

Anypoint Virtual Private Cloud, Dedicated Load Balancer and Virtual Private Network





About Author

Jitendra Bafna is a Senior MuleSoft Solution Architect. He is a MuleSoft Integration and Platform certified architect. Expertise in integrating SaaS applications like Salesforce, NetSuite, Snowflake and other applications like databases, SMTP, Web Services and rest-based APIs.

Having good experience in the MuleSoft platform setup and catalyst launch with VPC, VPN and Dedicated load balancer configurations. Expert in API Led connectivity and SEDA architecture with digitalization and open banking experience.

Expertise in EKS/RTF architecture, API Security, API Governance, API Platform etc.

Jitendra is also holding few MuleSoft Credentials.

- ❖ MuleSoft Ambassador
- ❖ MuleSoft Delivery Champion
- ❖ MuleSoft Go To Market Champion
- ❖ MuleSoft Industry Champion
- ❖ MuleSoft Surat, Nashik and Engineering Student Meetup Group

What is Anypoint Virtual Private Cloud?

VPC stands for Virtual Private Cloud, and it allows you to create logical or isolated networks in the cloud where you can deploy or run the resources securely. MuleSoft CloudHub is a multi-tenant integration platform as a service. Anypoint VPC allows you to create an isolated network where you can host the workers or mule applications.

Anypoint VPC allows you to extend your corporate network and allows CloudHub workers to connect resources behind the firewalls. VPC allows to connect CloudHub workers to on premise datacenter using below techniques

- Secure VPN Tunnel (IPsec Tunneling)
- Private AWS using VPC Peering
- AWS Direct Connect
- Transit Gateway Attachments

Anypoint Virtual Private Cloud – Advantages and Characteristics

Advantages

- Create a secure virtual network within CloudHub.
- Connect CloudHub to assets behind the firewall.
- Deploy mule runtime securely.
- Connect CloudHub to any public cloud or on-premises data center securely.

Characteristics

- Multiple VPC can be created in the same region.
- Always create VPC in the same region or near to your datacenter or AWS region (VPC peering).
- All non-prod environments like dev, test, sit can be mapped to non-prod Virtual Private Cloud and production environment to prod Virtual Private Cloud.
- Multiple environments can be mapped to the same VPC's. Always create the VPC in the parent business group and share with sub business groups.

Anypoint Virtual Private Cloud Best Practices



Always create a VPC in the same region or close to your datacenter or AWS region (VPC Peering).



Always choose a higher or appropriate range of CIDR masks because the CIDR mask cannot be updated once VPC is created. To change the CIDR mask, we need to re-create VPC, and it requires downtime for your applications.



Always choose a CIDR mask which does not overlap with your datacenter IP addresses or subnets.



Always create a separate VPC for production and non-production environments.



Always create VPC in parent business groups and share with child business groups.

Setting Up Anypoint Virtual Private Cloud

For setting up VPC, you need to navigate to **Runtime Manager** => **VPC** and Create VPC.

Provide **Name**, **CIDR Block** and select **environments** that need to be part of the VPC (there can be multiple environments mapped to a single VPC). Generally, we can create separate VPC for prod and non-prod environments (Map non prod environments like test, sandbox, UAT to non-prod VPC and production environments to prod VPC). Select the region which is near to your datacenter or AWS region (VPC peering).

Business Groups will be selected by default if your Anypoint Platform has a single business group. For multiple business groups, you can select from drop down and it is best practices to create VPC in the main business group and share with the child business group.



Learn more about VPCs

General Information

Name	vpc1
Region	US East (N. Virginia) ▼
CIDR Block	10.0.0.0/16
Environments	Design x ▼



Anypoint Virtual Private Cloud Firewall Rules

http.port	8081	Accessible from anywhere public internet over HTTP
https.port	8082	Accessible from anywhere public internet over HTTPS
http.private.port	8091	Accessible from anywhere within VPC over HTTP
https.private.port	8092	Accessible from anywhere within VPC over HTTPS

MuleSoft provides four firewall rules by default. You can add more firewall rules as per your requirements.

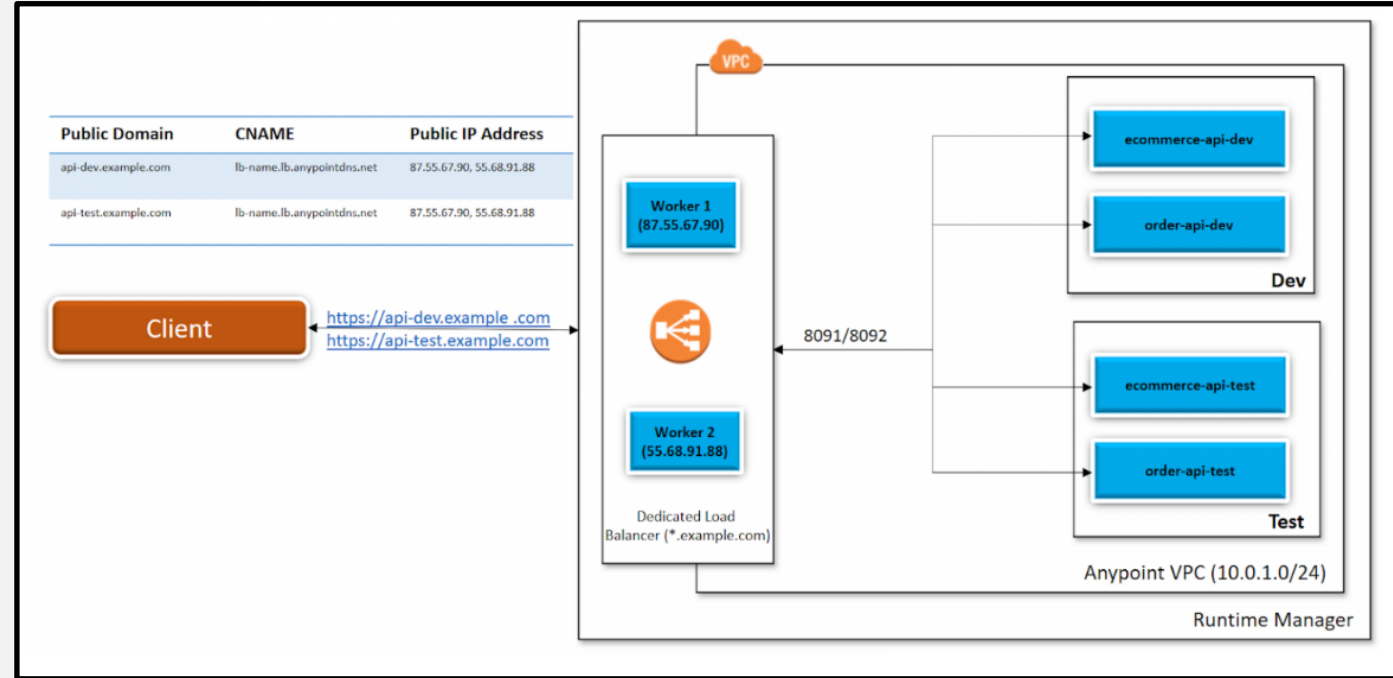
Whenever you deploy an application on port 8091 or 8092, it is accessible within VPC. This means the application cannot be accessible over the internet. To access such applications over the internet, you can create a dedicated load balancer within Virtual Private Cloud, and you can allow applications either to be accessed by everyone or you can whitelist the CIDRs.

What is Anypoint Dedicated Load Balancer?

Dedicated Load Balancer is optional components in Anypoint Platform which allows to route external HTTP/HTTPS traffic to multiple applications deployed to CloudHub within VPC.

Each dedicated load balancer exposes an external CNAME record **lb-name.lb.anypointdns.net** that resolves to the two or more public IP addresses and internal CNAME **internal-lb-name.lb.anypointdns.net**.

Dedicated Load Balancer Architecture



For example, dedicated load balancers created within Anypoint VPC are associated with the dev and test environments. There is a possibility that you can register two external DNS (api-dev.example.com for the dev environment and api-test.example.com for the test environment) that resolve to the same dedicated load balancer public IP addresses. Mapping rules are the attributes of the load balancer SSL endpoints, and they are recognized by certificate common name (CN).



Shared Load Balancer V/S Dedicated Load Balancer

Shared Load Balancer

- Shared Load Balancer available in all environments by default.
- Shared Load Balancer provided basic functionality like TCP load balancing.
- Shared Load Balancer does not allow you to configure custom SSL certificates and proxy rules.
- Shared Load Balancers have lower rate limits, and it is different for each region. Application deployed to CloudHub exceeds the rate limit for shared load balancers, it will return 503 - Service Unavailable.

Dedicated Load Balancer

- One of the limitations of SLB is the lower rate limit. To avoid that issue, you can use a dedicated load balancer.
- All applications can be hosted under a single domain.
- Custom SSL certificates can be configured on DLB, and optionally two-way authentication can be enforced. Handle load balancing among the different CloudHub workers that run your application.

Setting Up Anypoint Dedicated Load Balancer

For setting up a dedicated load balancer, you need to create VPC first and then create a dedicated load balancer within VPC.

HTTP Inbound Mode

- Off: Causes the load balancer to silently drop the request.
- On: Accepts the inbound request on the default SSL endpoint using the HTTP protocol.
- Redirect: Redirects the request to the same URL using the HTTPS protocol.

Other Configurations

- Disable Static IPs specifies to use dynamic IPs, which do not persist when the DLB restarts.
- Keep URL encoding specifies the DLB passes only the %20 and %23 characters as is.
- If you deselect this option, the DLB decodes the encoded part of the request URI before passing it to the CloudHub worker.
- Support TLS 1.0 specifies to support TLS 1.0 between the client and the DLB.
- Upstream TLS 1.2 specifies to force TLS 1.2 between the DLB and the upstream CloudHub worker.

Inbound HTTP Mode ① ☒ Off ☐ On ☐ Redirect

Options ☐ Disable Static IPs

☐ Keep URL encoding ①

☐ Support TLS 1.0 ①

☐ Upstream TLS 1.2 ①

General Configurations

Name

Target VPC US East 1

Workers Every entitlement includes 2 workers

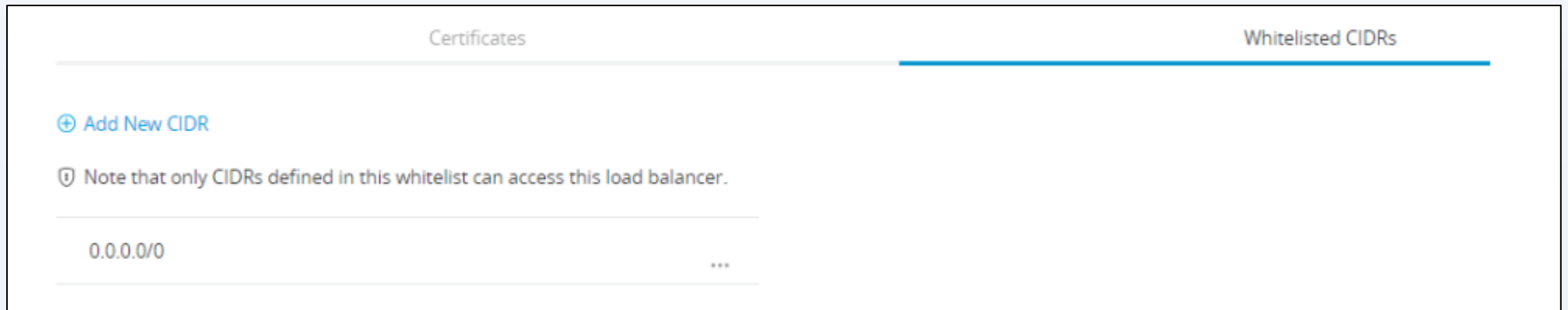
Timeout in Seconds ①



Dedicated Load Balancer Whitelisted CIDRs

To allow dedicated load balancers must be used by a set of IP addresses or single IP addresses, you need to add those IP addresses in the form of CIDR notations (e.g., 192.168.1.0/24).

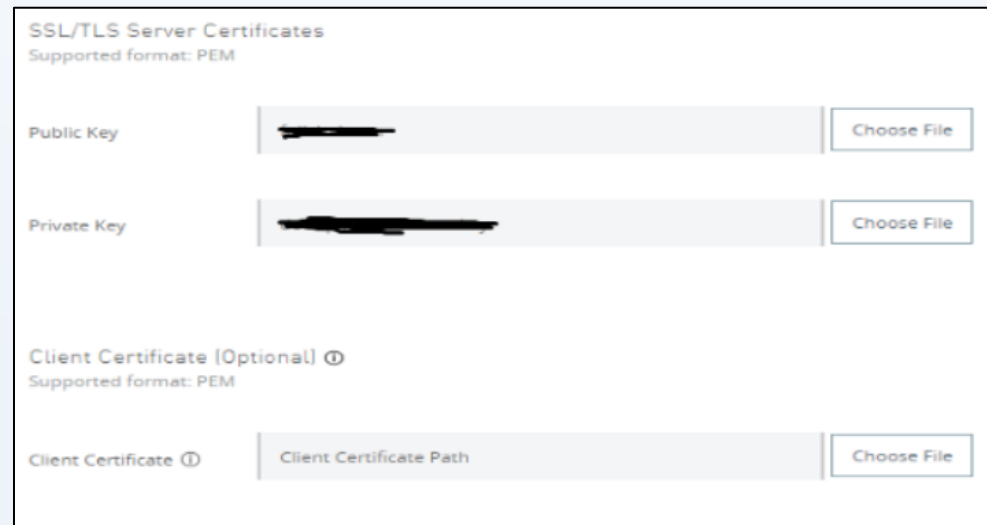
By default, the CIDR mask is 0.0.0.0/0 which means all IP addresses are allowed to access dedicated load balancer.



The screenshot shows a configuration interface with two tabs: 'Certificates' and 'Whitelisted CIDRs'. The 'Whitelisted CIDRs' tab is active, indicated by a blue underline. Below the tabs, there is a blue link '+ Add New CIDR'. A warning icon (a shield with an exclamation mark) is followed by the text 'Note that only CIDRs defined in this whitelist can access this load balancer.' Below this, there is a text input field containing '0.0.0.0/0' and a button with three dots '...'.

Dedicated Load Balancer Certificates

Configure SSL certificate to enable HTTPS (Public Key and Private Key). For two ways authentication, you can configure Client Certificate and that is optional. The dedicated load balancer must be associated with at least a pair of one certificate. Generally, we configure the certificates on Dedicated Load Balancer from CA authority. For testing purposes, you can use self-signed certificates. Dedicated Load Balancer also supports Wildcard certificates.



The screenshot shows a configuration window titled "SSL/TLS Server Certificates" with the subtitle "Supported format: PEM". It contains three sections for file selection:

- Public Key:** A text input field with a redacted value and a "Choose File" button.
- Private Key:** A text input field with a redacted value and a "Choose File" button.
- Client Certificate (Optional):** Indicated by a circled 'O' icon, with the subtitle "Supported format: PEM". It includes a text input field labeled "Client Certificate" with a circled 'I' icon and "Client Certificate Path", and a "Choose File" button.

```
openssl req -newkey rsa:2048 -nodes -keyout test-private.pem -x509 -days 3000 -out test-public-crt.pem
```



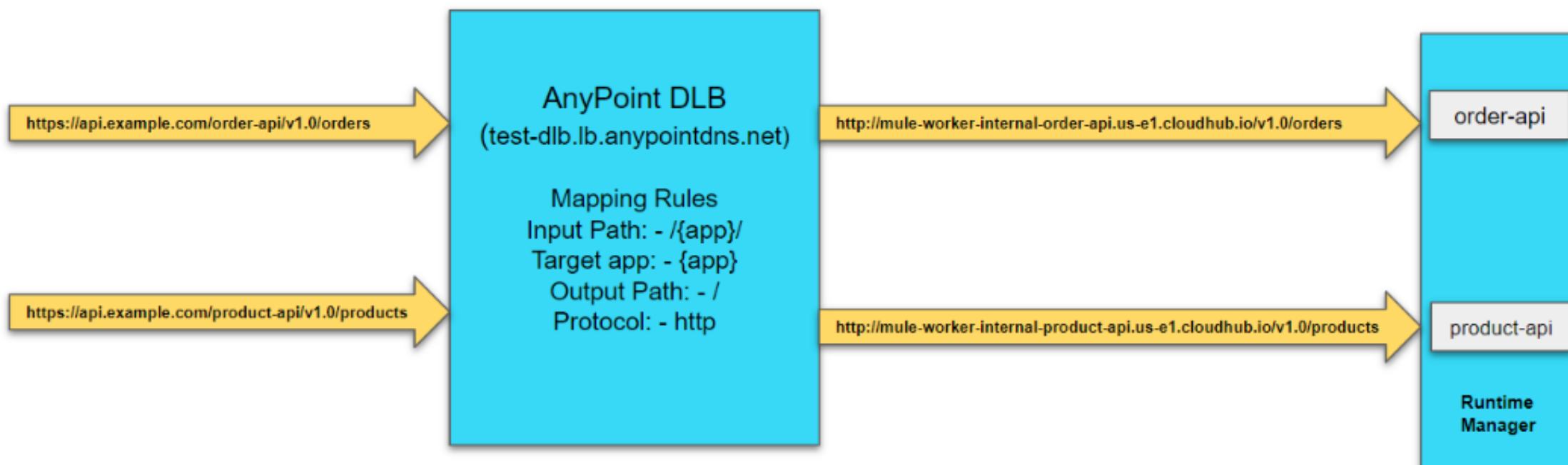
Anypoint Dedicated Load Balancer Mapping Rules

Mapping rules are used on dedicated load balancers to translate input URI to call applications deployed on CloudHub. A pattern is a string that defines a template for matching an input text. Whatever value is placed within curly brackets (`{ }`) is treated as a variable. Variable names can contain only lowercase letters (a-z) and no other characters, including slashes.



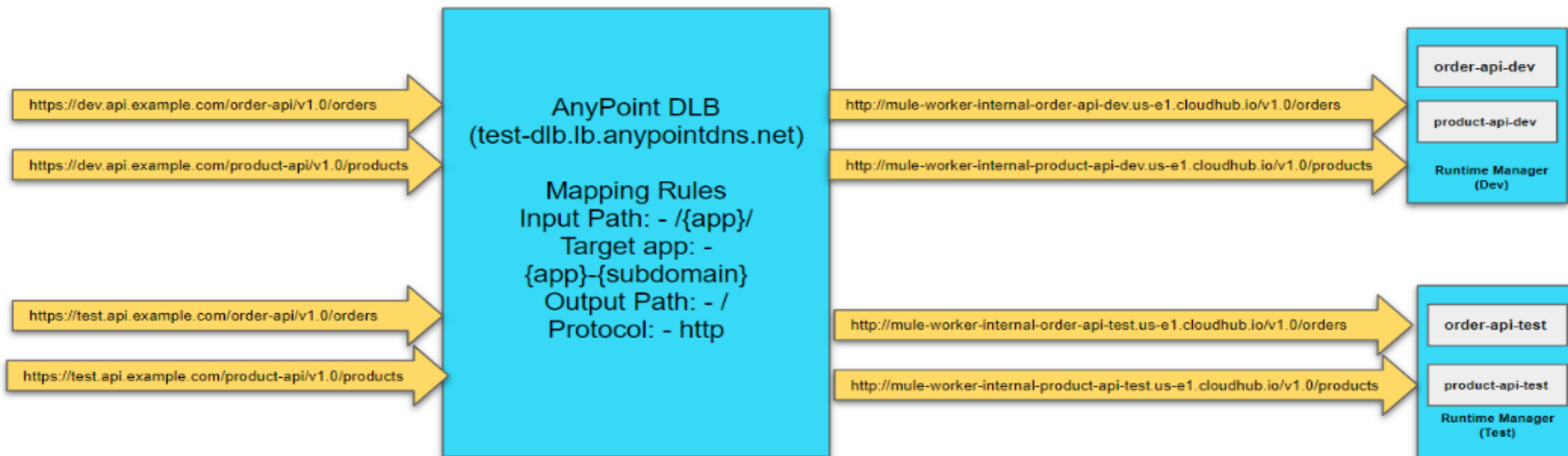
Dedicated Load Balancer Mapping Rules

Input Path	Target App	Output Path	Protocol
<code>/ {app} /</code>	<code>{app}</code>	<code>/</code>	http



Dedicated Load Balancer Mapping Rules

Input Path	Target App	Output Path	Protocol
/ {app}/	org- {app}- {subdomain}	/	http



What is Anypoint Virtual Private Network?

VPN stands for Virtual Private Network and [Anypoint VPN](#) creates a secure connection between CloudHub and On-Premises data centers.

- Anypoint VPN supports site-to-site internet protocol security (IPsec) connections.
- Each Anypoint VPN connection consists of two tunnels that enable you to connect to a single public IP address at a remote location. To connect additional remote locations, create another VPN.
- The physical or software appliances, called VPN endpoints, are terminators on your side of connection.
- The MuleSoft side of the connection is an implementation of a virtual private gateway (VGW). The MuleSoft VGW is associated with a single MuleSoft VPC but can support up to 10 VPN connections.
- The MuleSoft VGW implementation supports a maximum throughput of 1.25 Gbps.

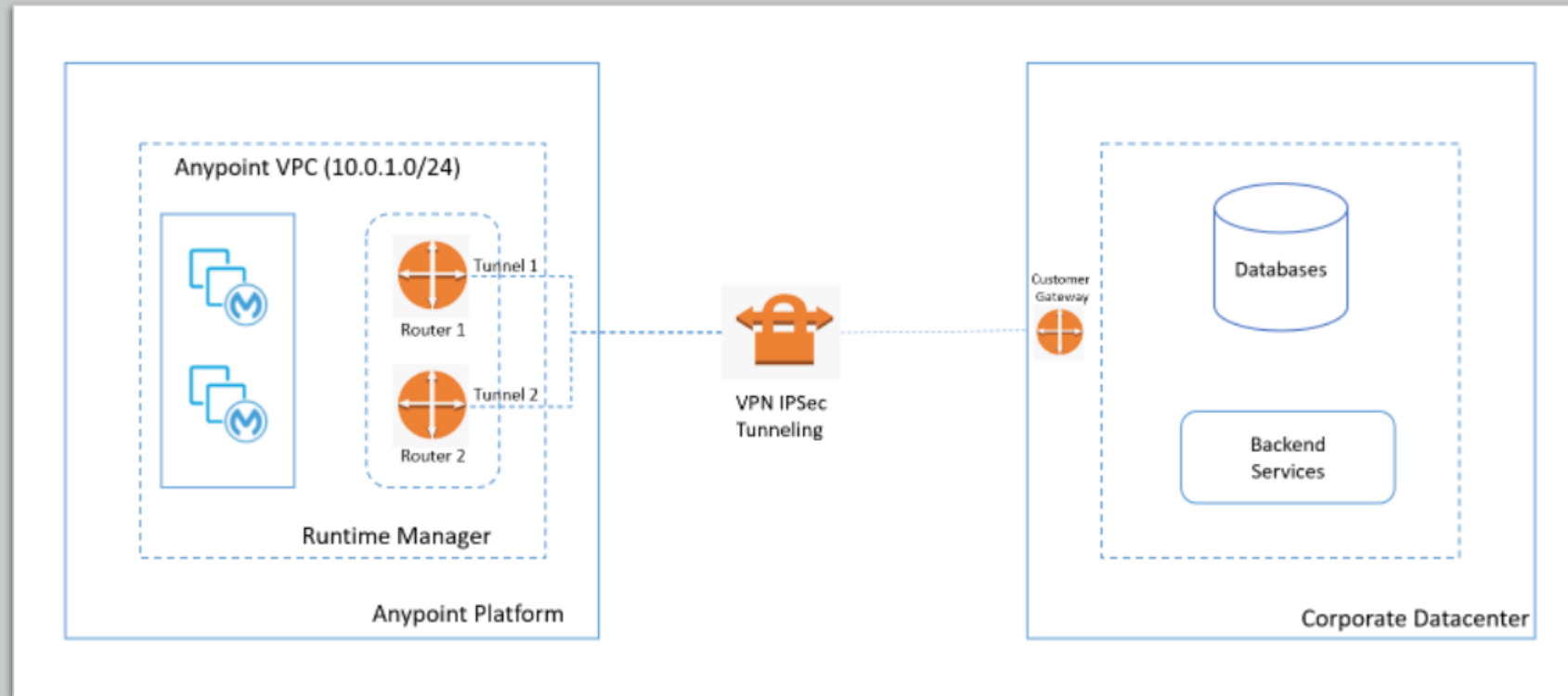


Static Routing	Dynamic Routing (BGP)
Static routing is also known as non-adaptive routing which doesn't change the routing tables unless the administrator modified or updated it manually.	Dynamic routing is also known as adaptive routing as routing tables are updated automatically if any changes happen in the network topology.
Static routing is implemented in smaller networks.	Dynamic is implemented in complex or bigger networks.
Static routing is highly secure.	Dynamic routing is less secure.
Static routing doesn't follow any specific protocols.	Dynamic routing supports BGP, RIP, EIGRP protocols.
Static routing doesn't use any complex routing algorithms to figure out the shortest path.	Dynamic routing uses complex routing algorithms to figure out the shortest path.

Types of VPN Routing

Anypoint VPN supports dynamic or static routing for VPN connections.

- **Dynamic routing** - Your device uses Border Gateway Protocol (BGP) to advertise routes to Anypoint VPN. Use BGP routing if your device supports this protocol.
- **Static routing** - Requires you to specify the routes (subnets) in your network that are accessible through Anypoint VPN.



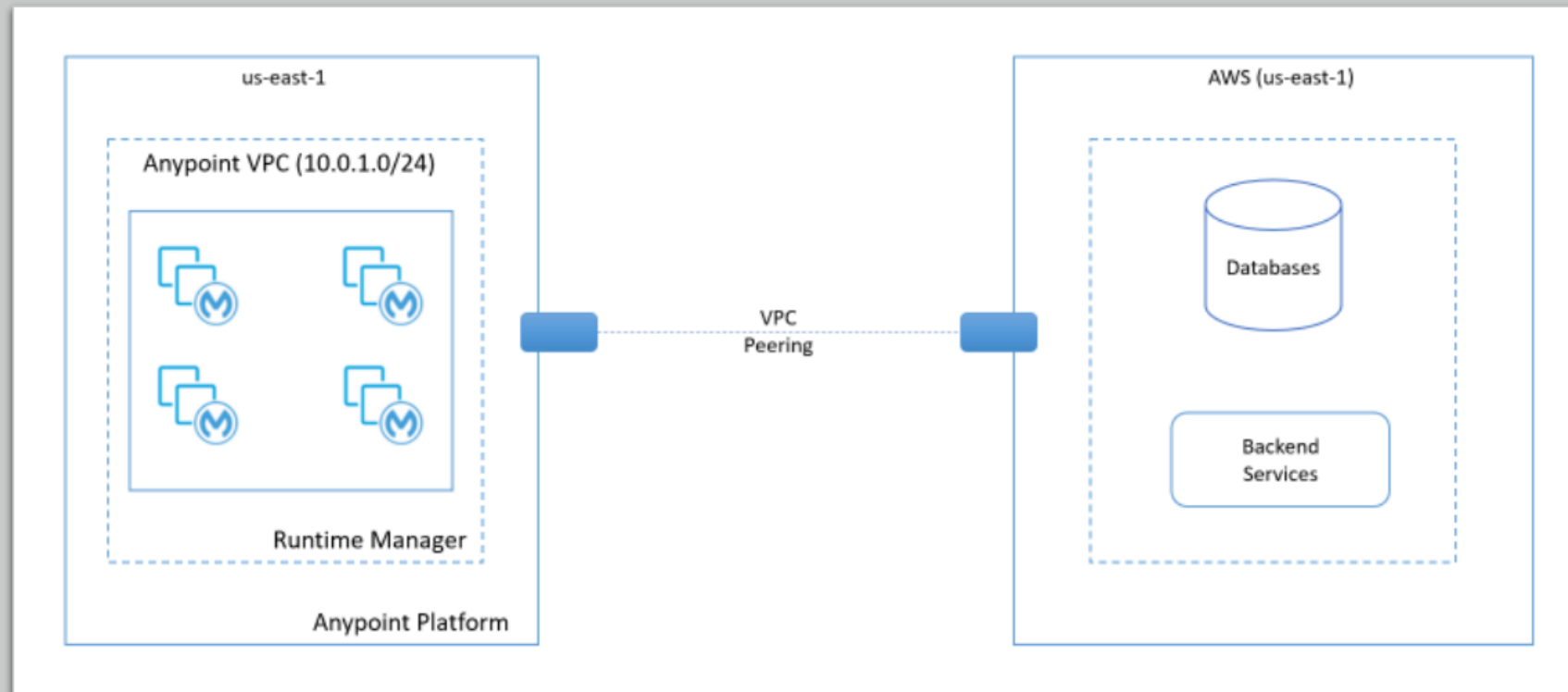
VPN IPsec Tunnelling

VPN IPsec tunnel is set of protocols or standards to establish the connection with on premise datacenter. IPsec tunnel is applied at the IP layer, and it allows to connect the entire network instead of a single device.

VPC Peering

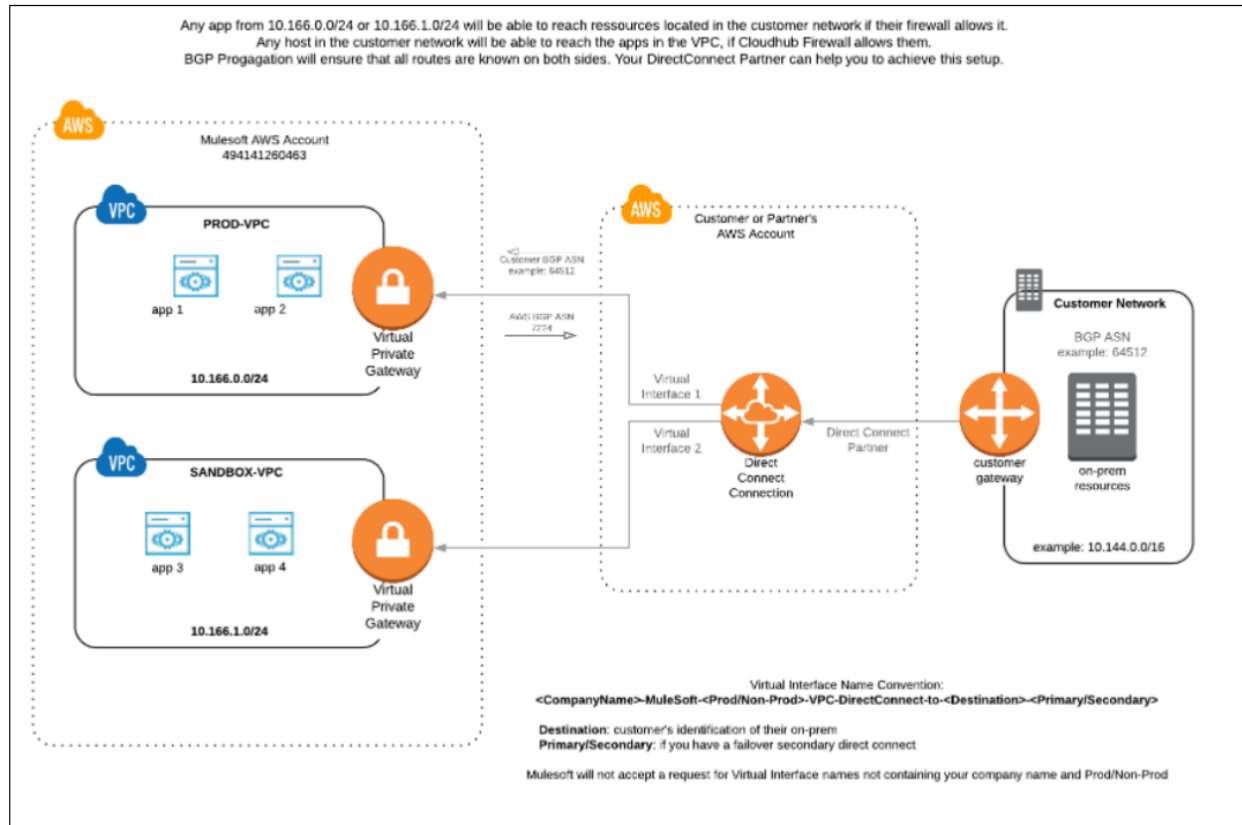
VPC peering connects two VPCs. In this case, it pairs your private Amazon VPC directly to your Anypoint VPC. This enables you to route traffic between the two VPCs so they can communicate as though they are in the same network.

VPC peering can be only done when Anypoint VPC and AWS VPC are in same region.



AWS Direct Connect

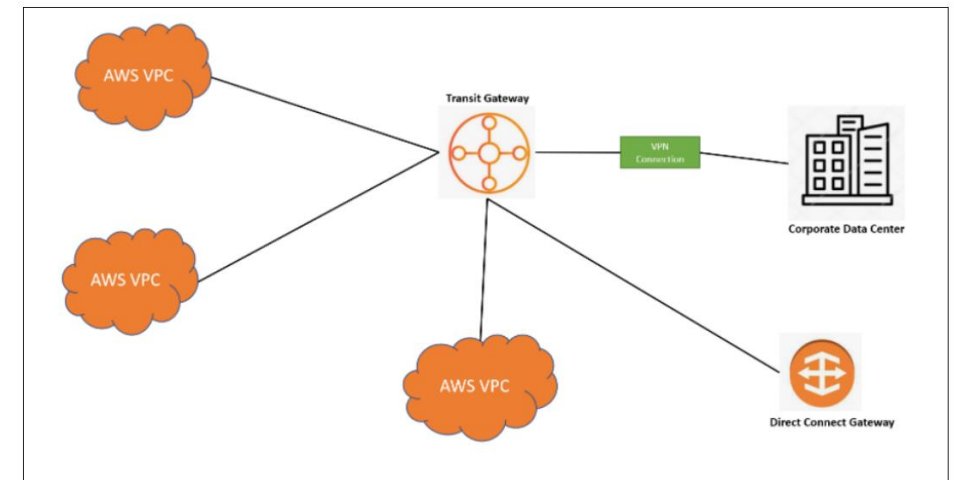
AWS Direct Connect (DX) lets you create a dedicated network connection between your network and one of the DX locations. Once you have established DX connectivity in your own (or your partner's) AWS account, you can establish connectivity with a CloudHub VPC. This article explains which options are available for connecting to a CloudHub VPC via Direct Connect.



Transit Gateway

Transit Gateway acts as a Cloud Router in AWS and simplify the network access between VPC's, on premise data centers and third-party software. It generally merge the on premise and cloud network into single network topology. You can add multiple transit gateway in your Anypoint Organization and that is completely depends on number of the Transit Gateway entitlement with your organizations.

To create Transit Gateway on Anypoint Platform, Anypoint Virtual Private Cloud and AWS Transit Gateway must exists in the same region. One of the main advantage of the Transit Gateway to simplify the network topology and merge all the network (On Premise or Cloud) to act as a single network topology.



Setting Up Anypoint Virtual Private Network



For Setting Up VPN, you navigate to **Runtime Manager** ⇒ **VPN**.

Name: Provide name of VPN

VPC: Select the VPC from the drop-down for which you need to create a VPN.

Remote IP Address: Enter Remote IP Address of your VPN Endpoint or VPN device.

Selecting the routing type Dynamic or Static

Dynamic Routing

Select Dynamic routing in case your VPN device supports BGP.

Enter Remote ASN (64512–65534) and the default is 65001. You can use an existing ASN in your network or a private ASN that is not assigned to your network.

Enter Local ASN (64512-65534) and the default is 64512. Use Private ASN and that should not be assigned to your network. This ASN is for MuleSoft.

A screenshot of the 'Create VPN' form in the Anypoint Platform. The form is titled 'Create VPN' and has a subtitle 'Secure connections to systems in your network hosted outside Anypoint Platform.' It is divided into a 'General Information' section. The form contains the following fields: 'Name' with the value 'my-datacenter-vpn' and a note 'Must be unique and contain alphanumeric characters and hyphens.'; 'VPC' with a dropdown menu showing 'Select VPC' and a note 'Select the VPC for your VPN connection.'; 'Remote IP Address' with the value '0.0.0.0'; 'Routing Type' with radio buttons for 'Static' and 'BGP', where 'BGP' is selected; 'Remote ASN' with the value '65001'; and 'Local ASN' with the value '64512'.

Setting Up Anypoint Virtual Private Network



Select Static routing and enter the CIDR range, that needs to be accessible through the VPN (e.g., 192.168.0.0/22). You can add more CIDR range using Add New Rules in static routes and up to 95 subnets can be added.

Select Tunnel Configuration 1.) Automatic 2.) Custom

In the case of Automatic, no other configuration required, and it will automatically create a tunnel for your Anypoint VPN, and which can be visible after creation. In the case of Custom, you need to provide PSK (8-64 characters) and point-to-point CIDR. You can specify a size /30 CIDR block from the 169.254.0.0/16 range. The CIDR block must be unique across all VPN connections. CIDR block not supported.

- 169.254.0.0/30
- 169.254.1.0/30
- 169.254.2.0/30
- 169.254.3.0/30
- 169.254.4.0/30
- 169.254.5.0/30
- 169.254.169.252/30

← Create VPN

Secure connections to systems in your network hosted outside Anypoint Platform.

General Information

Name
Must be unique and contain alphanumeric characters and hyphens.

VPC
Select the VPC for your VPN connection.

Remote IP Address

Routing Type ☒ Static ☐ BGP

Static Routes [+ Add New Rule](#)

CIDR
...

Local ASN

Setting Up Anypoint Virtual Private Network



Once VPN is created, you can download VPN config and share it with your network administrator to perform configuration on VPN devices.

Status	Tunnel 1/2	Description
Pending	Down/Down	A VPN connection is created and actions pending in the background.
Available	Down/Down	VPN is successfully created but the remote side is not configured.
Available	Up/Up or Up/Down	VPN is successfully created, and remote connection is established in Active/Active mode or Active/Passive mode.
Failed	Down/Down	A VPN connection is not created. You need to delete and try again.

Download VPN Config

Device Vendor:

Device Platform:

Device Software:

Cisco

Palo Alto Networks

Strongswan

Fortinet

generic

Check Point

Cancel

View Config

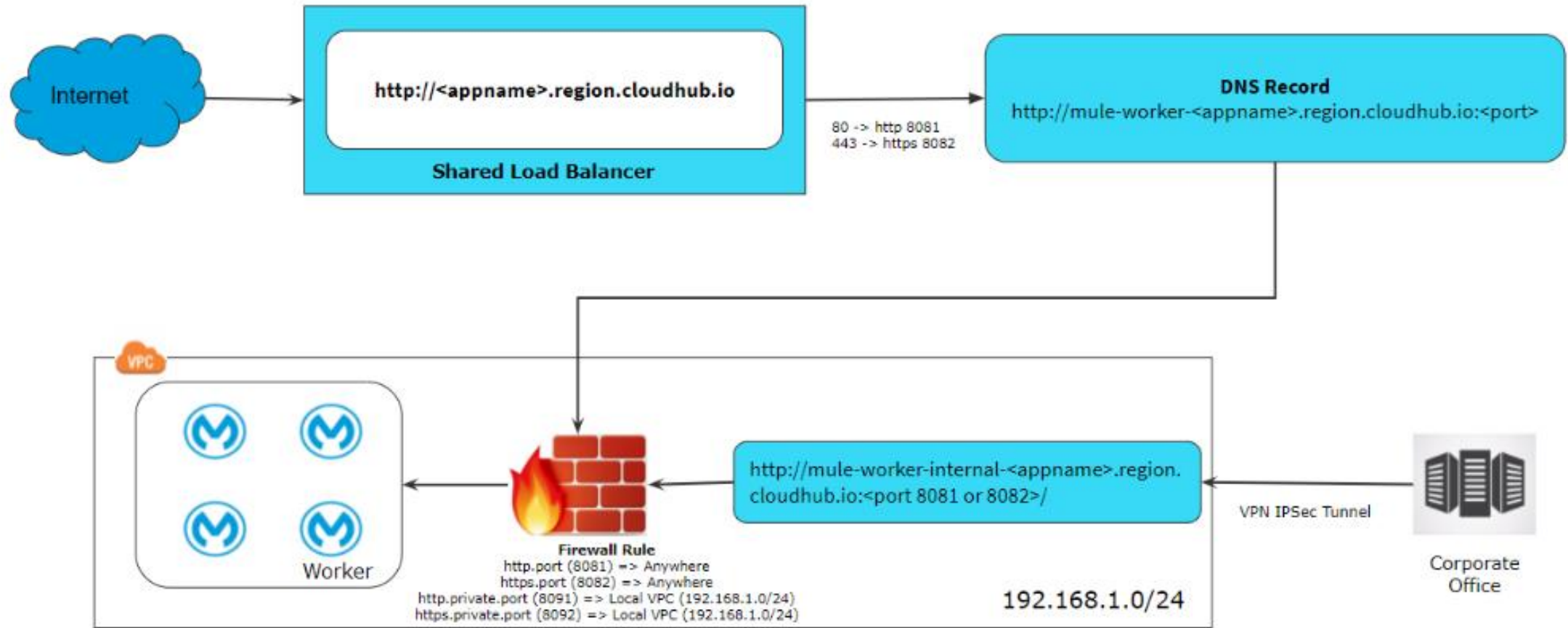
Anypoint Virtual Private Use Cases

- To run the integration or APIs within secure networks or private subnets, you can deploy API within the VPC. For example, you have system APIs that are accessing backend databases and those APIs must be deployed within a secure or private network in CloudHub, so it is accessible by the applications deployed within the same VPC.
- For creating the dedicated load balancer, we need to create a VPC.
- For creating VPN IPsec tunneling, AWS Direct Connect, or VPC peering, we need to create a VPC.

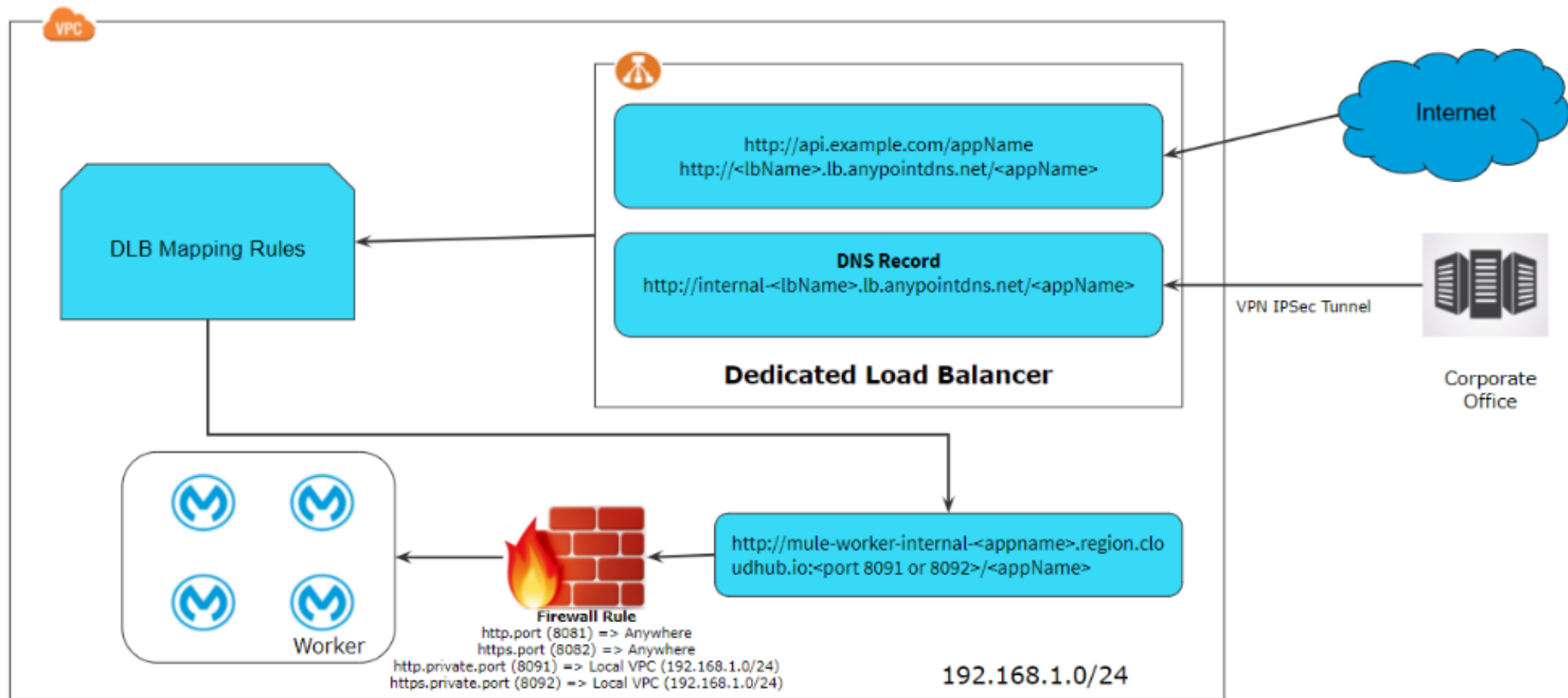
Accessing Application Over Public Internet When Deployed Within VPC

There are various ways that you can APIs over the public internet when an application is deployed within the VPC.

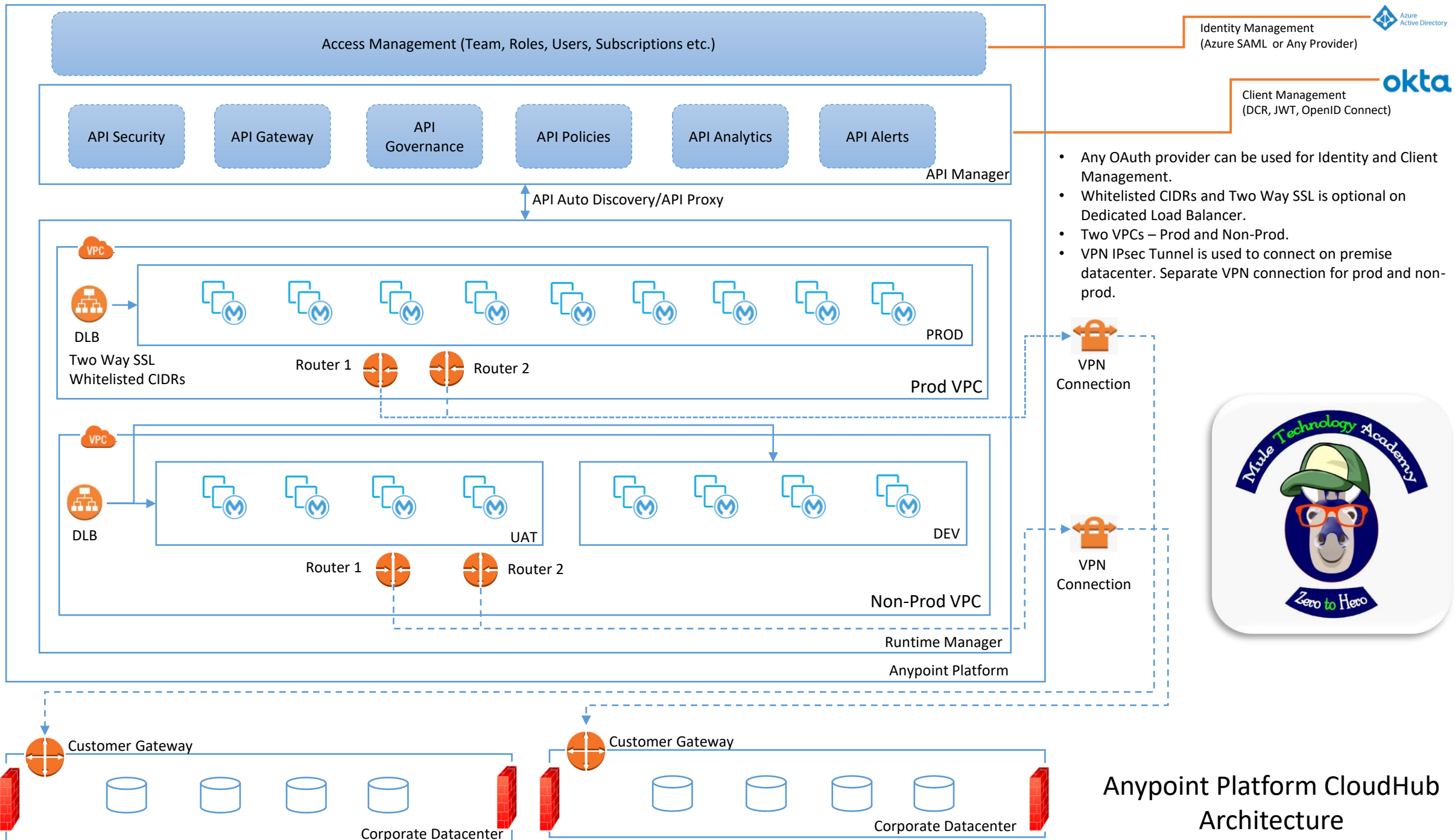
- Deploy the application on port **8081** (http.port) or **8082** (https.port), as per the default firewall rule these ports are accessible anywhere. So, this APIs can be access using **`http://<appname>.region.cloudhub.io/`** or **`https://<appname>.region.cloudhub.io/`**
- In case an application deployed on port **8091** (http.private.port) or **8092** (https.private.port), as per the default firewall rule these ports are accessible within VPC. So, these APIs can be accessed on our public internet using a dedicated load balancer.

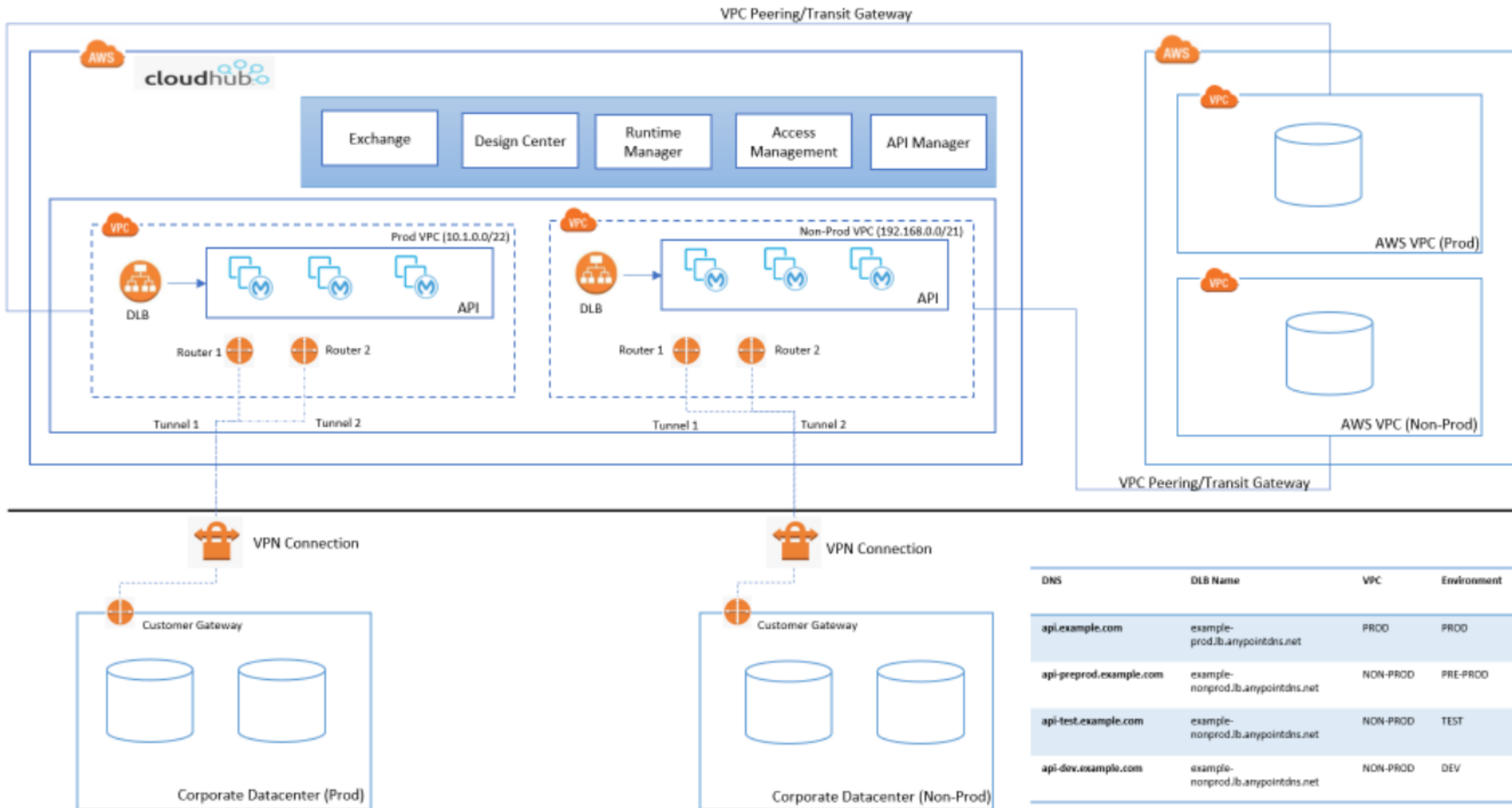


Accessing Application via Shared Load Balancer Deployed Within VPC



Accessing Application via Dedicated Load Balancer
Deployed Within VPC





References

- <https://dzone.com/articles/deep-dive-into-mulesoft-anypoint-vpc-vpn-and-dedic>
- [MuleSoft 4: Platform Architecture and Setup | Advanced MuleSoft – YouTube](#)
- <https://dzone.com/articles/introduction-to-anypoint-dedicated-load-balancer>
- <https://dzone.com/articles/what-is-cidr-classless-inter-domain-routing-in-mul>
- <https://dzone.com/articles/implementing-mapping-rules-with-mulesoft-dedicated>
- <https://docs.mulesoft.com/runtime-manager/virtual-private-cloud>
- <https://docs.mulesoft.com/runtime-manager/dedicated-load-balancer-tutorial>
- <https://blogs.mulesoft.com/dev-guides/how-to-tutorials/implement-dedicated-load-balancers/>
- <https://dzone.com/articles/establish-connection-between-google-cloud-platform>

Thank You

