



## **FINACLE CORE BANKING**

AN EDGENEXUS ADC DEPLOYMENT GUIDE



## Contents

Document Properties .....	3
Document Disclaimer .....	3
Copyrights .....	3
Trademarks .....	3
Edgenexus Support .....	3
Introduction .....	4
What is Finacle Core Banking? .....	4
Prerequisites for supporting Finacle Core Banking .....	4
Acronyms used .....	5
Sizing and clustering the EdgeADC .....	6
Sizing the EdgeADC .....	6
Clustering the EdgeADC .....	6
Deployment Scenario .....	8
Traffic movement with WAF .....	9
Virtual Service Methods .....	9
VIPs, Ports, and Other Bits .....	9
ADC 01 - VIP - L7 SSL Re-Encryption .....	11
Creating the ingress to the WAF .....	11
Basic Tab .....	11
Creating the HTTP to HTTPS rule .....	12
Creating the VIP for the Finacle Web servers .....	12
Basic Tab .....	13
Advanced Tab .....	13
Creating the HTTP Redirector VIP .....	14
Protecting with flightPATH .....	14
Illustration of ADC 01 VIPs .....	15
ADC 01 - VIP - L4 SSL Passthrough .....	16
Creating the VIP for the Finacle Web servers .....	16
Basic Tab .....	17
Advanced Tab .....	17
Creating the HTTP Redirector VIP .....	17
ADC 02 - VIP - L4 TCP / SSL Passthrough .....	19
The Basic Tab .....	20
The Advanced Tab .....	20
Creating the HTTP Redirector VIP .....	20

How GSLB Works.....	22
Resiliency and disaster recovery.....	22
Load balancing and geo-location .....	22
Commercial considerations.....	23
GSLB Mechanisms.....	23
Domain Name System Overview .....	23
Caching .....	24
Time To Live.....	24

## Document Properties

---

Document Number: 2.0.11.3.21.16.11

Document Creation Date: October 28, 2021

Document Last Edited: November 3, 2021

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: EdgeADC - Version All

## 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

---

© 2021 All rights reserved.

Information in this document is subject to change without prior notice and does not represent a commitment on the manufacturer's part. No part of this guide may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of the manufacturer. Registered trademarks are properties of their respective owners. Every effort is made to make this guide as complete and accurate as possible, but no warranty of fitness is implied. The authors and the publisher shall have neither responsibility nor liability to any person or entity for loss or damages arising from using the information contained in this guide.

## 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](mailto:support@edgenexus.io)

# Introduction

---

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

## What is Finacle Core Banking?

Built on an advanced architecture, Finacle Core Banking Solution offers a comprehensive suite of capabilities to power your banks' digital transformation.

With Finacle Core Banking Solution, your bank will gain a comprehensive set of capabilities, including flexible product factories, extensive parameterization, product bundling, and reusable business components, to help accelerate innovation-led growth.

With its real-time processing engine, open APIs, and embedded customer insights, Finacle delivers one of the most advanced digital banking foundations to engage demanding consumers.

## Prerequisites for supporting Finacle Core Banking

---

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 the level of redundancy and resilience required for mission-critical systems.
- The ADC is fully capable of load-balancing your Finacle Core Banking, and this guide explains how to set this up.
- When exposed to the Internet, we also recommend the use of EdgeWAF to protect the internal systems.

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 Finacle Core Banking 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 Finacle Core Banking should be installed and operational.
- The initial ADC configuration should be done against the Finacle Core Banking 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

VS – Virtual Service  
RSIP – Real Server IP

ADC – Edgenexus EdgeADC

# Sizing and clustering the EdgeADC

## Sizing the EdgeADC

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

In virtualized environments, we recommend that you set the ADC to a minimum specification of 8 vCPU with 16GB RAM, to begin with and scale up if required. You need to assess the number of requests being received and be handled by the Layer 7 load balancing method.

If you are deploying hardware ADCs, we recommend you use the certified hardware from HPE.

In both cases, 50-100GB of disk storage space should be sufficient to take into account logging and WAF data.

If you are in any doubt, please discuss it with our support department.

## 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 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 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):

Management

Unclaimed Devices		Priority	Status	Cluster Members
192.168.1.225 EADC	<input type="button" value="↑"/> <input type="button" value="←"/> <input type="button" value="→"/> <input type="button" value="↓"/>	1	<span style="color: green;">●</span>	192.168.1.220 EADC

- You will notice that there are two panels within the Management panel. On the left is the Unclaimed panel, and 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 Active will not be replicated to the Passive, so you must manually install and configure them on the Passive – examples are WAF, GSLB, etc.
- After clustering, the Management panel should look like the one below.

**Unclaimed Devices**

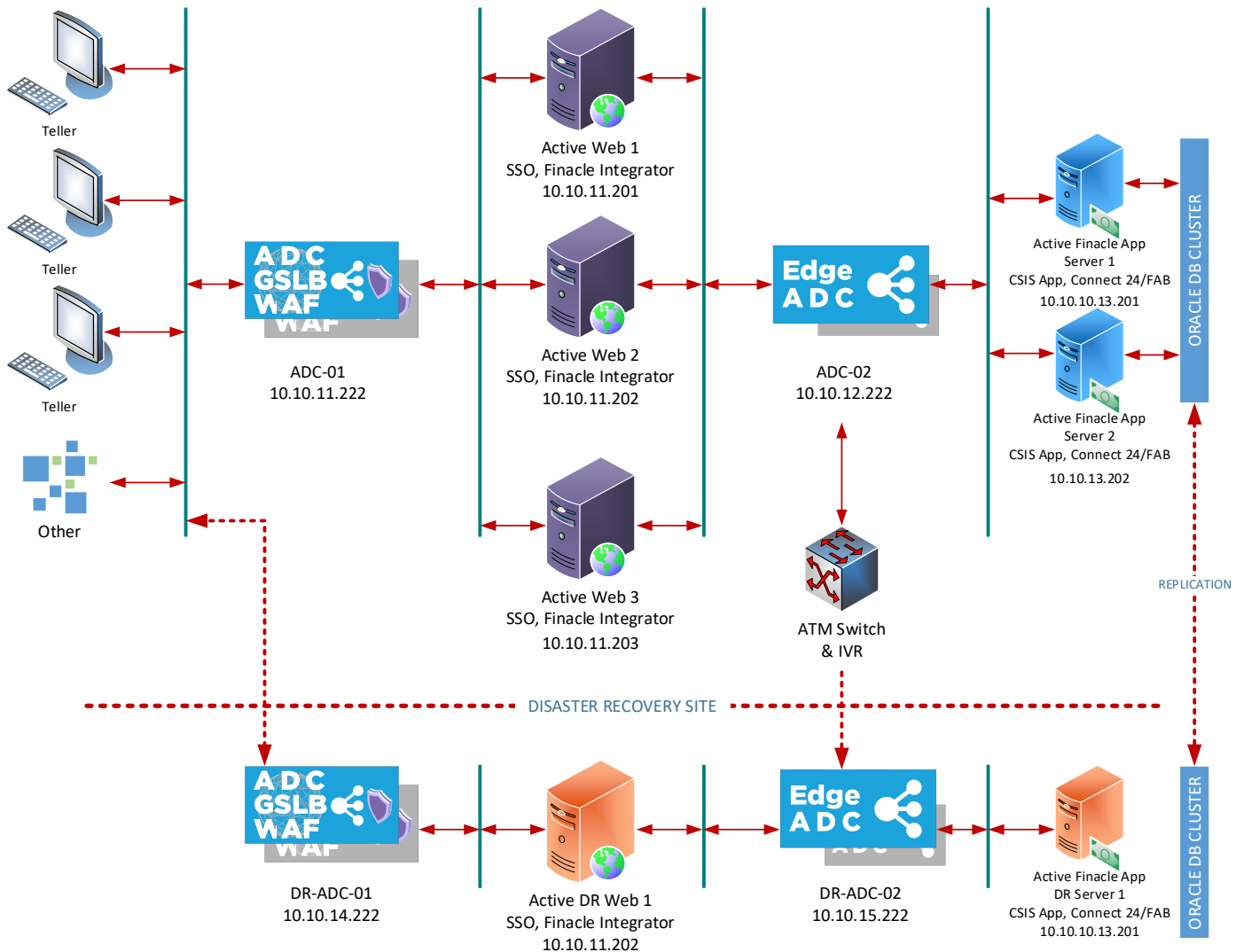


Priority	Status	Cluster Members
1	<span style="color: green;">●</span>	192.168.1.220 EADC
2	<span style="color: green;">●</span>	192.168.1.225 EADC



## Deployment Scenario

Connections to the Finacle Core Banking 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.



At this point, it is required that we explain the layout provided.

- The tellers are located in bank branches, from where they access the Finacle application using their Internet browsers.
- There are two data center tiers shown in the diagram
  - The main central data center
  - The lower level DR data center
- There are two levels of ADC within the central and DR data centers. The first is the main ingress ADC, and in our example, it has been equipped with EdgeWAF and EdgeGSLB add-ons. The ingress ADC-01 is also an ADC cluster pair. The ADC-02 between the Finacle Web and Finacle App servers is not equipped with WAF or GSLB. This ADC operates in Layer 4 TCP mode using SSL Passthrough.

The ATM switch connects directly to the second inner ADC, already part of the secured network.

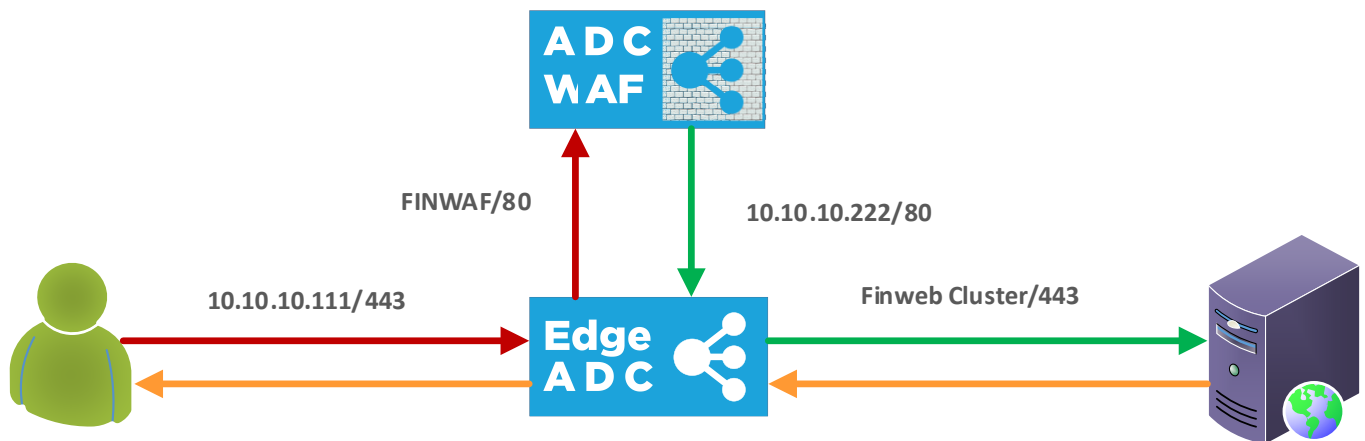
You will also note that there is a WAF and GSLB present. These are options, and you need not use them if you have other solutions in place.

### Traffic movement with WAF

When a WAF is in use, the traffic is directed slightly differently.

Traffic enters the ADC using the main ingress VIP and is sent to the WAF after SSL Offload. Using SSL Offload ensures that the WAF can see the content of the data and recognize attacks.

In EdgeWAF, the exit point is the second VIP that serves the actual Finacle web servers. See the representational diagram below.



### Virtual Service Methods

On advice from Edgeverve, we recommend configuring the ADC for use with Finacle Core Banking using SSL re-encryption (Layer 7 HTTPS), but you can use any of the following virtual service methods.

<b>SSL Re-Encryption</b>	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, and ADC service type HTTP is used.
<b>SSL Passthrough</b>	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.

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

### VIPs, Ports, and Other Bits

When load balancing Finacle Core Banking, the following VIPs will be needed for operations.

Port	Protocol	Service Type	Explanation
------	----------	--------------	-------------

---

443	TCP	Layer 4-TCP	This Port handles all HTTPS requests from client applications and sends them to the next stage with no intervention. Best suited for the second ADC if it is used.
443	TCP	Layer 7 HTTP	This Port handles all HTTPS requests from client applications where the traffic is offloaded internally and can then be examined using flightPATH before being re-encrypted and sent to the next stage. This method is useful when you want to examine and filter traffic entering through the main ingress point.

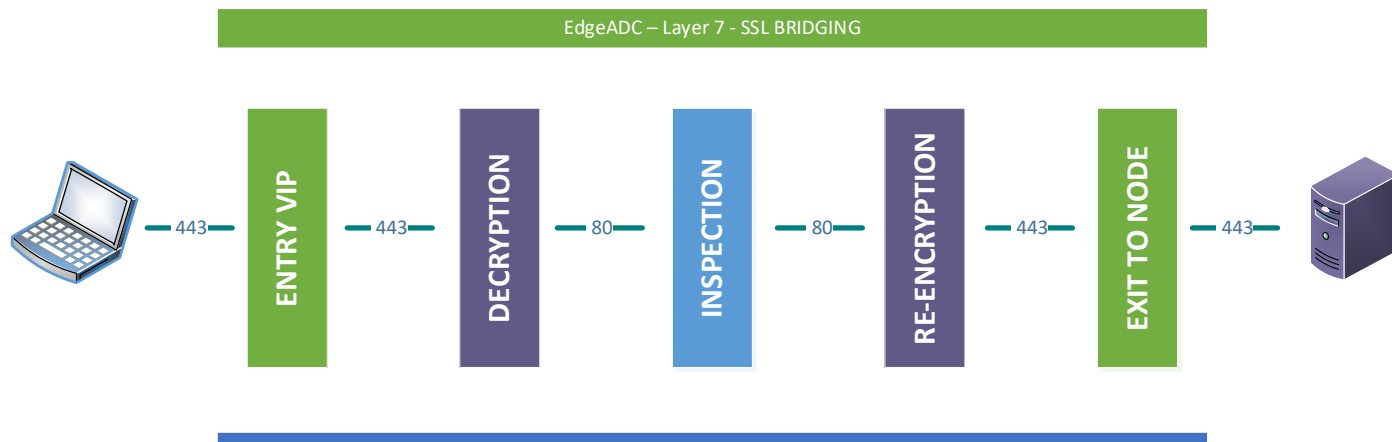
---

***IMPORTANT:** When using the EdgeWAF web application firewall, you will need to offload the SSL traffic to the WAF module and create a secondary VIP to accept the traffic sent from the WAF and then re-encrypt that to the next stage.*

---

## ADC 01 - VIP - L7 SSL Re-Encryption

The method being used here is SSL Bridging. In this method, the SSL traffic enters the ADC, is 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.



### Creating the ingress to the WAF

If you are not using the WAF module, please proceed to Creating the VIP for the Finacle Web servers

- The first step is to create the VIP (10.10.10.111) and initial VS that will point to the WAF.
- We will also create the VIP that will handle traffic from the WAF to the Real Servers.
- Log into the ADC and go to IP Services. This location should be the default ingress point.
- Click Add Service
- You will see an empty row into which you will 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
10.10.10.111	255.255.255.0	443	Ingress to WAF	HTTP

- Click Update

Now we need to define the Real Server entry for the WAF. The name we have given our WAF is Finwaf and **must** use this instead of the IP address.

Address	Port	Weight	Calculated Weight	Notes	ID
finwaf	80	100	100	FinWAF	

Now, we need to define the VIP for access to the Finacle web server cluster.

### Basic Tab

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

Field	Value
Load Balancing Policy	Least connections
Server Monitoring	TCP Connect
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	Your SSL certificate
Real Server SSL Cert	None

- Click Update when done.

### Creating the HTTP to HTTPS rule

When connections come into the ADC, we need to force them to use HTTPS. To do this, we need to add a secondary VS (virtual service) and a flightPATH rule.

- Select the VIP we created earlier (10.10.10.111 – Ingress to WAF).
- Click the Copy Service button to duplicate the rule
- Change the Port from 443 to 80, and a description such as HTTP-HTTPS
- Click Update to add the VS.
- From the Real Servers section, select the flightPATH tab.
- Select the Force HTTPS flightPATH rule and drag it to the right side.
- The rule is now activated.

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

### Creating the VIP for the Finacle Web servers

Go back to the Virtual Services section, and click Add Service. Fill in the details as required.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	80	WAF to FinWeb	HTTP

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	Finacle Web 01	
10.10.11.202	443	100	100	Finacle Web 02	
10.10.11.203	443	100	100	Finacle Web 03	

- Click the Copy Server button to copy the current row to a new one. The copy server function will save you time retyping data.
- 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, 2000K
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	No SSL
Real Server SSL Cert	Any

- 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.

## Protecting with flightPATH

You may wish to protect the system from unwanted access by utilizing flightPATH. An example of this may be:

In this example, we will restrict access to the primary ADC01 load balancer by using flightPATH. We will assume that the network for the tellers is 172.16.100.0, and their IP addresses are in the range 172.16.100.1 to 172.16.100.50, and we want to limit access only from this network/range and drop any other access requests.

These are the elements in flightPATH that we need to set:

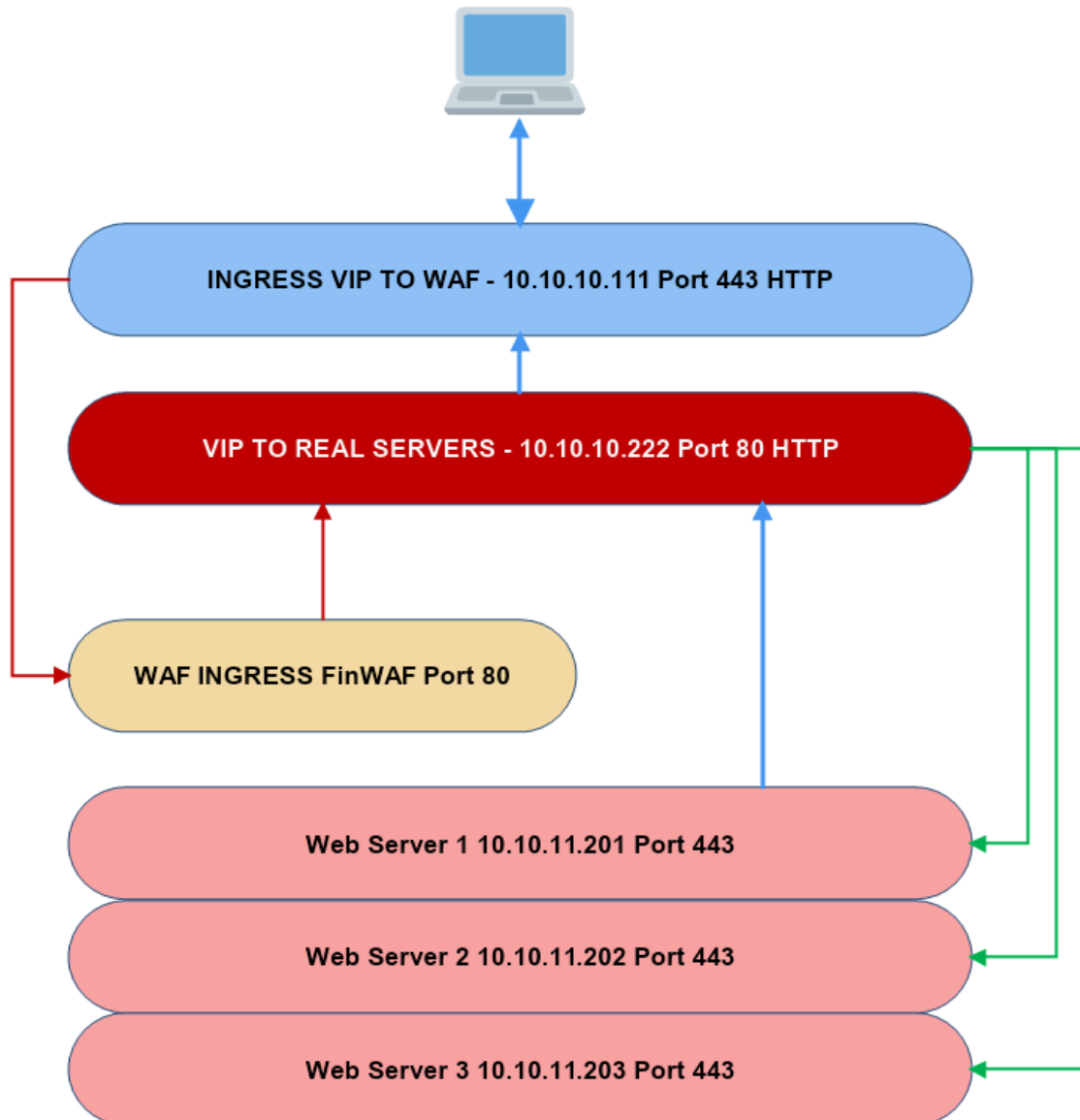
1. The name of the rule
2. The Condition value
3. The Action

The following steps outline this flightPATH rule:

Item	Description
FlightPATH Name	Fill in with a name and a description, so others know what the rule does.
Condition	Condition=SourceIP Sense=Doesn't Check=Equal Value= ^172\16\100\.[1-9][1-4]\d 50)\$
Action	Drop

## Illustration of ADC 01 VIPs

Below, you will find an illustration of the data flow within ADC 01. The diagram shows how data enters the ADC using Ingress VIP 10.10.10.111 and proceeds to the WAF before returning to a secondary VIP and proceeding to the Real Servers.

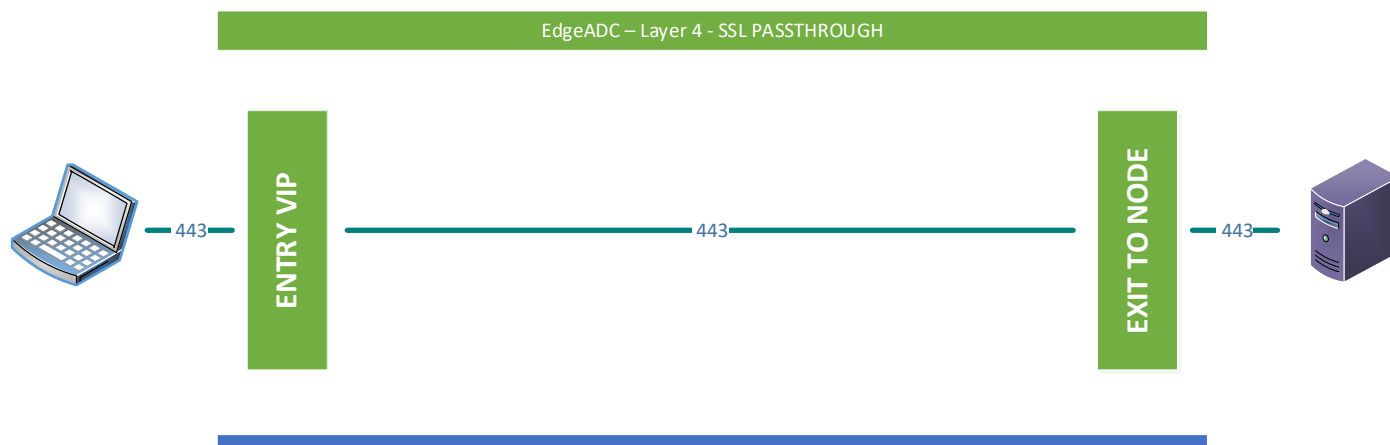




## ADC 01 - VIP - L4 SSL Passthrough

As an alternative, you could use SSL Passthrough, using Layer 4. The advantage of doing this is the speed, as no SSL operations are performed. The disadvantage is that you will not be able to utilize WAF or flightPATH traffic management.

The VIP is Layer 4 TCP and passes the traffic 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.



### Creating the VIP for the Finacle Web servers

Go back to the Virtual Services section, and click Add Service. Fill in the details as required.

IP Address	Subnet Mask	Port	Service Name	Service Type
10.10.10.222	255.255.255.0	443	Ingress to FinWeb	Layer 4 TCP

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	Finacle Web 01	
10.10.11.202	443	100	100	Finacle Web 02	
10.10.11.203	443	100	100	Finacle Web 03	

- Click the Copy Server button to copy the current row to a new one. The copy server function will save you time retyping data.
- 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, 2000K
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	No SSL
Real Server SSL Cert	No SSL

- 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

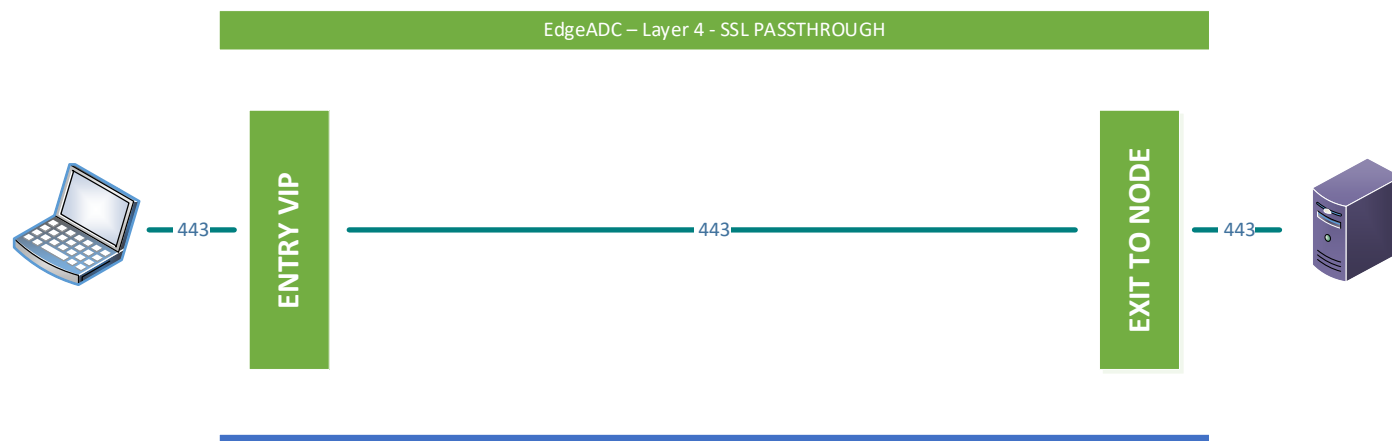
If your corporate IT rules dictate that all connections must be secure, you must create a redirector VIP. To do this, follow the procedure below:

- 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.

## ADC 02 - 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 into which you will 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
10.10.12.222	255.255.255.0	443	Finacle App	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 we have provided below. In our case, we have three array nodes, but you may have more.

Address	Port	Weight	Calculated Weight	Notes	ID
10.10.13.201	443	100	100	Finacle App 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
10.10.13.202	443	100	100	Finacle App 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	Persistent Cookie
Server Monitoring	TCP Connect, 2000K
Caching Strategy	Off
Acceleration	Compression
Virtual Service SSL Cert	None
Real Server SSL Cert	None

- Click Update when done.

## 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)	

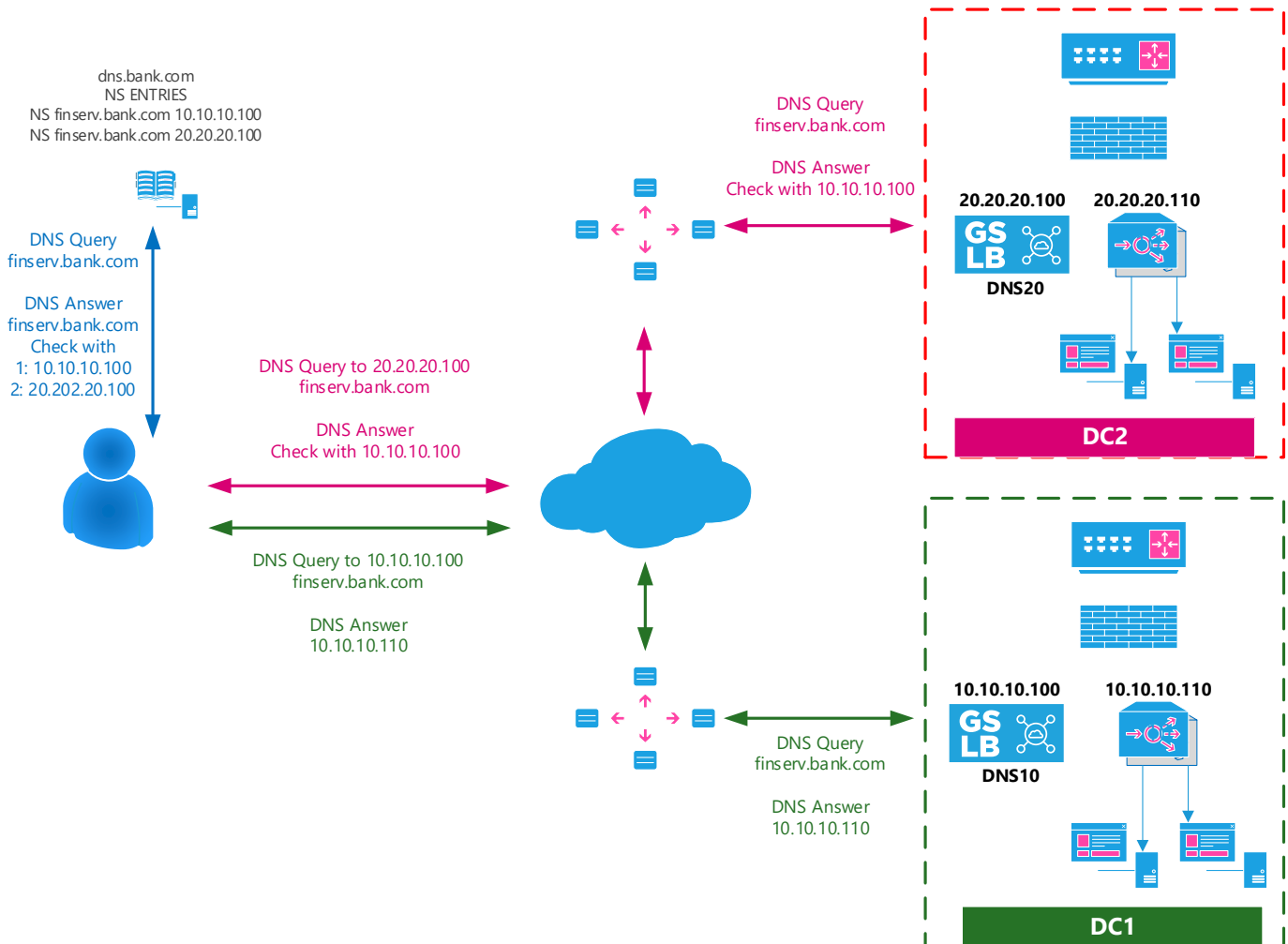
## Creating the HTTP Redirector VIP

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.

## How GSLB Works

Global Server Load Balancing (GSLB) is a term used to describe distributing network traffic around the Internet or MPLS WANs. GSLB is different from Server Load Balancing (SLB) or Application Load Balancing (ALB), as it's typically used to distribute traffic between multiple data centers, whereas a traditional ADC/SLB is used to distribute traffic within a single data center.



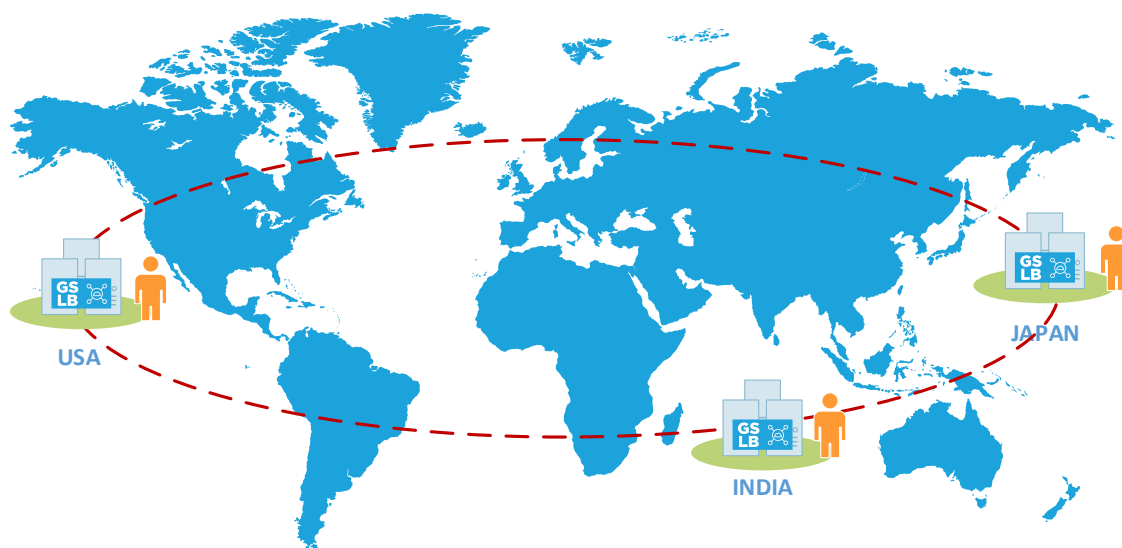
GSLB is typically used in the following situations:

### Resiliency and disaster recovery

You have multiple data centers, and you wish to run them in an Active-Passive situation so that if one data center fails, traffic will be sent to the other.

### Load balancing and geo-location

You would like to distribute traffic between data centers in an Active-Active situation based on specific criteria such as data center performance, data center capability, data center health check, and the Client's physical location (so you can send them to their closest data center), etc.



## Commercial considerations

Ensure users from specific geographic locations are sent to particular data centers. Ensure different content is served (or blocked) to other users, depending on several criteria such as the Client's country, the resource they are requesting, the language, etc.

## GSLB Mechanisms

GSLB is based on DNS.

The ADC can change the response based on several factors described later in the guide. The ADC uses the monitors to check for the availability of remote resources by accessing the resource itself. However, to apply any logic, the system must first receive the DNS request.

Several designs allow this.

The first is where the GSLB acts as the authoritative nameserver.

The second design is the most common implementation and is similar to the authoritative nameserver configuration but uses a sub-domain. The primary authoritative DNS server is not replaced by GSLB but delegates a sub-domain for resolution. Either directly delegating names or using CNAMEs allows you to control what is and is not handled by the GSLB. In this case, you don't have to route all the DNS traffic to the GSLB for systems that don't require GSLB.

Redundancy is provided so that if one nameserver (GSLB) fails, the remote nameserver automatically issues another request to another GSLB, preventing the site from going down.

## Domain Name System Overview

GSLB can be complex; thus, it is worth spending the time to understand how the mysterious Domain Name Server (DNS) system works.

DNS consists of three key components:

- The DNS resolver, i.e., the Client, is responsible for initiating the queries that ultimately lead to a full resolution of the resource required.
- Nameserver: this is the nameserver that the Client initially connects to perform DNS resolution.



- Authoritative Name Servers: Include the Top Level Domain (TLD) nameservers and root nameservers.

A typical DNS transaction is explained below:

- The user types in `https://finserv.bank.com` into their Internet browser.
- The Client resolver requests the `bank.com` DNS server that has been specified in the Client device for the IP address of `finserv.bank.com`.
- In the `bank.com` DNS server, two NS entries show that other authoritative DNS servers handle all records for the subdomain `finserv.bank.com`.
- In our example, these are `10.10.10.100` (DNS10) and `20.20.20.100` (DNS20).
- The `bank.com` DNS responds to the query by sending this information to the Client's resolver.
- The Client then asks the nameservers DNS10 and DNS20 for the IP address of `finserv.bank.com`. It does this using a Round Robin method.
- If we assume that both data centers are running, the DNS10 the GSLB will respond with the correct IP address of `10.10.10.110`. When DS20 is asked, the GSLB will respond, stating that DSN10 holds this information. As a result, the request will be routed to DNS10 that then answers with `10.10.10.110`.
- If, for example, data center DC1 went down, or some of the services handled by the ADC were not healthy, the GSLB will route automatically to DC2.
- The browser makes an HTTP request to the IP address provided by the GSLB.
- The server at that IP returns the webpage to be rendered in the browser.

This process can be further complicated:

## Caching

Resolving nameservers cache responses can send the same response to many clients. Client-side resolvers and applications may have different caching policies.

Note: For testing, we recommend you stop and disable the Windows DNS Client within the services section of your operating system. The DNS names will continue to be resolved; however, it will not cache the results or register the computer's name. Your system administrator will need to decide if this is the best option for your environment, as it may affect other services.

## Time To Live

The resolving name server may ignore the Time To Live (TTL), i.e., the caching time for the response.