ORACLE E-BUSINESS SUITE

AN EDGENEXUS ADC DEPLOYMENT GUIDE

EDGENEXUS

Contents

Document Properties

Document Number: 2.0.2.24.22.15.02

Document Creation Date: February 18, 2022

Document Last Edited: February 24, 2022

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: Choose an item. - Version Click or tap here to enter text.

Document Disclaimer

This manual's screenshots and graphics may differ slightly from your product due to your product release version differences. Edgenexus ensures that they make every reasonable effort to ensure that the information in this document is complete and accurate. However, Edgenexus assumes no liability for any errors. Edgenexus makes changes and corrections to the information in this document in future releases when the need arises.

Copyrights

Trademarks

The Edgenexus logo, Edgenexus, EdgeADC, EdgWAF, EdgeGSLB, EdgeDNS are all trademarks or registered trademarks of Edgenexus Limited. All other trademarks are the properties of their respective owners and are acknowledged.

Edgenexus Support

If you have any technical questions regarding this product, please raise a support ticket at: support@edgenexus.io

Introduction

This EdgeADC (ADC) application deployment guide is intended for persons administering the Oracle e-Business Suite and its load balancing. This document contains specific general suggestions and guidance, which may or may not be relevant for use within your organization.

Oracle E-Business Suite (EBS) is a complete set of business applications for managing and automating processes for your enterprise. EBS is also referred to as Oracle Enterprise Resource Planning (ERP), Oracle Apps, Oracle Applications, and Oracle Financials on the market.

We recommend the following:

The ADC is deployed as a pair of appliances in either a virtualization technology, installing it as a virtualized appliance or as a hardware appliance in approved server hardware.

When external users access the network via the Internet, we recommend that the ADC pair is deployed in the DMZ and the traffic rerouted through the firewall to the LAN zone.

The ADC's operate in a high-availability (HA) mode when placed in pairs and provide you with the level of redundancy and resilience required for mission-critical systems.

The ADC is fully capable of load-balancing your Oracle e-Business Suite, and this guide explains how to set this up.

Prerequisites for supporting Oracle e-Business Suite

As usual, it is assumed that the person installing and configuring the ADC is familiar with the terminology used within this document and networking in general. We strongly suggest that both the network technician and Oracle e-Business Suite administrator work in tandem when setting up the load balancing and that this is first done for a sandbox environment before replicating to the production environment.

Further, it is also recommended you follow the below requirements, which are regarded as the minimum:

- The latest ADC firmware should be used
- The Oracle e-Business Suite version 12 and above should be installed and operational.
- The initial ADC configuration should be against an Oracle e-Business Suite sandbox deployment.
- DNS entries for both internal and external access should be configured and working.
- The ADC should be reachable using a web browser and the management IP.

Acronyms used

VIP – Virtual IP
RS – Real Server
ADC – Edgenexus EdgeADC

VS – Virtual Service
RSIP – Real Server IP

VIPs, Ports, and Other Bits

When load balancing Oracle e-Business Suite, the following VIPs will be needed for operations.

Port	Protocol	Service Type	Explanation
443	TCP	L4-TCP or L7 HTTP	This port is used to handle all HTTPS requests from client applications. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.
80	TCP	L4-TCP or L7 HTTP	This port is used to handle all HTTP requests from client applications. You can use Layer 4 TCP with SSL Passthrough or Layer 7 with SSL Offload or SSL Bridging.

Sizing the EdgeADC

The ADC can operate in either physical or virtual deployments. The ADC will use all available threads automatically. The reverse proxy engine within the ADC is optimized for speed and efficiency.

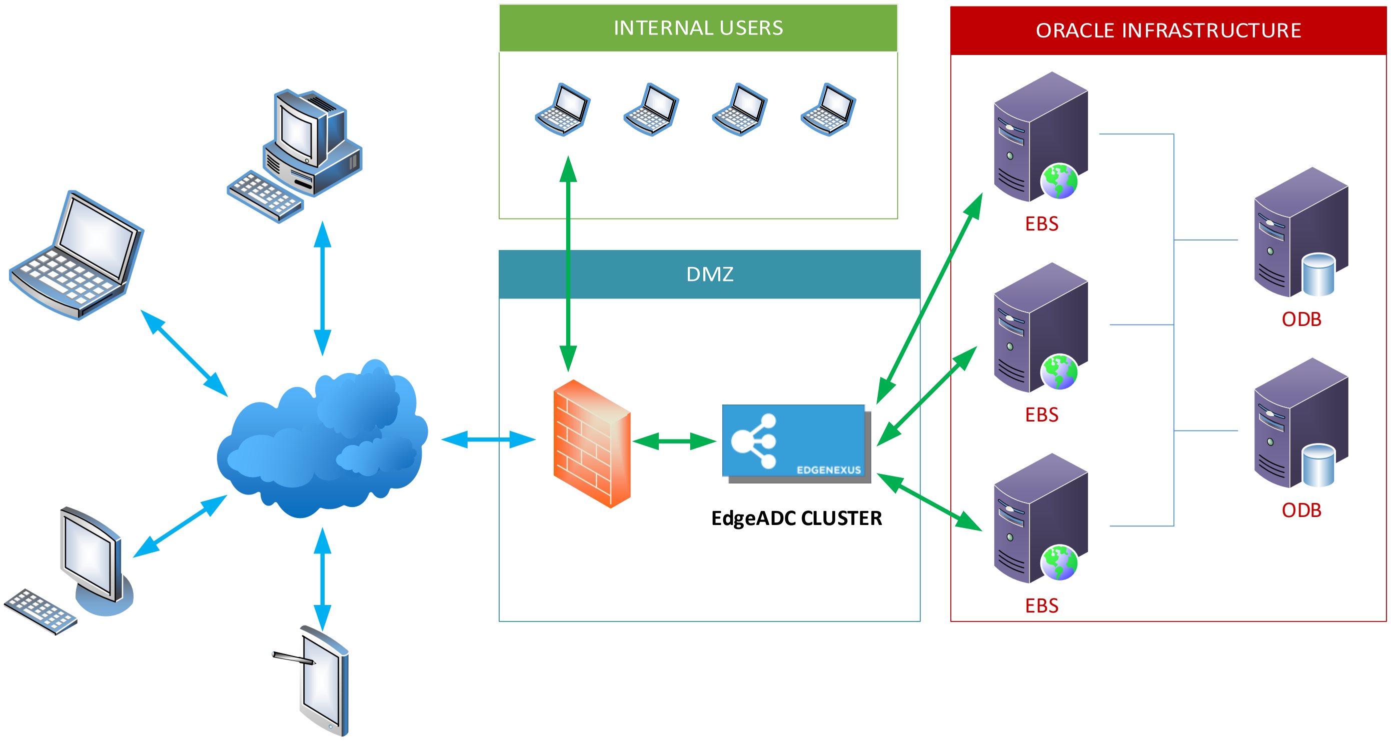
In virtualized environments, we recommend that you set the ADC to 4 vCPU with 8GB RAM, to begin with and scale up when you need to.

We recommend that you utilize the hardware platforms from our partners in physical environments, with the base system being a quad-core Intel Xeon with 8GB RAM.

In both cases, 50GB of disk storage space should be sufficient.

Deployment Scenarios

Connections to the Oracle e-Business Suite system occur by clients connecting to the VIP or Virtual IP service created on the ADC. The ADC then load-balances the connections to the nodes configured within the ADC and linked to the VIP. An example diagram is shown below.



Virtual Service Methods

There are several ways to configure the ADC with Oracle e-Business Suite.

SSL Passthrough In this mode, the traffic enters the ADC on port 443 using SSL. Then, the traffic is sent onto the nodes without inspection. ADC service type Layer 4 TCP is used.

SSL Bridging In this mode, the SSL traffic is terminated in the ADC and then re-encrypted before passing to the nodes. When this mode is chosen, you will need to install the SSL certificate on the nodes and install it in the ADC. This mode is the recommended best practice method for security reasons. ADC service type HTTP is used.

SSL Termination This mode allows SSL traffic to be received by the ADC, which then terminates the SSL encryption internally before passing it to the nodes using unencrypted SSL. This mode may not be the desired choice for security reasons. ADC service type HTTP is used.

Oracle EBS is very flexible in the ports it can use, and so the configuration we have outlined is a guideline example. However, we would advise you to consider using Port 443 for the ingress VIP, and then either SSL with 443 for the connection to the EBS servers or port 80 with un-encrypted traffic if you consider it safe.

Persistence Methods

Since your users will be connecting to web-based application servers that connect to database servers, users mustn't be shifted to servers other than the server they have logged on. If this happens, their session will be lost, and they will need to log onto the system again.

IP List Based

This load balancing policy ensures that users connected to a particular server stay connected to the same server during their current session.

Note: You need to be aware that users connecting from a NAT'd network will all be seen to be from the gateway IP of the network.

Cookie-based

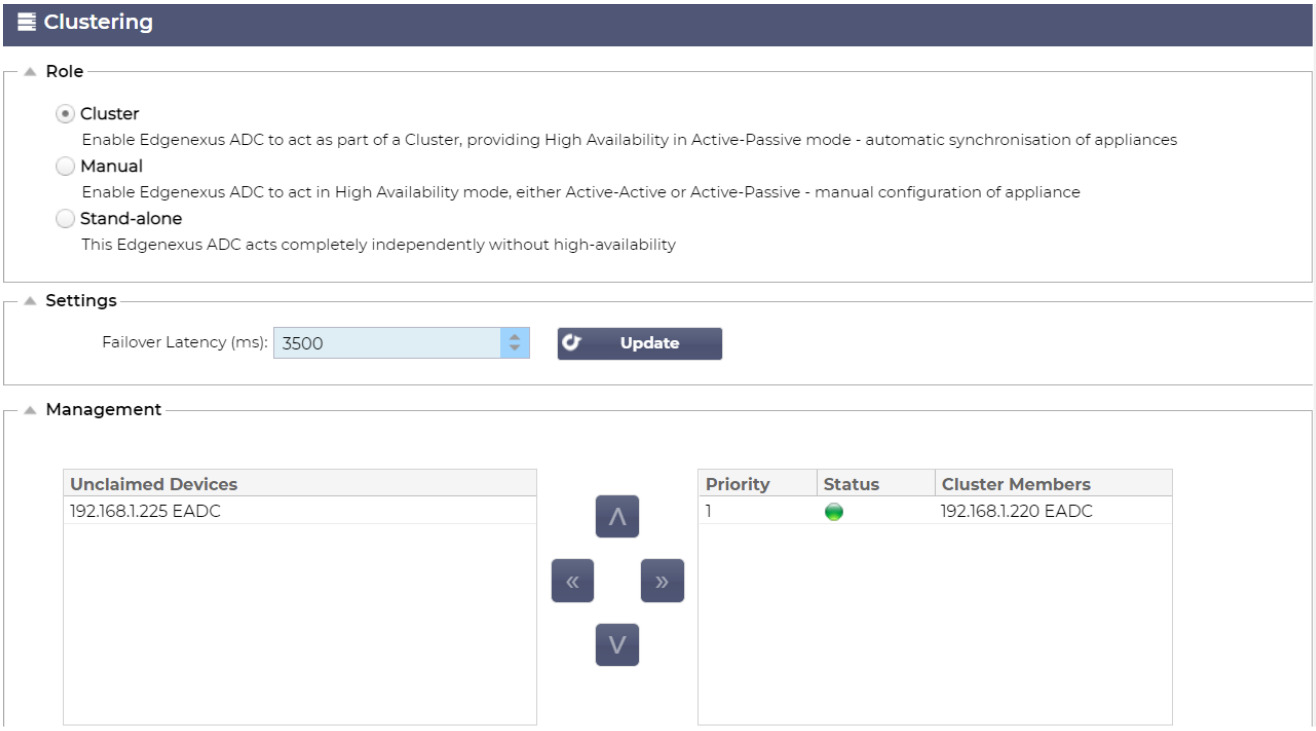
There are a variety of cookie-based persistence methods that will all work well. The most commonly used cookie-based method is Persistence Cookie.

The following pages will take you through the VIP configuration. Please take care to configure correctly to avoid issues in operations.

Clustering the EdgeADC

The EdgeADC can operate as a stand-alone appliance, and it is incredibly reliable. However, in terms of best practice, we must accept that it is as critical as the servers it is load balancing, and we would therefore recommend placing it in a cluster.

- First, stand up a second EdgeADC in the same subnet as the primary.
- Once you have licensed it logon to your Primary EdgeADC
- Proceed to System > Clustering
- You should see the page as below.



Clustering

Role

● Cluster
Enable Edgenexus ADC to act as part of a Cluster, providing High Availability in Active-Passive mode - automatic synchronisation of appliances

○ Manual
Enable Edgenexus ADC to act in High Availability mode, either Active-Active or Active-Passive - manual configuration of appliance

○ Stand-alone
This Edgenexus ADC acts completely independently without high-availability

Settings

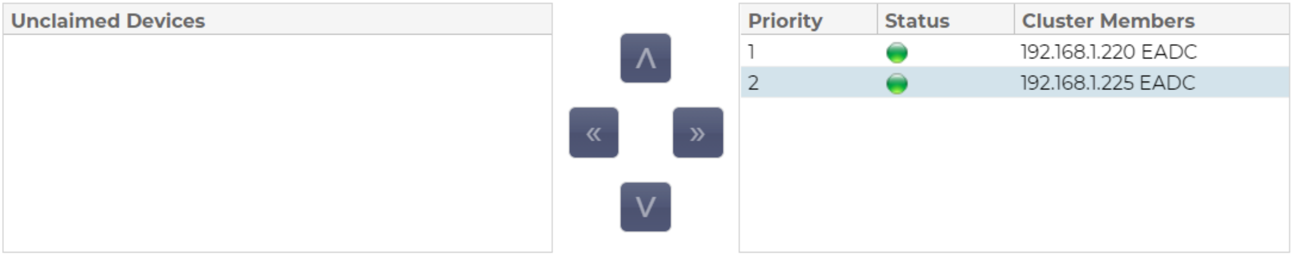
Failover Latency (ms): 3500

Management

Unclaimed Devices
192.168.1.225 EADC

Priority	Status	Cluster Members
1	●	192.168.1.220 EADC

- You will notice that there are two panels within the Management panel. On the left is the Unclaimed panel. On the right is the Cluster showing the cluster members, their priority, and status.
- In between the two panels is a cluster of arrow buttons.
- Click on the EdgeADC that is in the Unclaimed Panel and click the RIGHT arrow button.
- This action moved the unclaimed EdgeADC into the cluster.
- Immediately it is moved across; the Primary will replicate its settings, including VIPs to the secondary. Note that any apps you have added to the Primary will not be replicated to the Secondary – examples are WAF, GSLB, etc.
- After clustering, the Management panel should look like the one below.

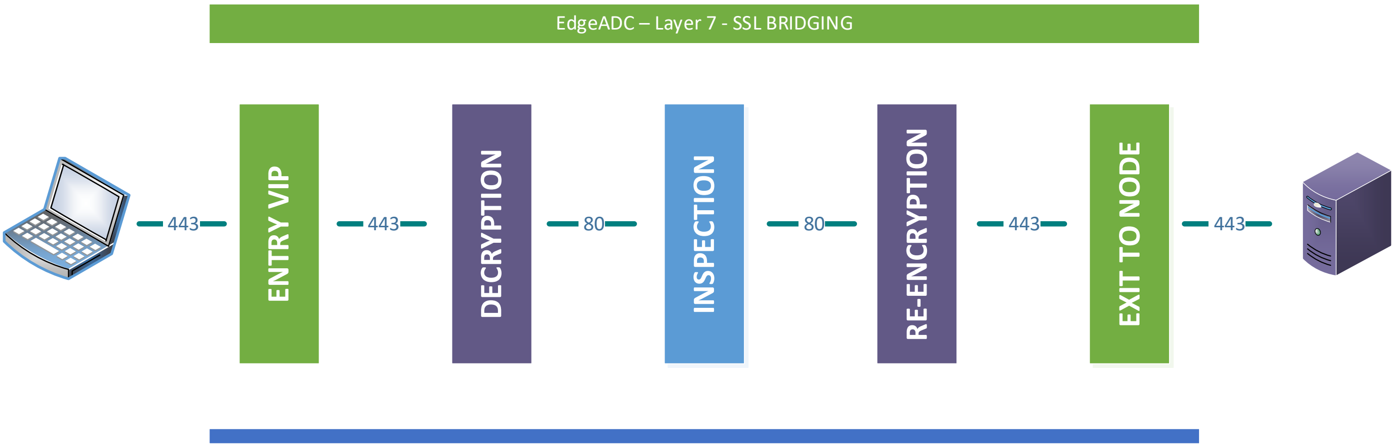


Unclaimed Devices

Priority	Status	Cluster Members
1	●	192.168.1.220 EADC
2	●	192.168.1.225 EADC

VIP – L7 SSL Re-encryption

The method being used here is SSL Bridging. In this method, the SSL traffic enters the ADC, is then terminated internally, any inspection required is carried out, and the traffic is then re-encrypted and sent to the nodes. An SSL certificate is required to be present on the ADC for this mode to work.



- The first step is to create the VIP and initial VS
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row to add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	443	*Oracle EBS*	HTTP

- Click Update

Now we will define the Real Servers (RS) section.

- The cursor will automatically be taken to a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples we have provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.201	443	100	100	EBS Node 1	

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.202	443	100	100	EBS Node 2	

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.203	443	100	100	EBS Node 3	

- Click Update to save.

You can add a name for the server group if you wish.

We have now defined our first VIP, and its two connected Real Server nodes. We have to do some more work yet to do.

Basic Tab

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Persistent Cookie
Server Monitoring	TCP Connect, 200 OK
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	Your SSL certificate

- Click Update when done.

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

Advanced Tab

There are no configurations to be done within the Advanced tab.

- Click the Advanced tab within the Real Servers section.
- Make changes as follows:

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Checked
Client SSL Resumption	Checked
SNI Default Certificate	None
Security Log	On
Connection Timeout (sec)	600
Monitoring Interval (sec)	10

Monitoring Timeout (sec)	10
Monitoring In Count	2
Monitoring Out Count	3
Switch to Offline on Failure	Unchecked
Max Connections (per RS)	

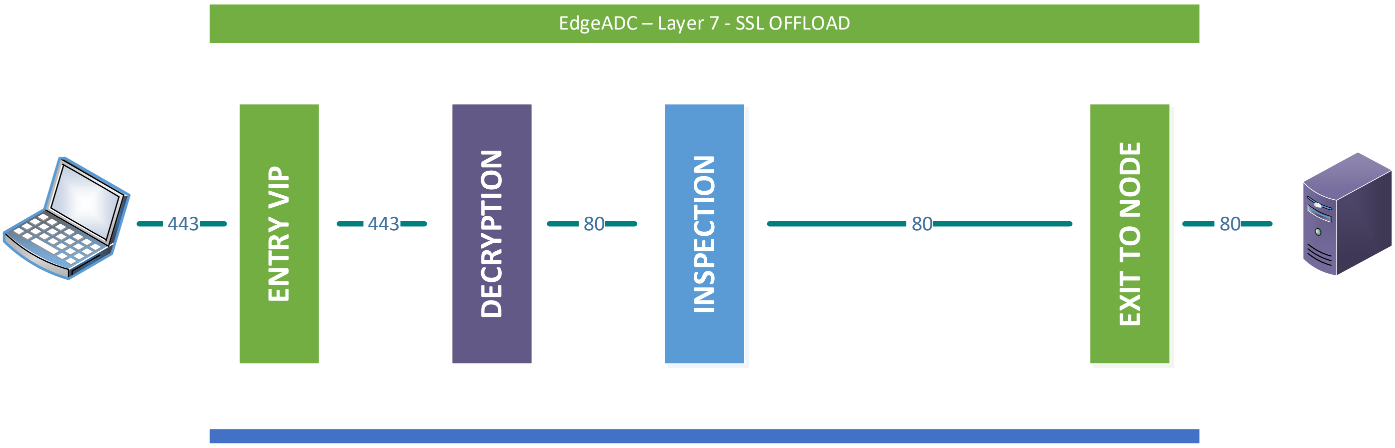
Creating the HTTP Redirector VIP

If your corporate IT rules dictate that all connections must be secure, you must create a redirector VIP. To do this, follow the procedure below:

- Click on the 443 VIP you want redirection to from Port 80
- Click the Copy Service button
- A copy of the service is created, and you will be placed in edit mode.
- Change the port to 80
- Change the Service Name to 80 to 443 Redirector
- Change the Service Type to **HTTP**, if different, and click Update
- Now go to the flightPATH tab in the Real Servers section.
- Select Force HTTPS and click the Right-Arrow button in the central cluster.
- The flightPATH rule is now activated, and all traffic entering the VIP on port 80 will be switched to use port 443.

VIP – L7 SSL Offload

Traffic enters the ADC as Layer 7 HTTPS and is subsequently decrypted. Once done, the traffic can then be inspected and sent onto the servers using Port 80. An SSL certificate is required to be present on the ADC. An SSL certificate is required to be present on the ADC.



- The first step is to create the VIP and initial VS
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row to add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	443	*Oracle EBS*	HTTP

- Click Update

Now we will define the Real Servers (RS) section.

- The cursor will automatically be taken to a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples we have provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.201	80	100	100	EBS Node 1	

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.202	80	100	100	EBS Node 2	

- Click Update to save.
- Click the Copy Server button and make changes for the third array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.10.203	80	100	100	EBS Node 2	

- Click Update to save.

You can add a name for the server group if you wish.

We have now defined our first VIP and its connected Real Server nodes. We have to do some more work yet to do.

The Basic Tab

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Persistence
Server Monitoring	TCP Connect, 200 OK
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	None

The above configuration will ensure SSL termination/offload.

- Click Update when done.

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

The Advanced Tab

There are no configurations to be done within the Advanced tab.

- Click on the Advanced tab within the Real Servers section.
- Make changes as follows:

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Checked
Client SSL Resumption	Checked
SNI Default Certificate	None
Security Log	On
Connection Timeout (sec)	600
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10

Monitoring In Count	2
Monitoring Out Count	3
Switch to Offline on Failure	Unchecked
Max Connections (per RS)	

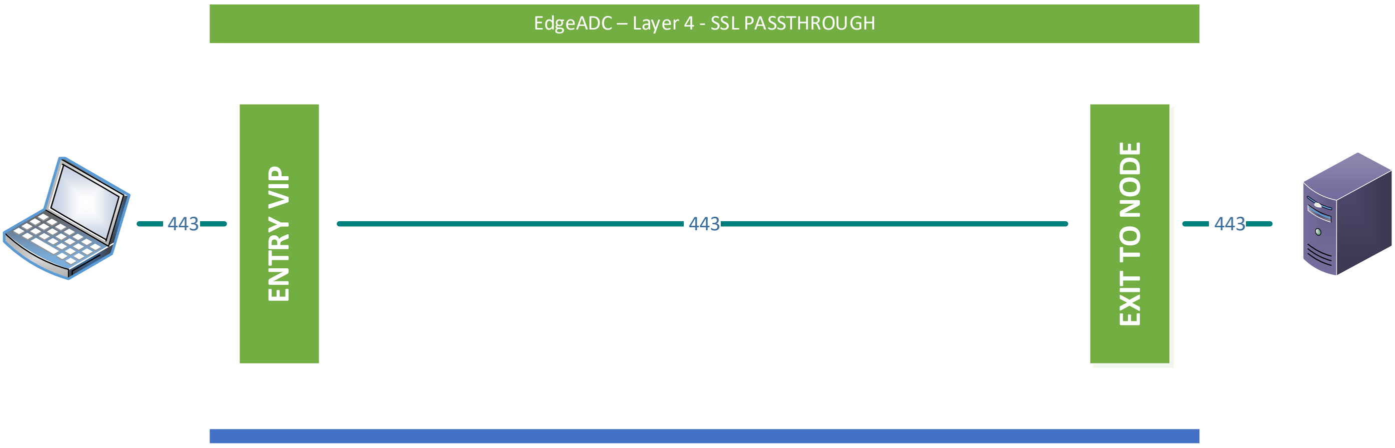
Creating the HTTP Redirector VIP

If your corporate IT rules dictate that all connections must be secure, you must create a redirector VIP. To do this, follow the procedure below:

- Click on the 443 VIP you want redirection to from Port 80
- Click the Copy Service button
- A copy of the service is created, and you will be placed in edit mode.
- Change the port to 80
- Change the Service Name to 80 to 443 Redirector
- Change the Service Type to **HTTP**, if different, and click Update
- Now go to the flightPATH tab in the Real Servers section.
- Select Force HTTPS and click the Right-Arrow button in the central cluster.
- The flightPATH rule is now activated, and all traffic entering the VIP on port 80 will be switched to use port 443.

VIP – L4 TCP / SSL Passthrough

This VIP is Layer 4 TCP and passes the traffic through to the end nodes without decryption or inspection. The advantage of this type of VIP is the speed that it delivers, but the lack of inspection means there is no control over the traffic.



- The first step is to create the VIP and initial VS
- Log into the ADC and go to IP Services. This location should be the default entry point.
- Click Add Service
- You will see an empty row to add values similar to the one below. The field values we provide are examples for your reference.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	443	*Oracle EBS*	Layer 4 TCP

- Click Update

Now we will define the Real Servers (RS) section.

- The cursor will automatically be taken to a ready-created blank entry to aid you in adding the RS entries.
- Please enter the details relevant to your infrastructure following the examples provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.201	443	100	100	EBS Node 1	

- Click Update to save.
- Click the Copy Server button and make changes for the second array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.11.202	443	100	100	EBS Node 2	

- Click Update to save.
- Click the Copy Server button and make changes for the third array node.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.10.203	443	100	100	EBS Node 2	

- Click Update to save.

You can add a name for the server group if you wish.

We have now defined our first VIP and its connected Real Server nodes. We have to do some more work yet to do.

The Basic Tab

- Click on the Basic tab within the Real Servers section.
- Make changes as follows:

Field	Value
Load Balancing Policy	Persistence
Server Monitoring	TCP Connect, 200 OK
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	None
Real Server SSL Cert	None

- Click Update when done.

Note: To add your SSL certificate, please consult the EdgeADC Administration Guide

The Advanced Tab

There are no configurations to be done within the Advanced tab.

- Click on the Advanced tab within the Real Servers section.
- Make changes as follows:

Field	Value
Connectivity	Reverse Proxy
Cipher Options	Defaults
Client SSL Renegotiation	Checked
Client SSL Resumption	Checked
SNI Default Certificate	None
Security Log	On
Connection Timeout (sec)	600
Monitoring Interval (sec)	10
Monitoring Timeout (sec)	10
Monitoring In Count	2

Monitoring Out Count	3
Switch to Offline on Failure	Unchecked
Max Connections (per RS)	

Creating the HTTP Redirector VIP

If your corporate IT rules dictate that all connections must be secure, you must create a redirector VIP. To do this, follow the procedure below:

- Click on the 443 VIP you want redirection to from Port 80
- Click the Copy Service button
- A copy of the service is created, and you will be placed in edit mode.
- Change the port to 80
- Change the Service Name to 80 to 443 Redirector
- Change the Service Type to HTTP, if different, and click Update
- Now go to the flightPATH tab in the Real Servers section.
- Select Force HTTPS and click the Right-Arrow button in the central cluster.
- The flightPATH rule is now activated, and all traffic entering the VIP on port 80 will be switched to use port 443.