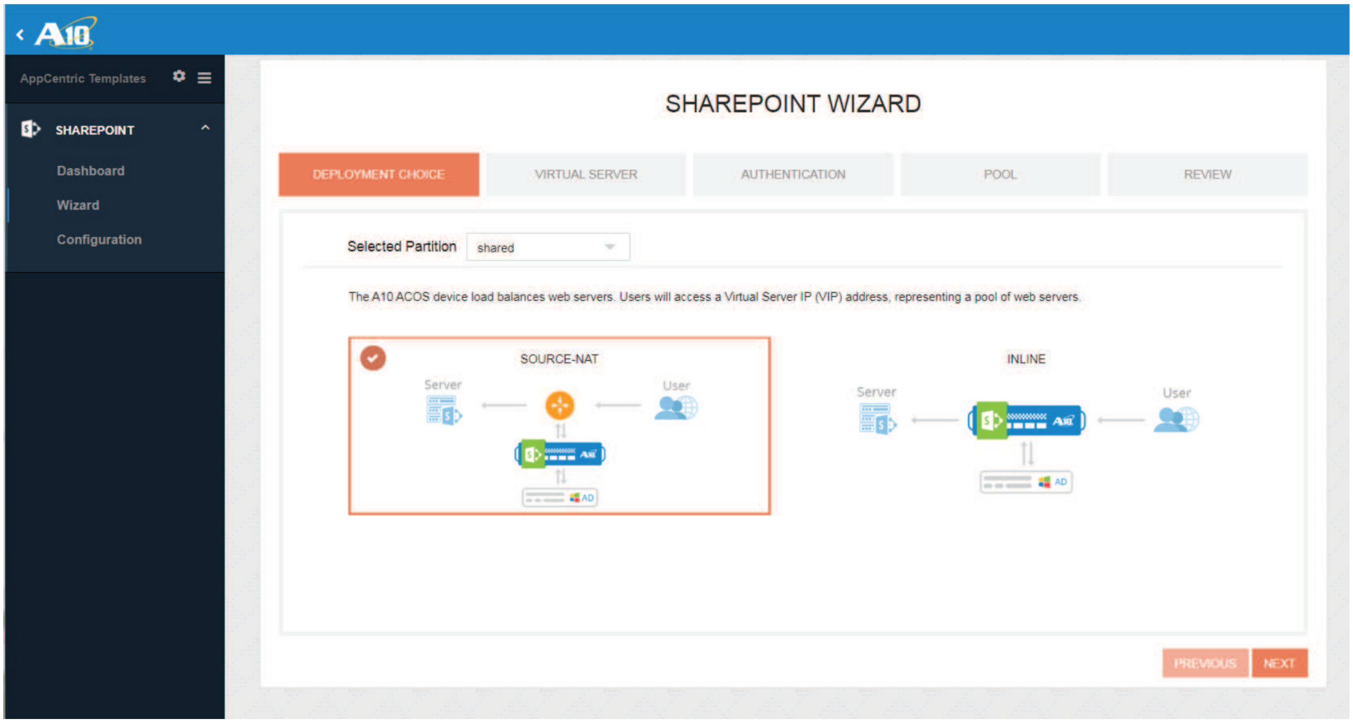
1. **Dashboard**: The dashboard gives users a view of different statistics related to the current state of the system, including traffic statistics.
2. **Wizard**: The wizard provides users with a guided flow for deployment of SharePoint with Thunder ADC.
3. **Configuration**: This section provides users with the current configuration of the device as well as access to some advanced options.

WIZARD – DEPLOYMENT CHOICE

In the left-pane, go to SharePoint > Wizard

Depending on the mode of deployment, select either “Source-NAT” or “Inline:”

- In this deployment we’ve used the “Source-NAT” deployment mode.



AppCentric Templates

SHAREPOINT

- Dashboard
- Wizard
- Configuration

SHAREPOINT WIZARD

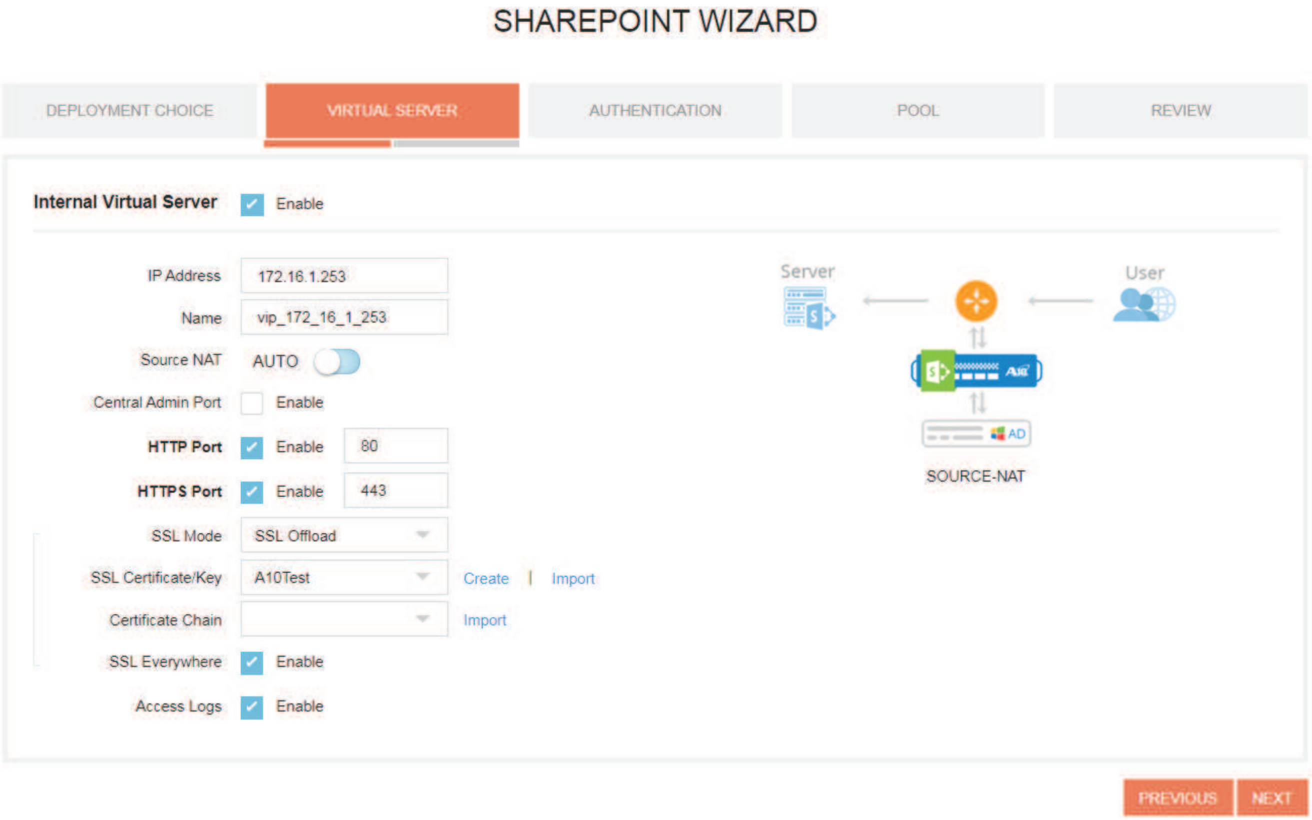
DEPLOYMENT CHOICE | VIRTUAL SERVER | AUTHENTICATION | POOL | REVIEW

Selected Partition: shared

The A10 ACOS device load balances web servers. Users will access a Virtual Server IP (VIP) address, representing a pool of web servers.

Figure 3: Select the topology: 'Source-NAT' vs. 'Inline'

WIZARD – VIRTUAL SERVER (INTERNAL)



SHAREPOINT WIZARD

DEPLOYMENT CHOICE | VIRTUAL SERVER | AUTHENTICATION | POOL | REVIEW

Internal Virtual Server ☑ Enable

IP Address: 172.16.1.253

Name: vip_172_16_1_253

Source NAT: AUTO

Central Admin Port: □ Enable

HTTP Port ☑ Enable 80

HTTPS Port ☑ Enable 443

SSL Mode: SSL Offload

SSL Certificate/Key: A10Test Create | Import

Certificate Chain: Import

SSL Everywhere: ☑ Enable

Access Logs: ☑ Enable

Figure 4: Internal Virtual Server details

In this deployment the following options were configured:

Internal Virtual IP Address: 172.16.1.253

Source-NAT: Enabled (Auto).
ACT will also configure an HTTP template to insert the client-IP address in the request sent to the SharePoint server.

Central Admin Port: Not enabled
In SharePoint 2016, the Central Administration web site is now provisioned only on the first server in a farm by default when using the SharePoint Products Configuration Wizard. Additional servers do not host the Central Administration web site by default. In this setup we use this default setting and the Central Administration website is hosted on a single SharePoint application server and thus this option is not enabled. If you enable this option you also need to specify the port on which the Central Administration web site is accessible.

HTTP Port: Enabled using port 80
The client traffic on HTTP port 80 will be redirected to HTTPS port 443 by enabling the "SSL Everywhere" option.

HTTPS Port: Enabled using port 443

SSL Mode: SSL offload
Instead of having SharePoint servers handling the SSL processing, Thunder ADC will decrypt and encrypt all HTTPS traffic from the internal clients, and will forward the traffic to the servers over HTTP (unsecured).

SSL Certificate/Key: A10Test (self-signed certificate/key)
This is the certificate and key that will be used for securing the traffic between the internal clients and Thunder ADC. You can either generate a self-signed certificate and key by clicking on "Create" or use "Import" to import an existing certificate/key. In this setup, we use a self-signed certificate for ease of deployment.

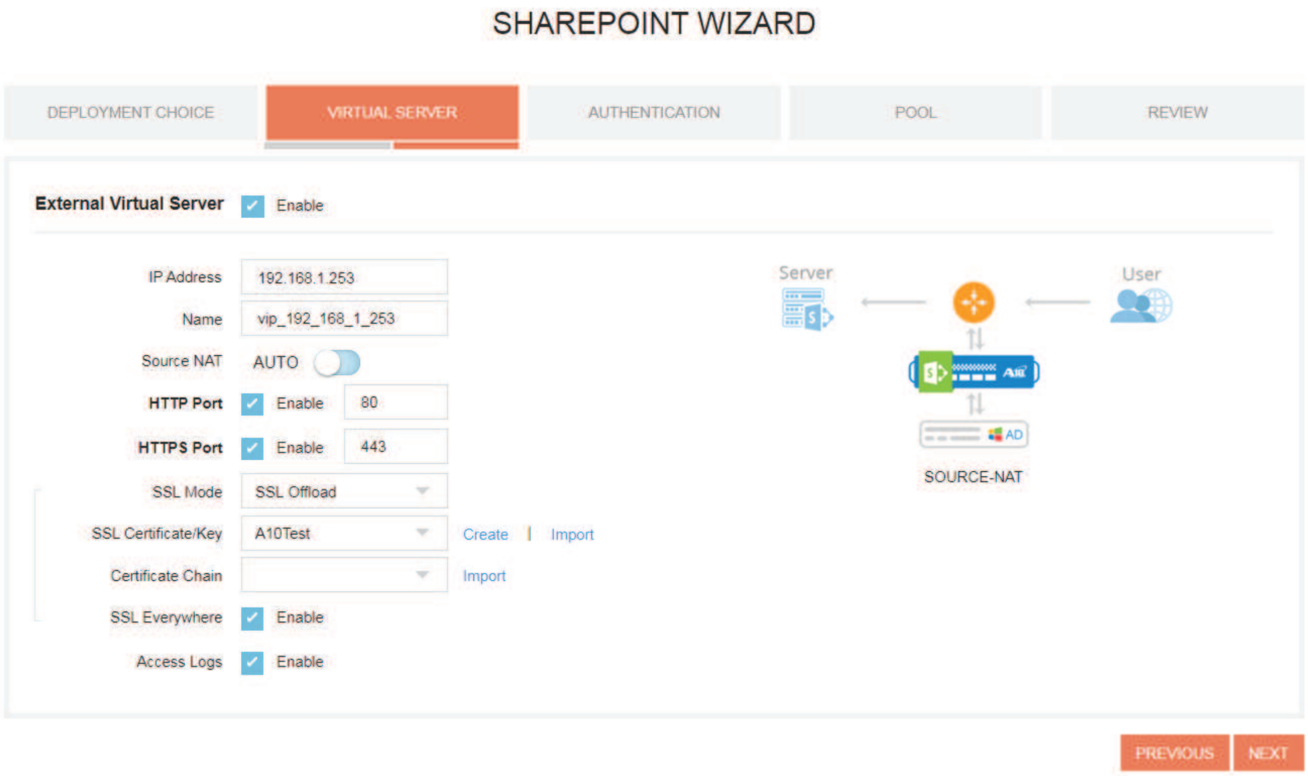
Certificate Chain: Depends on the certificate; not required in this example.

SSL Everywhere: Enabled
This will configure the following recommended security features:

- HTTP-to-HTTPS redirection
- HTTP Strict Transport Security (HSTS)
- Perfect Forward Secrecy (PFS) cipher suites will be preferred

Access Logs: Enabled

WIZARD – VIRTUAL SERVER (EXTERNAL)



External Virtual Server ☑ Enable

IP Address: 192.168.1.253

Name: vip_192_168_1_253

Source NAT: AUTO

HTTP Port: ☑ Enable 80

HTTPS Port: ☑ Enable 443

SSL Mode: SSL Offload

SSL Certificate/Key: A10Test Create | Import

Certificate Chain: Import

SSL Everywhere: ☑ Enable

Access Logs: ☑ Enable

Figure 5: External Virtual Server details

In this deployment the following options were configured:

External Virtual IP address: 192.168.1.253

Source NAT: Enabled (auto).
ACT will also configure an HTTP template to insert the client-IP address.

HTTP Port: Enabled using port 80
The client traffic on HTTP port 80 will be redirected to HTTPS port 443 by enabling the "SSL Everywhere" option.

HTTPS Port: Enabled using port 443

SSL Mode: SSL offload
Instead of having SharePoint Servers handling the SSL processing, Thunder ADC will decrypt and encrypt all HTTPS traffic from external clients, and will forward the traffic to the servers over HTTP (unsecured).

SSL Certificate/Key: A10Test (self-signed certificate/key)

This is the certificate and key that will be used for securing the traffic between the external clients and Thunder ADC. You can either generate a self-signed certificate and key by clicking on "Create" or use "Import" to import an existing certificate/key. In this setup, we use a self-signed certificate for ease of deployment.

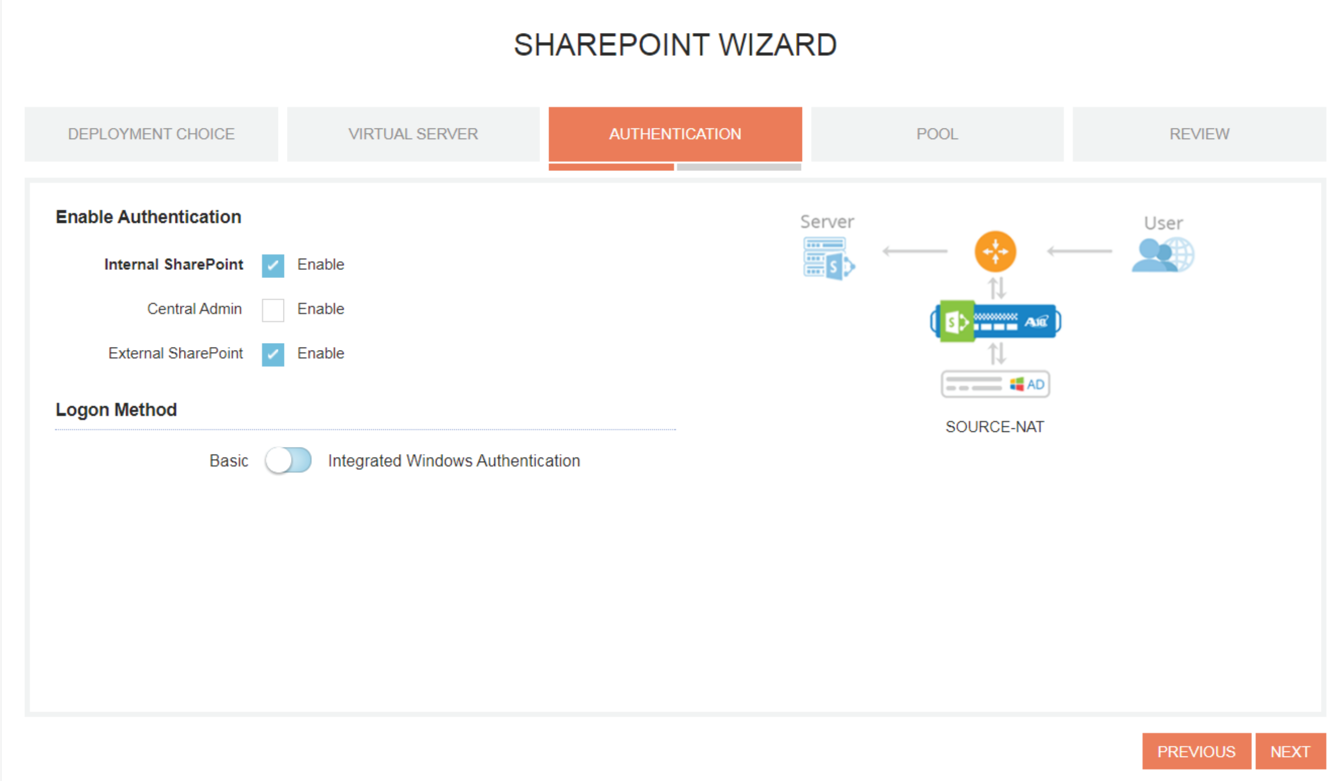
Certificate Chain: Depends on the certificate; not required in this example.

SSL Everywhere: Enabled
This will configure the following recommended security features:

- HTTP-to-HTTPS redirection
- HTTP Strict Transport Security (HSTS)
- Perfect Forward Secrecy (PFS) cipher suites will be preferred

Access Logs: Enabled

WIZARD – AUTHENTICATION (ENABLE)



SHAREPOINT WIZARD

Enable Authentication

Internal SharePoint	☑ Enable
Central Admin	□ Enable
External SharePoint	☑ Enable

Logon Method

Basic ○ Integrated Windows Authentication

Figure 6: Enable authentication for internal and external access to SharePoint sites

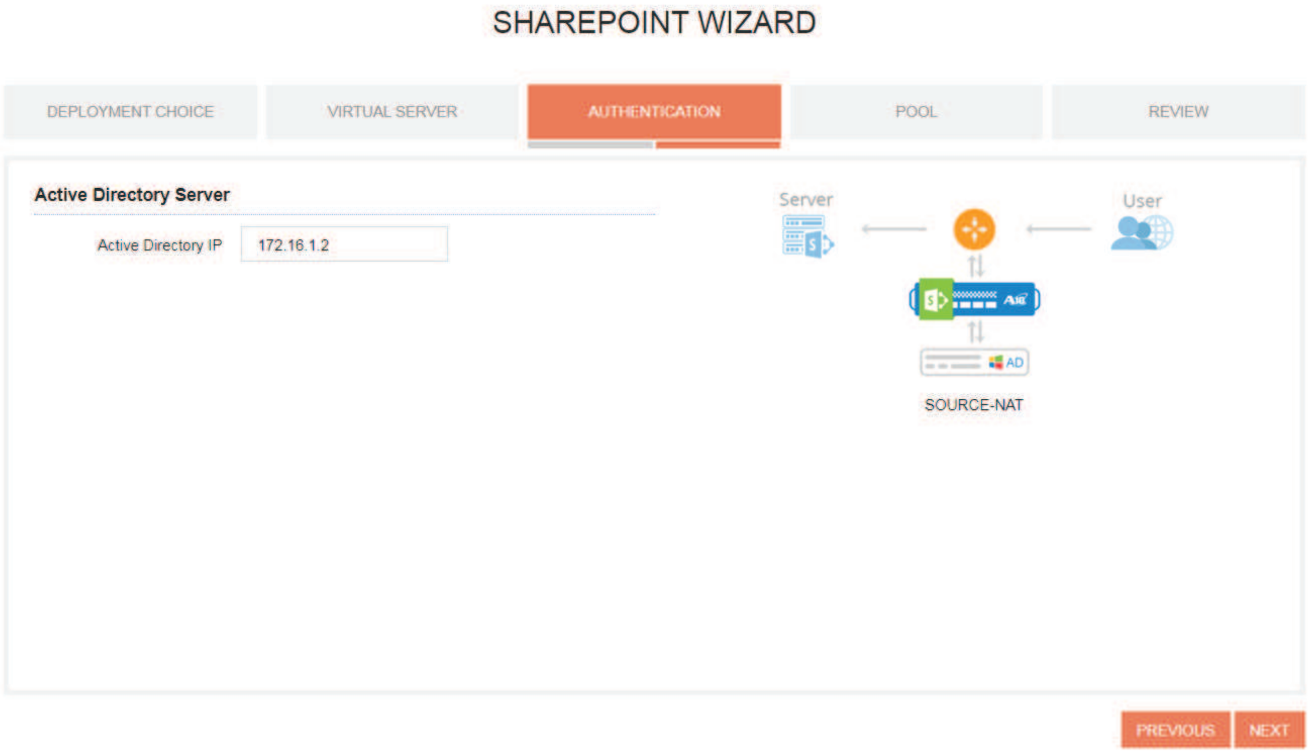
Enable Authentication:
Internal SharePoint: Enable
External SharePoint: Enable

This will enable authentication to be performed by Thunder ADC. In this deployment, we enable the authentication for access to SharePoint web sites by both internal and external clients.

Optionally, you can enable the authentication to be done for access to the SharePoint Central Administration website if it is hosted on the front-end server.

Logon Method: Basic
The client logon method is set to HTTP basic authentication. ACT will configure the authentication relay method to be NTLM.

WIZARD – AUTHENTICATION (ACTIVE DIRECTORY)



SHAREPOINT WIZARD

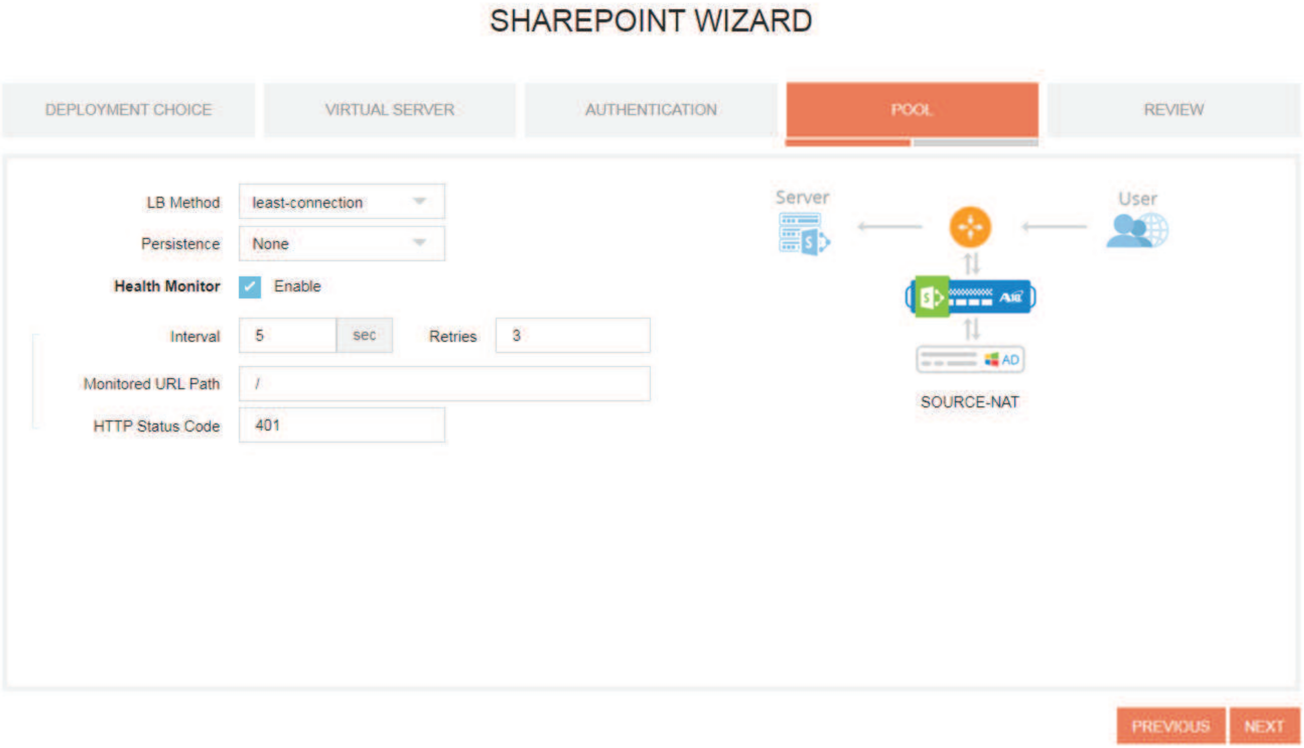
Active Directory Server

Active Directory IP: 172.16.1.2

Figure 7: Active Directory server for Authentication

Active Directory: 172.16.1.2
If you enable the option of authentication to be performed by the Thunder ADC, you need to additionally specify the IP address of Active Directory server.

WIZARD – POOL (LOAD BALANCING METHOD AND HEALTH MONITOR)



SHAREPOINT WIZARD

LB Method: least-connection

Persistence: None

Health Monitor: ☑ Enable

Interval: 5 sec Retries: 3

Monitored URL Path: /

HTTP Status Code: 401

Figure 8: Load Balancing Method and Health Monitoring

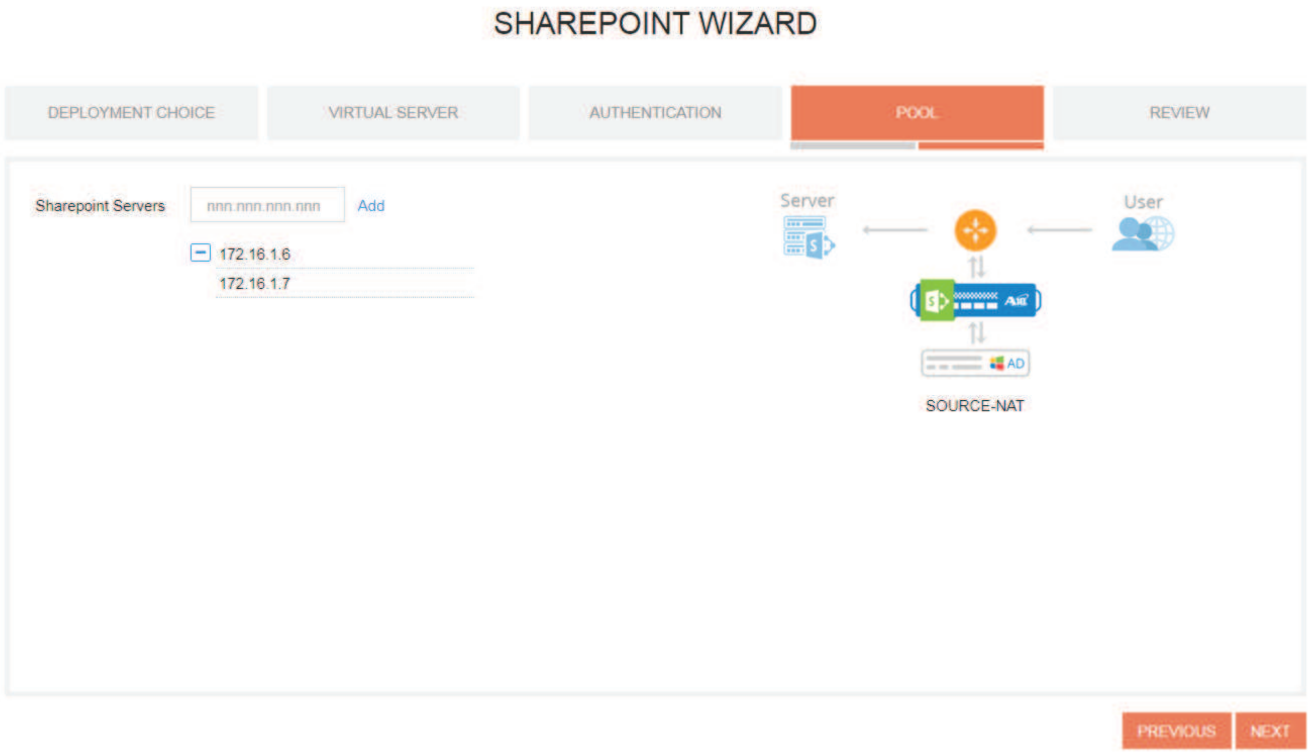
Load Balancing Method: Least Connection
In this deployment, we choose the least-connection method of load balancing.

Persistence: None
Like SharePoint 2013, you don't need to configure session persistence in SharePoint 2016 since the distributed cache service stores each user login token and shared the authentication information among all the SharePoint web servers.

Health Monitor: Enabled
Monitored URL Path: /
HTTP Status Code: 401

The Thunder ADC will perform health-checks for the SharePoint servers by sending an HTTP GET request for the default index page. Since authentication is enabled on the SharePoint server, when the Thunder ADC sends the GET request, the server will respond with a 401 unauthorized message and thus the Thunder ADC will wait for the response code 401 for the health check to be successful.

WIZARD – POOL (SHAREPOINT SERVERS)



Sharepoint Servers: nnn.nnn.nnn.nnn
172.16.1.6
172.16.1.7

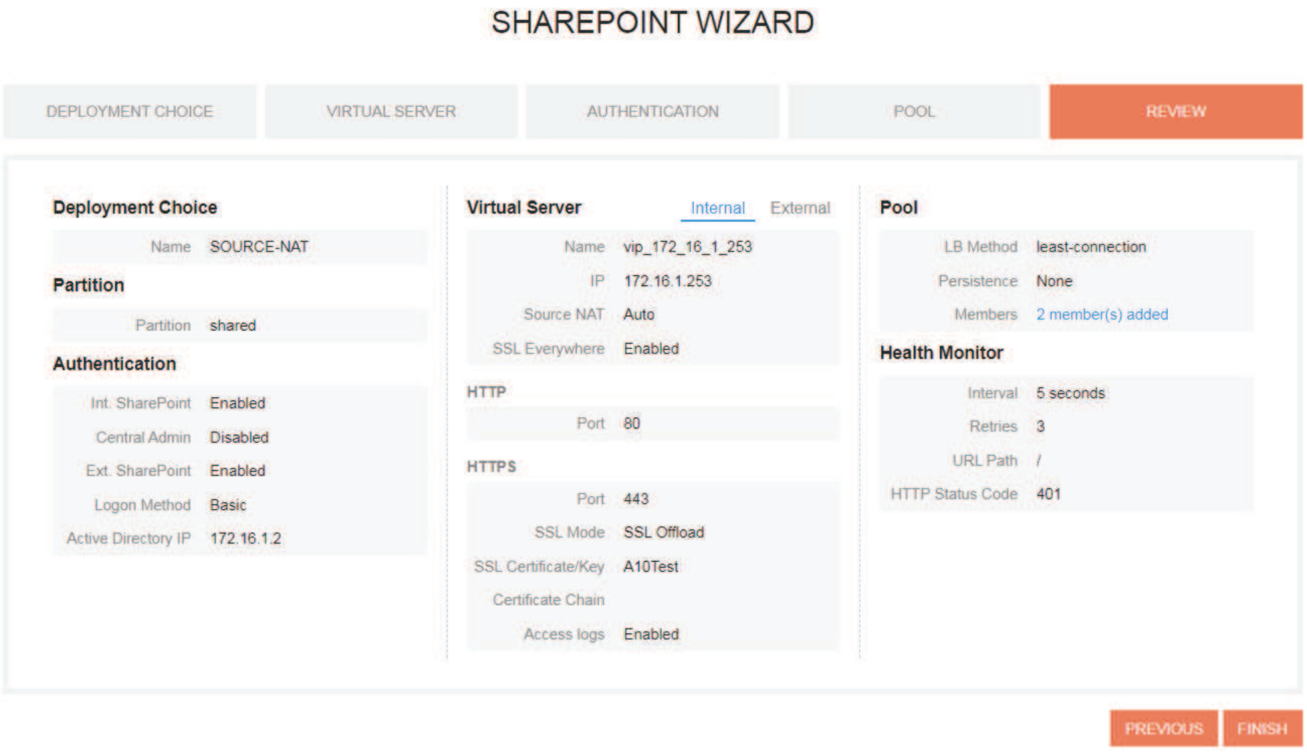
Figure 9: SharePoint Front-End servers

SharePoint Front-End Servers:
172.16.1.6
172.16.1.7

Here we specify the IP addresses of the SharePoint front-end servers.

WIZARD – REVIEW (INTERNAL VIRTUAL SERVER)

This section gives an overview of the settings for internal and external virtual servers.



SHAREPOINT WIZARD

Deployment Choice

Name	SOURCE-NAT

Partition

Partition	shared

Authentication

Int. SharePoint	Enabled
Central Admin	Disabled
Ext. SharePoint	Enabled
Logon Method	Basic
Active Directory IP	172.16.1.2

Virtual Server Internal External

Name	vip_172_16_1_253
IP	172.16.1.253
Source NAT	Auto
SSL Everywhere	Enabled

HTTP

Port	80

HTTPS

Port	443
SSL Mode	SSL Offload
SSL Certificate/Key	A10Test
Certificate Chain	
Access logs	Enabled

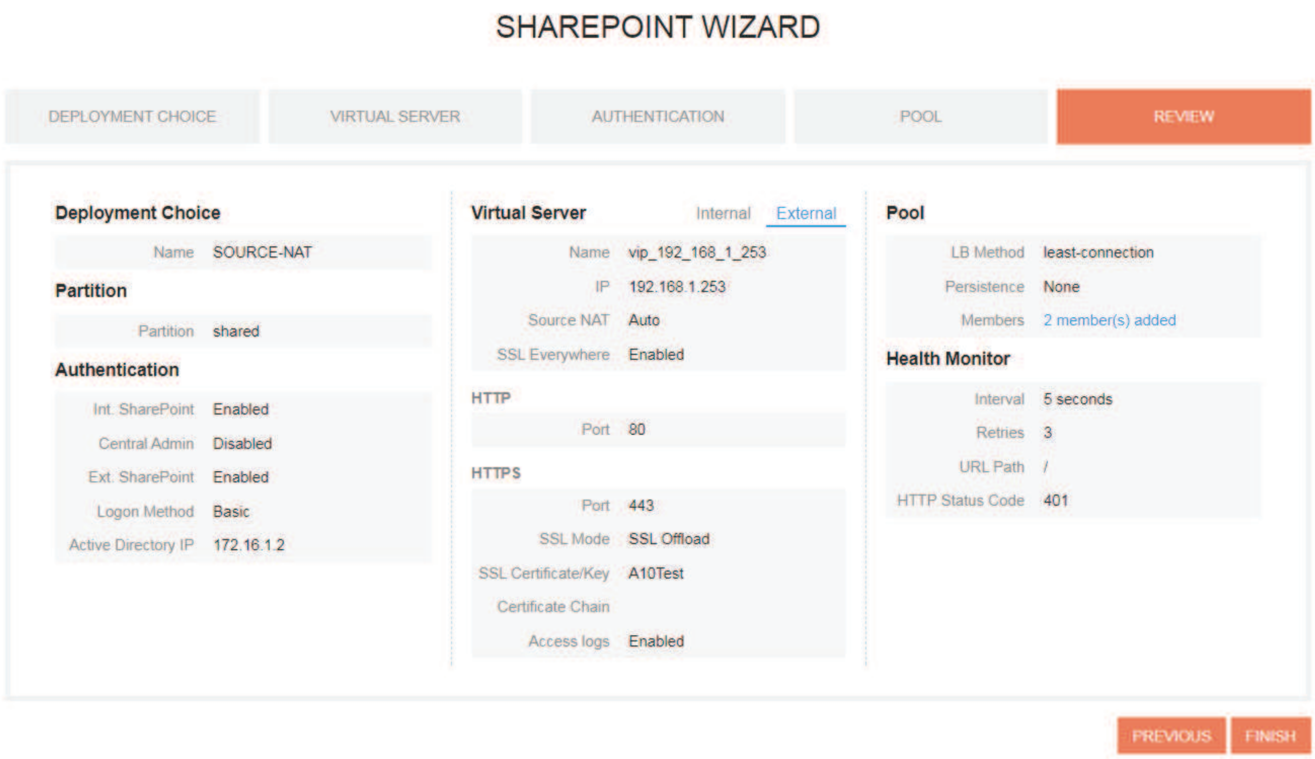
Pool

LB Method	least-connection
Persistence	None
Members	2 member(s) added

Health Monitor

Interval	5 seconds
Retries	3
URL Path	/
HTTP Status Code	401

Figure 10: Internal virtual server settings



Deployment Choice

Name	SOURCE-NAT

Partition

Partition	shared

Authentication

Int. SharePoint	Enabled
Central Admin	Disabled
Ext. SharePoint	Enabled
Logon Method	Basic
Active Directory IP	172.16.1.2

Virtual Server Internal External

Name	vip_192_168_1_253
IP	192.168.1.253
Source NAT	Auto
SSL Everywhere	Enabled

HTTP

Port	80

HTTPS

Port	443
SSL Mode	SSL Offload
SSL Certificate/Key	A10Test
Certificate Chain	
Access logs	Enabled

Pool

LB Method	least-connection
Persistence	None
Members	2 member(s) added

Health Monitor

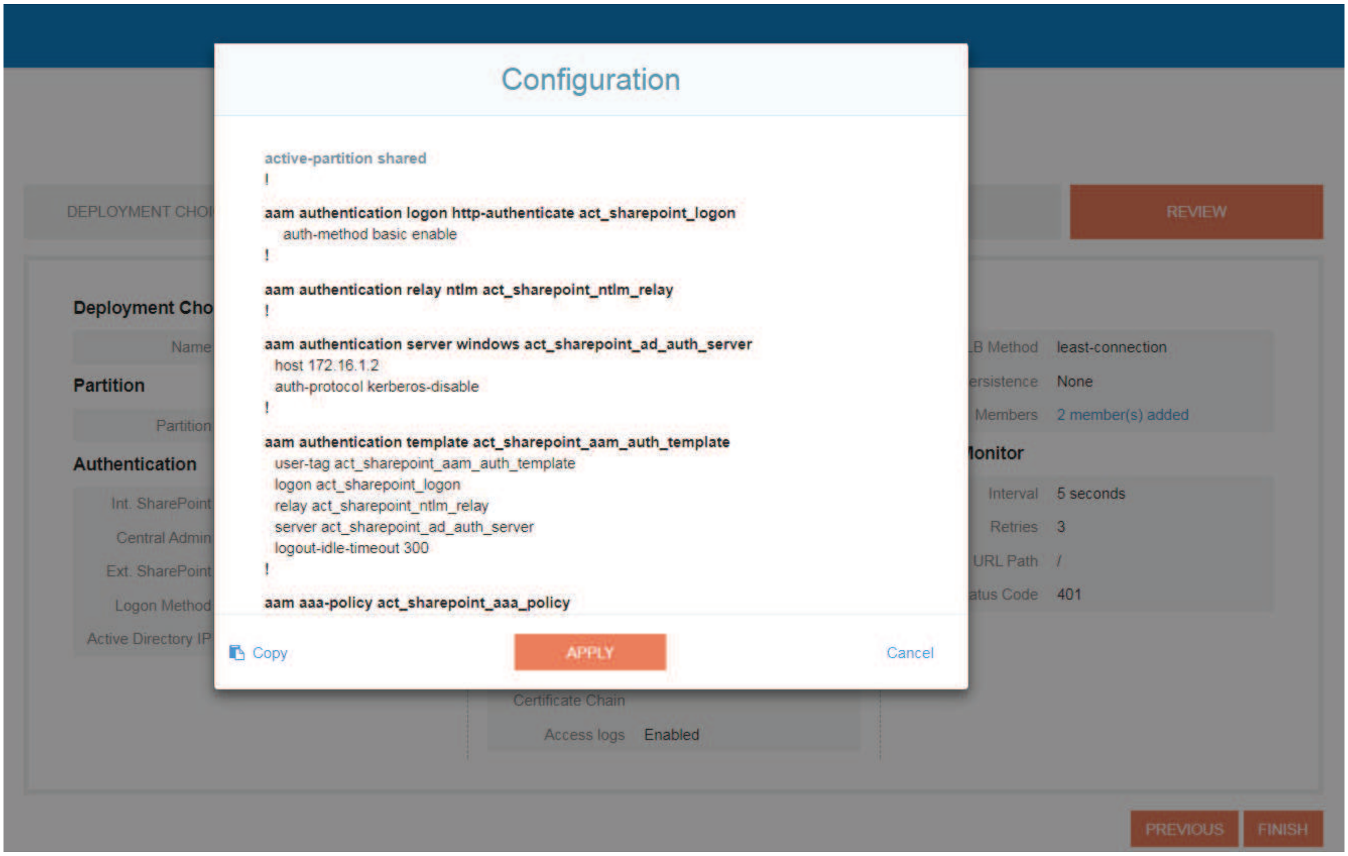
Interval	5 seconds
Retries	3
URL Path	/
HTTP Status Code	401

Figure 11: External virtual server settings

Review the settings and click “Finish” if fine.

You will then see a popup window with the equivalent CLI configuration generated by ACT.

WIZARD – APPLY



```
active-partition shared
!
aam authentication logon http-authenticate act_sharepoint_logon
  auth-method basic enable
!
aam authentication relay ntlm act_sharepoint_ntlm_relay
!
aam authentication server windows act_sharepoint_ad_auth_server
  host 172.16.1.2
  auth-protocol kerberos-disable
!
aam authentication template act_sharepoint_aam_auth_template
  user-tag act_sharepoint_aam_auth_template
  logon act_sharepoint_logon
  relay act_sharepoint_ntlm_relay
  server act_sharepoint_ad_auth_server
  logout-idle-timeout 300
!
aam aaa-policy act_sharepoint_aaa_policy
```

Deployment Cho
Name

Partition
Partition

Authentication
Int. SharePoint
Central Admin
Ext. SharePoint
Logon Method
Active Directory IP

LB Method least-connection
ersistence None
Members 2 member(s) added

lonitor
Interval 5 seconds
Retries 3
URL Path /
atus Code 401

Certificate Chain
Access logs Enabled

Figure 12: SharePoint configuration generated by ACT

You can either click “APPLY” to push the configuration to the Thunder ADC device, or you can click “Copy” to copy the configuration and then manually apply it through the CLI.

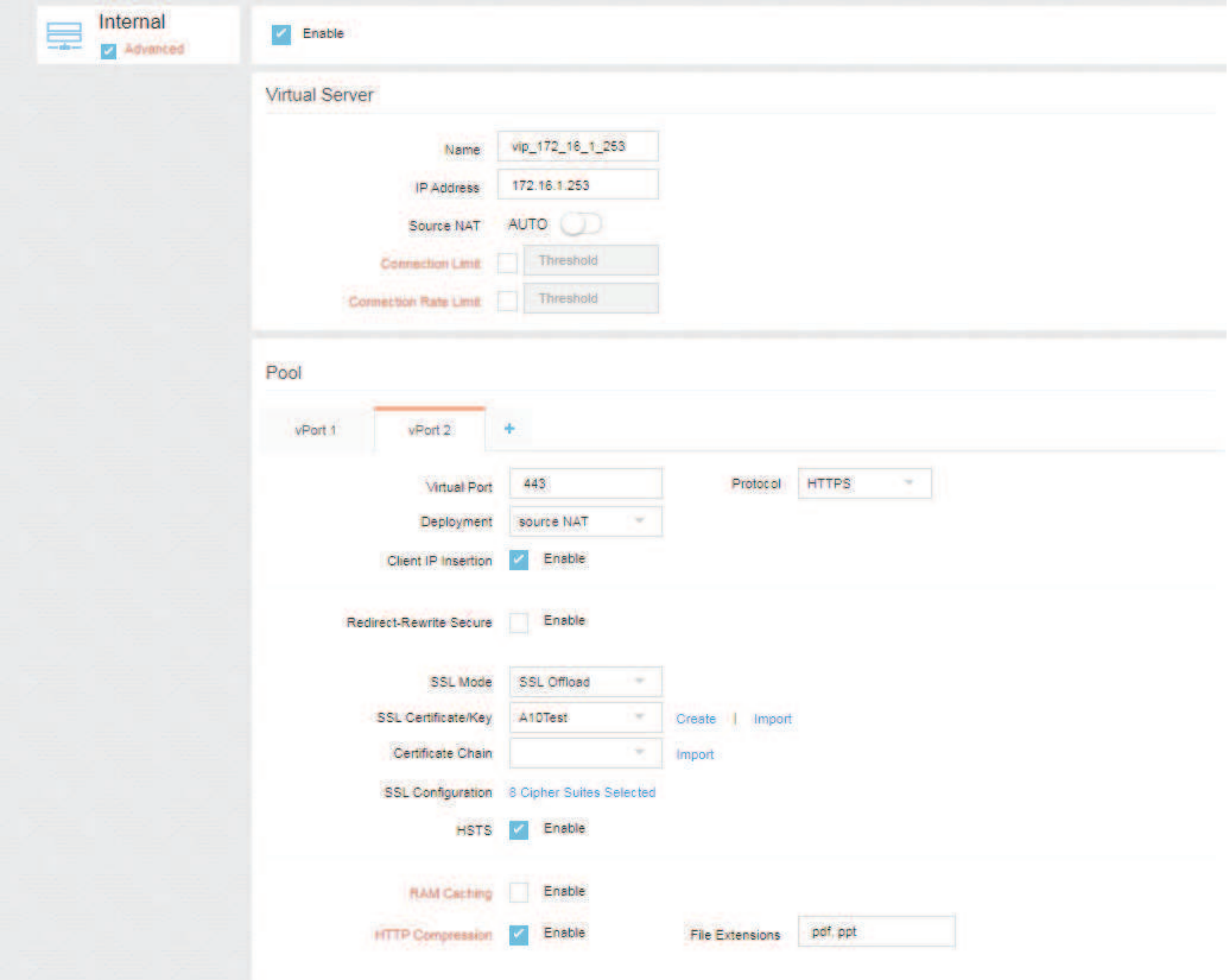
To view the complete configuration in text format, refer to Appendix A.

Once it’s applied, you can go to the SharePoint > Configuration page to look at the current configuration applied to the Thunder ADC device and make any additional changes.

ADVANCED CONFIGURATION OPTIONS

Go to SharePoint > Configuration page

INTERNAL VIRTUAL SERVER – ENABLE ADVANCED OPTIONS



Internal

☑ Advanced

☑ Enable

Virtual Server

Name: vip_172_16_1_253

IP Address: 172.16.1.253

Source NAT: AUTO

Connection Limit: ☐ Threshold

Connection Rate Limit: ☐ Threshold

Pool

vPort 1 | vPort 2 | +

Virtual Port: 443

Protocol: HTTPS

Deployment: source NAT

Client IP Insertion: ☑ Enable

Redirect-Rewrite Secure: ☐ Enable

SSL Mode: SSL Offload

SSL Certificate/Key: A10Test Create | Import

Certificate Chain: Import

SSL Configuration: 8 Cipher Suites Selected

HSTS: ☑ Enable

RAM Caching: ☐ Enable

HTTP Compression: ☑ Enable

File Extensions: pdf, ppt

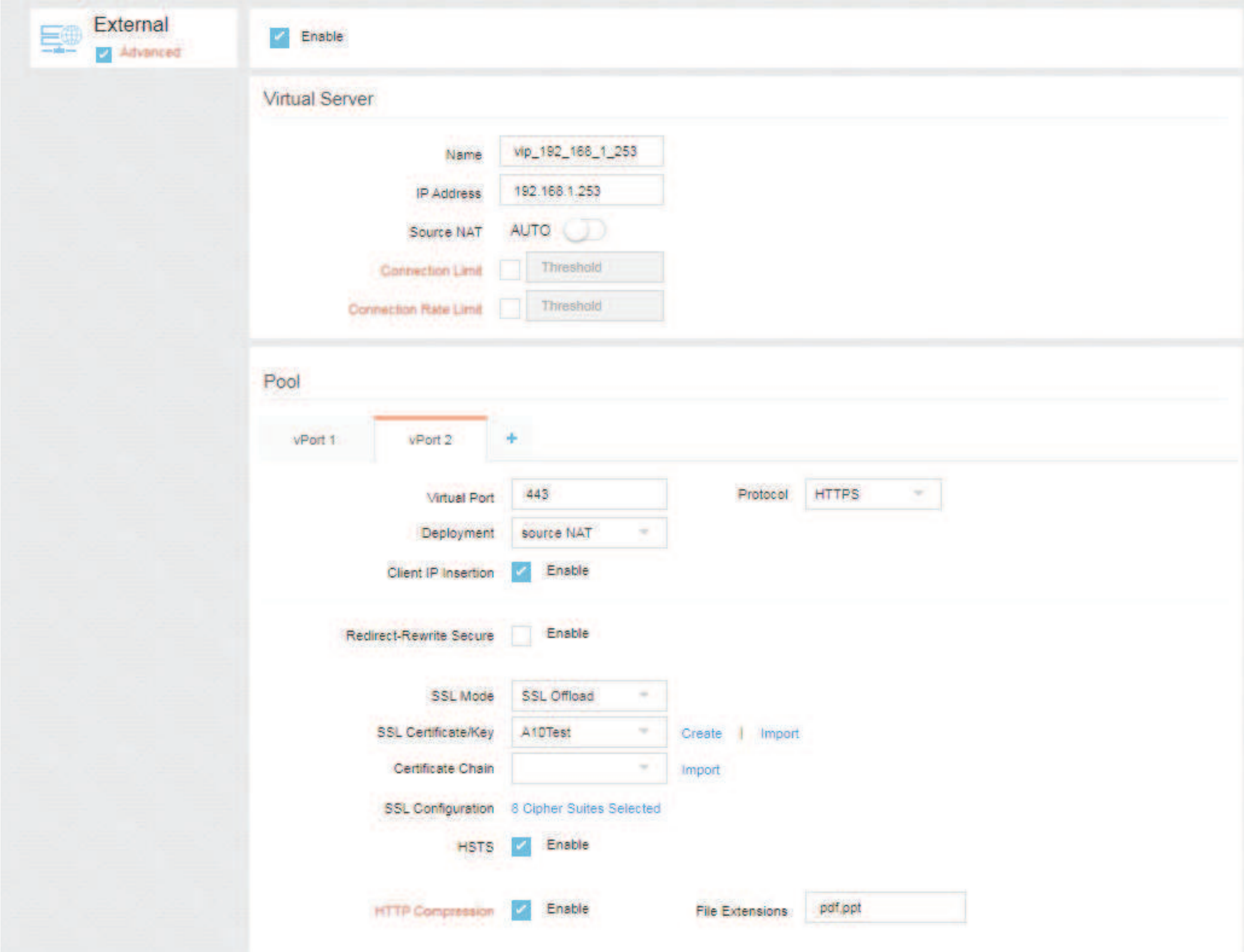
Figure 13: Advanced configuration parameters for internal virtual server

In this deployment, we enable the following additional optimization for internal virtual server on virtual port 443:

HTTP Compression: Enabled for file extensions pdf, ppt
Since we have secure redirect to HTTPS configured on virtual port 80, we need to enable this option only on the virtual port 443.

EXTERNAL VIRTUAL SERVER – ENABLE ADVANCED OPTIONS

Scroll down to enable the same option for the external virtual server on virtual port 443. Since we have secure redirect to HTTPS configured on virtual port 80, we need to enable this option only on the virtual port 443.



External
☑ Advanced

☑ Enable

Virtual Server

Name: vip_192_168_1_253
IP Address: 192.168.1.253
Source NAT: AUTO
Connection Limit: □ Threshold
Connection Rate Limit: □ Threshold

Pool

vPort 1 | vPort 2 | +

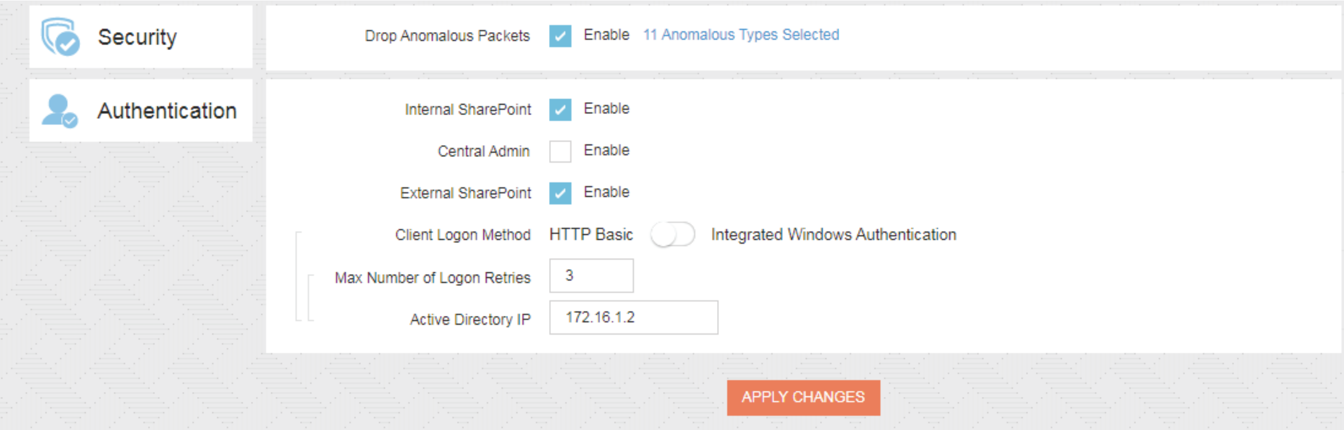
Virtual Port: 443
Protocol: HTTPS
Deployment: source NAT
Client IP Insertion: ☑ Enable
Redirect-Rewrite Secure: □ Enable
SSL Mode: SSL Offload
SSL Certificate/Key: A10Test — Create | Import
Certificate Chain: — Import
SSL Configuration: 8 Cipher Suites Selected
HSTS: ☑ Enable
HTTP Compression: ☑ Enable
File Extensions: pdf,ppt

Figure 14: Advanced configuration parameters for external virtual server

DDOS MITIGATION

In this deployment, we will also enable the check to drop anomalous packets to protect applications from distributed denial of service (DDoS) attacks.

Scroll down and in the "Security" section enable the checkbox for "Drop Anomalous Packets." Optionally, you can choose the packet types to be dropped using the "Drop Selected" option.



Security

Drop Anomalous Packets ☑ Enable 11 Anomalous Types Selected

Authentication

Internal SharePoint ☑ Enable

Central Admin □ Enable

External SharePoint ☑ Enable

Client Logon Method HTTP Basic ○ Integrated Windows Authentication

Max Number of Logon Retries 3

Active Directory IP 172.16.1.2

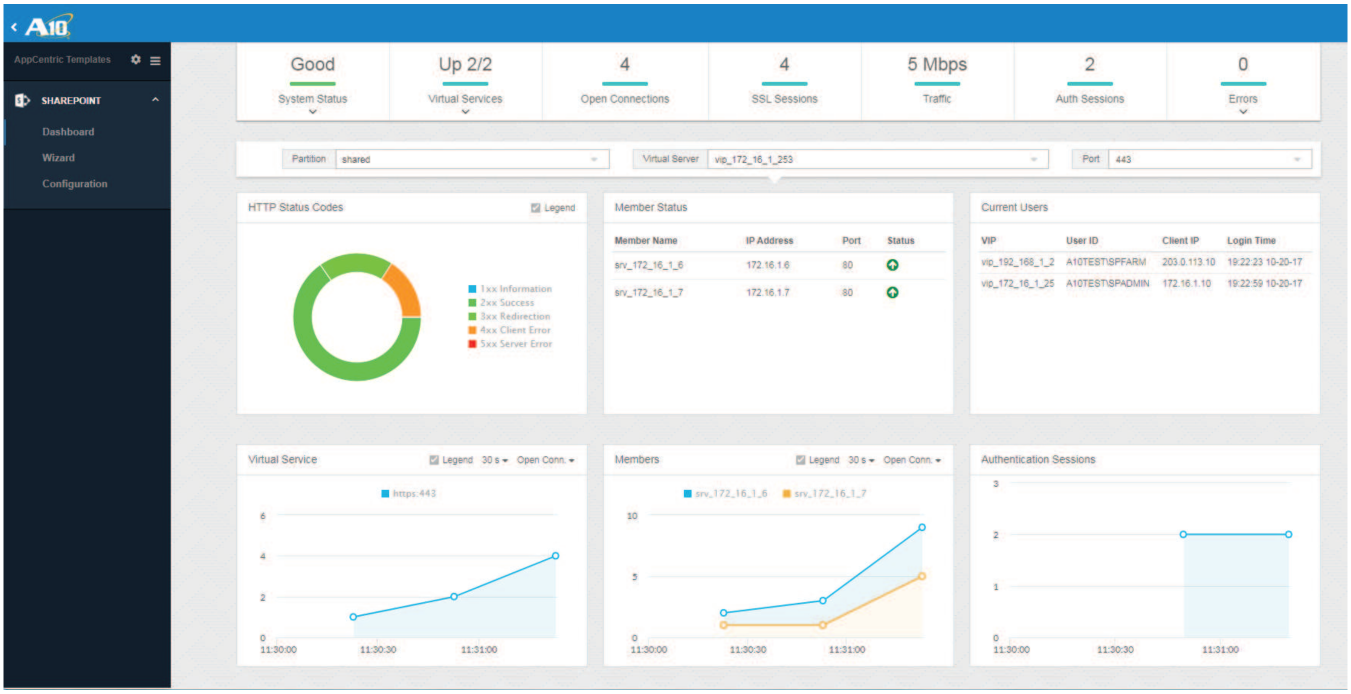
Figure 15: DDoS mitigation

Click on "Apply Changes" at the end of the page to push the new configuration changes to the Thunder ADC.

DASHBOARD

To review the current operational status and traffic analytics for the SharePoint deployment, go to SharePoint > Dashboard. Here you can view information such as:

- Overall system status (total memory, SSL memory, control CPU and data CPU)
- Health of the SharePoint virtual services and the member servers
- Traffic throughput
- Number of open SSL connections
- If Thunder ADC is configured as an authentication proxy, you can also view the number of authentication sessions and details about the corresponding users who have logged-in into SharePoint web site



Good	Up 2/2	4	4	5 Mbps	2	0
System Status	Virtual Services	Open Connections	SSL Sessions	Traffic	Auth Sessions	Errors

Partition shared

Virtual Server vip_172_16_1_253

Port 443

HTTP Status Codes

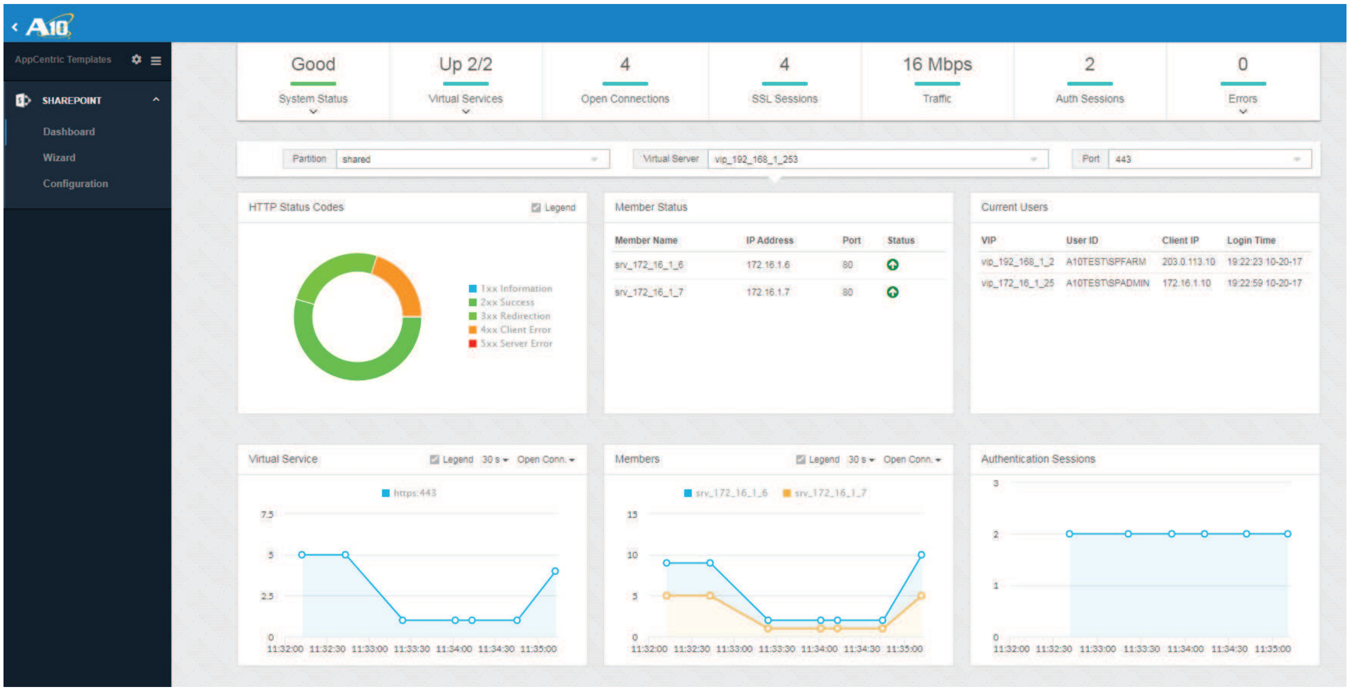
Member Status

Member Name	IP Address	Port	Status
srv_172_16_1_6	172.16.1.6	80	⬆
srv_172_16_1_7	172.16.1.7	80	⬆

Current Users

VIP	User ID	Client IP	Login Time
vip_192_168_1_2	A10TEST\SPFARM	203.0.113.10	19:22:23 10-20-17
vip_172_16_1_25	A10TEST\SPADMIN	172.16.1.10	19:22:59 10-20-17

Figure 16: SharePoint internal virtual service



Good	Up 2/2	4	4	16 Mbps	2	0
System Status	Virtual Services	Open Connections	SSL Sessions	Traffic	Auth Sessions	Errors

Partition: shared
Virtual Server: vip_192_168_1_253
Port: 443

HTTP Status Codes

Member Status

Member Name	IP Address	Port	Status
srv_172_16_1_6	172.16.1.6	80	⬆
srv_172_16_1_7	172.16.1.7	80	⬆

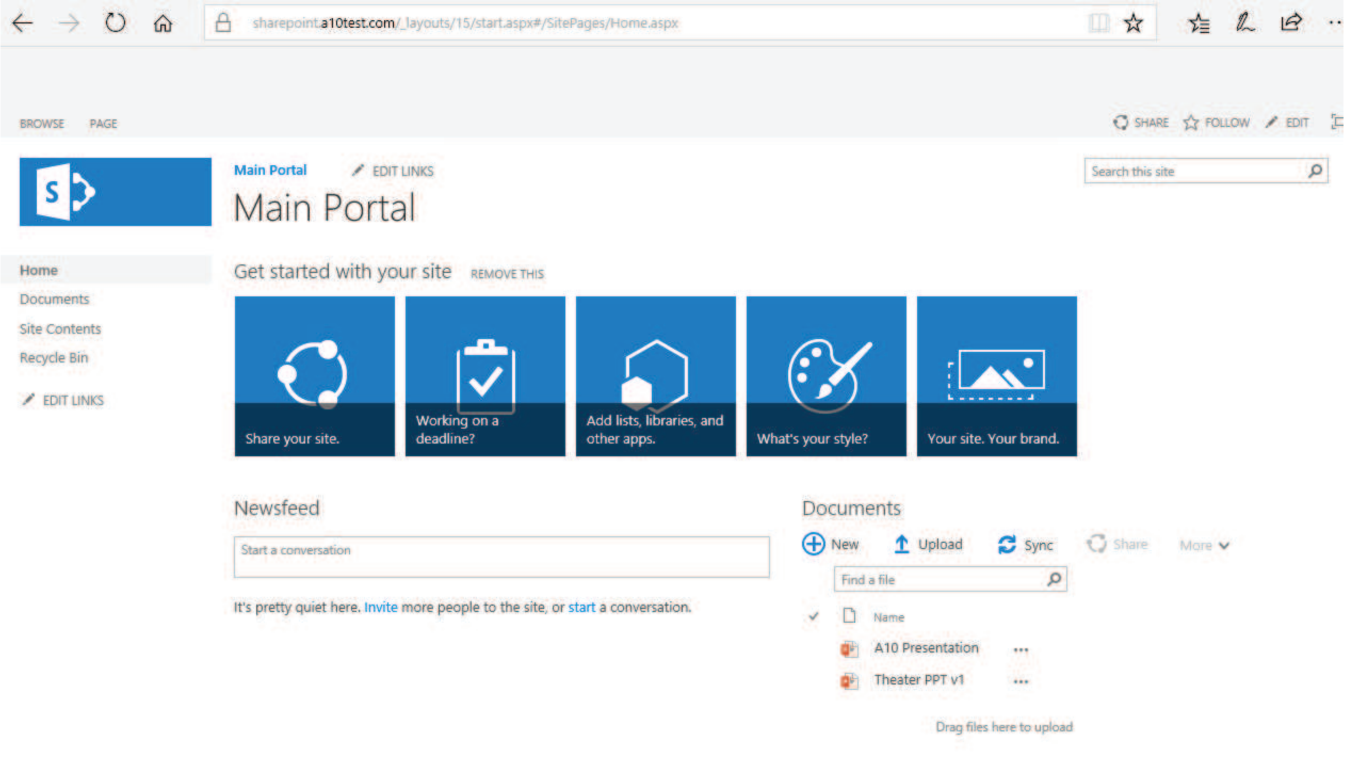
Current Users

VIP	User ID	Client IP	Login Time
vip_192_168_1_2	A10TEST\SPFARM	203.0.113.10	19:22:23 10-20-17
vip_172_16_1_25	A10TEST\SPADMIN	172.16.1.10	19:22:59 10-20-17

Figure 17: SharePoint external virtual service

SHAREPOINT WEB SITE

Both internal and external clients can access the SharePoint web site at the URL https://sharepoint.a10test.com. The clients will be automatically redirected to the secure web site URL if they specify the protocol as HTTP instead of HTTPS.


sharepoint.a10test.com/_layouts/15/start.aspx#/SitePages/Home.aspx

It's pretty quiet here. Invite more people to the site, or start a conversation.

Figure 18: SharePoint web site

SUMMARY

This document describes how to configure Thunder ADC as a load balancer to support a Microsoft SharePoint 2016 Server deployment using A10 AppCentric Templates. The Thunder ADC, powered by ACOS, enhances Microsoft SharePoint 2016 by providing the following:

- High availability for SharePoint servers, ensuring that users can access SharePoint sites without disruption
- Scalability, as the Thunder ADC device transparently load balances multiple SharePoint servers
- Higher connection throughput to enhance the end user experience
- Improved server performance due to server optimizations such as SSL offload and HTTP compression
- Highest levels of security with PFS ciphers, HSTS and HTTP-to-HTTPS redirection
- Protection against DDoS attacks using integrated DDoS protection capabilities
- Centralized administration and monitoring of client sessions by authenticating the clients
- Ease of deployment with AppCentric Templates (ACT)

For more information about Thunder ADC products, please refer to:

https://www.a10networks.com/products/thunder-series/thunder-application_delivery_controller

https://www.a10networks.com/resources/solution-briefs

https://www.a10networks.com/resources/case-studies

APPENDIX A – THUNDER ADC TEST CONFIGURATION

Here is the Thunder ADC configuration used in an actual test environment.

```
!
ip anomaly-drop packet-deformity layer-3
ip anomaly-drop packet-deformity layer-4
ip anomaly-drop security-attack layer-3
ip anomaly-drop security-attack layer-4
ip anomaly-drop frag
ip anomaly-drop ip-option
ip anomaly-drop land-attack
ip anomaly-drop ping-of-death
ip anomaly-drop tcp-no-flag
ip anomaly-drop tcp-syn-fin
ip anomaly-drop tcp-syn-frag
!
vlan 101
  untagged ethernet 2
  router-interface ve 101
!
vlan 102
  untagged ethernet 3
  router-interface ve 102
!
interface management
  ip address 10.100.2.31 255.255.255.0
  ip default-gateway 10.100.2.1
  enable
!
interface ethernet 1
!
interface ethernet 2
  enable
!
interface ethernet 3
  enable
!
interface ve 101
  ip address 172.16.1.1 255.255.255.0
!
interface ve 102
  ip address 192.168.1.1 255.255.255.0
!
!
ip route 0.0.0.0 /0 192.168.1.254
!
aam authentication logon http-authenticate
act_sharepoint_logon
  auth-method basic enable
!
!
slb common
  enable-l7-req-acct
!
health monitor Hm_vip_172_16_1_253_80_http
  user-tag act_sharepoint_Hm_
vip_172_16_1_253_80_http
  method http expect response-code 401 url GET
/
!
health monitor Hm_vip_172_16_1_253_443_http
  user-tag act_sharepoint_Hm_
vip_172_16_1_253_443_http
  method http expect response-code 401 url GET
/
!
health monitor Hm_vip_192_168_1_253_80_http
  user-tag act_sharepoint_Hm_
vip_192_168_1_253_80_http
  method http expect response-code 401 url GET
/
!
health monitor Hm_vip_192_168_1_253_443_http
  user-tag act_sharepoint_Hm_
vip_192_168_1_253_443_http
  method http expect response-code 401 url GET
/
!
aam authentication server windows act_
sharepoint_ad_auth_server
  host 172.16.1.2
  auth-protocol kerberos-disable
!
aam authentication relay ntlm act_sharepoint_ntlm_relay
!
aam authentication template act_sharepoint_aam_auth_template
  logon act_sharepoint_logon
  relay act_sharepoint_ntlm_relay
  server act_sharepoint_ad_auth_server
  user-tag act_sharepoint_aam_auth_template
!
aam aaa-policy act_sharepoint_aaa_policy
  user-tag act_sharepoint_aaa_policy
  aaa-rule 1
    action allow
    authentication-template act_sharepoint_aam_auth_template
!
slb template cipher Ccipher_vip_172_16_1_253_443
  TLS1_RSA_AES_128_SHA
  TLS1_RSA_AES_256_SHA
  TLS1_RSA_AES_128_GCM_SHA256
  TLS1_RSA_AES_256_GCM_SHA384
  TLS1_ECDHE_RSA_AES_128_SHA priority 10
  TLS1_ECDHE_RSA_AES_256_SHA priority 10
  TLS1_ECDHE_RSA_AES_128_SHA256 priority 10
  TLS1_ECDHE_RSA_AES_128_GCM_SHA256 priority 10
  user-tag act_sharepoint_Ccipher_vip_172_16_1_253_443
!
slb template cipher Ccipher_vip_192_168_1_253_443
  TLS1_RSA_AES_128_SHA
  TLS1_RSA_AES_256_SHA
  TLS1_RSA_AES_128_GCM_SHA256
  TLS1_RSA_AES_256_GCM_SHA384
  TLS1_ECDHE_RSA_AES_128_SHA priority 10
  TLS1_ECDHE_RSA_AES_256_SHA priority 10
  TLS1_ECDHE_RSA_AES_128_SHA256 priority 10
  TLS1_ECDHE_RSA_AES_128_GCM_SHA256 priority 10
  user-tag act_sharepoint_Ccipher_vip_192_168_1_253_443
!
slb server srv_172_16_1_6 172.16.1.6
  user-tag act_sharepoint_srv_172_16_1_6
  port 80 tcp
    health-check ping
    user-tag act_sharepoint_srv_172_16_1_6_port_80
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server srv_172_16_1_7 172.16.1.7
  user-tag act_sharepoint_srv_172_16_1_7
  port 80 tcp
    health-check ping
    user-tag act_sharepoint_srv_172_16_1_7_port_80
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb service-group vip_172_16_1_253_443_https_sg tcp
  method least-connection
  health-check Hm_vip_172_16_1_253_443_http
  user-tag act_sharepoint_vip_172_16_1_253_443_https_sg
  member srv_172_16_1_6 80
  member srv_172_16_1_7 80
!
slb service-group vip_172_16_1_253_80_http_sg tcp
  method least-connection
  health-check Hm_vip_172_16_1_253_80_http
  user-tag act_sharepoint_vip_172_16_1_253_80_http_sg
  member srv_172_16_1_6 80
  member srv_172_16_1_7 80
```

```
!
slb service-group vip_192_168_1_253_443_https_sg tcp
  method least-connection
  health-check Hm_vip_192_168_1_253_443_http
  user-tag act_sharepoint_vip_192_168_1_253_443_https_sg
  member srv_172_16_1_6 80
  member srv_172_16_1_7 80
!
slb service-group vip_192_168_1_253_80_http_sg tcp
  method least-connection
  health-check Hm_vip_192_168_1_253_80_http
  user-tag act_sharepoint_vip_192_168_1_253_80_http_sg
  member srv_172_16_1_6 80
  member srv_172_16_1_7 80
!
slb template client-ssl Cssl_vip_172_16_1_253_443
  cert A10Test
  enable-tls-alert-logging fatal
  key A10Test
  template cipher Ccipher_vip_172_16_1_253_443
  disable-sslv3
  user-tag act_sharepoint_Cssl_vip_172_16_1_253_443
!
slb template client-ssl Cssl_vip_192_168_1_253_443
  cert A10Test
  enable-tls-alert-logging fatal
  key A10Test
  template cipher Ccipher_vip_192_168_1_253_443
  disable-sslv3
  user-tag act_sharepoint_Cssl_vip_192_168_1_253_443
!
slb template http Http_templ_vip_172_16_1_253_80
  insert-client-ip
  redirect secure port 443
  user-tag act_sharepoint_vip_172_16_1_253_80
!
slb template http Http_templ_vip_172_16_1_253_443
  compression content-type pdf
  compression content-type ppt
  compression enable
  insert-client-ip
  response-header-insert strict-transport-security:max-age=31536000
  user-tag act_sharepoint_vip_172_16_1_253_443
!
slb template http Http_templ_vip_192_168_1_253_80
  insert-client-ip
  redirect secure port 443
  user-tag act_sharepoint_vip_192_168_1_253_80
!
slb template http Http_templ_vip_192_168_1_253_443
  compression content-type pdf
  compression content-type ppt
  compression enable
  insert-client-ip
  response-header-insert strict-transport-security:max-age=31536000
  user-tag act_sharepoint_vip_192_168_1_253_443
!
slb virtual-server vip_172_16_1_253 172.16.1.253
  user-tag act_sharepoint_internal_vip_172_16_1_253
  port 80 http
    aflex _act_http_log
    source-nat auto
    service-group vip_172_16_1_253_80_http_sg
    template http Http_templ_vip_172_16_1_253_80
    user-tag vip_172_16_1_253_port_80_http
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
  port 443 https
```

```
    aflex _act_http_log
    source-nat auto
    service-group vip_172_16_1_253_443_https_sg
    template http Http_templ_vip_172_16_1_253_443
    template client-ssl Cssl_vip_172_16_1_253_443
    aaa-policy act_sharepoint_aaa_policy
    user-tag vip_172_16_1_253_port_443_https
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
!
slb virtual-server vip_192_168_1_253 192.168.1.253
  user-tag act_sharepoint_external_vip_192_168_1_253
  port 80 http
    aflex _act_http_log
    source-nat auto
    service-group vip_192_168_1_253_80_http_sg
    template http Http_templ_vip_192_168_1_253_80
    user-tag vip_192_168_1_253_port_80_http
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
  port 443 https
    aflex _act_http_log
    source-nat auto
    service-group vip_192_168_1_253_443_https_sg
    template http Http_templ_vip_192_168_1_253_443
    template client-ssl Cssl_vip_192_168_1_253_443
    aaa-policy act_sharepoint_aaa_policy
    user-tag vip_192_168_1_253_port_443_https
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
!
end
```

APPENDIX B – APPCENTRIC TEMPLATES UPGRADE

To upgrade ACT to the latest version, one of the following two methods can be used:

UPGRADING ACT USING CLOUD-BASED UPDATE

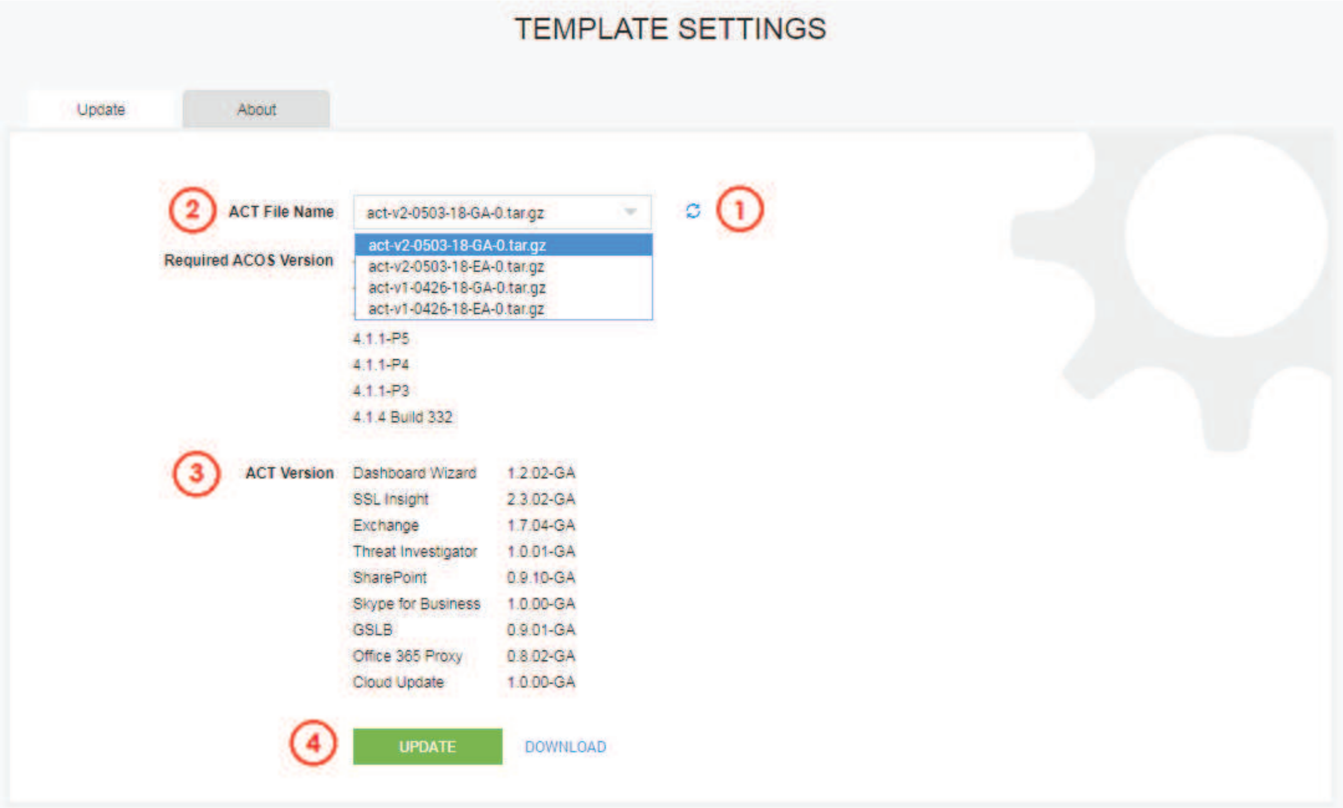
ACT can be upgraded to the latest version directly from the cloud.

To do so, login to ACOS GUI and navigate to **System > App Template**. This will take you to the current version of ACT available on your device. If prompted, login to ACT using your ACOS credentials.

From the landing page, navigate to the **Settings** page.

> ***NOTE***: *Depending on the ACT version you are currently using, you will either find the Settings link on the left pane or as a gear icon in the top right corner of the screen.*

1. Under the **Update** tab on the **Settings** page, click on the refresh icon next to "ACT File Name" dropdown menu.



TEMPLATE SETTINGS

ACT File Name: act-v2-0503-18-GA-0.tar.gz

act-v2-0503-18-GA-0.tar.gz
act-v2-0503-18-EA-0.tar.gz
act-v1-0426-18-GA-0.tar.gz
act-v1-0426-18-EA-0.tar.gz

Required ACOS Version:
4.1.1-P5
4.1.1-P4
4.1.1-P3
4.1.4 Build 332

ACT Version:

Dashboard Wizard	1.2.02-GA
SSL Insight	2.3.02-GA
Exchange	1.7.04-GA
Threat Investigator	1.0.01-GA
SharePoint	0.9.10-GA
Skype for Business	1.0.00-GA
GSLB	0.9.01-GA
Office 365 Proxy	0.8.02-GA
Cloud Update	1.0.00-GA

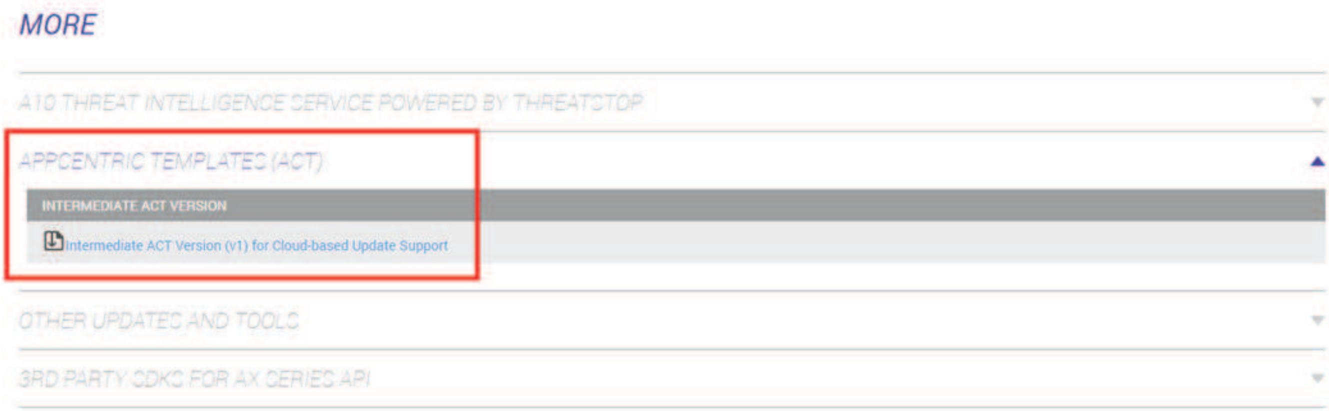
2. Select the desired ACT build from the dropdown menu and verify that your ACOS version is listed below for compatibility.
3. Also make sure that the Application for which you want to upgrade ACT is included in the build.
4. Click **Update**.

> ***NOTE***: *You can find the current version of ACT running on your device by navigating to the **About** tab on the **Settings** page.*

UPGRADING ACT USING MANUAL UPDATE

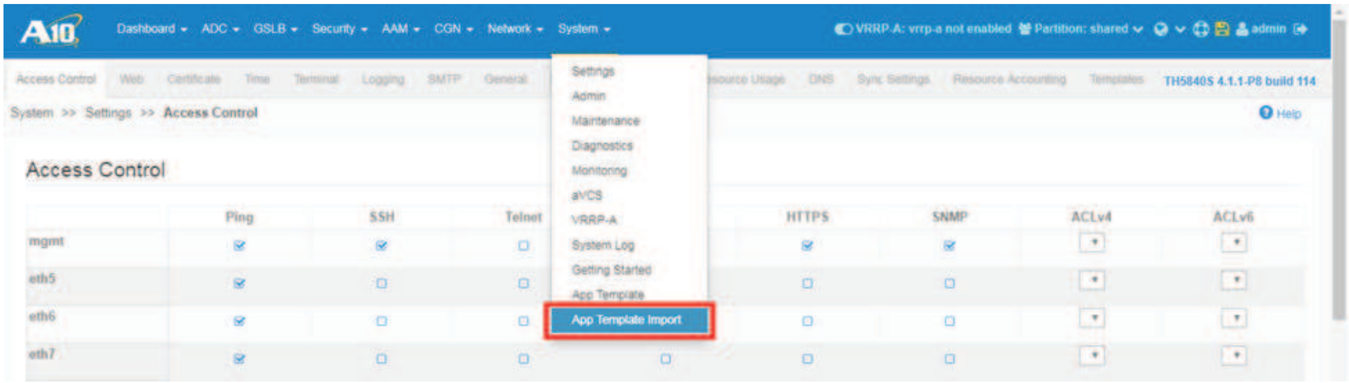
If your current ACT version does not support cloud-based updates, you can use the manual update option to upgrade to an intermediary version that does support cloud-based updates. You can then update to your desired ACT version using the steps mentioned above.

The intermediary ACT version can be downloaded as a tar.gz file to your computer from this link or by navigating to the **More** section of the **A10 Networks Support Portal**. Make sure that the package is not decompressed.

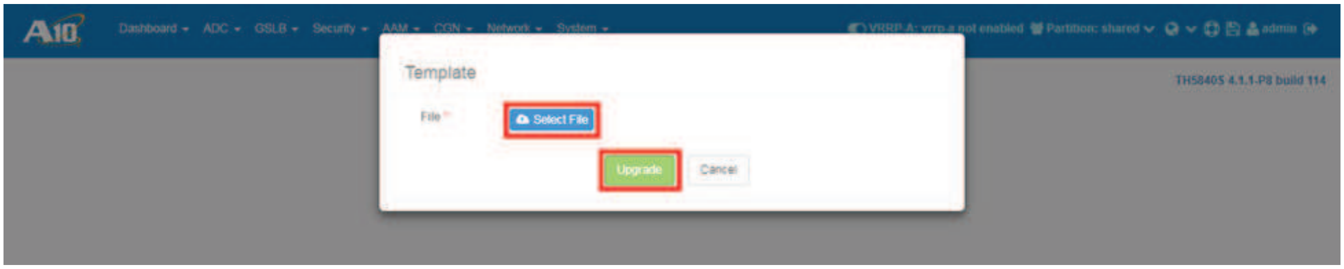

MORE
A10 THREAT INTELLIGENCE SERVICE POWERED BY THREATSTOP
APPCENTRIC TEMPLATES (ACT)
INTERMEDIATE ACT VERSION
Intermediate ACT Version (v1) for Cloud-based Update Support
OTHER UPDATES AND TOOLS
3RD PARTY SDKS FOR AX SERIES API

***NOTE**: This ACT version requires your device to be upgraded to ACOS version 4.1.1-P3 or later.*

To start, login to ACOS GUI and navigate to **System > App Template Import**.



The following pop-up will appear:



- Click **Select File** and browse to the package downloaded earlier.
- Click **Upgrade**.

***NOTE**: At this point, wait patiently and do not close the window or interrupt the upgrade process in any way.*

Once successfully upgraded, either click on the **Jump Now!** link that appears in the popup, or navigate to **System > App Template** from the ACOS GUI.

> ***NOTE***: *In rare cases, after updating the ACT, you might experience that the ACT isn't loading. In such a scenario, logout from the ACOS GUI, and clear any cookies from the browser that are related to the A10 GUI or ACT. Alternatively, you can also clear the whole browser cache and then launch ACT.*

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-DG-16167-EN-02   JUL 2018