MULESOFT ARCHITECTURE:

Anypoint Platform Network Architecture

PRACTIC LEARNING

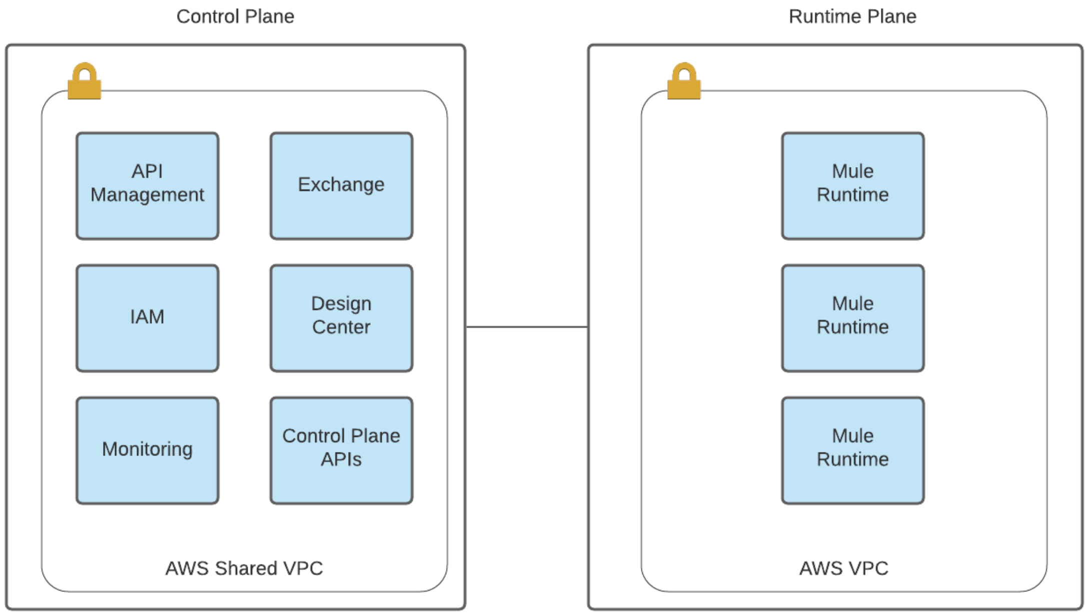
Anypoint Platform Network Architecture Introduction

1. Runtime Plane and Control Plane overview
2. VPCs
3. Load balancing
4. Networking options for deploying to MuleSoft’s cloud
5. Networking scenarios

Runtime Plane and Control Plane

MuleSoft Core Concept: Runtime Plane vs. Control Plane

- Runtime Plane is where applications/APIs are deployed and run
  - Runs on an AWS VPC if deploying to MuleSoft's Runtime Plane or your network/servers if you deploy in a hybrid or on-prem model
- Control Plane is used to manage the Anypoint Platform and the applications/APIs that are deployed to the Runtime Plane



Control Plane

- Accessed via browser or API
- Contains a well-documented set of APIs on Anypoint Exchange
  - Great for systematic access to Anypoint Access Management, API Manager, deployments, and much more
- Lives in a shared AWS VPC on the backend
- Communicates over the internet

MuleSoft Deployment Options

Determine the Runtime Plane from the available deployment options MuleSoft offers

Deploy to MuleSoft's Cloud

- CloudHub
- GovCloud

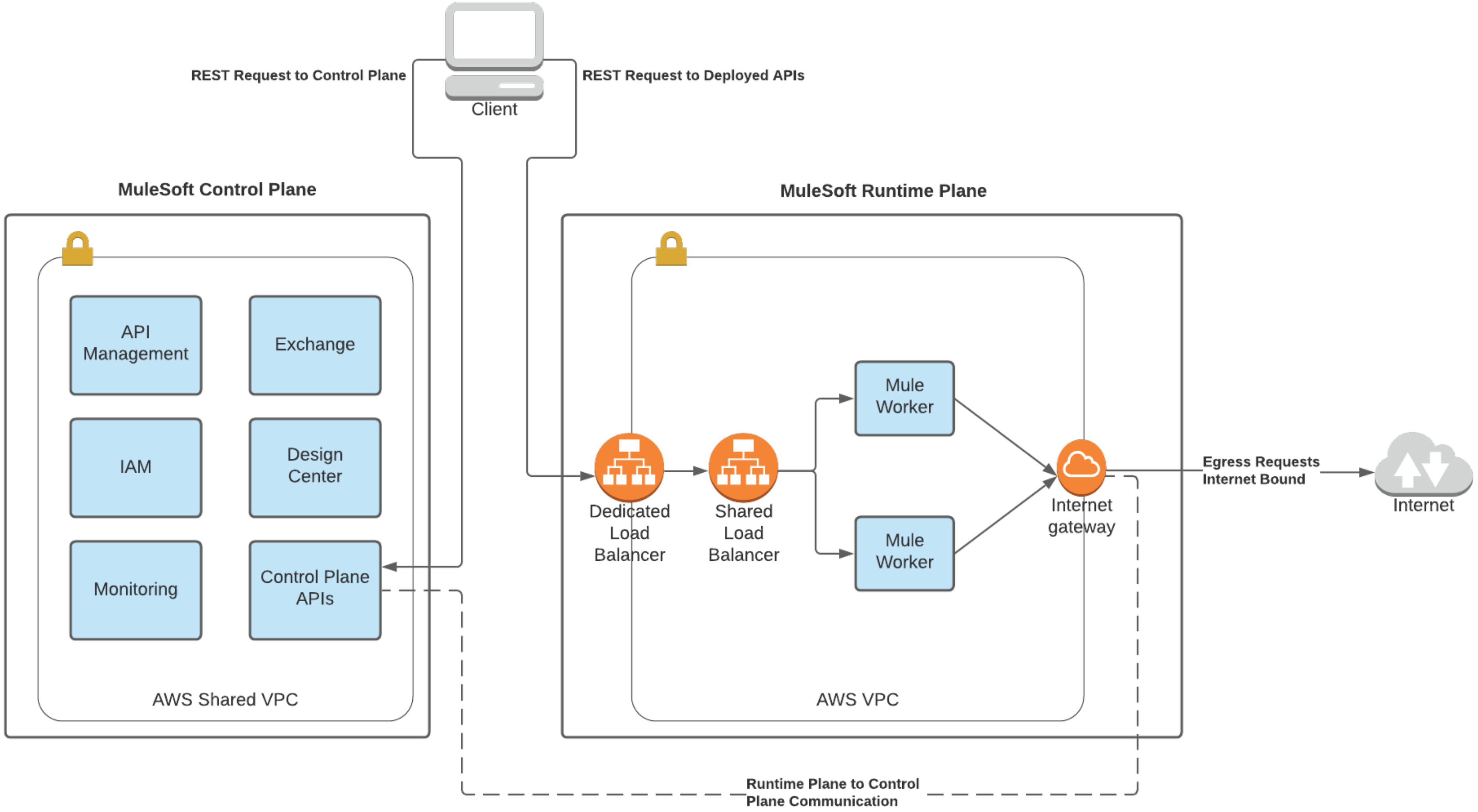
Deploy to Managed Servers

- Runtime Fabric
- Hybrid
- Private Cloud Edition (PCE)
- On-prem

MuleSoft Architecture on AWS

- MuleSoft’s Control Plane and Runtime Plane both run on AWS
- Control Plane
  - Uses a shared AWS VPC
- Runtime Plane
  - Deploys MuleSoft APIs/apps to Amazon EC2 within an AWS VPC in the background
  - Utilizes AWS VPCs, networking components, and load balancers
  - Ingress traffic to APIs is load balanced out of the box
    - A MuleSoft application is comprised of one or more load balanced workers
      - Workers are replicas of an application
- Runtime Plane and Control Plane communicate with each other over the internet

MuleSoft Runtime Plane Architecture



VPCs

MuleSoft VPC Basics

- A VPC can be used when deploying to MuleSoft's Runtime Plane (CloudHub or GovCloud)
  - If you create a VPC from Runtime Manager, your applications can be deployed in the VPC of your choosing
  - If you don't create a VPC from Runtime Manager, your applications are still deployed to a VPC, but they are deployed to a MuleSoft designated VPC, rather than a VPC of your choosing
  - All VPCs are AWS VPCs under the hood
- When to use a VPC in MuleSoft's cloud
  - When you need to connect MuleSoft's cloud to an on-prem network, another AWS VPC, or another AWS instance
  - Control of IP address ranges
  - Control of AWS region you deploy to
- Separating VPCs
  - Typical setup will have one VPC for all non-prod environments and one VPC for Production
    - MuleSoft standard license comes with 2 VPCs
    - Can purchase more VPCs from MuleSoft
  - VPCs are associated with the CloudHub region and can be created per region

MuleSoft VPC Advanced Concepts and Networking

- A VPC can be shared with any business group
- Many organizations choose to carve out private IP address space from an existing network for the MuleSoft VPC
  - Makes network extension and security requests easier
  - Include enough IP addresses for 10x the number of planned MuleSoft applications deployed in a single VPC
- The underlying AWS VPC is divided into availability zones (AZs) for fault tolerance
- Use VPC firewall rules to allow ingress traffic
- Can set VPC internal DNS for intra-VPC traffic

Load Balancing

MuleSoft Dedicated Load Balancer (DLB) Overview

- Load balancer that you can optionally create and govern through the Control Plane
- Load balances traffic to an APIs Shared Load Balancer (SLB)
- Reasons for creating a DLB
  - Creating central access point to APIs
  - Associate your own domain name for requests to your APIs

DLB Advanced Concepts and Networking

- DLB is associated with a MuleSoft VPC
- DLB runs on workers
  - Apply 2+ workers to the DLB for HA
  - Each worker has an IP address associated with it
- Can access the internal DNS of the DLB by adding “internal-” to the DLB DNS
- Combine with VPC firewall rules to force ingress requests coming from the internet to go through the DLB, disallowing requests directly to the SLB

MuleSoft Shared Load Balancer (SLB) Overview

- Load balances traffic to MuleSoft workers
  - Allows for worker horizontal scaling behind the SLB
- SLB comes out of the box with each CloudHub application and cannot be modified
- Associated with the cloudhub.io domain
- Can be bypassed by pointing directly to the worker's DNS or IP address

Networking Options

MuleSoft Deployment Options Networking

Deploy to MuleSoft's Cloud

- If connectivity is needed to your organization's data, create a MuleSoft VPC and connect the VPC to other AWS instances or managed servers

Deploy to Managed Servers

- Full control of the network architecture, so the options are only limited to the capabilities of the managed server's network

Runtime Plane Network Connectivity Options

For connecting MuleSoft's cloud Runtime Plane to an organization's data there are 3 options

1. Direct Connect

2. VPC Peering

3. IPSec Tunnel

Runtime Plane Network Connectivity Details

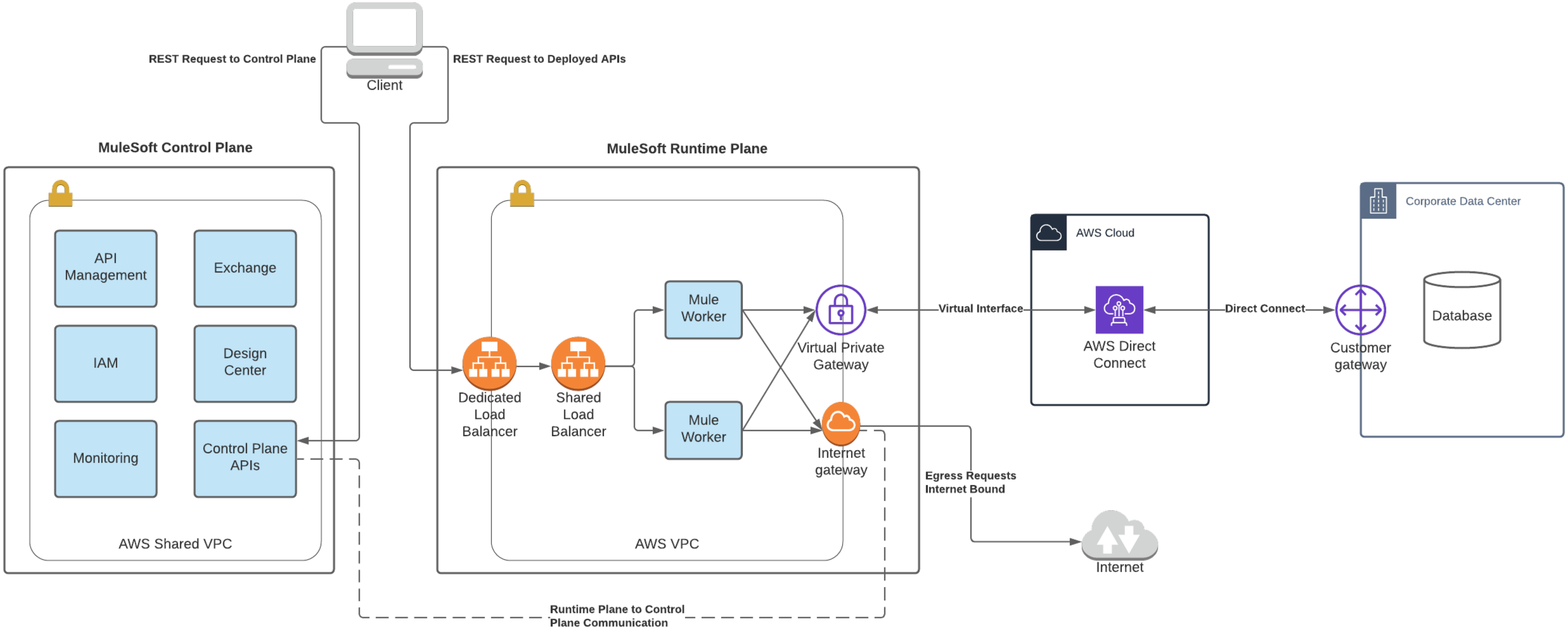
	Direct Connect (DX)	VPC Peering	IPSec Tunnel
Description	Connect MuleSoft’s Runtime Plane with another AWS instance	Connect MuleSoft’s Runtime Plane with another AWS VPC	Connect MuleSoft’s Runtime Plane with any IPSec endpoint that exists
Benefits	Highly scalable, high throughput, reliable and consistent connection	High throughput and private connection not over the internet	Most flexible option, connect to any network that can handle IPSec, encrypted
Drawbacks	Only for AWS, can incur costly AWS expenses, connection made over the internet unencrypted making use of BGP routes	Only for AWS, need a single VPC to connect to	Lowest throughput option, need to build in high availability, internet connection

Design Scenarios

Networking Scenario #1

An organization deploys their MuleSoft applications to CloudHub. The business has a need to connect their deployed MuleSoft applications to their AWS instance with high throughput and reliability at any cost. The architect must recommend the best option to establish connectivity.

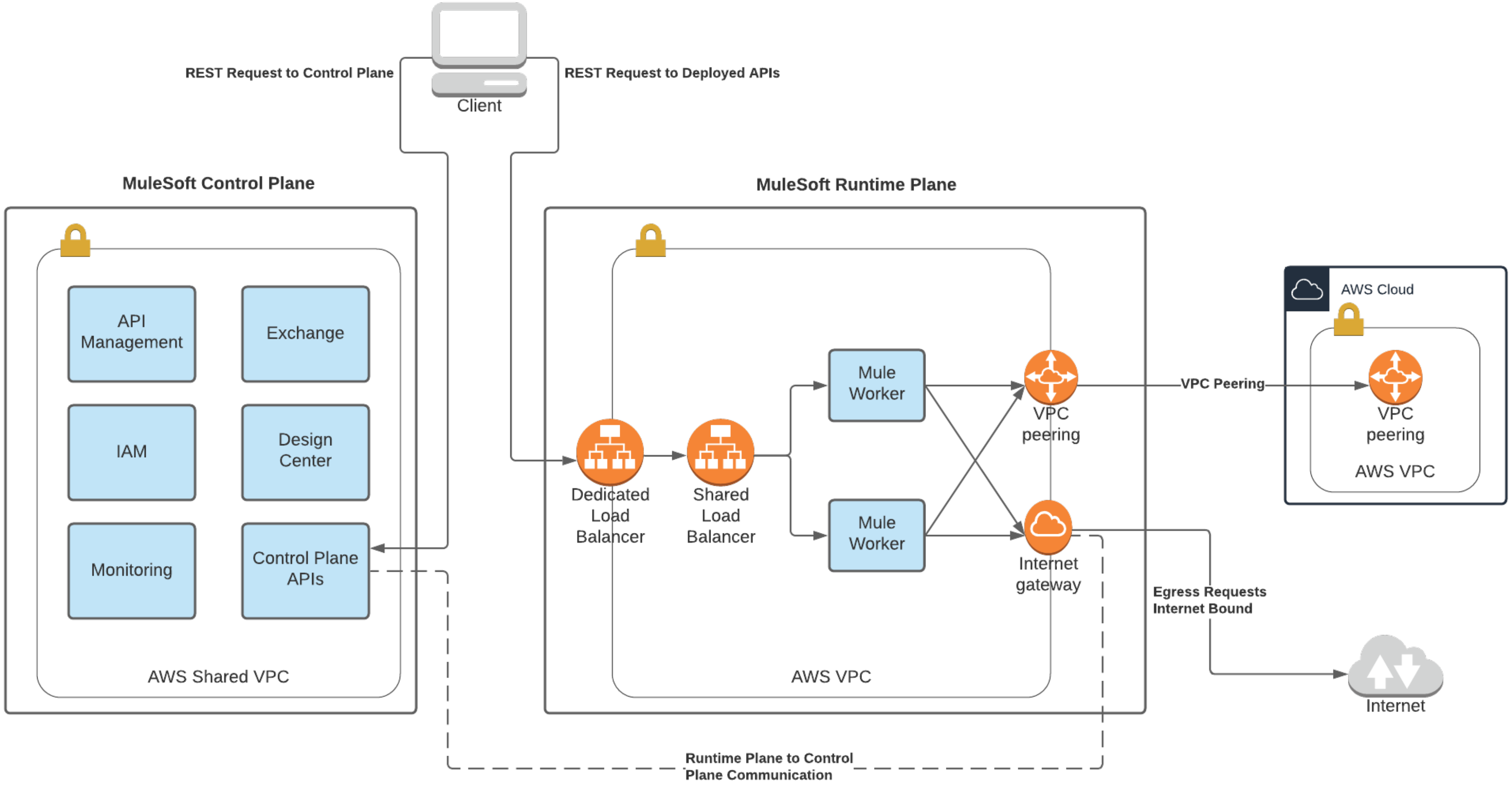
Networking Scenario #1 Architecture



Networking Scenario #2

An organization deploys their MuleSoft applications to CloudHub. This business has a need to connect their deployments to an AWS VPC in their AWS network through a private connection that does not traverse the internet. The architect must recommend the best option to establish connectivity.

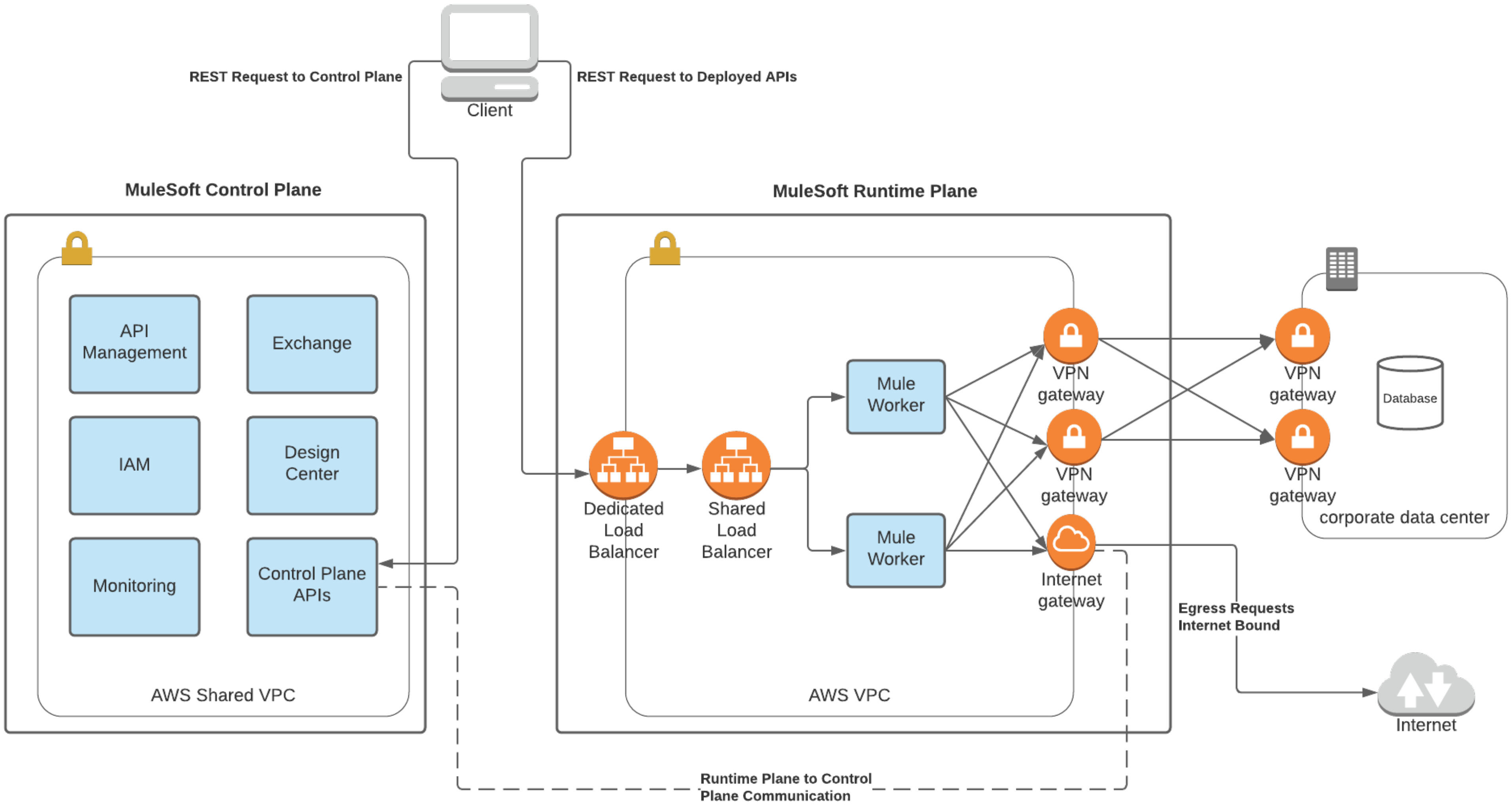
Networking Scenario #2 Architecture



Networking Scenario #3

An organization deploys their MuleSoft applications to CloudHub. This business has a need to connect their deployments to their on-prem corporate data center where their data is housed with a highly available connection that encrypts data in transit. The architect must recommend the best option to establish connectivity.

Networking Scenario #3 Architecture



Anypoint Platform Network Architecture Summary

- Runtime Plane and Control Plane functions
- Control Plane APIs
- Runtime Plane deployment options
- Runtime Plane underlying architecture
- VPCs and load balancing
- Runtime Plane connectivity methods

Additional Reading

- https://docs.mulesoft.com/general/intro-platform-hosting
- https://docs.mulesoft.com/runtime-manager/cloudhub-networking-guide
- https://docs.mulesoft.com/runtime-manager/cloudhub-dedicated-load-balancer
- https://docs.mulesoft.com/runtime-manager/lb-architecture
- https://docs.mulesoft.com/runtime-manager/vpc-architecture-concept
- https://docs.mulesoft.com/runtime-manager/vpc-provisioning-concept
- https://docs.mulesoft.com/runtime-manager/vpc-connectivity-methods-concept
- https://docs.mulesoft.com/runtime-manager/vpc-firewall-rules-concept
- https://docs.mulesoft.com/runtime-manager/resolve-private-domains-vpc-task
- https://docs.mulesoft.com/runtime-manager/deployment-strategies
- https://anypoint.mulesoft.com/exchange/portals/anypoint-platform/?search=api
- https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html