DEPLOYMENT GUIDE

MICROSOFT SKYPE FOR BUSINESS SERVER 2015 DEPLOYMENT WITH THUNDER ADC USING APPCENTRIC TEMPLATES (ACT)

A10 THUNDER ADC FOR INTELLIGENT LOAD BALANCING, SECURITY, ACCELERATION AND OPTIMIZATION FOR SKYPE FOR BUSINESS SERVER 2015

OVERVIEW

A10 Networks® Thunder® ADC line of Application Delivery Controllers provides intelligent load balancing, security, acceleration and optimization for Microsoft Skype for Business Server 2015.

The purpose of this guide is to provide a step-by-step process for deploying A10 Thunder ADC as a load balancer in a Microsoft Skype for Business Server 2015 deployment using AppCentric Templates (ACT). Refer to Appendix A for the equivalent CLI-based configuration.

The following topology (Figure 1) is designed to support Skype for Business voice services, presence, instant messaging, desktop sharing, collaboration and Enterprise Voice Features for both internal and external users with a high availability (HA) system architecture. In this guide, one A10 Networks vThunder® ADC with four Application Delivery Partitions (ADPs) was used to deploy four (4) different zones/services: Front End, Internal Edge, External Edge and Reverse Proxy. The solution can be deployed with separate virtual or physical appliances for each service in the same way.

For additional Microsoft deployment guides such as Lync Server, Microsoft Exchange and/or SharePoint, 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.

SKYPE FOR BUSINESS SERVER 2015 ROLES

Each server running Skype for Business Server runs one or more server roles. A server role is a defined set of Skype for Business Server functionalities provided by that server. The primary server roles are described below[1].

FRONT END SERVERS

In Skype for Business Server Enterprise Edition, the Front End Server is the core server role, and runs many basic Skype for Business Server functions.

The Front End Server includes the following:

- User authentication and registration
- Presence information and contact card exchange
- Address book services and distribution list expansion
- IM functionality, including multiparty IM conferences
- Web conferencing, PSTN Dial-in conferencing and A/V conferencing (if deployed)
- Application hosting, for both applications included with Skype for Business Server (for example, Conferencing Attendant and Response Group application), and third-party applications
- Web components to supported web-based tasks such as web scheduler and join launcher
- (Optionally) Archiving, to archive IM communications and meeting content for compliance reasons
- (Optionally if Persistent Chat is enabled) Persistent Chat Web Services for Chat Room Management and Persistent Chat Web Services for File Upload/Download
- (Optionally) Monitoring, to collect usage information in the form of call detail records (CDRs) and call error records (CERs), which provide metrics about the quality of the media (audio and video) traversing your network for both Enterprise Voice calls and A/V conferences

A Front End pool is a set of Front End Servers, configured identically, that work together to provide services for a common group of users. Standard Edition servers cannot be pooled, whereas multiple Enterprise Edition Servers can exist in a pool to provide redundancy and scalability.

BACK END (BE) SERVER

The Back End (BE) Servers run Microsoft SQL and provide database services for the front end pool. The information stored in the SQL servers includes user contact lists, presence information, conferencing details and conferencing schedule information. The SQL server can be configured as a single back end server; however, a cluster of two or more servers is recommended for failover. The BE Servers do not run any Skype for Business Server software. The BE server requirement can be implemented with Microsoft SQL Server 2012 or Microsoft SQL Server 2014 – Standard and Enterprise (64-bit edition)[2].

EDGE SERVER

Edge Server enables your users to communicate and collaborate with users outside the organization's firewalls. These external users can include: the organization's own users who are currently working offsite; users from federated partner organizations; and outside users who have been invited to join conferences hosted on your Skype for Business Server deployment. Each Edge Server has two network interfaces, external and internal. The external interface accepts connections initiated from the Internet, and the internal interface accepts connections initiated from the internal network.

[1] https://technet.microsoft.com/en-us/library/dn933894.aspx

[2] https://technet.microsoft.com/en-us/library/dn951388.aspx#DBs

OFFICE ONLINE SERVER

Office Online Server is the next version of Office Web Apps Server and is used in Skype for Business Server 2015 for sharing and rendering of PowerPoint presentations.

REVERSE PROXY

Reverse Proxy publishes to the Internet the web components of Front End Servers and Office Online Server (OOS) services.

DEPLOYMENT TOPOLOGY

Figure 1 shows a Skype for Business Server 2015 deployment using Thunder ADCs. It provides the following services:

- Login and Presence functionality
- Instant Messaging, including multiparty IM conferences
- Audio/video calls
- Desktop sharing
- PowerPoint sharing

In this setup, one single vThunder ADC with four ADPs was used to deploy four (4) different zones/services: Internal/Front End, Internal Edge, External Edge and Reverse Proxy thereby enabling consolidation of resources.

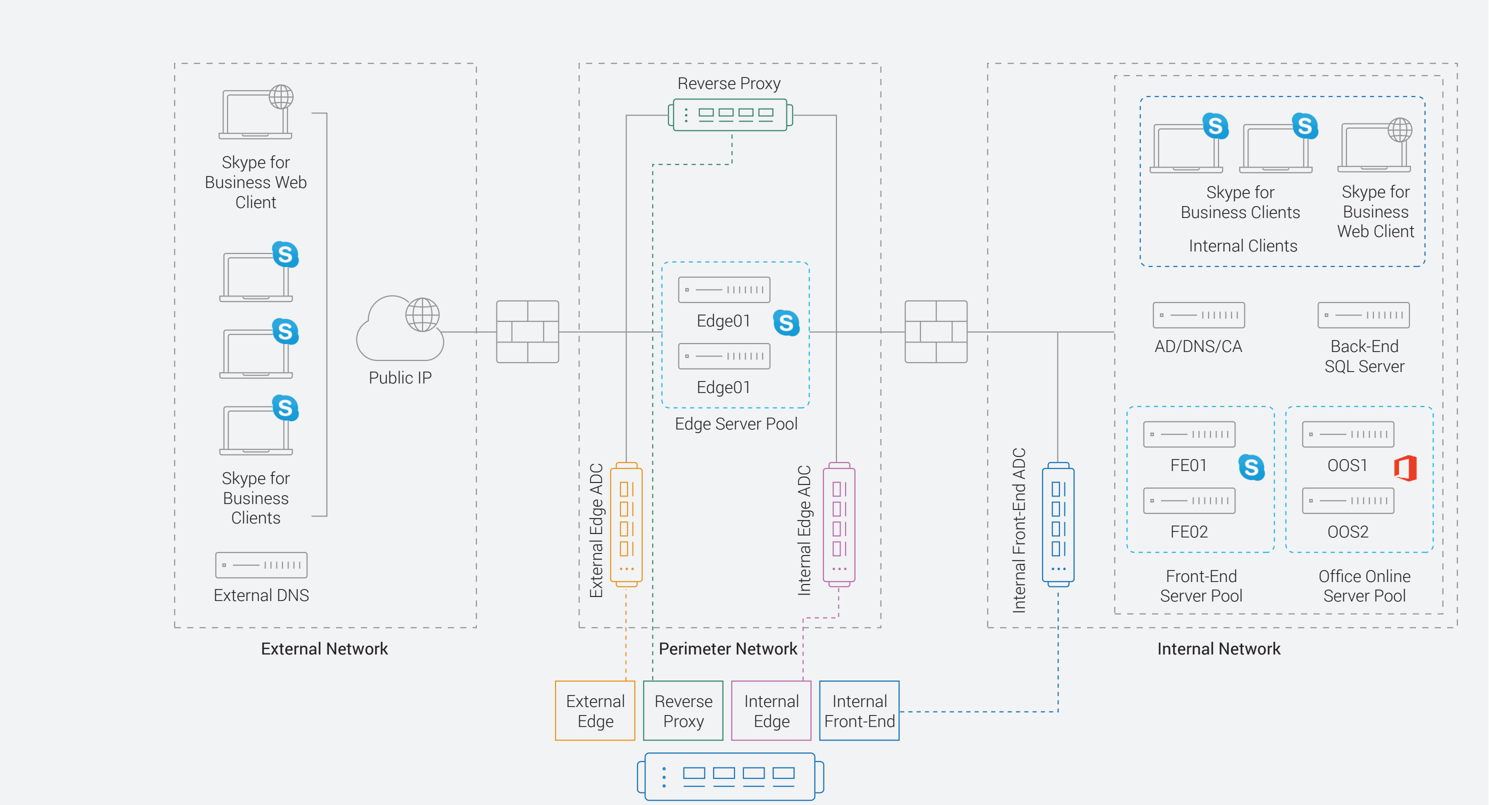


Figure 1: Lab topology

Table 1 shows Hostname and IP address on each element/device used in this guide (as shown in the above diagram).

ROLE	*LOAD BALANCING VIP*	*DEVICE HOSTNAME*	*IP ADDRESS*
Active Directory (AD), Internal Certificate Authority (CA), Internal DNS	NA	DC	10.0.3.10/24
Front End	10.0.3.123/24	FE01	10.0.3.12/24
		FE02	10.0.3.13/24
Back End	NA	SQL	10.0.3.11/24
External Edge	192.0.2.111, 112, 113/24	Edge01	192.0.2.21, 22, 23/24
		Edge02	192.0.2.31, 32, 33/24
Internal Edge	10.0.4.30/24	Edge01	10.0.4.31/24
		Edge02	10.0.4.32/24
Office Online Server (previously Office Web Apps Server)	10.0.3.125/24	OOS1	10.0.3.15/24
		OOS2	10.0.3.16/24
Reverse Proxy	192.0.2.108	Front End VIP	10.0.3.123/24
		OOS VIP	10.0.3.125/25
External DNS	NA	ExternalDNS	198.51.100.10
External Clients (Multiple)	NA	ExternalClient<number>	198.51.100.x/24
Internal Clients (Multiple)	NA	InternalClient<number>	10.0.3.x/24

Notes specific to this guide:

1. This setup was tested with A10 Thunder ADC appliance running the A10 Networks Advanced Core Operating System (ACOS®) version 4.1.1-P1.
2. The A10 Networks AppCentric Templates (ACT) version was act-0911-17 (see Appendix B for details).
3. The solution was deployed with a single vThunder ADC device with four ADPs, one for each of the four (4) different zones/services: Internal/Front End, Internal Edge, External Edge and Reverse Proxy. The solution can also be deployed in the same way using separate virtual or physical appliances for each service. Two devices are going to be required for high availability.
4. Microsoft Skype for Business Server 2015 was tested through communication with IM, Presence, Desktop Collaboration and Audio Video (AV) conferencing. Testing was performed for both internal and external users.
5. Testing was performed using Microsoft Skype for Business Server 2015 Enterprise Edition Server with 64-bit Microsoft SQL Server 2012 Enterprise Edition.
6. Skype for Business 2015 Server Front End and Edge Server components were running on Windows 2012 R2 (64-bit) Standard Edition Server. Office Online Server was running on Windows Server 2012 Datacenter Edition.
7. Skype for Business Basic Client 64-bit on Windows 10 was used for desktop client.
8. Office Online Server (OOS) was tested with PowerPoint presentation sharing.

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 ACOS. Refer to Appendix B for details on how to acquire and import the file. The 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.*

SERVICES REQUIRED FOR SKYPE FOR BUSINESS 2015 DEPLOYMENT

The following tables list the load-balancing services required for a Skype for Business 2015 Enterprise Server deployment.

Table 2: Services on Front End Server

SERVICE NAME	PORT	VPORT TYPE	SOURCE NAT	FEATURE TEMPLATE	USAGE NOTE
Front End Service	135	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Used for Distributed Component Object Model (DCOM)-based operations such as Moving Users, User Replicator Synchronization and Address Book Synchronization.
Web Compatibility Service	443	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Used for communication from Front End Servers to web farm fully qualified domain names (FQDNs) (the URLs used by IIS web components). Client SSL template is required if SSL offload is configured.
Web Server Component	4443	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Used for web access from remote user. Client SSL template is required if SSL offload is configured.
Front End Service	444	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Used for HTTPS communication between the Focus (Skype for Business Server component that manages conference state) and the individual servers. This port is also used for TCP communication between Survivable Branch Appliances and Front End Servers.
Front End Service	5061	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	All internal SIP communications between servers (MTLS). SIP communications between Server and Client (TLS). SIP communications between Front End Servers and Mediation Servers (MTLS). Also used for communications with Monitoring Server.

Table 3: Optional Services on Front End Server

SERVICE NAME	PORT	VPORT TYPE	SOURCE NAT	FEATURE TEMPLATE	USAGE NOTE
Application Sharing Service	5065	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Used for incoming SIP listening requests for application sharing
Response Group Service	5071	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Used for incoming SIP requests for the Response Group application
Conferencing Attendant Service (Dial-in Conferencing)	5072	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Used for incoming SIP requests for Attendant (dial-in conferencing)
Conferencing Announcement Service	5073	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Used for incoming SIP requests for the Skype for Business Server Conferencing Announcement service (that is, for dial-in conferencing)
Call Park Service	5075	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Used for incoming SIP requests for the Call Park application
Audio Test Service	5076	TCP	Yes	Persistence: Source-IP TCP: TCP Health Monitor: TCP port	Used for incoming SIP requests for the Audio Test service

***NOTE**: Details of port and protocol Skype for Business 2015 Front End Server uses are described at the following URL: https://technet.microsoft.com/en-us/library/gg398833.aspx*

SERVICE NAME	*PORT*	*VPORT TYPE*	*SOURCE NAT*	*FEATURE TEMPLATE*	*USAGE NOTE*
STUN/ MSTURN	443	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Fallback path for A/V media transfer between internal and external users if UDP communication cannot be established. TCP is used for file transfer and desktop sharing.
STUN/ MSTURN	3478	UDP	Yes	Persistence: Source-IP Health Monitor: UDP port	Preferred path for A/V media transfer between internal and external users.
Access/SIP	5061	TCP/MTLS	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Inbound/Outbound SIP traffic (to/from Director, Director pool virtual IP address, Front End Server or Front End pool virtual IP address) from/to Edge Server internal interface.
SIP/MTLS	5062	TCP	Yes	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Authentication of A/V users (A/V authentication service) from Front End Server or Front End pool IP address or any Survivable Branch Appliance or Survivable Branch Server using this Edge Server.

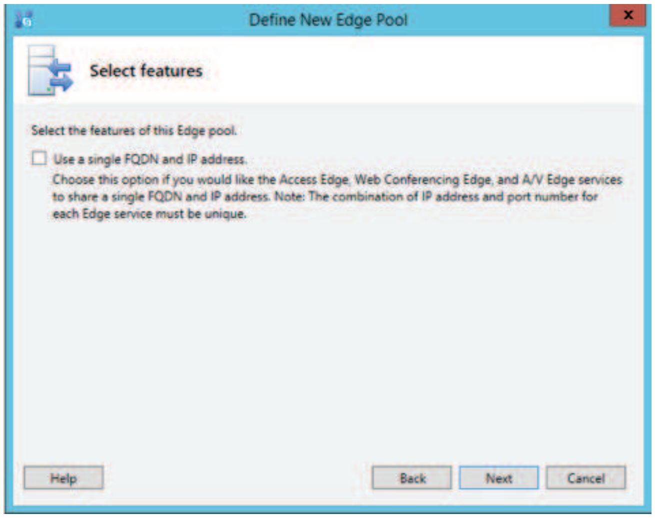
Table 4: Services on Internal Edge

***NOTE**: Details of port and protocol Skype for Business 2015 Edge Server uses are described at the following URL: https://technet.microsoft.com/en-us/library/mt346416.aspx*

SERVICE NAME	*PORT*	*VPORT TYPE*	*SOURCE NAT*	*FEATURE TEMPLATE*	*USAGE NOTE*
Access/SIP(TLS)	443	TCP	No (Optional: Yes)	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Client-to-server SIP traffic for external user access
Access/SIP(MTLS)	5061	TCP	No (Optional: Yes)	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	SIP signaling, federated and public IM connectivity using SIP
Web Conferencing/ PSOM(TLS)	443	TCP	No (Optional: Yes)	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	Web Conferencing media
A/V/ STUN, MSTURN	443	TCP	No	Persistence: Source-IP TCP: TCP idle-timeout Health Monitor: TCP port	STUN/TURN negotiation of candidates over TCP/443
A/V/ STUN, MSTURN	3478	UDP	No	Persistence: Source-IP Health Monitor: UDP port	STUN/TURN negotiation of candidates over UDP/3478

Table 5: Services on External Edge

***NOTE**: During feature selection (Figure 2) of the external Edge pool installation, you will be asked to deploy the Skype Edge Server pool with either single or multiple FQDNs and IP addresses. Deselecting the use a single FQDN and IP address option will enable the external Edge pool to have multiple IP configurations. The Thunder ADC device can be deployed in either a single IP configuration or a multiple IP configuration. In a multiple IP configuration, three public virtual IP addresses (VIPs) will be required for Access, WebConf and AV. For a single FQDN and IP address configuration, one public VIP will be required.*



Define New Edge Pool

Select features

Select the features of this Edge pool.

□ Use a single FQDN and IP address.

Choose this option if you would like the Access Edge, Web Conferencing Edge, and A/V Edge services to share a single FQDN and IP address. Note: The combination of IP address and port number for each Edge service must be unique.

Figure 2: External Edge pool server feature selection

SERVICE NAME	PORT	VPORT TYPE	SOURCE NAT	FEATURE TEMPLATE	USAGE NOTE
Office Online Server Service	443	TCP	Yes	Persistence: Cookie Health Monitor: HTTP Client SSL template: Required	Used for PowerPoint content sharing to Skype for Business clients. SSL Offload is recommended.

Table 6: Service on Office Online Server (Option)

SERVICE NAME	PORT	VPORT TYPE	SOURCE NAT	FEATURE TEMPLATE	USAGE NOTE
Published Web Service	443 >> 4443 (redirect)	HTTPS	Auto	Health Monitor: TCP port Client SSL template: Required Server SSL Template: Required A10 Networks aFleX® TCL Scripting Technology or HTTP Template: Required	Used for communication to Skype Front End Web service from remote user. Traffic sent to port 443 on the Reverse Proxy external interface is redirected to a pool on port 4443 from the Reverse Proxy internal interface so that the pool Web Services can distinguish it from internal web traffic.
Office Online Server Service	443	HTTPS	Auto	Health Monitor: TCP port Client SSL Template: Required Server SSL Template: Required aFleX TCL Scripting or HTTP Template: Required	Used for PowerPoint content sharing/shared from remote users.

Table 7: Services on Reverse Proxy (Option)

NOTE*: Details of ports and protocol of Reverse Proxy is described at the following URL: https://technet.microsoft.com/en-us/library/gg615011.aspx*

THUNDER ADC CONFIGURATION USING APPCENTRIC TEMPLATES

APPCENTRIC TEMPLATES (ACT) OVERVIEW

ACT is an embedded wizard-based configuration tool that enables organizations to apply best practices to deploying and securing their Skype for Business 2015 solution with minimal effort. A10 highly recommends the use of this configuration tool for the deployment and management of Skype for Business 2015, 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.

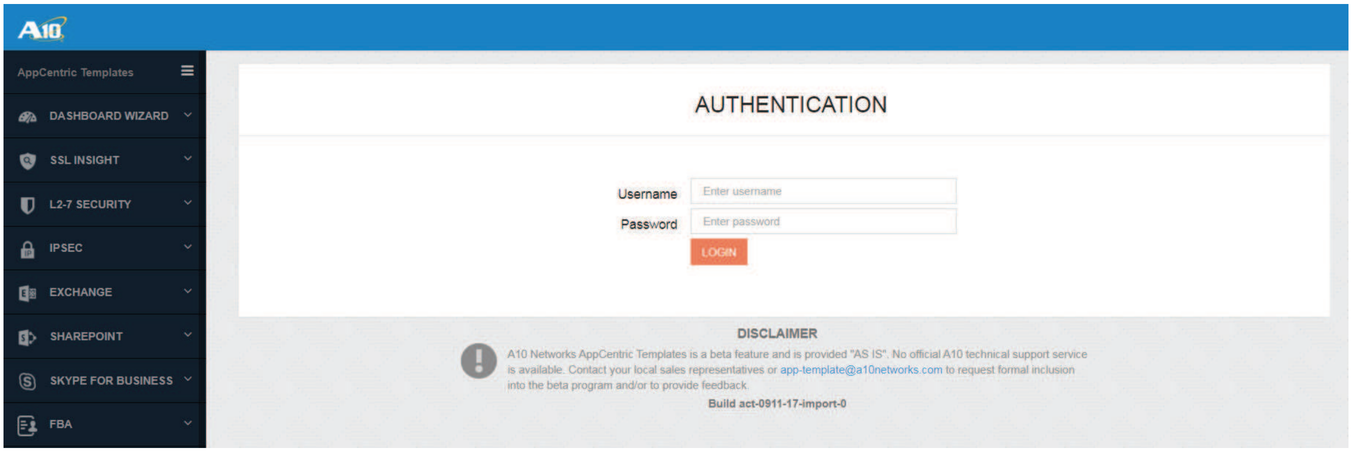
CONFIGURATION USING ACT

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, log into ACT using your regular admin credentials:



DISCLAIMER

A10 Networks AppCentric Templates is a beta feature and is provided "AS IS". No official A10 technical support service is available. Contact your local sales representatives or app-template@a10networks.com to request formal inclusion into the beta program and/or to provide feedback.

Build act-0911-17-import-0

Figure 3: ACT login page

Once you’ve logged into ACT, select Skype for Business from the AppCentric Templates menu.

There are four main sections in the Skype 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. **Topology Builder**: This section enables you to configure partitions and network settings.
3. **Wizard**: The wizard provides users with a guided flow for deployment of Skype with Thunder ADC.
4. **Configuration**: This section provides users with the current configuration of the device as well as access to some advanced options.

Deploying Skype using ACT consists of two main series of steps:

1. Building the topology using Topology Builder: Skype for Business requires four application delivery partitions on a single Thunder ADC or four individual A10 Thunder ADC devices corresponding to the four server roles. If you plan to deploy Thunder ADC using ADPs, you need to first configure the topology using this Topology Builder.
2. Configuration of Skype deployment parameters using the Wizard

TOPOLOGY BUILDER

In the left-pane, go to Skype for Business > Topology Builder

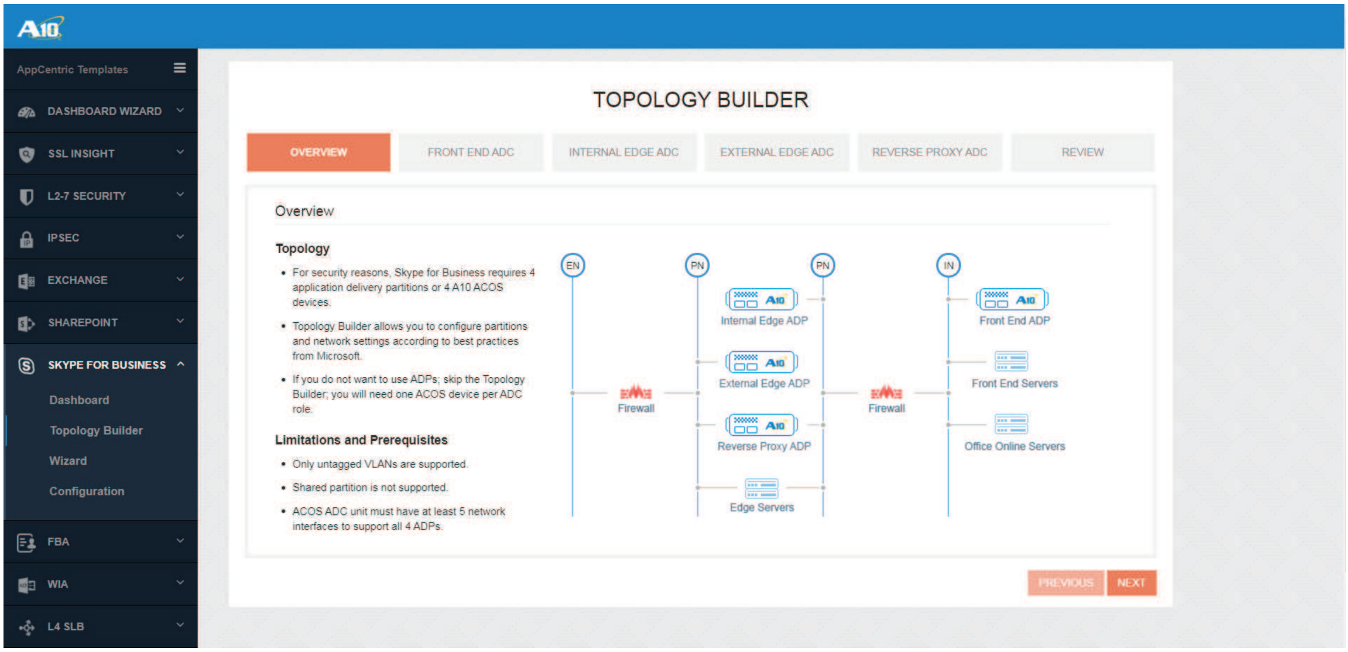
Overview

This section gives an overview of the topology we will deploy. The topology includes three subnets:

- Internal network: 10.0.3.0/24
- Internal perimeter network: 10.0.4.0/24
- External perimeter network: 192.0.2.0/24

Topology Builder will guide you to divide the Thunder ADC into 4 ADPs for the following roles:

- Front End ADC
- Internal Edge ADC
- External Edge ADC
- Reverse Proxy ADC



Overview

Topology

- For security reasons, Skype for Business requires 4 application delivery partitions or 4 A10 ACOS devices.
- Topology Builder allows you to configure partitions and network settings according to best practices from Microsoft.
- If you do not want to use ADPs; skip the Topology Builder; you will need one ACOS device per ADC role.

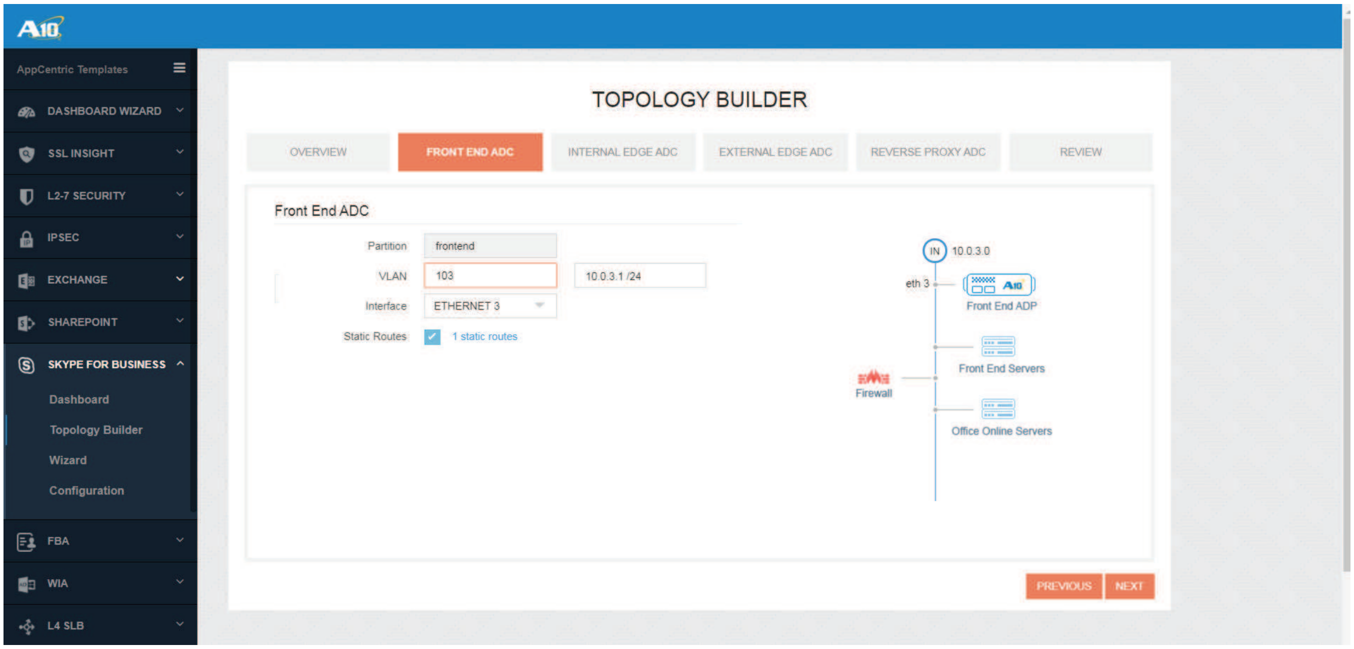
Limitations and Prerequisites

- Only untagged VLANs are supported.
- Shared partition is not supported.
- ACOS ADC unit must have at least 5 network interfaces to support all 4 ADPs.

Figure 4: Topology Builder

FRONT END ADC

The Front End ADC load-balances traffic to the Front End Servers and optionally to the Office Online Servers. It is connected to the internal network 10.0.3.0/24.



Front End ADC

Partition: frontend

VLAN: 103 | 10.0.3.1 /24

Interface: ETHERNET 3

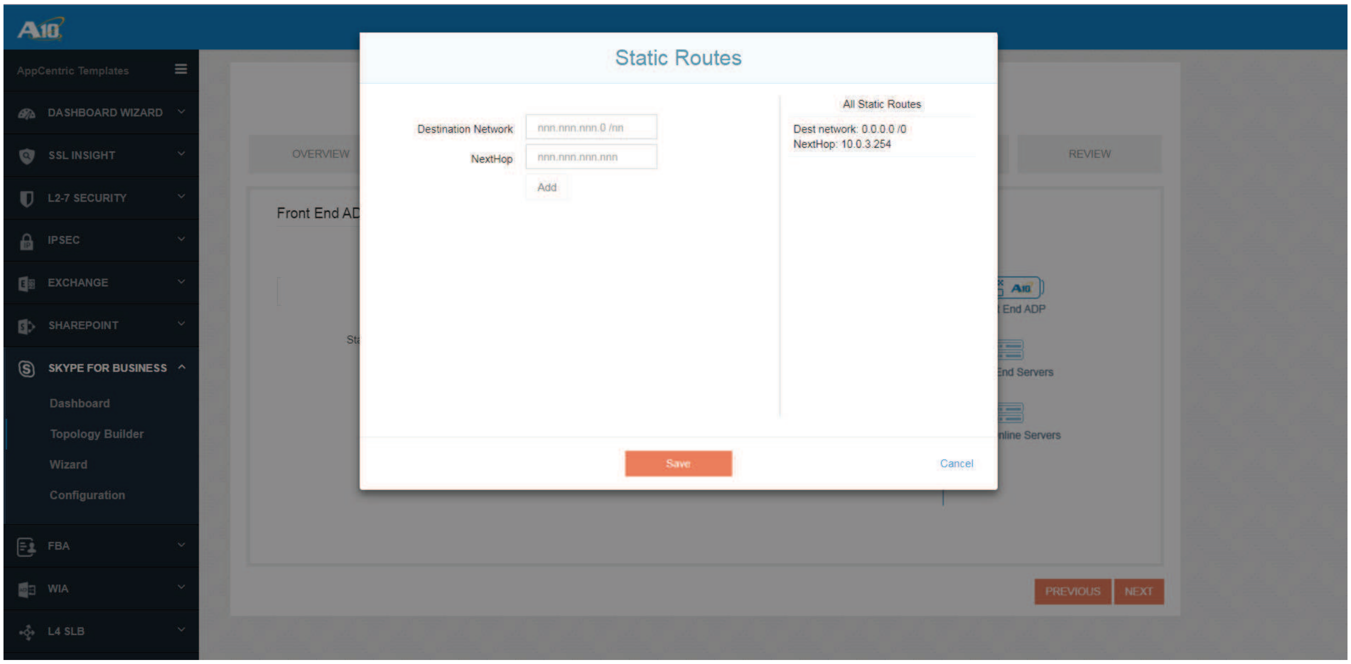
Static Routes: ☑ 1 static routes

Figure 5: Network interface configuration on Front End ADC

VLAN: 103 with IP address 10.0.3.1 /24
The VLAN ID and corresponding virtual interface IP address.

Interface: The physical port that is connected to the network – Ethernet 3.

Static Routes: The routes to be configured on this ADC. Enable this option and define a default route (0.0.0.0 /0) with gateway address of 10.0.3.254:



Static Routes

Destination Network: nnn.nnn.nnn.0 /nn

NextHop: nnn.nnn.nnn.nnn

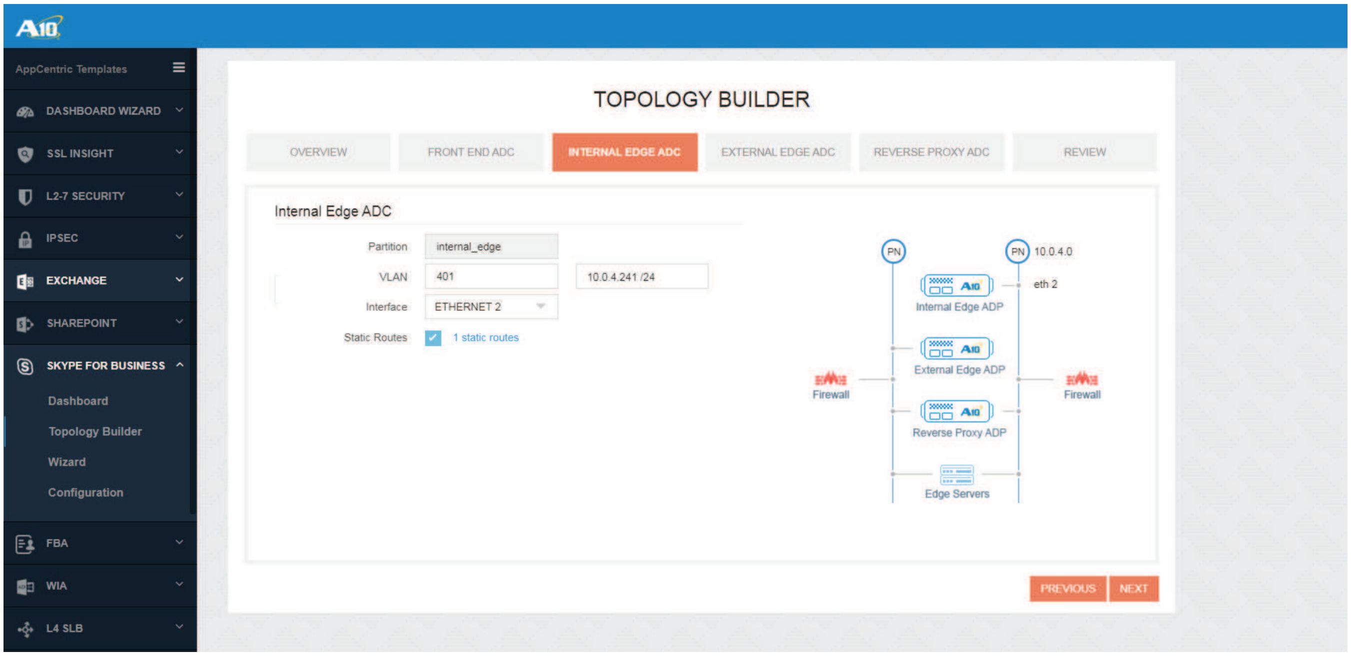
All Static Routes

Dest network: 0.0.0.0 /0
NextHop: 10.0.3.254

Figure 6: Route configuration on Front End ADC

INTERNAL EDGE ADC

The Internal Edge ADC load-balances traffic towards the internal edge interfaces of the Edge servers. It is connected to the internal perimeter network 10.0.4.0/24.



TOPOLOGY BUILDER

Internal Edge ADC

Partition: internal_edge

VLAN: 401 | 10.0.4.241 /24

Interface: ETHERNET 2

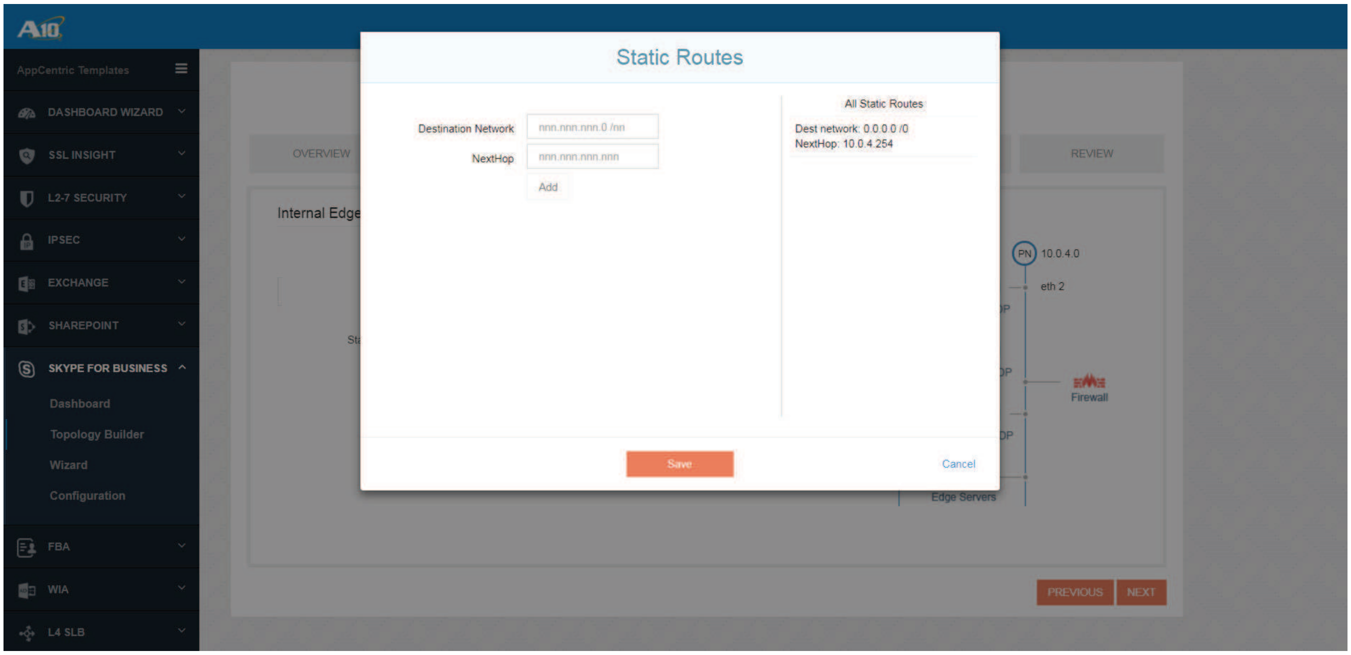
Static Routes: ☑ 1 static routes

Figure 7: Network interface configuration on Internal Edge ADC

VLAN: 401 with IP address 10.0.4.241 /24
The VLAN ID and corresponding virtual interface IP address.

Interface: The physical port that is connected to the network – Ethernet 2.

Static Routes: The routes to be configured on this ADC. Enable this option and define a default route (0.0.0.0 /0) with gateway address of 10.0.4.254:



Static Routes

Destination Network: nnn.nnn.nnn.0 /nn

NextHop: nnn.nnn.nnn.nnn

Add

All Static Routes

Dest network: 0.0.0.0 /0
NextHop: 10.0.4.254

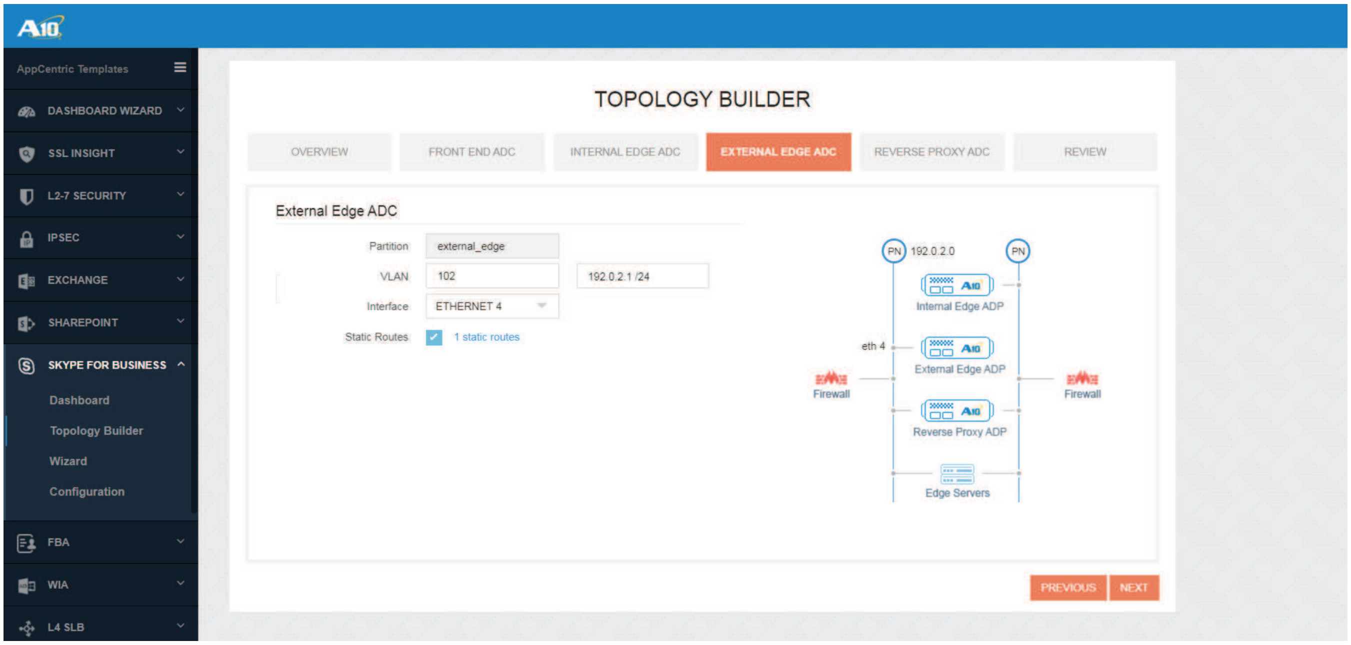
Save

Cancel

Figure 8: Route configuration on Internal Edge ADC

EXTERNAL EDGE ADC

The External Edge ADC load-balances traffic from external clients to the external edge interfaces of the Edge servers. It is connected to the external perimeter network 192.0.2.0/24.



External Edge ADC

Partition: external_edge

VLAN: 102 | 192.0.2.1 /24

Interface: ETHERNET 4

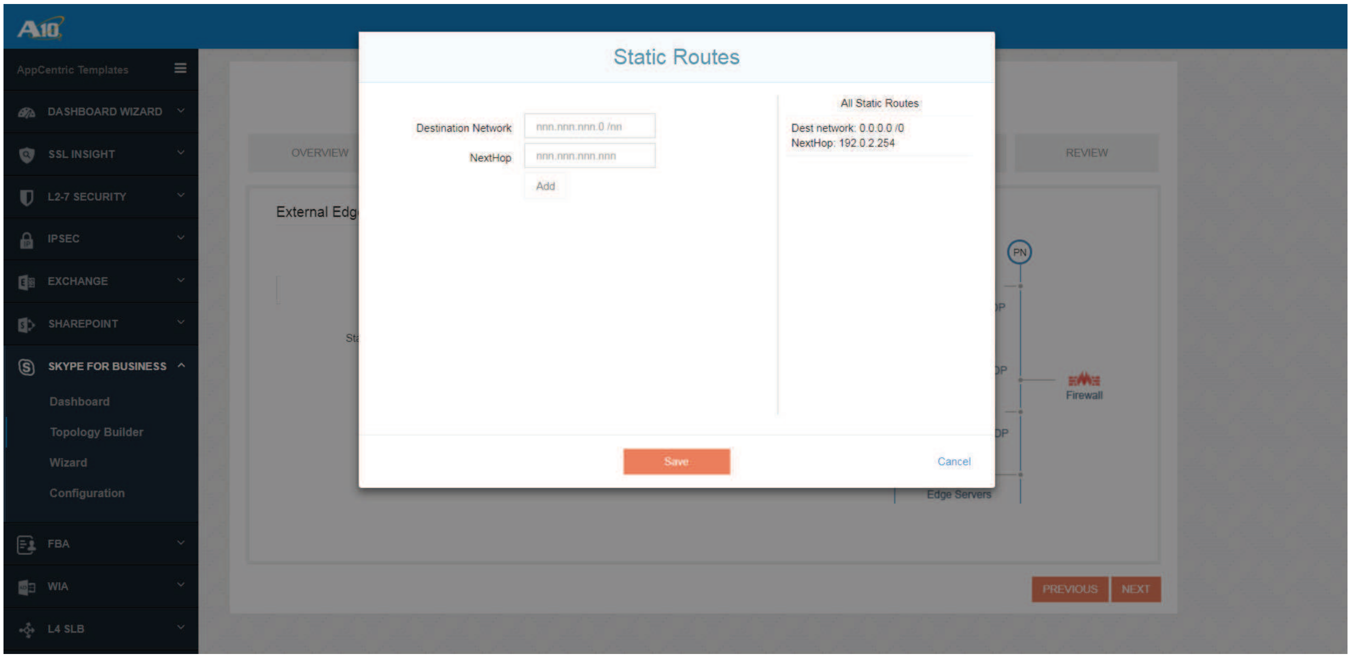
Static Routes: ☑ 1 static routes

Figure 9: Network interface configuration on External Edge ADC

VLAN: 102 with IP address 192.0.2.1 /24
The VLAN ID and corresponding virtual interface IP address.

Interface: The physical port that is connected to the network – Ethernet 4.

Static Routes: The routes to be configured on this ADC. Enable this option and define a default route (0.0.0.0 /0) with gateway address of 192.0.2.254:



Static Routes

Destination Network: nnn.nnn.nnn.0 /nn

NextHop: nnn.nnn.nnn.nnn

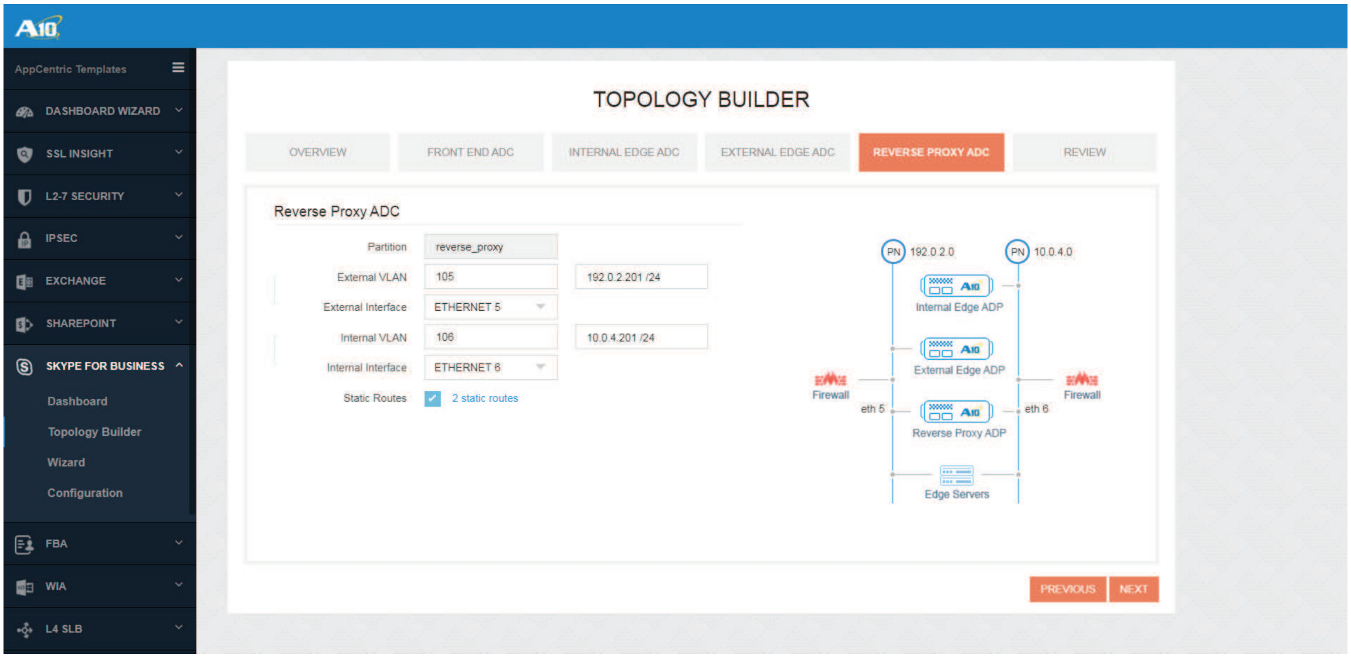
All Static Routes

Dest network: 0.0.0.0 /0
NextHop: 192.0.2.254

Figure 10: Route configuration on External Edge ADC

REVERSE PROXY ADC

The Reverse Proxy ADC is connected to two networks, the external perimeter network 192.0.2.0 /24 and the internal perimeter network 10.0.4.0 /24.



Reverse Proxy ADC

Partition	reverse_proxy	
External VLAN	105	192.0.2.201 /24
External Interface	ETHERNET 5	
Internal VLAN	106	10.0.4.201 /24
Internal Interface	ETHERNET 6	
Static Routes	☑ 2 static routes	

Figure 11: Network interface configuration on Reverse Proxy ADC

External VLAN: 105 with IP address 192.0.2.201 /24
The VLAN ID and corresponding virtual interface IP address.

External Interface: The physical port that is connected to the external perimeter network – Ethernet 5.

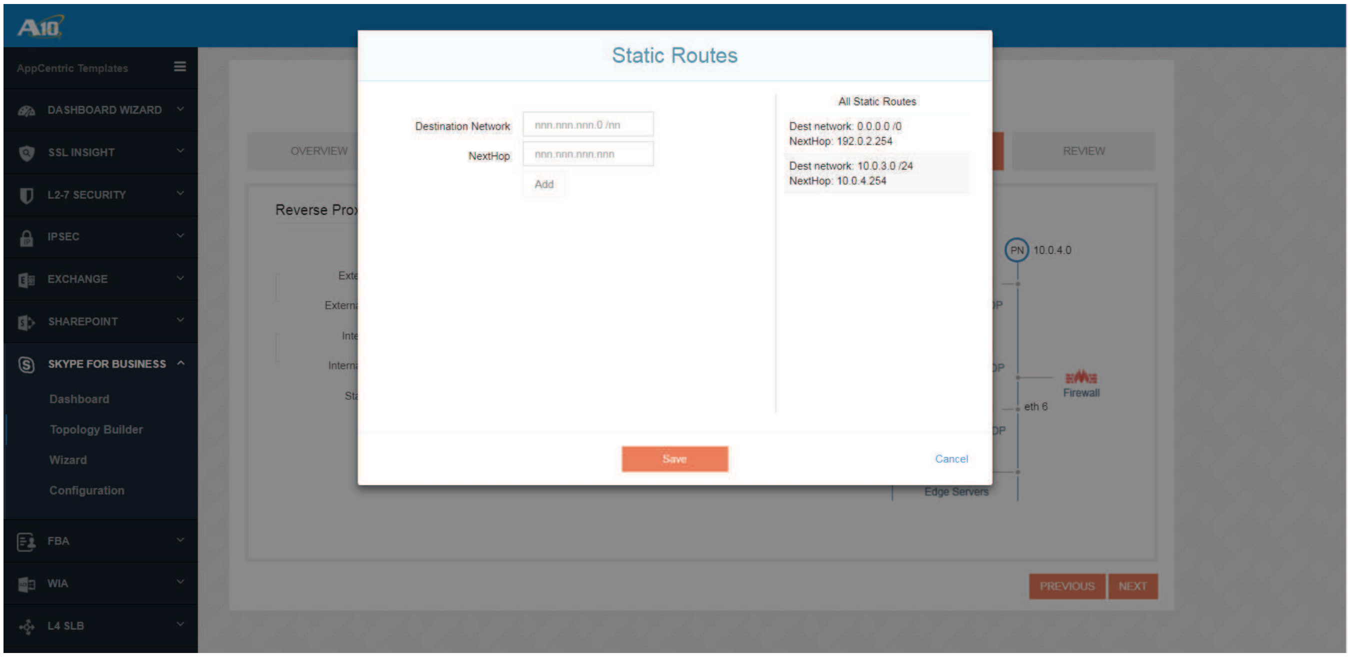
Internal VLAN: 106 with IP address 10.0.4.201 /24

The VLAN ID and corresponding virtual interface IP address.

Internal Interface: The physical port that is connected to the internal perimeter network – Ethernet 6.

Static Routes: The routes to be configured on this ADC. Enable this option and define the following static routes:

- Default route (0.0.0.0 /0) with next hop IP address 192.0.2.254
- Destination network 10.0.3.0 /24 with next hop IP address 10.0.4.254



Static Routes

Destination Network: nnn.nnn.nnn.0 /nn

NextHop: nnn.nnn.nnn.nnn

All Static Routes

Dest network: 0.0.0.0 /0
NextHop: 192.0.2.254

Dest network: 10.0.3.0 /24
NextHop: 10.0.4.254

Figure 12: Route configuration on Reverse Proxy ADC

REVIEW

This section gives you an overview of the network topology.

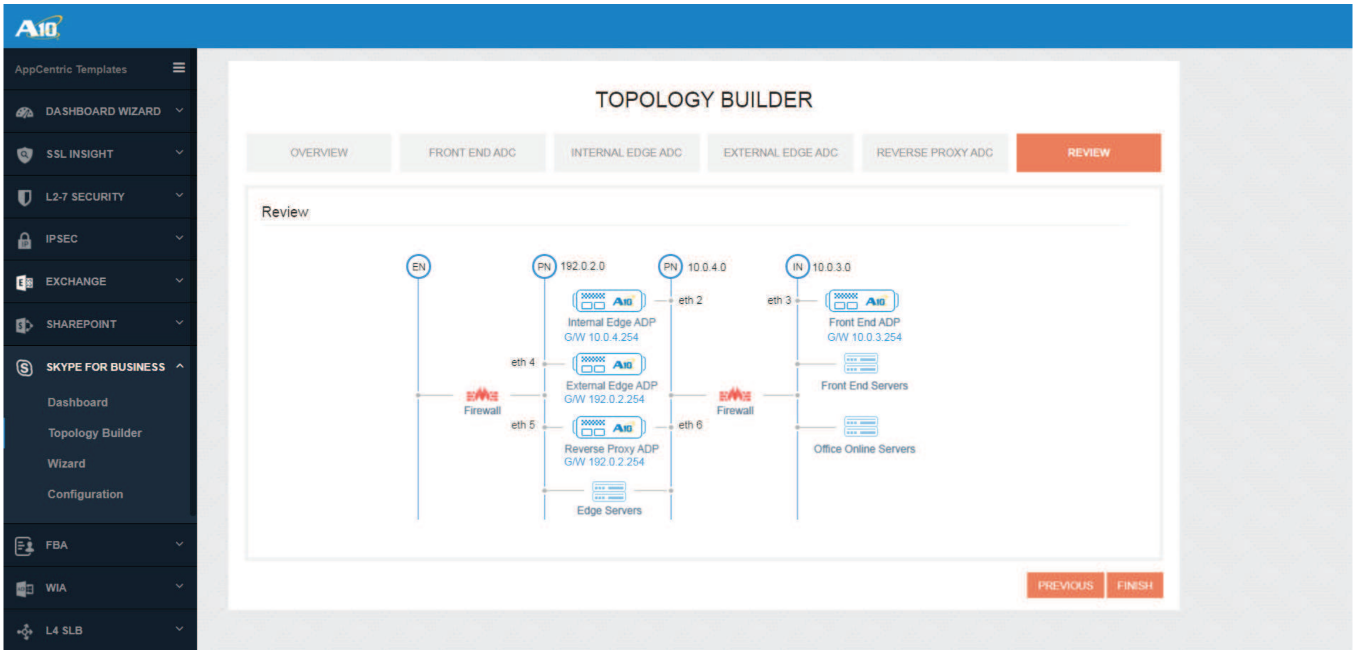
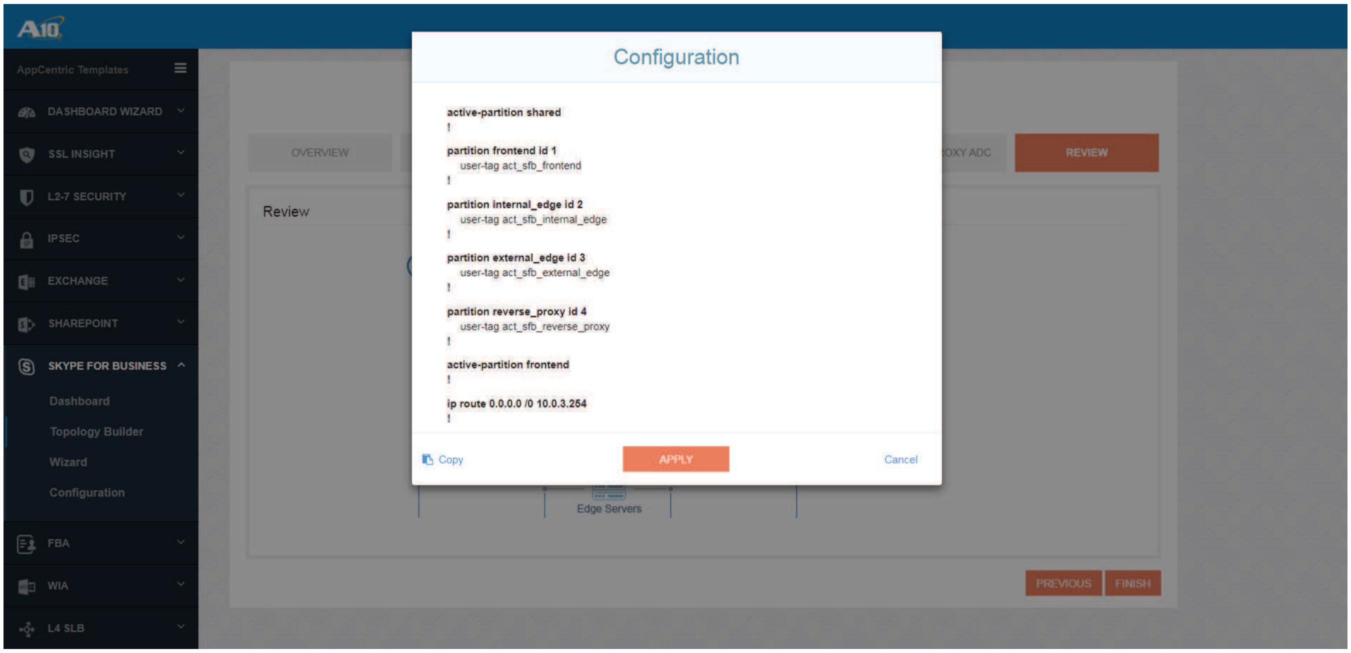


Figure 13: Configuration overview

If fine, click Finish and you will be able to see the equivalent CLI configuration that will be pushed to the Thunder ADC:



```
active-partition shared
!
partition frontend id 1
   user-tag act_sfb_frontend
!
partition internal_edge id 2
   user-tag act_sfb_internal_edge
!
partition external_edge id 3
   user-tag act_sfb_external_edge
!
partition reverse_proxy id 4
   user-tag act_sfb_reverse_proxy
!
active-partition frontend
!
ip route 0.0.0.0 /0 10.0.3.254
!
```

Figure 14: CLI configuration generated by ACT

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

WIZARD

Once you have finished defining the four ADPs on the Thunder ADC with the corresponding network configuration, launch the Skype Wizard to create load balancing virtual services and policies for Skype for Business.

To access Wizard, in the left-pane, go to Skype for Business > Wizard

You will see the two deployment options:

- Multiple ADPs on a single A10 ACOS device
- Single A10 ACOS device per role

In this setup, we used the option of multiple ADPs on a single device, hence choose that option and click Next.

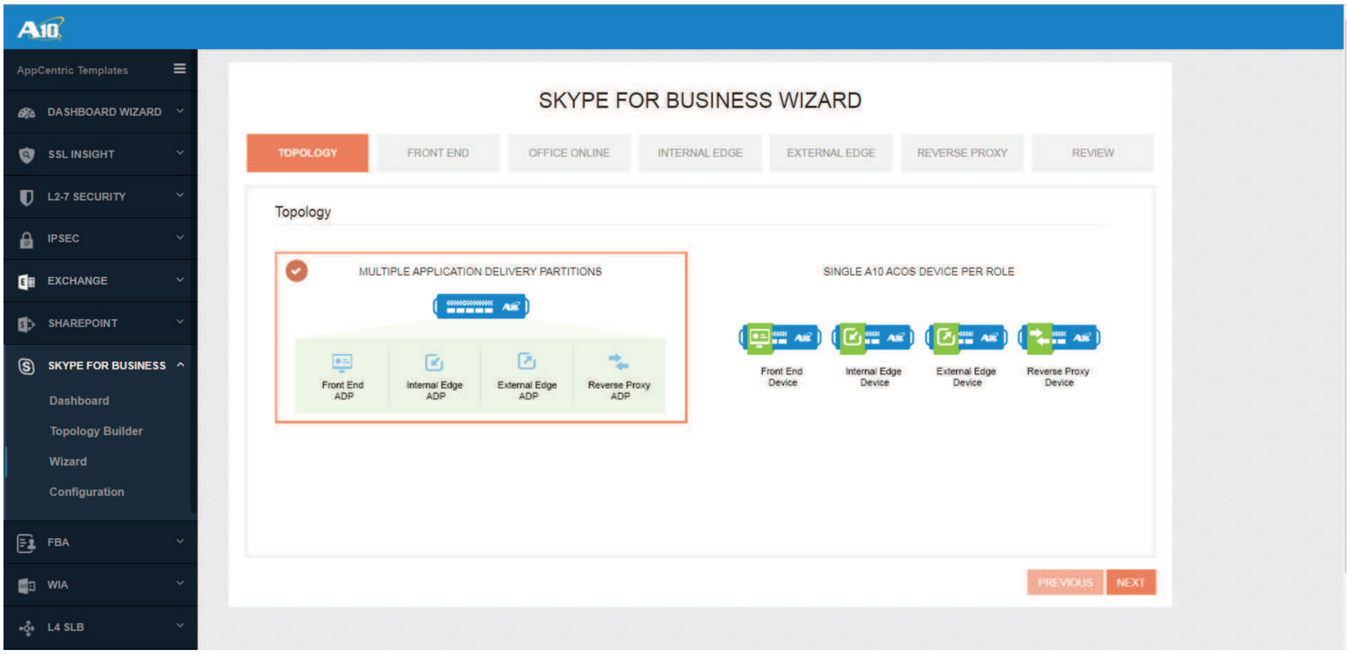


Figure 15: Skype for Business Wizard - Deployment options

WIZARD – FRONT END

The Skype Front End Server pool is a core component and composed of one or more Skype Front End Servers. IM/Presence, every Conference service, collaboration and voice are some of the services provided by the Front End pool. If there are multiple Front End Servers in a pool and one of them is under service outage mode, the rest of the healthy Front End Servers continue to provide all services to the end user.

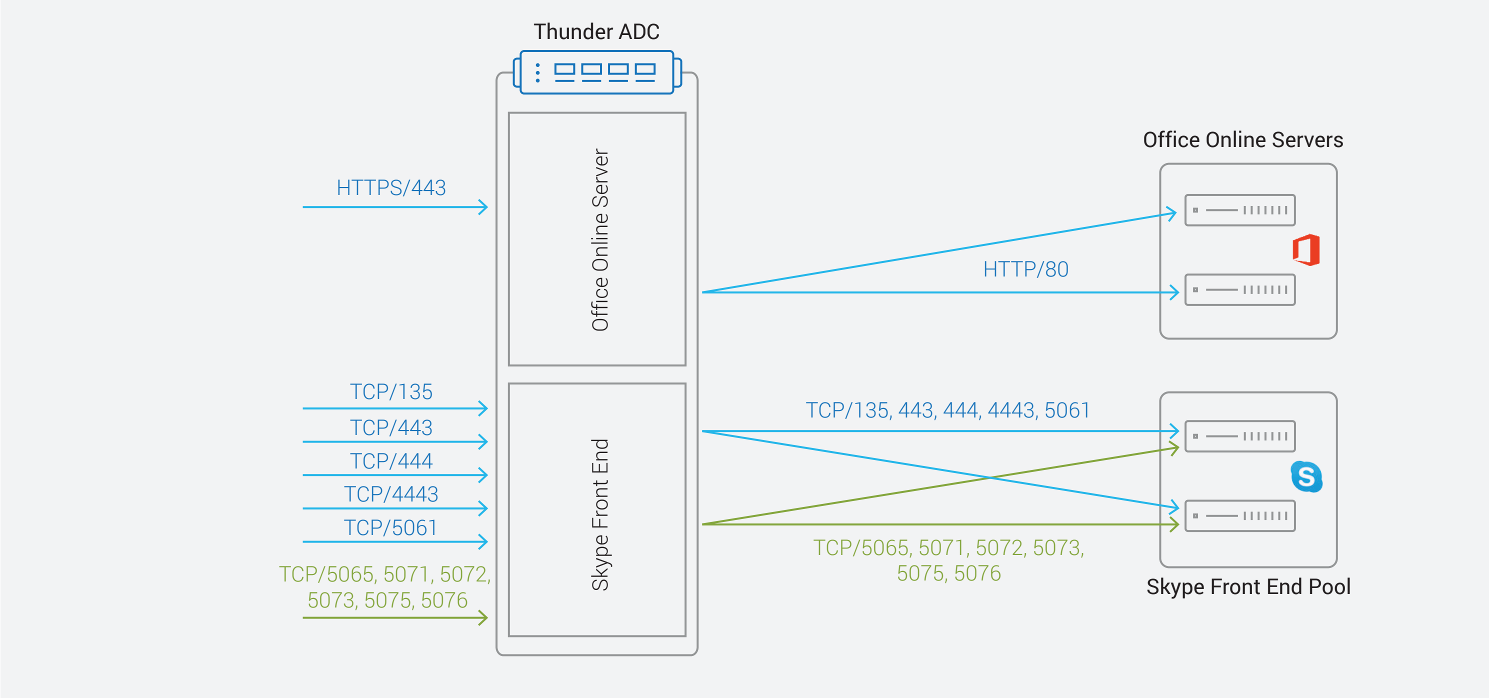
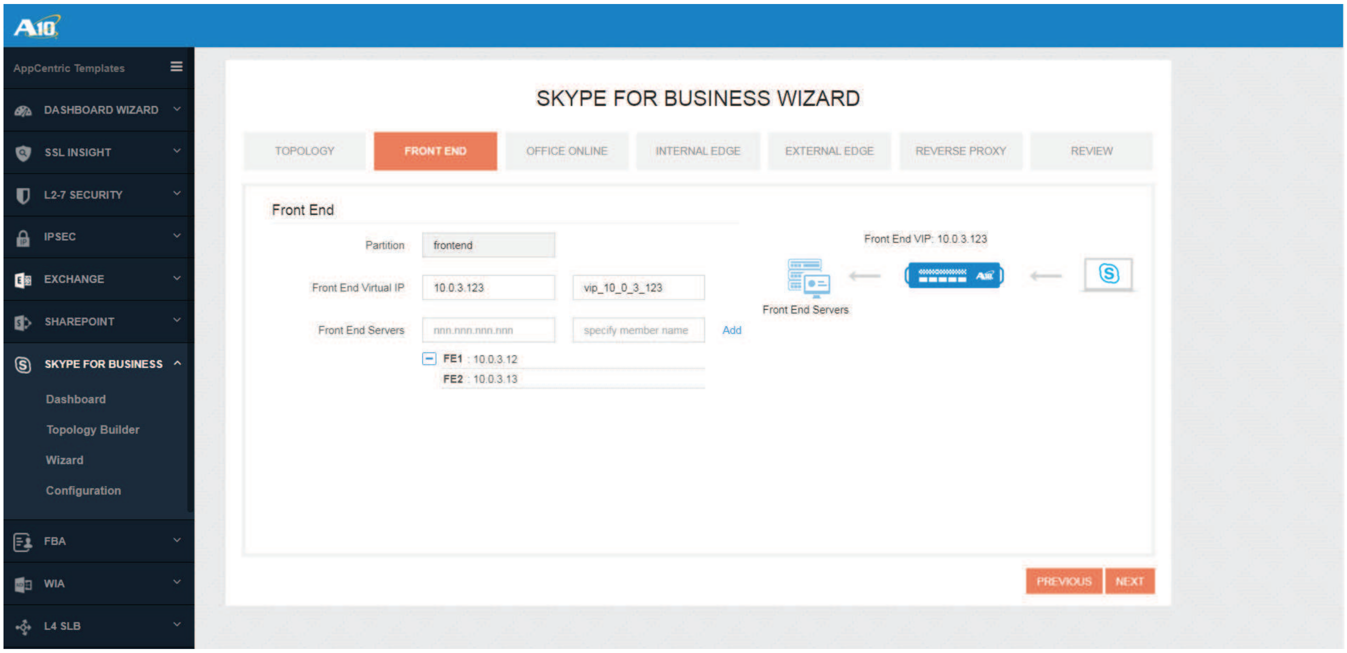


Figure 16: Load balancing diagram for Front End pool and Office Online Servers

In this section, we configure a redundant Skype Server Front End Enterprise pool (services) on the Thunder ADC. Wizard automatically configures all required virtual services to load balance the Front End Enterprise pool.



Front End

Partition: frontend

Front End Virtual IP: 10.0.3.123 vip_10_0_3_123

Front End Servers: nnn.nnn.nnn.nnn specify member name Add

FE1 : 10.0.3.12

FE2 : 10.0.3.13

Figure 17: Front End ADP configuration for Skype Front End servers

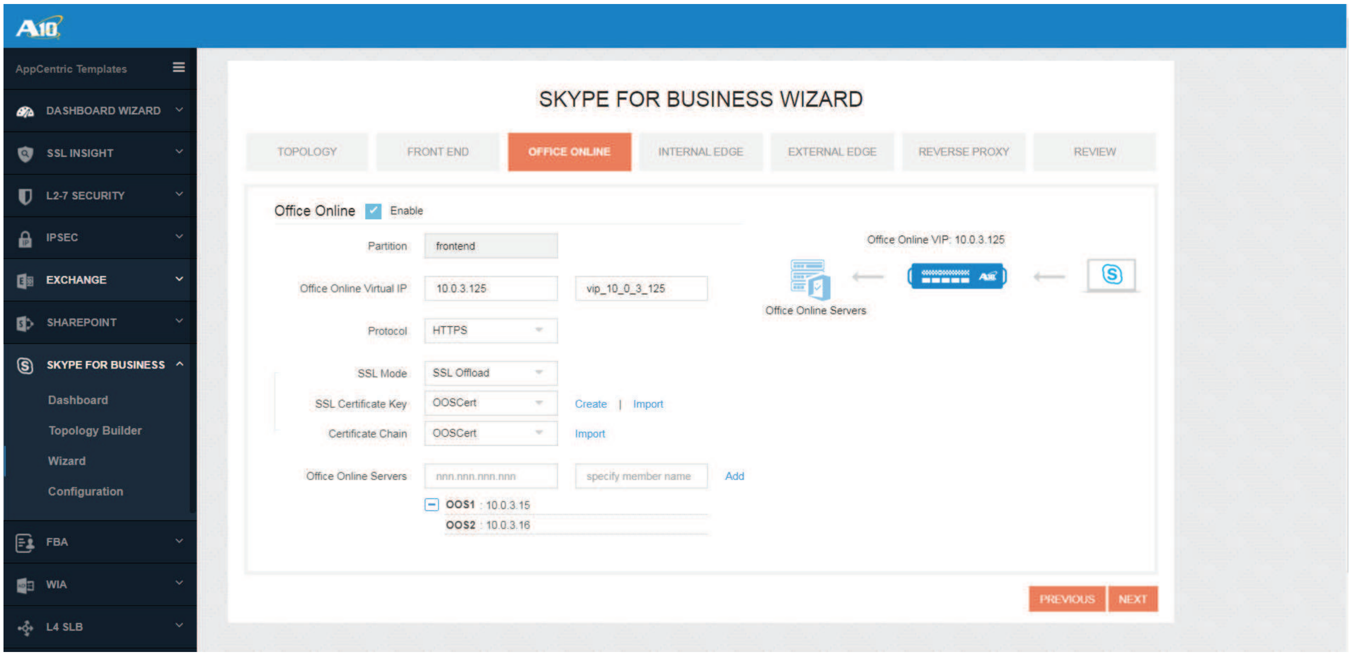
- Front End Virtual IP: 10.0.3.123
- Front End Servers:
  - FE1: 10.0.3.12
  - FE2: 10.0.3.13

WIZARD - OFFICE ONLINE SERVER FARM

Office Online Server (OOS) is the successor to Office Web Apps Server 2013. With Skype for Business Server 2015, OOS enables high fidelity viewing of PowerPoint Online when sharing PowerPoint presentations during meetings.

This section is optional and describes how to configure load balancing for an OOS server farm on Thunder ADC along with SSL Offload. SSL offload configuration is recommended for Office Online Server according to the Microsoft Tech Net site[3].

[3] https://technet.microsoft.com/en-us/library/jj219435(v=office.16).aspx#loadbalancer



SKYPE FOR BUSINESS WIZARD

Office Online ☑ Enable

Partition: frontend

Office Online Virtual IP: 10.0.3.125 vip_10_0_3_125

Protocol: HTTPS

SSL Mode: SSL Offload

SSL Certificate Key: OOSCert

Certificate Chain: OOSCert

Office Online Servers: nnn.nnn.nnn.nnn specify member name

OOS1 : 10.0.3.15

OOS2 : 10.0.3.16

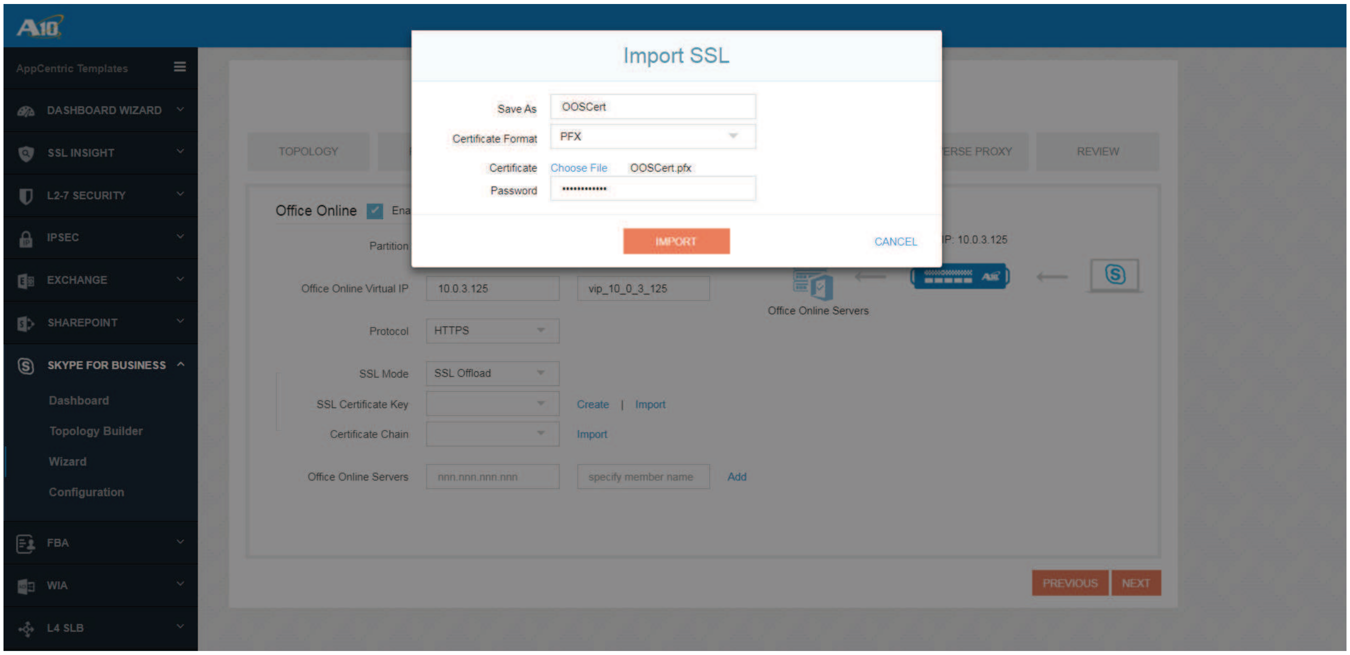
Figure 18: Front End ADP configuration for Skype Office Online Servers

- Office Online Virtual IP : 10.0.3.125
- Office Online Servers:
  - OOS1: 10.0.3.15
  - OOS2: 10.0.3.16

CREATE OR IMPORT SSL CERTIFICATE

Create or import SSL server certificate to perform SSL Offload on Thunder ADC. In this test environment, the following data is being used:

- Save As: OOSCert
- Certificate Format: PFX (choose proper certificate file format)
- Certificate File: OOSCert.pfx (located on local computer)
- Password: Password used to protect the pfx file



Import SSL

Save As: OOSCert

Certificate Format: PFX

Certificate: Choose File OOSCert.pfx

Password: ••••••••••••

IMPORT CANCEL

Office Online ☑ Ena

Partition

Office Online Virtual IP: 10.0.3.125 vip_10_0_3_125

Protocol: HTTPS

SSL Mode: SSL Offload

SSL Certificate Key: Create | Import

Certificate Chain: Import

Office Online Servers: nnn.nnn.nnn.nnn specify member name Add

Figure 19: Import SSL server certificate into Front End ADP

ACT will additionally configure the following for the front-end and office online services:

- Load-balancing using least-connection method
- TCP template with idle-timeout of 1800 seconds
- Source-IP and cookie persistence templates
- Per-port health check monitors
- Cipher template consisting of the following ciphers:
  - 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
  - TLS1_ECDHE_RSA_AES_256_SHA
  - TLS1_ECDHE_RSA_AES_128_SHA256
  - TLS1_ECDHE_RSA_AES_128_GCM_SHA256

WIZARD - INTERNAL EDGE

The internal Edge pool handles traffic from internal Skype server components or from Skype clients to remote Skype clients. An internal Edge pool doesn’t have multiple roles, unlike an external Edge pool (Access, Web Conf, A/V).

Note that the internal Edge interface and external Edge interface must use the same type of load balancing. You cannot use DNS load balancing on one interface and hardware load balancing on the other.

Wizard automatically configures all required virtual services to load balance the internal edge pool.

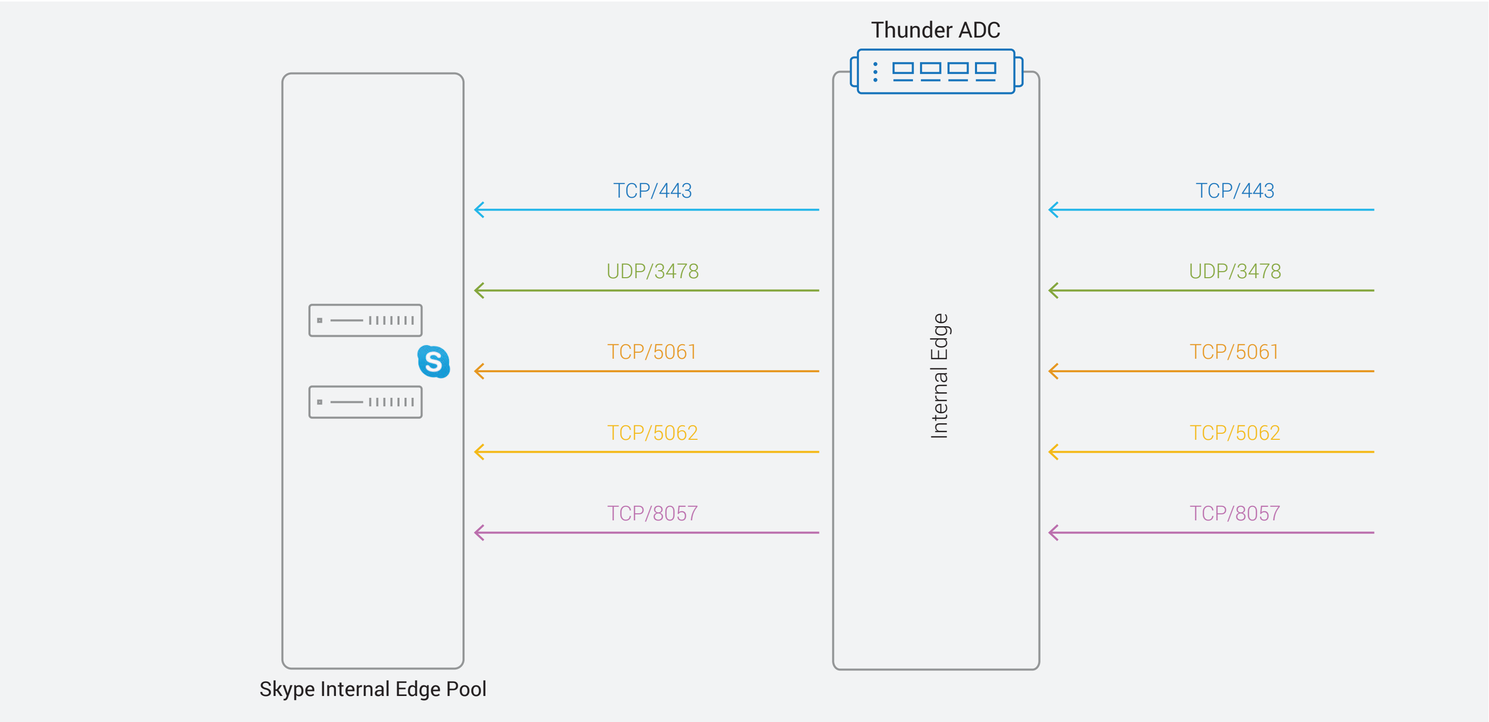
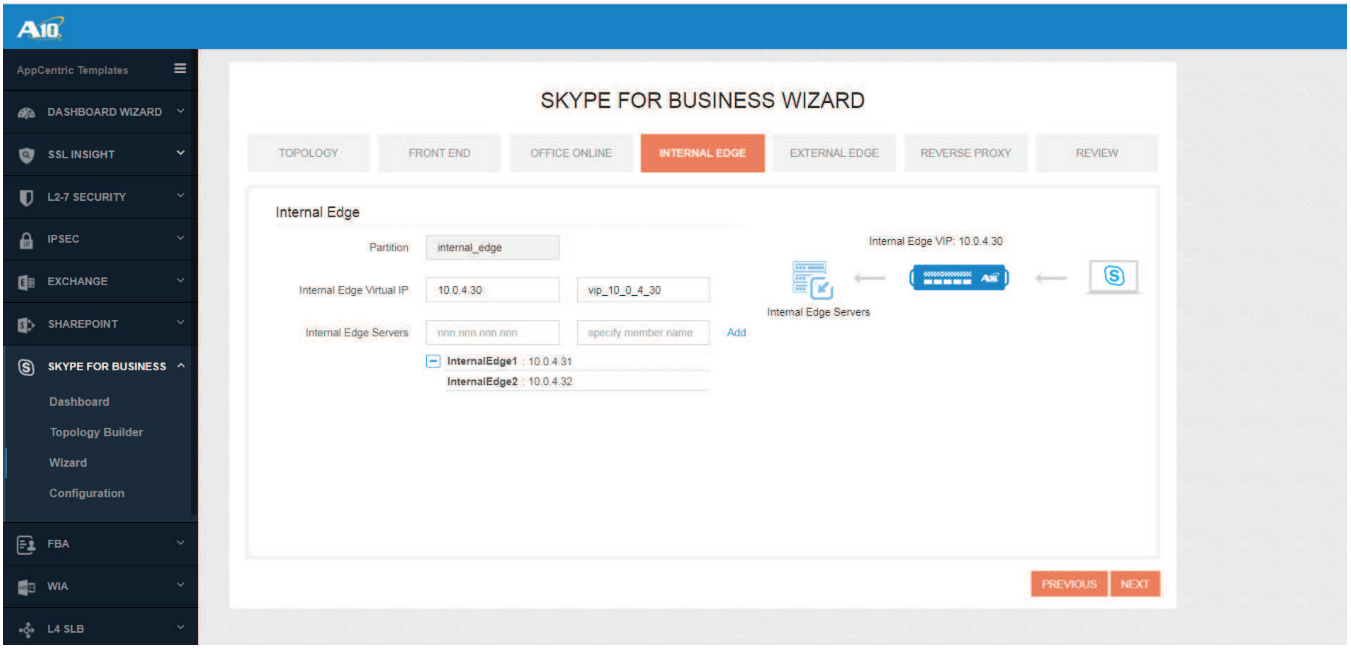


Figure 20: Load balancing diagram for internal Skype Edge pool



SKYPE FOR BUSINESS WIZARD

Internal Edge

Partition: internal_edge

Internal Edge Virtual IP: 10.0.4.30 | vip_10_0_4_30

Internal Edge Servers: nnn.nnn.nnn.nnn | specify member name

InternalEdge1 : 10.0.4.31

InternalEdge2 : 10.0.4.32

Figure 21: Internal Edge ADP configuration

- Internal Edge Virtual IP : 10.0.4.30
- Internal Edge Servers:
    - InternalEdge1: 10.0.4.31
    - InternalEdge2: 10.0.4.32

ACT will additionally configure the following:

- Load-balancing using least-connection method
- TCP template with idle-timeout of 1800 seconds
- Source-IP persistence template
- Per-port health check monitors

WIZARD - EXTERNAL EDGE

Skype Edge Server allows remote users to access internal Front End Server resources through the enterprise firewall and the DMZ/perimeter network. Remote users can use full Skype functionalities, including IM/Presence, Conference, Collaboration and Enterprise Voice without a VPN connection if the Skype Edge pool is deployed.

The Skype Edge pool can be deployed with either a single Edge Server or multiple Edge Servers. For redundancy purposes, load balancing is required in order to deploy multiple Edge Servers.

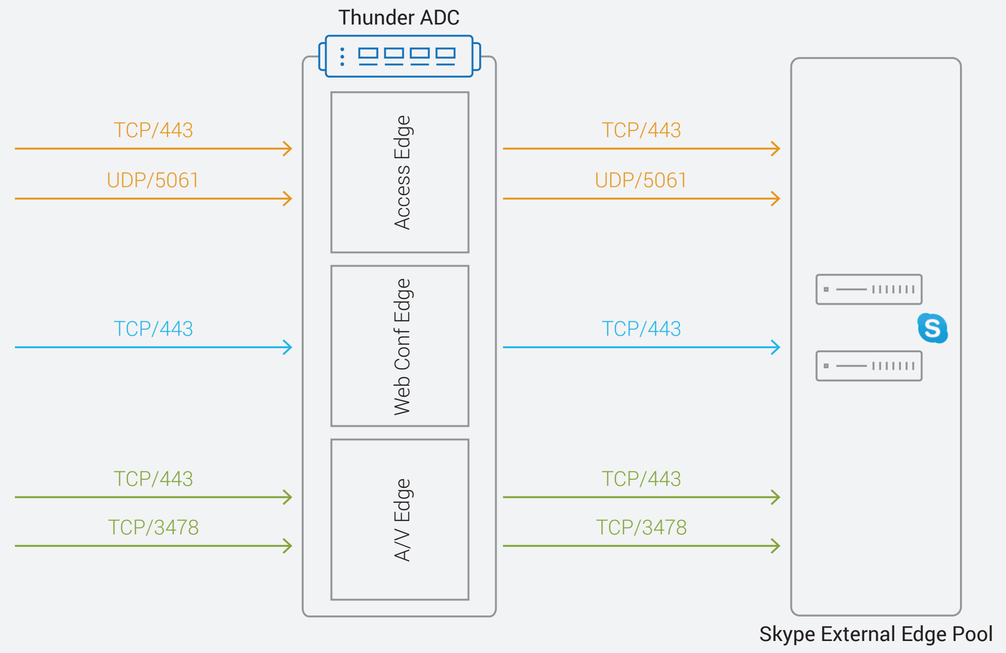
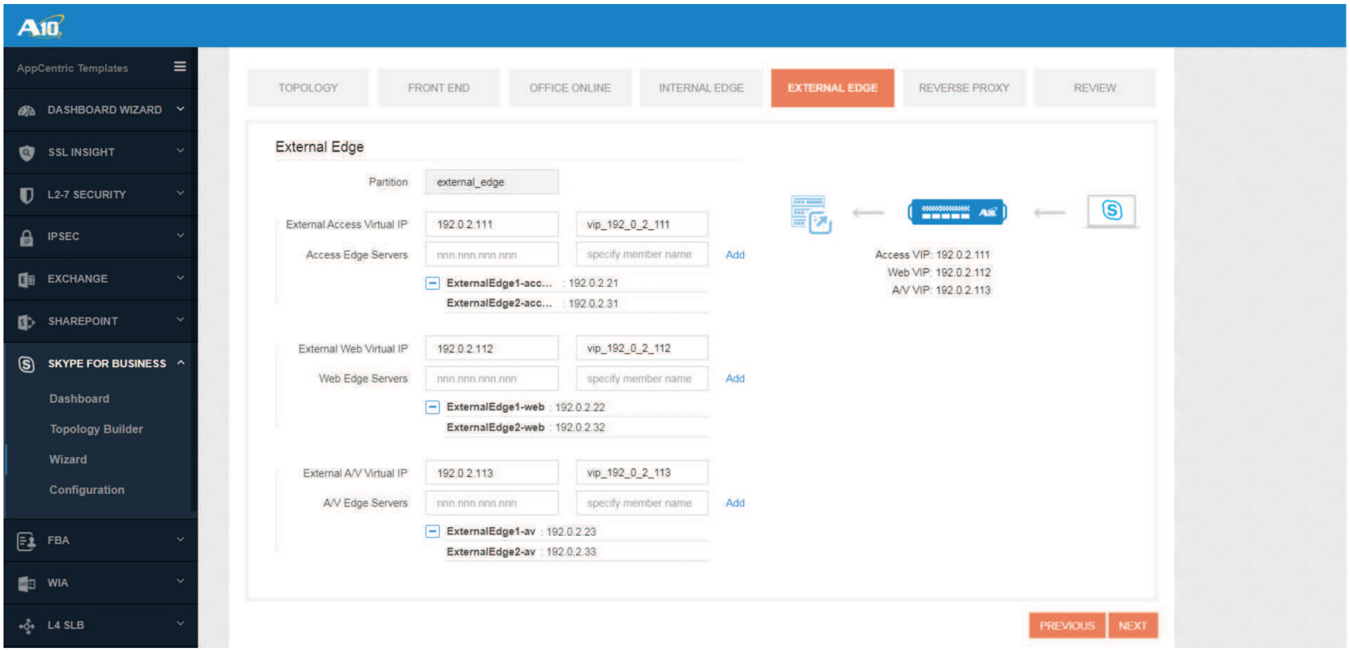


Figure 22: Load balancing diagram for external Edge pool

In figure 2, we had deselected the **use a single FQDN and IP address** option for the external Edge pool and hence over here we configure the External Edge ADC with three unique virtual IP addresses (VIPs) for Access, WebConf and A/V.

Wizard automatically configures all required virtual services to load balance the external edge pool.



External Edge

Partition: external_edge

External Access Virtual IP: 192.0.2.111 | vip_192_0_2_111

Access Edge Servers: nnn.nnn.nnn.nnn | specify member name

- ExternalEdge1-acc... : 192.0.2.21
- ExternalEdge2-acc... : 192.0.2.31

External Web Virtual IP: 192.0.2.112 | vip_192_0_2_112

Web Edge Servers: nnn.nnn.nnn.nnn | specify member name

- ExternalEdge1-web : 192.0.2.22
- ExternalEdge2-web : 192.0.2.32

External A/V Virtual IP: 192.0.2.113 | vip_192_0_2_113

A/V Edge Servers: nnn.nnn.nnn.nnn | specify member name

- ExternalEdge1-av : 192.0.2.23
- ExternalEdge2-av : 192.0.2.33

Access VIP: 192.0.2.111
Web VIP: 192.0.2.112
A/V VIP: 192.0.2.113

Figure 23: External Edge ADP configuration

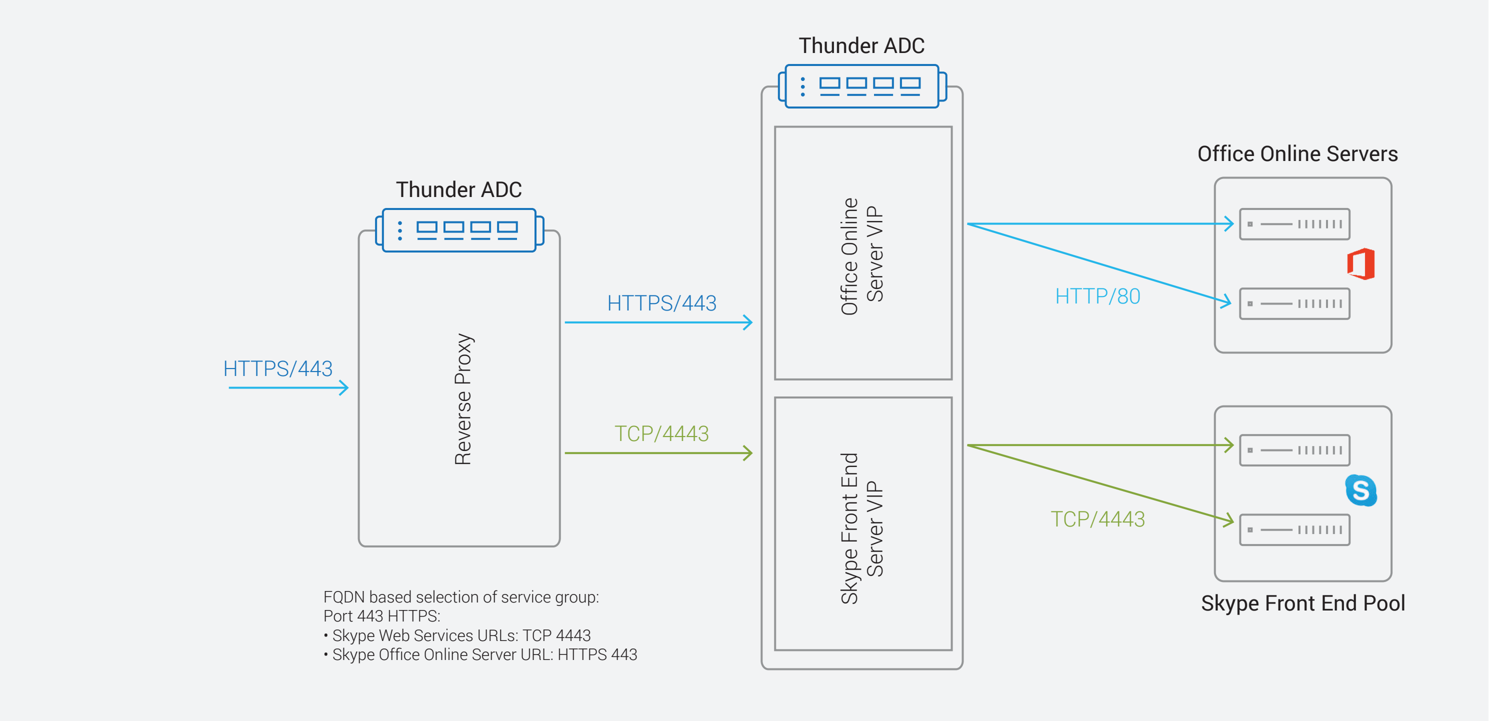
- External Edge Virtual IP :
  - Access: 192.0.2.111
  - Web Conference: 192.0.2.112
  - A/V: 192.0.2.113
- External Edge Servers:
  - Access
    - ExternalEdge1-access: 192.0.2.21
    - ExternalEdge2-access: 192.0.2.31
  - Web Conference:
    - ExternalEdge1-web: 192.0.2.22
    - ExternalEdge2-web: 192.0.2.32
  - A/V
    - ExternalEdge1-av: 192.0.2.23
    - ExternalEdge2-av: 192.0.2.33

ACT will additionally configure the following:

- Load-balancing using least-connection method
- TCP template with idle-timeout of 1800 seconds
- Source-IP persistence template
- Per-port health check monitors

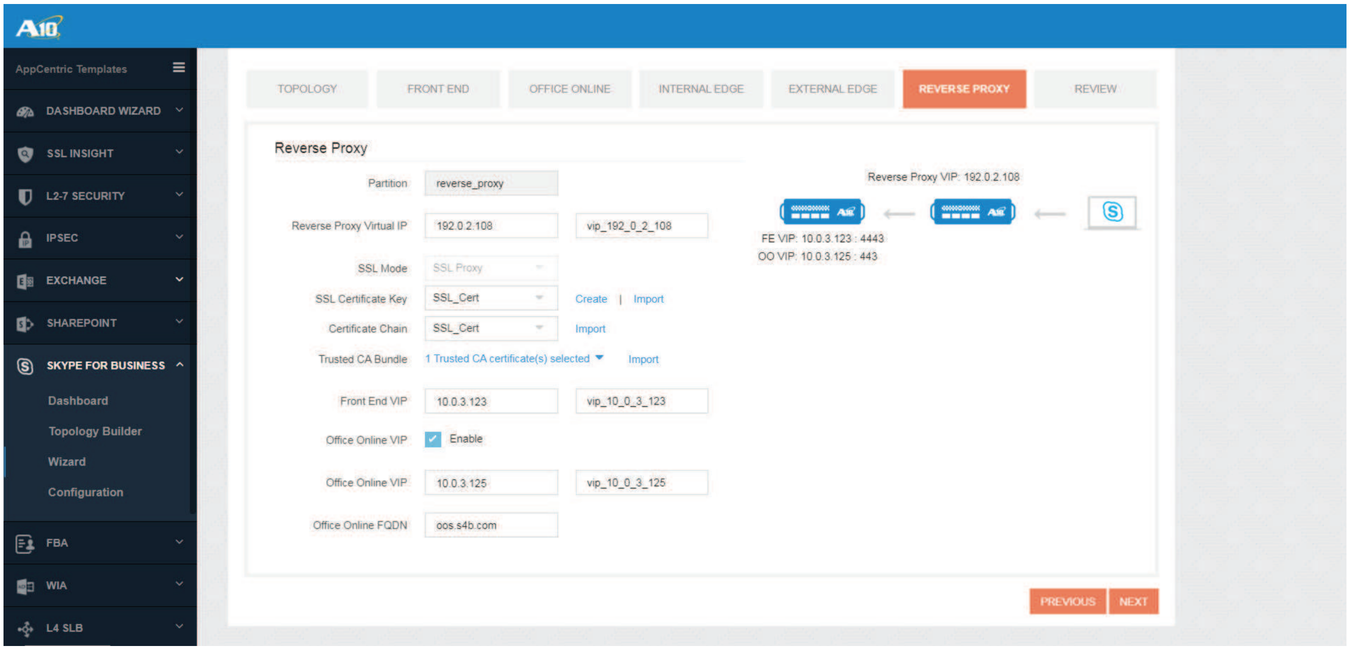
WIZARD - REVERSE PROXY

Reverse Proxy is used for publishing Web Services of Skype Front End Server and Office Online Servers to remote access users through the Internet.



FQDN based selection of service group:
Port 443 HTTPS:
- Skype Web Services URLs: TCP 4443
- Skype Office Online Server URL: HTTPS 443

Figure 24: Load-balancing diagram for Reverse Proxy



Reverse Proxy

Partition	reverse_proxy	
Reverse Proxy Virtual IP	192.0.2.108	vip_192_0_2_108
SSL Mode	SSL Proxy	
SSL Certificate Key	SSL_Cert	
Certificate Chain	SSL_Cert	
Trusted CA Bundle	1 Trusted CA certificate(s) selected	
Front End VIP	10.0.3.123	vip_10_0_3_123
Office Online VIP	☑ Enable	
Office Online VIP	10.0.3.125	vip_10_0_3_125
Office Online FQDN	oos.s4b.com	

Reverse Proxy VIP: 192.0.2.108
FE VIP: 10.0.3.123 : 4443
OO VIP: 10.0.3.125 : 443

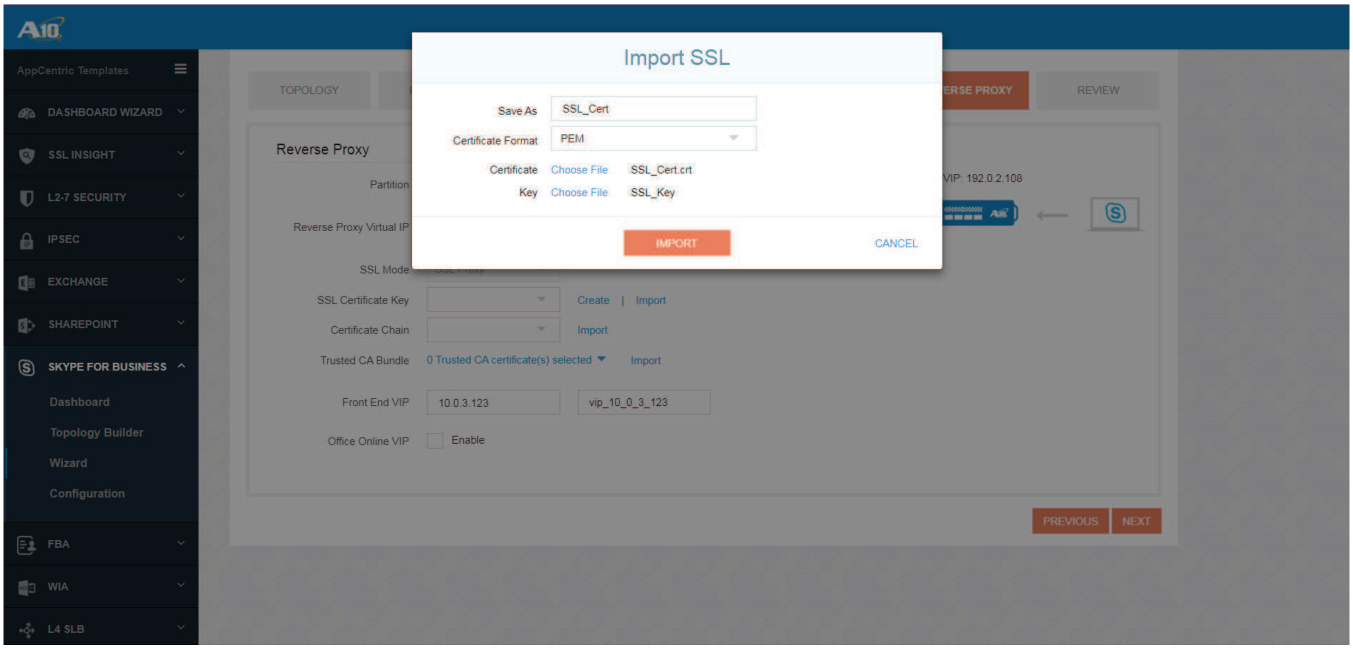
Figure 25: Reverse Proxy ADP configuration

- Reverse Proxy Virtual IP: 192.0.2.108
- Front End VIP: 10.0.3.123
- Office Online VIP: 10.0.3.125
- Office Online FQDN: oos.s4b.com

CREATE OR IMPORT CERTIFICATES

Import the SSL server certificate used for access by remote users. Usually it is issued by a public CA. In this test environment, the following data is being used:

- Save As: SSL_Cert
  - Certificate Format: PEM
  - Server Certificate File: SSL_Cert.crt (on local computer)
  - Server Private Key File: SSL_Key (on local computer)



Import SSL

Save As: SSL_Cert
Certificate Format: PEM
Certificate: Choose File SSL_Cert.crt
Key: Choose File SSL_Key

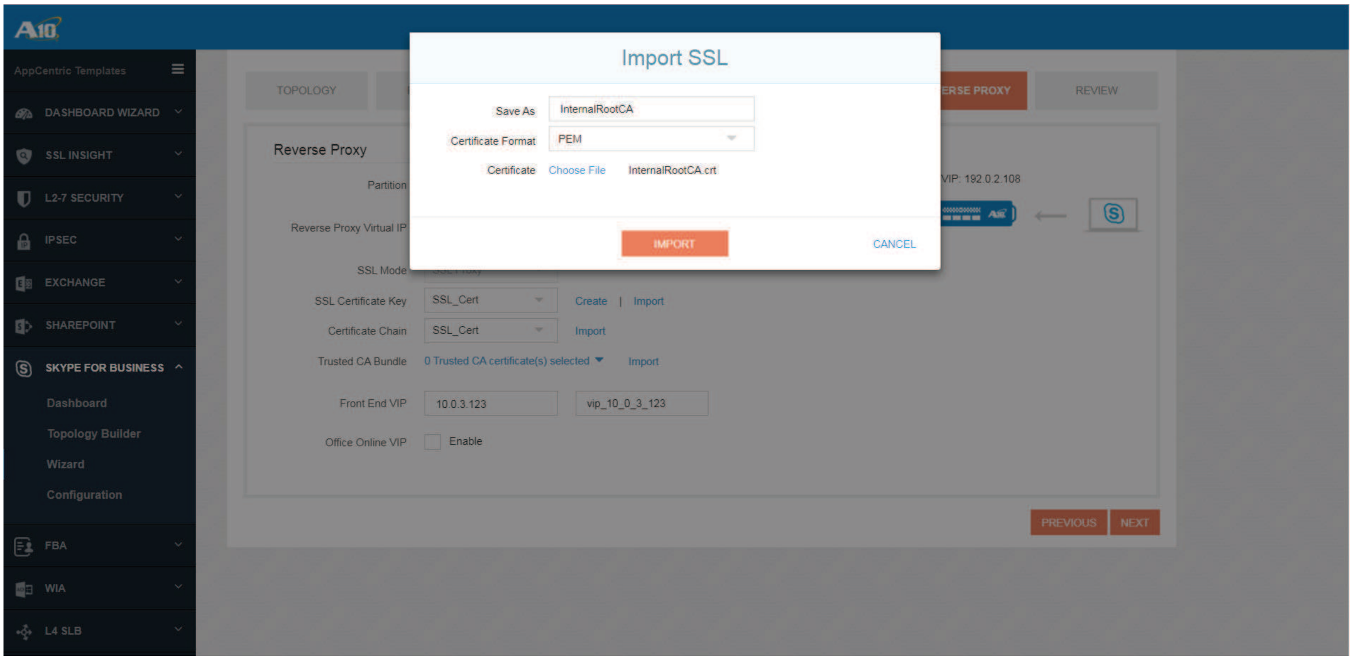
IMPORT   CANCEL

Reverse Proxy
Partition
Reverse Proxy Virtual IP
SSL Mode
SSL Certificate Key: Create | Import
Certificate Chain: Import
Trusted CA Bundle: 0 Trusted CA certificate(s) selected Import
Front End VIP: 10.0.3.123   vip_10_0_3_123
Office Online VIP: □ Enable

Figure 26: Import SSL server certificate on Reverse Proxy ADP

The Reverse Proxy uses TLS to communicate with the Front End ADC and thus you need to also import the root certificate of the CA, which issues the internal SSL server certificate for Skype Front End Pool and OOS. Usually, the internal enterprise CA is used for issuing internal SSL server certificates.

- Save As: InternalRootCA
- Certificate Format: PEM
- Certificate File: InternalRootCA.crt (on local computer)



Import SSL

Save As: InternalRootCA

Certificate Format: PEM

Certificate: Choose File InternalRootCA.crt

IMPORT CANCEL

Reverse Proxy

Partition

Reverse Proxy Virtual IP

SSL Mode

SSL Certificate Key: SSL_Cert Create | Import

Certificate Chain: SSL_Cert Import

Trusted CA Bundle: 0 Trusted CA certificate(s) selected Import

Front End VIP: 10.0.3.123 vip_10_0_3_123

Office Online VIP: □ Enable

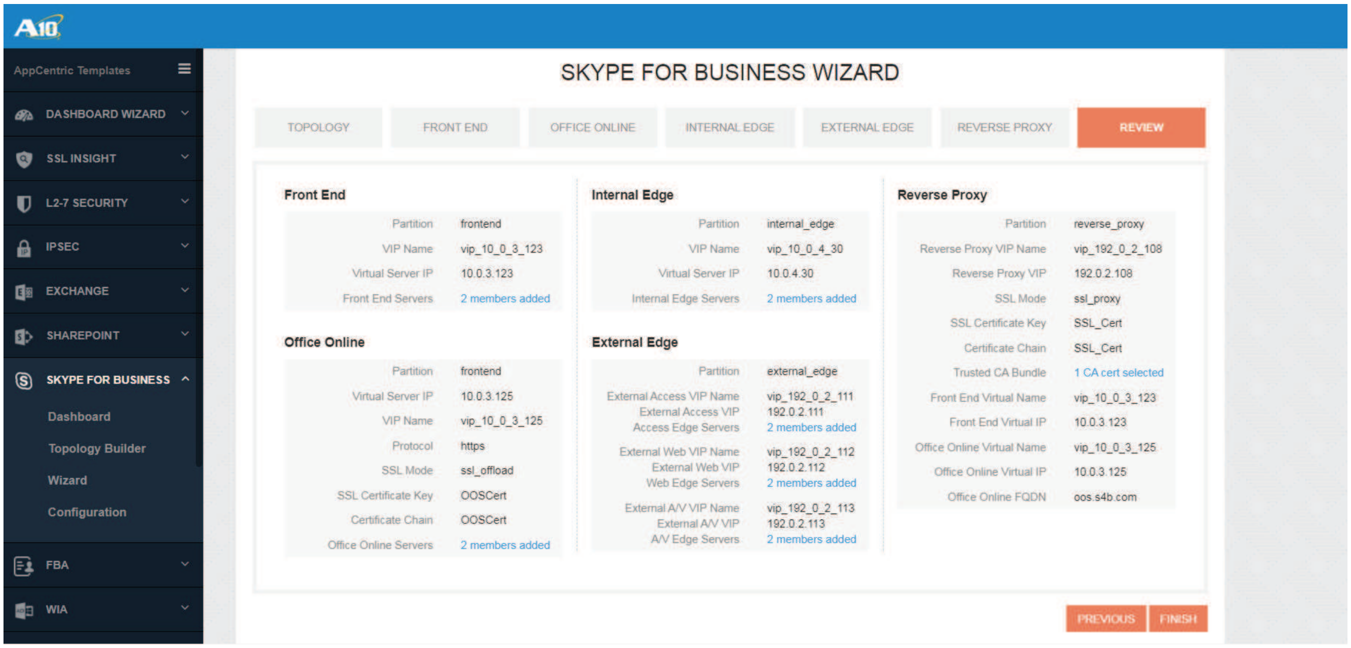
Figure 27: Import CA certificate on Reverse Proxy ADP

ACT will additionally configure the following:

- Per-port health check monitors
- Cipher template consisting of the following ciphers:
  - 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
  - TLS1_ECDHE_RSA_AES_256_SHA
  - TLS1_ECDHE_RSA_AES_128_SHA256
  - TLS1_ECDHE_RSA_AES_128_GCM_SHA256
- URL/host switching to switch traffic to either the Office Online VIP or to Front End VIP on the Front End ADC based on the URL. Traffic with FQDN of oos.s4b.com will be directed towards Office Online VIP (port 443) while other traffic will be sent to the Front End VIP (port 4443).

WIZARD - REVIEW

This section gives an overview of the configurations settings made using ACT:



Front End

Partition	frontend
VIP Name	vip_10_0_3_123
Virtual Server IP	10.0.3.123
Front End Servers	2 members added

Office Online

Partition	frontend
Virtual Server IP	10.0.3.125
VIP Name	vip_10_0_3_125
Protocol	https
SSL Mode	ssl_offload
SSL Certificate Key	OOSCert
Certificate Chain	OOSCert
Office Online Servers	2 members added

Internal Edge

Partition	internal_edge
VIP Name	vip_10_0_4_30
Virtual Server IP	10.0.4.30
Internal Edge Servers	2 members added

External Edge

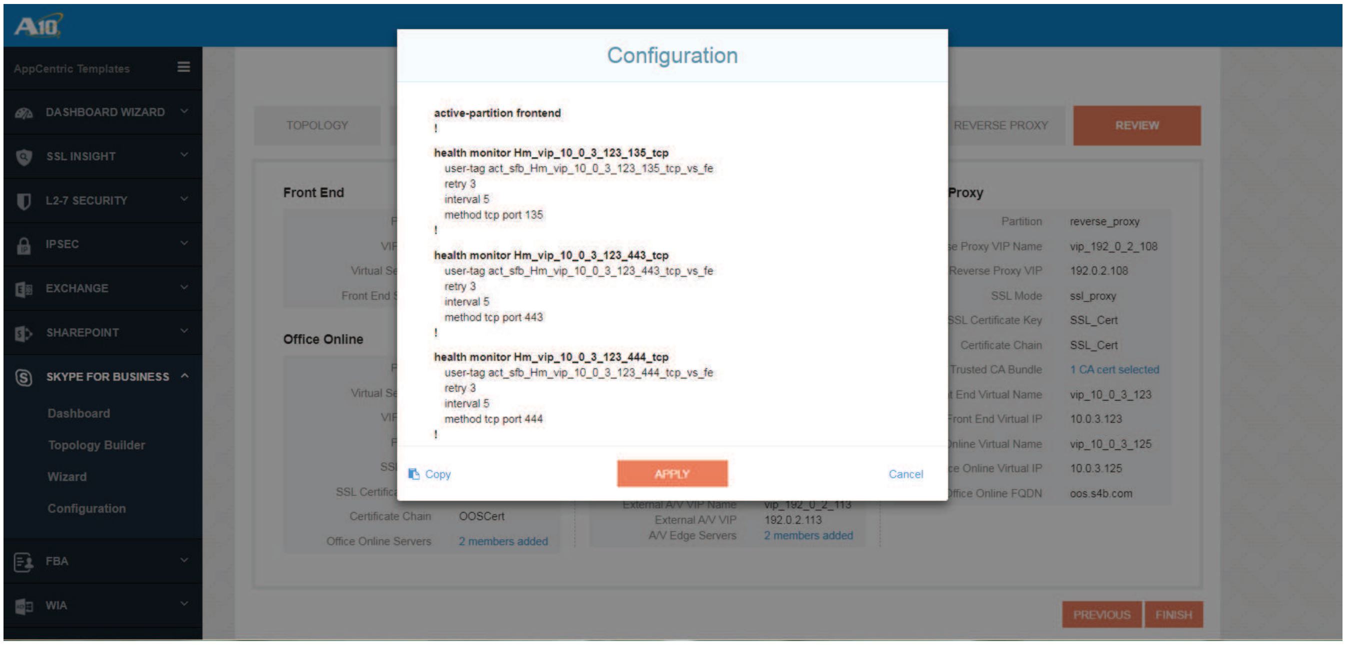
Partition	external_edge
External Access VIP Name	vip_192_0_2_111
External Access VIP	192.0.2.111
Access Edge Servers	2 members added
External Web VIP Name	vip_192_0_2_112
External Web VIP	192.0.2.112
Web Edge Servers	2 members added
External A/V VIP Name	vip_192_0_2_113
External A/V VIP	192.0.2.113
A/V Edge Servers	2 members added

Reverse Proxy

Partition	reverse_proxy
Reverse Proxy VIP Name	vip_192_0_2_108
Reverse Proxy VIP	192.0.2.108
SSL Mode	ssl_proxy
SSL Certificate Key	SSL_Cert
Certificate Chain	SSL_Cert
Trusted CA Bundle	1 CA cert selected
Front End Virtual Name	vip_10_0_3_123
Front End Virtual IP	10.0.3.123
Office Online Virtual Name	vip_10_0_3_125
Office Online Virtual IP	10.0.3.125
Office Online FQDN	oos.s4b.com

Figure 28: Configuration overview

If fine, click Finish and you will be able to see the equivalent CLI configuration that will be pushed to the Thunder ADC:



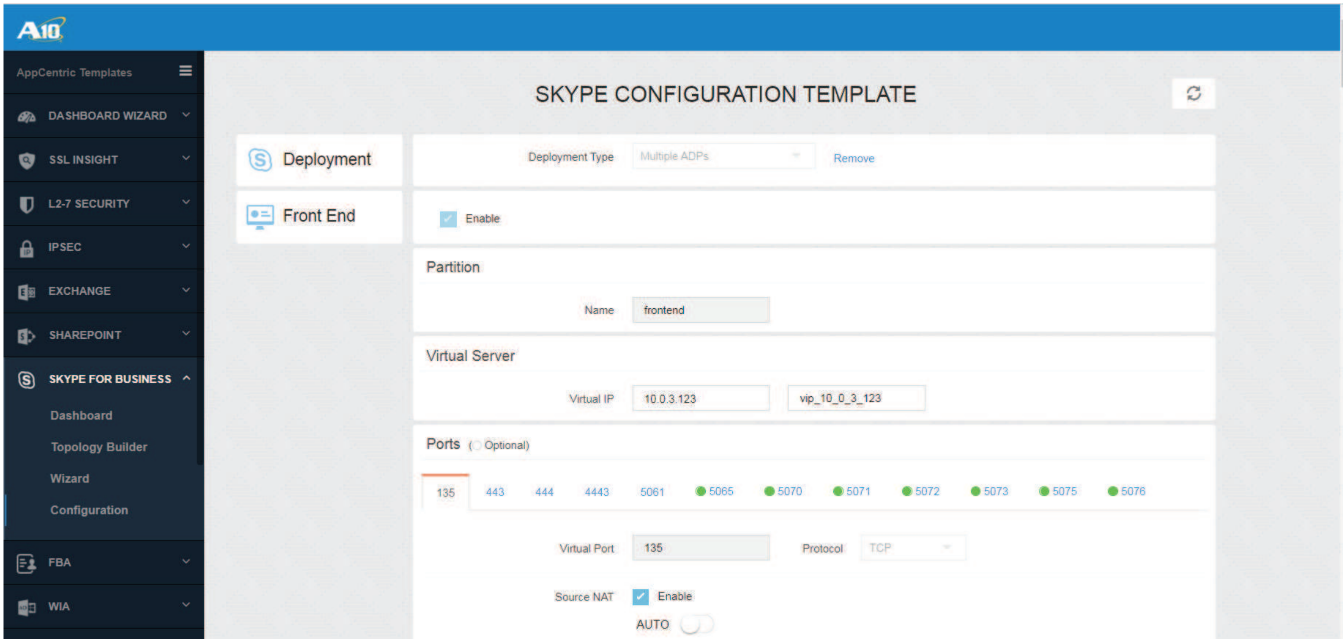
```
active-partition frontend
!
health monitor Hm_vip_10_0_3_123_135_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_135_tcp_vs_fe
  retry 3
  interval 5
  method tcp port 135
!
health monitor Hm_vip_10_0_3_123_443_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_443_tcp_vs_fe
  retry 3
  interval 5
  method tcp port 443
!
health monitor Hm_vip_10_0_3_123_444_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_444_tcp_vs_fe
  retry 3
  interval 5
  method tcp port 444
!
```

Figure 29: CLI configuration generated by ACT

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

CONFIGURATION

The configuration section provides users with the current configuration of the device as well as access to some advanced options.



SKYPE CONFIGURATION TEMPLATE

Deployment Type: Multiple ADPs — Remove

☑ Enable

Partition

Name: frontend

Virtual Server

Virtual IP: 10.0.3.123 — vip_10_0_3_123

Ports (○ Optional)

135 | 443 | 444 | 4443 | 5061 | ● 5065 | ● 5070 | ● 5071 | ● 5072 | ● 5073 | ● 5075 | ● 5076

Virtual Port: 135 — Protocol: TCP

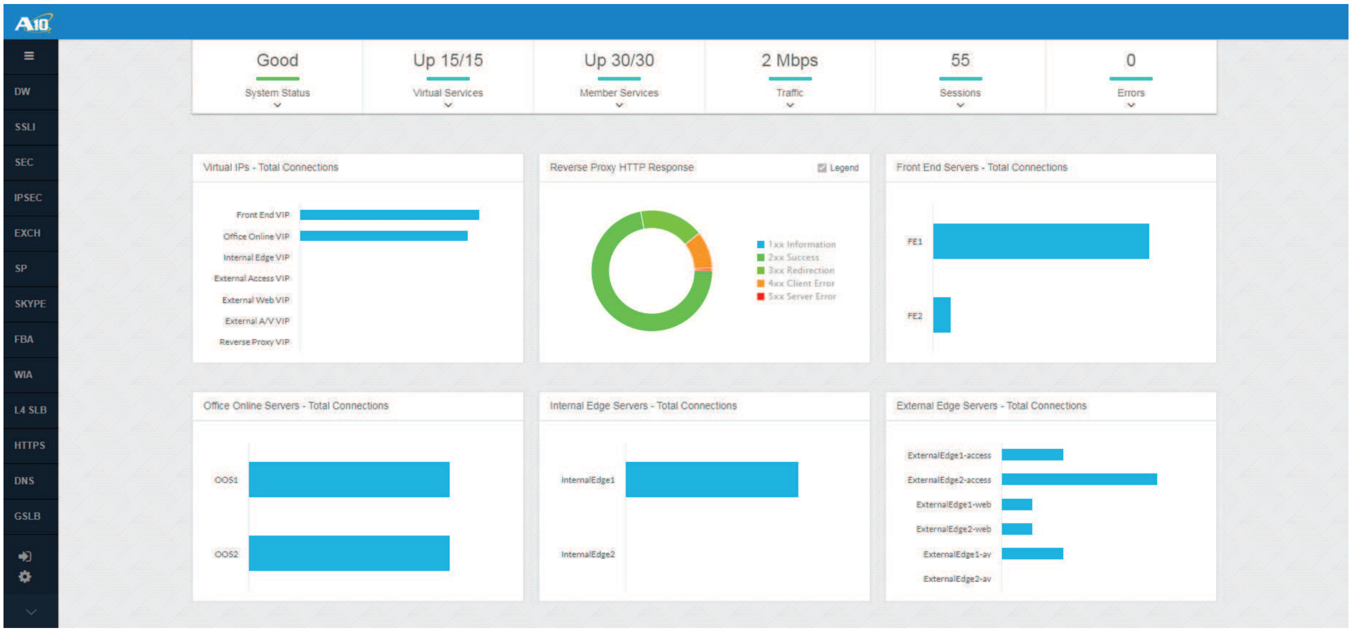
Source NAT: ☑ Enable

AUTO ○

Figure 30: Advanced configuration options

DASHBOARD

The dashboard provides real-time visibility into the Skype application by rendering pre-defined tiles and charts. These visuals provide an optimized view for real-time application monitoring.



Good	Up 15/15	Up 30/30	2 Mbps	55	0
System Status	Virtual Services	Member Services	Traffic	Sessions	Errors

Figure 31: Dashboard for real-time monitoring

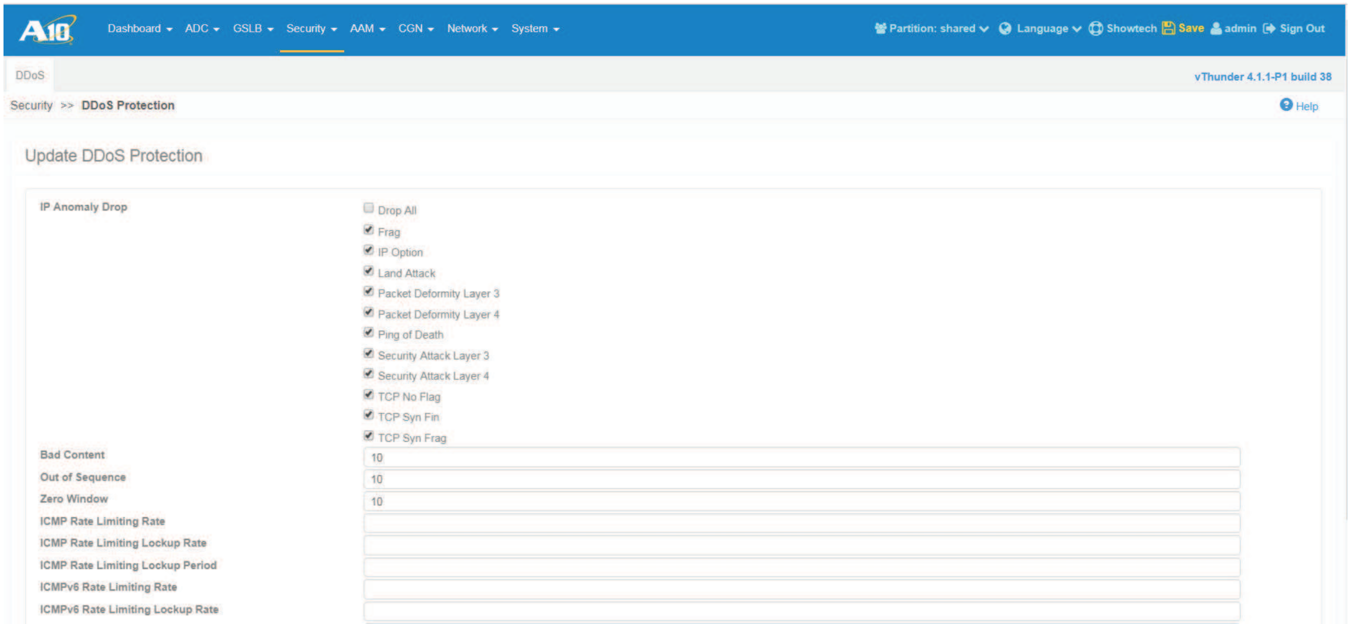
ADDITIONAL SECURITY FEATURE – DDOS MITIGATION (OPTIONAL)

The following section shows an additional security feature called DDoS Mitigation that can be implemented within the deployed solution.

DDOS MITIGATION

This section describes an additional security feature to protect applications from Distributed Denial of Service (DDoS) attacks. To configure this feature within the ACOS solution, navigate to **Security > > DDoS**.

The DDoS protection feature is a global configuration. To enable this feature, select the necessary DDoS attacks you would like to drop. In the below figure, we have selected the DDoS attack mitigation required. Once completed, click **Update** and **Save** to save the configuration.



Update DDoS Protection

IP Anomaly Drop
□ Drop All
☑ Frag
☑ IP Option
☑ Land Attack
☑ Packet Deformity Layer 3
☑ Packet Deformity Layer 4
☑ Ping of Death
☑ Security Attack Layer 3
☑ Security Attack Layer 4
☑ TCP No Flag
☑ TCP Syn Fin
☑ TCP Syn Frag

Bad Content	10
Out of Sequence	10
Zero Window	10
ICMP Rate Limiting Rate	
ICMP Rate Limiting Lockup Rate	
ICMP Rate Limiting Lockup Period	
ICMPv6 Rate Limiting Rate	
ICMPv6 Rate Limiting Lockup Rate	

Figure 32: DDoS protection

The following IP anomaly filters are supported for system-wide Policy-Based Server Load Balancing (PBSLB), although you can also use them with¬out PBSLB:

- Invalid HTTP or SSL payload
- Zero-length TCP window
- Out-of-sequence packet

__NOTE__: These filters are supported only for HTTP and HTTPS traffic.

SUMMARY

This document describes how to configure Thunder ADC as a load balancer and Reverse Proxy to support Microsoft Skype for Business Server 2015 and Office Online Server (OOS) using AppCentric Templates (ACT).

Deploying Thunder ADC as a load balancer and Reverse Proxy for Microsoft Skype for Business Server 2015 and OOS offers the following features and benefits:

- Transparent application load sharing
- High availability for Skype servers, ensuring users can access Skype applications without disruption
- Scalability, as the Thunder ADC device transparently load balances multiple Skype communication servers
- Higher connection throughput to enhance end user experience
- Improved server performance due to server offloading, including SSL Offload
- Protection against DDoS attacks using integrated DDoS protection capabilities
- Protection against web application attacks through Web Application Firewall (WAF)
- Consolidated roles on a single platform through multiple partitions

Thunder ADC offers a cost-effective way for organizations to optimize their Skype for Business Server 2015 deployments, empowering employees to connect, communicate, and collaborate with Skype.

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

www.a10networks.com/adc

www.a10networks.com/resources/solution-briefs

www.a10networks.com/resources/case-studies

APPENDIX A – THUNDER ADC TEST CONFIGURATION

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

FRONT END

```
active-partition frontend
!
!
vlan 103
  untagged ethernet 3
  router-interface ve 103
  user-tag act_sfb_frontend_vlan_103
!
interface ethernet 3
  enable
  user-tag act_sfb_frontend_eth_3
!
interface ve 103
  user-tag act_sfb_frontend_ve_103
  ip address 10.0.3.1 255.255.255.0
!
!
ip route 0.0.0.0 /0 10.0.3.254
!
health monitor Hm_vip_10_0_3_123_135_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_135_
tcp_vs_fe
  method tcp port 135
!
health monitor Hm_vip_10_0_3_123_443_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_443_
tcp_vs_fe
  method tcp port 443
!
health monitor Hm_vip_10_0_3_123_444_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_444_
tcp_vs_fe
  method tcp port 444
!
health monitor Hm_vip_10_0_3_123_4443_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_4443_
tcp_vs_fe
  method tcp port 4443
!
health monitor Hm_vip_10_0_3_123_5061_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_5061_
tcp_vs_fe
  method tcp port 5061
!
health monitor Hm_vip_10_0_3_123_5065_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_5065_
tcp_vs_fe
  method tcp port 5065
!
health monitor Hm_vip_10_0_3_123_5070_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_5070_
tcp_vs_fe
  method tcp port 5070
!
health monitor Hm_vip_10_0_3_123_5071_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_5071_
tcp_vs_fe
  method tcp port 5071
!
health monitor Hm_vip_10_0_3_123_5072_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_5072_
tcp_vs_fe
  method tcp port 5072
!
health monitor Hm_vip_10_0_3_123_5073_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_5073_
tcp_vs_fe
  method tcp port 5073
!
health monitor Hm_vip_10_0_3_123_5075_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_5075_
tcp_vs_fe
  method tcp port 5075
!
```

```
health monitor Hm_vip_10_0_3_123_5076_tcp
  user-tag act_sfb_Hm_vip_10_0_3_123_5076_
tcp_vs_fe
  method tcp port 5076
!
health monitor Hm_vip_10_0_3_125_80_http
  user-tag act_sfb_Hm_vip_10_0_3_125_80_
http_vs_oo
  method http port 80 expect wopi-discovery
url GET /hosting/discovery
!
slb template cipher Ccipher_
vip_10_0_3_125_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
  TLS1_ECDHE_RSA_AES_256_SHA
  TLS1_ECDHE_RSA_AES_128_SHA256
  TLS1_ECDHE_RSA_AES_128_GCM_SHA256
  user-tag act_sfb_Ccipher_
vip_10_0_3_125_443_vs_oo
!
slb template persist cookie persist_
template_vip_10_0_3_125_443
  user-tag act_sfb_persist_template_
vip_10_0_3_125_443_vs_oo
!
slb template persist source-ip persist_
template_vip_10_0_3_123_135
  user-tag act_sfb_persist_template_
vip_10_0_3_123_135_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_443
  user-tag act_sfb_persist_template_
vip_10_0_3_123_443_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_444
  user-tag act_sfb_persist_template_
vip_10_0_3_123_444_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_4443
  user-tag act_sfb_persist_template_
vip_10_0_3_123_4443_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_5061
  user-tag act_sfb_persist_template_
vip_10_0_3_123_5061_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_5065
  user-tag act_sfb_persist_template_
vip_10_0_3_123_5065_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_5070
  user-tag act_sfb_persist_template_
vip_10_0_3_123_5070_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_5071
  user-tag act_sfb_persist_template_
vip_10_0_3_123_5071_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_5072
  user-tag act_sfb_persist_template_
vip_10_0_3_123_5072_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_5073
  user-tag act_sfb_persist_template_
vip_10_0_3_123_5073_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_5075
  user-tag act_sfb_persist_template_
vip_10_0_3_123_5075_vs_fe
!
slb template persist source-ip persist_
template_vip_10_0_3_123_5076
  user-tag act_sfb_persist_template_
vip_10_0_3_123_5076_vs_fe
!
slb template tcp vip_10_0_3_123_135_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_135_tcp_
```

```
vs_fe
!
slb template tcp vip_10_0_3_123_443_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_443_tcp_
vs_fe
!
slb template tcp vip_10_0_3_123_444_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_444_tcp_
vs_fe
!
slb template tcp vip_10_0_3_123_4443_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_4443_
tcp_vs_fe
!
slb template tcp vip_10_0_3_123_5061_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_5061_
tcp_vs_fe
!
slb template tcp vip_10_0_3_123_5065_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_5065_
tcp_vs_fe
!
slb template tcp vip_10_0_3_123_5070_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_5070_
tcp_vs_fe
!
slb template tcp vip_10_0_3_123_5071_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_5071_
tcp_vs_fe
!
slb template tcp vip_10_0_3_123_5072_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_5072_
tcp_vs_fe
!
slb template tcp vip_10_0_3_123_5073_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_5073_
tcp_vs_fe
!
slb template tcp vip_10_0_3_123_5075_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_5075_
tcp_vs_fe
!
slb template tcp vip_10_0_3_123_5076_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_3_123_5076_
tcp_vs_fe
!
slb server FE1 10.0.3.12
  user-tag act_sfb_FE1
  port 135 tcp
    user-tag act_sfb_FE1_port_135_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 443 tcp
    user-tag act_sfb_FE1_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 444 tcp
    user-tag act_sfb_FE1_port_444_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 4443 tcp
    user-tag act_sfb_FE1_port_4443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5061 tcp
```

```
    user-tag act_sfb_FE1_port_5061_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5065 tcp
    user-tag act_sfb_FE1_port_5065_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5070 tcp
    user-tag act_sfb_FE1_port_5070_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5071 tcp
    user-tag act_sfb_FE1_port_5071_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5072 tcp
    user-tag act_sfb_FE1_port_5072_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5073 tcp
    user-tag act_sfb_FE1_port_5073_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5075 tcp
    user-tag act_sfb_FE1_port_5075_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5076 tcp
    user-tag act_sfb_FE1_port_5076_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server FE2 10.0.3.13
  user-tag act_sfb_FE2
  port 135 tcp
    user-tag act_sfb_FE2_port_135_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 443 tcp
    user-tag act_sfb_FE2_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 444 tcp
    user-tag act_sfb_FE2_port_444_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 4443 tcp
    user-tag act_sfb_FE2_port_4443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5061 tcp
    user-tag act_sfb_FE2_port_5061_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
```

```
port 5065 tcp
  user-tag act_sfb_FE2_port_5065_tcp
  sampling-enable total_conn
  sampling-enable total_fwd_bytes
  sampling-enable total_rev_bytes
  sampling-enable total_req
port 5070 tcp
  user-tag act_sfb_FE2_port_5070_tcp
  sampling-enable total_conn
  sampling-enable total_fwd_bytes
  sampling-enable total_rev_bytes
  sampling-enable total_req
port 5071 tcp
  user-tag act_sfb_FE2_port_5071_tcp
  sampling-enable total_conn
  sampling-enable total_fwd_bytes
  sampling-enable total_rev_bytes
  sampling-enable total_req
port 5072 tcp
  user-tag act_sfb_FE2_port_5072_tcp
  sampling-enable total_conn
  sampling-enable total_fwd_bytes
  sampling-enable total_rev_bytes
  sampling-enable total_req
port 5073 tcp
  user-tag act_sfb_FE2_port_5073_tcp
  sampling-enable total_conn
  sampling-enable total_fwd_bytes
  sampling-enable total_rev_bytes
  sampling-enable total_req
port 5075 tcp
  user-tag act_sfb_FE2_port_5075_tcp
  sampling-enable total_conn
  sampling-enable total_fwd_bytes
  sampling-enable total_rev_bytes
  sampling-enable total_req
port 5076 tcp
  user-tag act_sfb_FE2_port_5076_tcp
  sampling-enable total_conn
  sampling-enable total_fwd_bytes
```

```
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server OOS1 10.0.3.15
  user-tag act_sfb_OOS1
  port 80 tcp
    user-tag act_sfb_OOS1_port_80_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server OOS2 10.0.3.16
  user-tag act_sfb_OOS2
  port 80 tcp
    user-tag act_sfb_OOS2_port_80_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb service-group vip_10_0_3_123_135_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_135_tcp
  user-tag act_sfb_vip_10_0_3_123_135_tcp_
sg_vs_fe
  member FE1 135
  member FE2 135
!
slb service-group vip_10_0_3_123_443_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_443_tcp
  user-tag act_sfb_vip_10_0_3_123_443_tcp_
sg_vs_fe
  member FE1 443
  member FE2 443
!
slb service-group vip_10_0_3_123_4443_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_4443_tcp
  user-tag act_sfb_vip_10_0_3_123_4443_tcp_
sg_vs_fe
  member FE1 4443
  member FE2 4443
!
slb service-group vip_10_0_3_123_444_tcp_sg
tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_444_tcp
  user-tag act_sfb_vip_10_0_3_123_444_tcp_
sg_vs_fe
  member FE1 444
  member FE2 444
!
slb service-group vip_10_0_3_123_5061_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_5061_tcp
  user-tag act_sfb_vip_10_0_3_123_5061_tcp_
sg_vs_fe
  member FE1 5061
  member FE2 5061
!
slb service-group vip_10_0_3_123_5065_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_5065_tcp
  user-tag act_sfb_vip_10_0_3_123_5065_tcp_
sg_vs_fe
  member FE1 5065
  member FE2 5065
!
slb service-group vip_10_0_3_123_5070_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_5070_tcp
  user-tag act_sfb_vip_10_0_3_123_5070_tcp_
sg_vs_fe
  member FE1 5070
  member FE2 5070
!
slb service-group vip_10_0_3_123_5071_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_5071_tcp
  user-tag act_sfb_vip_10_0_3_123_5071_tcp_
sg_vs_fe
  member FE1 5071
  member FE2 5071
!
slb service-group vip_10_0_3_123_5072_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_5072_tcp
  user-tag act_sfb_vip_10_0_3_123_5072_tcp_
sg_vs_fe
  member FE1 5072
  member FE2 5072
!
slb service-group vip_10_0_3_123_5073_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_5073_tcp
  user-tag act_sfb_vip_10_0_3_123_5073_tcp_
sg_vs_fe
  member FE1 5073
  member FE2 5073
!
slb service-group vip_10_0_3_123_5075_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_5075_tcp
  user-tag act_sfb_vip_10_0_3_123_5075_tcp_
sg_vs_fe
  member FE1 5075
  member FE2 5075
!
slb service-group vip_10_0_3_123_5076_tcp_
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_123_5076_tcp
  user-tag act_sfb_vip_10_0_3_123_5076_tcp_
sg_vs_fe
  member FE1 5076
  member FE2 5076
!
slb service-group vip_10_0_3_125_80_https_
```

```
sg tcp
  method least-connection
  health-check Hm_vip_10_0_3_125_80_http
  user-tag act_sfb_vip_10_0_3_125_80_https_
sg_vs_oo
  member OOS1 80
  member OOS2 80
!
slb template client-ssl Cssl_
vip_10_0_3_125_443
  template cipher Ccipher_
vip_10_0_3_125_443
  chain-cert OOSCert
  cert OOSCert
  enable-tls-alert-logging fatal
  key OOSCert
  user-tag act_sfb_Cssl_vip_10_0_3_125vs_
oo_443
!
slb virtual-server vip_10_0_3_123
10.0.3.123
  user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123
  port 135 tcp
    source-nat auto
    service-group vip_10_0_3_123_135_tcp_sg
    template persist source-ip persist_
template_vip_10_0_3_123_135
    template tcp vip_10_0_3_123_135_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_135_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 443 tcp
    source-nat auto
    service-group vip_10_0_3_123_443_tcp_sg
    template persist source-ip persist_
template_vip_10_0_3_123_443
    template tcp vip_10_0_3_123_443_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_443_tcp
    sampling-enable total_req
```

```
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 444 tcp
    source-nat auto
    service-group vip_10_0_3_123_444_tcp_sg
    template persist source-ip persist_
template_vip_10_0_3_123_444
    template tcp vip_10_0_3_123_444_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_444_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 4443 tcp
    source-nat auto
    service-group vip_10_0_3_123_4443_tcp_
sg
    template persist source-ip persist_
template_vip_10_0_3_123_4443
    template tcp vip_10_0_3_123_4443_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_4443_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5061 tcp
    source-nat auto
    service-group vip_10_0_3_123_5061_tcp_
sg
    template persist source-ip persist_
template_vip_10_0_3_123_5061
    template tcp vip_10_0_3_123_5061_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_5061_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5065 tcp
    source-nat auto
    service-group vip_10_0_3_123_5065_tcp_
sg
    template persist source-ip persist_
template_vip_10_0_3_123_5065
    template tcp vip_10_0_3_123_5065_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_5065_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5070 tcp
    source-nat auto
    service-group vip_10_0_3_123_5070_tcp_
sg
    template persist source-ip persist_
template_vip_10_0_3_123_5070
    template tcp vip_10_0_3_123_5070_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_5070_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5071 tcp
    source-nat auto
    service-group vip_10_0_3_123_5071_tcp_
sg
    template persist source-ip persist_
template_vip_10_0_3_123_5071
    template tcp vip_10_0_3_123_5071_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_5071_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5072 tcp
    source-nat auto
    service-group vip_10_0_3_123_5072_tcp_
sg
    template persist source-ip persist_
template_vip_10_0_3_123_5072
    template tcp vip_10_0_3_123_5072_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_5072_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5073 tcp
    source-nat auto
    service-group vip_10_0_3_123_5073_tcp_
sg
    template persist source-ip persist_
template_vip_10_0_3_123_5073
    template tcp vip_10_0_3_123_5073_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_5073_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5075 tcp
    source-nat auto
    service-group vip_10_0_3_123_5075_tcp_
sg
    template persist source-ip persist_
template_vip_10_0_3_123_5075
    template tcp vip_10_0_3_123_5075_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_5075_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5076 tcp
    source-nat auto
    service-group vip_10_0_3_123_5076_tcp_
sg
    template persist source-ip persist_
template_vip_10_0_3_123_5076
    template tcp vip_10_0_3_123_5076_tcp
    user-tag act_sfb_frontend_vs_fe_
vip_10_0_3_123_5076_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
!
slb virtual-server vip_10_0_3_125 10.0.3.125
  user-tag act_sfb_frontend_vs_oo_vip_10_0_3_125
  port 443 https
    source-nat auto
    service-group vip_10_0_3_125_80_https_sg
    template persist cookie persist_template_vip_10_0_3_125_443
    template client-ssl Cssl_vip_10_0_3_125_443
    user-tag act_sfb_frontend_vs_oo_vip_10_0_3_125_443_https
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
!
end
```

INTERNAL EDGE

```
active-partition internal_edge
!
!
vlan 401
  untagged ethernet 2
  router-interface ve 401
  user-tag act_sfb_internal_edge_vlan_401
!
interface ethernet 2
  enable
  user-tag act_sfb_internal_edge_eth_2
!
interface ve 401
  user-tag act_sfb_internal_edge_ve_401
  ip address 10.0.4.241 255.255.255.0
!
!
ip route 0.0.0.0 /0 10.0.4.254
!
health monitor Hm_vip_10_0_4_30_443_tcp
  user-tag act_sfb_Hm_vip_10_0_4_30_443_tcp_vs_ie
  method tcp port 443
!
health monitor Hm_vip_10_0_4_30_3478_udp
  user-tag act_sfb_Hm_vip_10_0_4_30_3478_udp_vs_ie
  method udp port 3478
!
health monitor Hm_vip_10_0_4_30_5061_tcp
  user-tag act_sfb_Hm_vip_10_0_4_30_5061_tcp_vs_ie
  method tcp port 5061
!
health monitor Hm_vip_10_0_4_30_5062_tcp
  user-tag act_sfb_Hm_vip_10_0_4_30_5062_tcp_vs_ie
  method tcp port 5062
!
slb template persist source-ip persist_template_vip_10_0_4_30_443
  user-tag act_sfb_persist_template_vip_10_0_4_30_443_vs_ie
!
slb template persist source-ip persist_template_vip_10_0_4_30_3478
  user-tag act_sfb_persist_template_vip_10_0_4_30_3478_vs_ie
!
slb template persist source-ip persist_template_vip_10_0_4_30_5061
  user-tag act_sfb_persist_template_vip_10_0_4_30_5061_vs_ie
!
slb template persist source-ip persist_template_vip_10_0_4_30_5062
  user-tag act_sfb_persist_template_vip_10_0_4_30_5062_vs_ie
!
slb template tcp vip_10_0_4_30_443_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_4_30_443_tcp_vs_ie
!
```

```
slb template tcp vip_10_0_4_30_5061_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_4_30_5061_tcp_vs_ie
!
slb template tcp vip_10_0_4_30_5062_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_10_0_4_30_5062_tcp_vs_ie
!
slb server InternalEdge1 10.0.4.31
  user-tag act_sfb_InternalEdge1
  port 443 tcp
    user-tag act_sfb_InternalEdge1_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 3478 udp
    user-tag act_sfb_InternalEdge1_port_3478_udp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5061 tcp
    user-tag act_sfb_InternalEdge1_port_5061_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5062 tcp
    user-tag act_sfb_InternalEdge1_port_5062_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server InternalEdge2 10.0.4.32
  user-tag act_sfb_InternalEdge2
  port 443 tcp
    user-tag act_sfb_InternalEdge2_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 3478 udp
    user-tag act_sfb_InternalEdge2_port_3478_udp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5061 tcp
    user-tag act_sfb_InternalEdge2_port_5061_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 5062 tcp
    user-tag act_sfb_InternalEdge2_port_5062_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb service-group vip_10_0_4_30_3478_udp_sg udp
  method least-connection
  health-check Hm_vip_10_0_4_30_3478_udp
  user-tag act_sfb_vip_10_0_4_30_3478_udp_sg_vs_ie
  member InternalEdge1 3478
  member InternalEdge2 3478
!
slb service-group vip_10_0_4_30_443_tcp_sg tcp
  method least-connection
  health-check Hm_vip_10_0_4_30_443_tcp
  user-tag act_sfb_vip_10_0_4_30_443_tcp_sg_vs_ie
  member InternalEdge1 443
  member InternalEdge2 443
!
slb service-group vip_10_0_4_30_5061_tcp_sg tcp
  method least-connection
  health-check Hm_vip_10_0_4_30_5061_tcp
  user-tag act_sfb_vip_10_0_4_30_5061_tcp_sg_vs_ie
  member InternalEdge1 5061
  member InternalEdge2 5061
!
slb service-group vip_10_0_4_30_5062_tcp_sg tcp
  method least-connection
  health-check Hm_vip_10_0_4_30_5062_tcp
  user-tag act_sfb_vip_10_0_4_30_5062_tcp_sg_vs_ie
  member InternalEdge1 5062
  member InternalEdge2 5062
!
slb virtual-server vip_10_0_4_30 10.0.4.30
  user-tag act_sfb_internal_edge_vs_ie_vip_10_0_4_30
  port 443 tcp
    source-nat auto
    service-group vip_10_0_4_30_443_tcp_sg
    template persist source-ip persist_template_vip_10_0_4_30_443
    template tcp vip_10_0_4_30_443_tcp
    user-tag act_sfb_internal_edge_vs_ie_vip_10_0_4_30_443_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 3478 udp
    source-nat auto
    service-group vip_10_0_4_30_3478_udp_sg
    template persist source-ip persist_template_vip_10_0_4_30_3478
    user-tag act_sfb_internal_edge_vs_ie_vip_10_0_4_30_3478_udp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5061 tcp
    source-nat auto
    service-group vip_10_0_4_30_5061_tcp_sg
    template persist source-ip persist_template_vip_10_0_4_30_5061
    template tcp vip_10_0_4_30_5061_tcp
    user-tag act_sfb_internal_edge_vs_ie_vip_10_0_4_30_5061_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 5062 tcp
    source-nat auto
    service-group vip_10_0_4_30_5062_tcp_sg
    template persist source-ip persist_template_vip_10_0_4_30_5062
    template tcp vip_10_0_4_30_5062_tcp
    user-tag act_sfb_internal_edge_vs_ie_vip_10_0_4_30_5062_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
!
end
```

EXTERNAL EDGE

```
active-partition external_edge
!
!
vlan 102
  untagged ethernet 4
  router-interface ve 102
  user-tag act_sfb_external_edge_vlan_102
!
```

```
interface ethernet 4
  enable
  user-tag act_sfb_external_edge_eth_4
!
interface ve 102
  user-tag act_sfb_external_edge_ve_102
  ip address 192.0.2.1 255.255.255.0
!
!
ip route 0.0.0.0 /0 192.0.2.254
!
health monitor Hm_vip_192_0_2_111_443_tcp
  user-tag act_sfb_Hm_vip_192_0_2_111_443_tcp_vs_eea
  method tcp port 443
!
health monitor Hm_vip_192_0_2_112_443_tcp
  user-tag act_sfb_Hm_vip_192_0_2_112_443_tcp_vs_eew
  method tcp port 443
!
health monitor Hm_vip_192_0_2_113_443_tcp
  user-tag act_sfb_Hm_vip_192_0_2_113_443_tcp_vs_eeav
  method tcp port 443
!
health monitor Hm_vip_192_0_2_113_3478_udp
  user-tag act_sfb_Hm_vip_192_0_2_113_3478_udp_vs_eeav
  method udp port 3478
!
slb template persist source-ip persist_template_vip_192_0_2_111_443
  user-tag act_sfb_persist_template_vip_192_0_2_111_443_vs_eea
!
slb template persist source-ip persist_template_vip_192_0_2_112_443
  user-tag act_sfb_persist_template_vip_192_0_2_112_443_vs_eew
!
slb template persist source-ip persist_template_vip_192_0_2_113_443
  user-tag act_sfb_persist_template_vip_192_0_2_113_443_vs_eeav
!
slb template persist source-ip persist_template_vip_192_0_2_113_3478
  user-tag act_sfb_persist_template_vip_192_0_2_113_3478_vs_eeav
!
slb template tcp vip_192_0_2_111_443_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_192_0_2_111_443_tcp_vs_eea
!
slb template tcp vip_192_0_2_112_443_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_192_0_2_112_443_tcp_vs_eew
!
slb template tcp vip_192_0_2_113_443_tcp
  idle-timeout 1800
  user-tag act_sfb_vip_192_0_2_113_443_tcp_vs_eeav
!
slb server ExternalEdge1-access 192.0.2.21
  user-tag act_sfb_ExternalEdge1-access
  port 443 tcp
    user-tag act_sfb_ExternalEdge1-access_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server ExternalEdge1-av 192.0.2.23
  user-tag act_sfb_ExternalEdge1-av
  port 443 tcp
    user-tag act_sfb_ExternalEdge1-av_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 3478 udp
    user-tag act_sfb_ExternalEdge1-av_
```

```
port_3478_udp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server ExternalEdge1-web 192.0.2.22
  user-tag act_sfb_ExternalEdge1-web
  port 443 tcp
    user-tag act_sfb_ExternalEdge1-web_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server ExternalEdge2-access 192.0.2.31
  user-tag act_sfb_ExternalEdge2-access
  port 443 tcp
    user-tag act_sfb_ExternalEdge2-access_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server ExternalEdge2-av 192.0.2.33
  user-tag act_sfb_ExternalEdge2-av
  port 443 tcp
    user-tag act_sfb_ExternalEdge2-av_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
  port 3478 udp
    user-tag act_sfb_ExternalEdge2-av_port_3478_udp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server ExternalEdge2-web 192.0.2.32
  user-tag act_sfb_ExternalEdge2-web
  port 443 tcp
    user-tag act_sfb_ExternalEdge2-web_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb service-group vip_192_0_2_111_443_tcp_sg tcp
  method least-connection
  health-check Hm_vip_192_0_2_111_443_tcp
  user-tag act_sfb_vip_192_0_2_111_443_tcp_sg_vs_eea
  member ExternalEdge1-access 443
  member ExternalEdge2-access 443
!
slb service-group vip_192_0_2_112_443_tcp_sg tcp
  method least-connection
  health-check Hm_vip_192_0_2_112_443_tcp
  user-tag act_sfb_vip_192_0_2_112_443_tcp_sg_vs_eew
  member ExternalEdge1-web 443
  member ExternalEdge2-web 443
!
slb service-group vip_192_0_2_113_3478_udp_sg udp
  method least-connection
  health-check Hm_vip_192_0_2_113_3478_udp
  user-tag act_sfb_vip_192_0_2_113_3478_udp_sg_vs_eeav
  member ExternalEdge1-av 3478
  member ExternalEdge2-av 3478
!
slb service-group vip_192_0_2_113_443_tcp_sg tcp
  method least-connection
  health-check Hm_vip_192_0_2_113_443_tcp
  user-tag act_sfb_vip_192_0_2_113_443_tcp_
```

```
sg_vs_eeav
  member ExternalEdge1-av 443
  member ExternalEdge2-av 443
!
slb virtual-server vip_192_0_2_111 192.0.2.111
  user-tag act_sfb_external_edge_vs_eea_vip_192_0_2_111
  port 443 tcp
    service-group vip_192_0_2_111_443_tcp_sg
    template persist source-ip persist_template_vip_192_0_2_111_443
    template tcp vip_192_0_2_111_443_tcp
    user-tag act_sfb_external_edge_vs_eea_vip_192_0_2_111_443_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
!
slb virtual-server vip_192_0_2_112 192.0.2.112
  user-tag act_sfb_external_edge_vs_eew_vip_192_0_2_112
  port 443 tcp
    service-group vip_192_0_2_112_443_tcp_sg
    template persist source-ip persist_template_vip_192_0_2_112_443
    template tcp vip_192_0_2_112_443_tcp
    user-tag act_sfb_external_edge_vs_eew_vip_192_0_2_112_443_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
!
slb virtual-server vip_192_0_2_113 192.0.2.113
  user-tag act_sfb_external_edge_vs_eeav_vip_192_0_2_113
  port 443 tcp
    service-group vip_192_0_2_113_443_tcp_sg
    template persist source-ip persist_template_vip_192_0_2_113_443
    template tcp vip_192_0_2_113_443_tcp
    user-tag act_sfb_external_edge_vs_eeav_vip_192_0_2_113_443_tcp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
  port 3478 udp
    service-group vip_192_0_2_113_3478_udp_sg
    template persist source-ip persist_template_vip_192_0_2_113_3478
    user-tag act_sfb_external_edge_vs_eeav_vip_192_0_2_113_3478_udp
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
!
end
```

REVERSE PROXY

```
active-partition reverse_proxy
!
!
vlan 105
  untagged ethernet 5
  router-interface ve 105
  user-tag act_sfb_reverse_proxy_vlan_105
!
vlan 106
  untagged ethernet 6
  router-interface ve 106
  user-tag act_sfb_reverse_proxy_vlan_106
!
interface ethernet 5
  enable
  user-tag act_sfb_reverse_proxy_eth_5
!
interface ethernet 6
```

```
  enable
  user-tag act_sfb_reverse_proxy_eth_6
!
interface ve 105
  user-tag act_sfb_reverse_proxy_ve_105
  ip address 192.0.2.201 255.255.255.0
!
interface ve 106
  user-tag act_sfb_reverse_proxy_ve_106
  ip address 10.0.4.201 255.255.255.0
!
!
ip route 0.0.0.0 /0 192.0.2.254
!
ip route 10.0.3.0 /24 10.0.4.254
!
health monitor Hm_vip_192_0_2_108_4443_tcp
  user-tag act_sfb_Hm_vip_192_0_2_108_4443_tcp_vs_rp
  method tcp port 4443
!
health monitor Hm_vip_192_0_2_108_443_tcp
  user-tag act_sfb_Hm_vip_192_0_2_108_443_tcp_vs_rp
  method tcp port 443
!
slb template cipher Ccipher_vip_192_0_2_108_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
  TLS1_ECDHE_RSA_AES_256_SHA
  TLS1_ECDHE_RSA_AES_128_SHA256
  TLS1_ECDHE_RSA_AES_128_GCM_SHA256
  user-tag act_sfb_Ccipher_vip_192_0_2_108_443_vs_rp
!
slb template server-ssl Sssl_vip_192_0_2_108_443
  ca-cert InternalRootCA
  user-tag act_sfb_Sssl_vip_192_0_2_108_443_vs_rp
!
slb server vip_10_0_3_123 10.0.3.123
  user-tag act_sfb_vip_10_0_3_123
  port 4443 tcp
    user-tag act_sfb_vip_10_0_3_123_port_4443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb server vip_10_0_3_125 10.0.3.125
  user-tag act_sfb_vip_10_0_3_125
  port 443 tcp
    user-tag act_sfb_vip_10_0_3_125_port_443_tcp
    sampling-enable total_conn
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_req
!
slb service-group vip_192_0_2_108_443_tcp_sg tcp
  method least-connection
  health-check Hm_vip_192_0_2_108_443_tcp
  user-tag act_sfb_vip_192_0_2_108_443_tcp_sg_vs_rp
  member vip_10_0_3_125 443
!
slb service-group vip_192_0_2_108_4443_tcp_sg tcp
  method least-connection
  health-check Hm_vip_192_0_2_108_4443_tcp
  user-tag act_sfb_vip_192_0_2_108_4443_tcp_sg_vs_rp
  member vip_10_0_3_123 4443
!
slb template client-ssl Cssl_vip_192_0_2_108_443
  template cipher Ccipher_vip_192_0_2_108_443
  chain-cert SSL_Cert
  cert SSL_Cert
  enable-tls-alert-logging fatal
  key SSL_Cert
  user-tag act_sfb_Cssl_vip_192_0_2_108vs_
rp_443
!
slb template http templ_http_
vip_192_0_2_108_443_tcp
  host-switching equals oos.s4b.com
service-group vip_192_0_2_108_443_tcp_sg
  user-tag act_sfb_templ_http_
vip_192_0_2_108_443_tcp_vs_rp
!
slb virtual-server vip_192_0_2_108
192.0.2.108
  user-tag act_sfb_reverse_proxy_vs_rp_
vip_192_0_2_108
  port 443 https
    source-nat auto
    service-group vip_192_0_2_108_4443_tcp_
sg
    template http templ_http_
vip_192_0_2_108_443_tcp
    template server-ssl Sssl_
vip_192_0_2_108_443
    template client-ssl Cssl_
vip_192_0_2_108_443
    user-tag act_sfb_reverse_proxy_vs_rp_
vip_192_0_2_108_443_https
    sampling-enable total_req
    sampling-enable total_fwd_bytes
    sampling-enable total_rev_bytes
    sampling-enable total_conn
!
end
```

SHARED PARTITION

```
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 bad-content 10
ip anomaly-drop frag
ip anomaly-drop ip-option
ip anomaly-drop land-attack
ip anomaly-drop out-of-sequence 10
ip anomaly-drop ping-of-death
ip anomaly-drop tcp-no-flag
ip anomaly-drop tcp-syn-fin
ip anomaly-drop tcp-syn-frag
!
partition frontend id 1 application-type adc
  user-tag act_sfb_frontend
!
partition internal_edge id 2 application-
type adc
  user-tag act_sfb_internal_edge
!
partition external_edge id 3 application-
type adc
  user-tag act_sfb_external_edge
!
partition reverse_proxy id 4 application-
type adc
  user-tag act_sfb_reverse_proxy
!
interface management
  ip address 10.100.2.144 255.255.255.0
  ip default-gateway 10.100.2.1
!
interface ethernet 1
!
interface ethernet 2
!
interface ethernet 3
!
interface ethernet 4
!
interface ethernet 5
!
interface ethernet 6
!
!
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

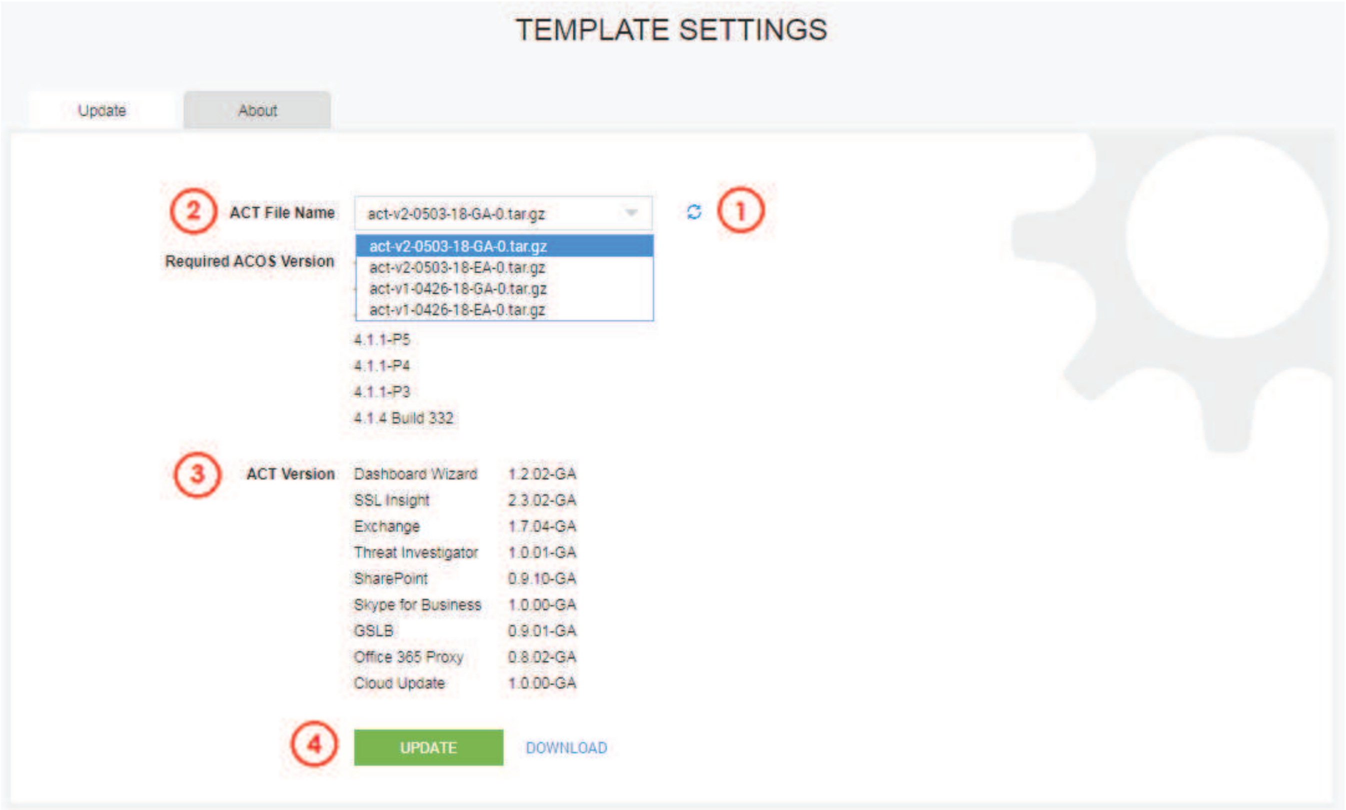
ACT can be upgraded to the latest version directly from the cloud.

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.



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

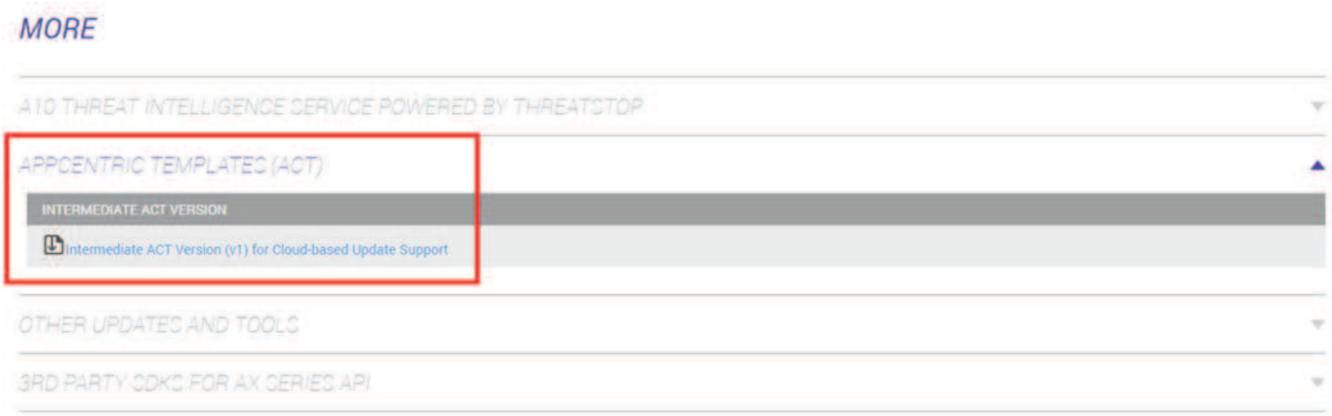
2. Select the desired ACT build from the dropdown menu and verify that your ACOS version is listed below for compatibility.
3. Also make sure that the Application for which you want to upgrade ACT is included in the build.
4. Click **Update**.

> ***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

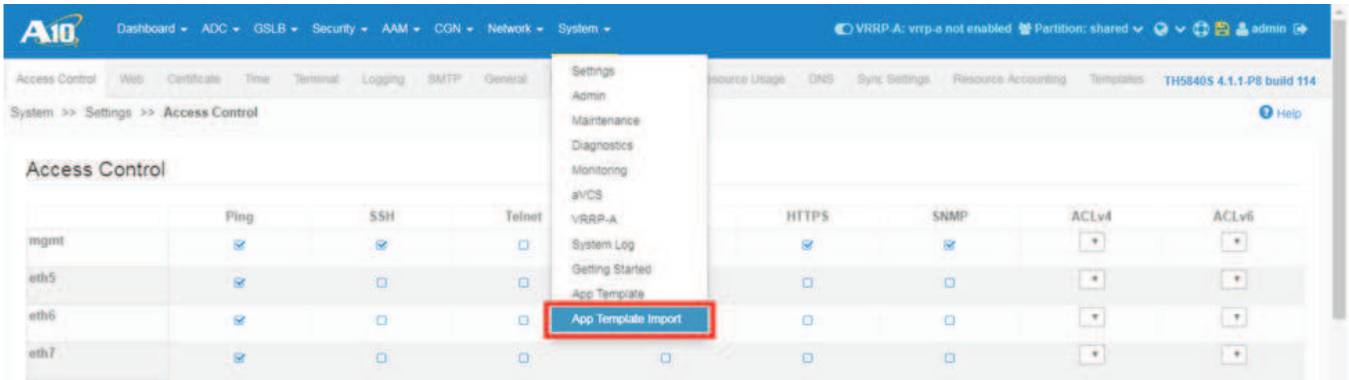
If your current ACT version does not support cloud-based updates, you can use the manual update option to upgrade to an intermediary version that does support cloud-based updates. You can then update to your desired ACT version using the steps mentioned above.

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.

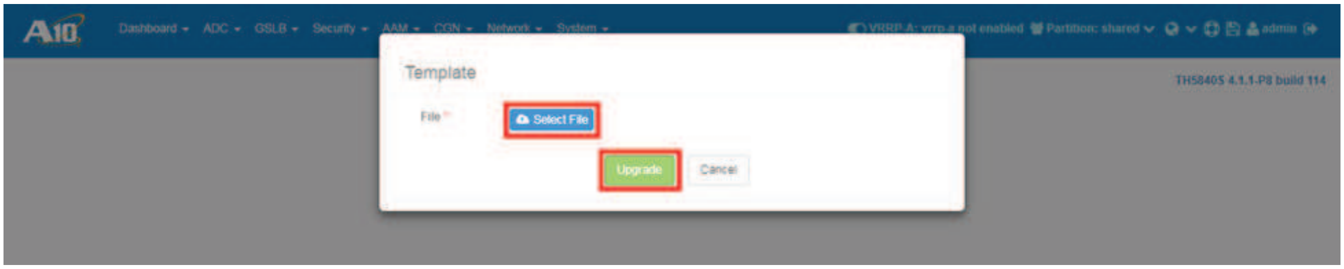

MORE
A10 THREAT INTELLIGENCE SERVICE POWERED BY THREATSTOP
APPCENTRIC TEMPLATES (ACT)
INTERMEDIATE ACT VERSION
Intermediate ACT Version (v1) for Cloud-based Update Support
OTHER UPDATES AND TOOLS
3RD PARTY SDKS FOR AX SERIES API

__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**.


A10
Dashboard ▾ ADC ▾ GSLB ▾ Security ▾ AAM ▾ CGN ▾ Network ▾ System ▾
VRRP-A: vrrp-a not enabled Partition: shared admin
Access Control Web Certificate Time Terminal Logging SMTP General
source Usage DNS Sync Settings Resource Accounting Templates
TH5840S 4.1.1-P8 build 114
System >> Settings >> Access Control
Help
Access Control
Ping SSH Telnet HTTPS SNMP ACLv4 ACLv6
mgmt
eth5
eth6
eth7
Settings
Admin
Maintenance
Diagnostics
Monitoring
aVCS
VRRP-A
System Log
Getting Started
App Template
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-16165-EN-02   AUG 2018