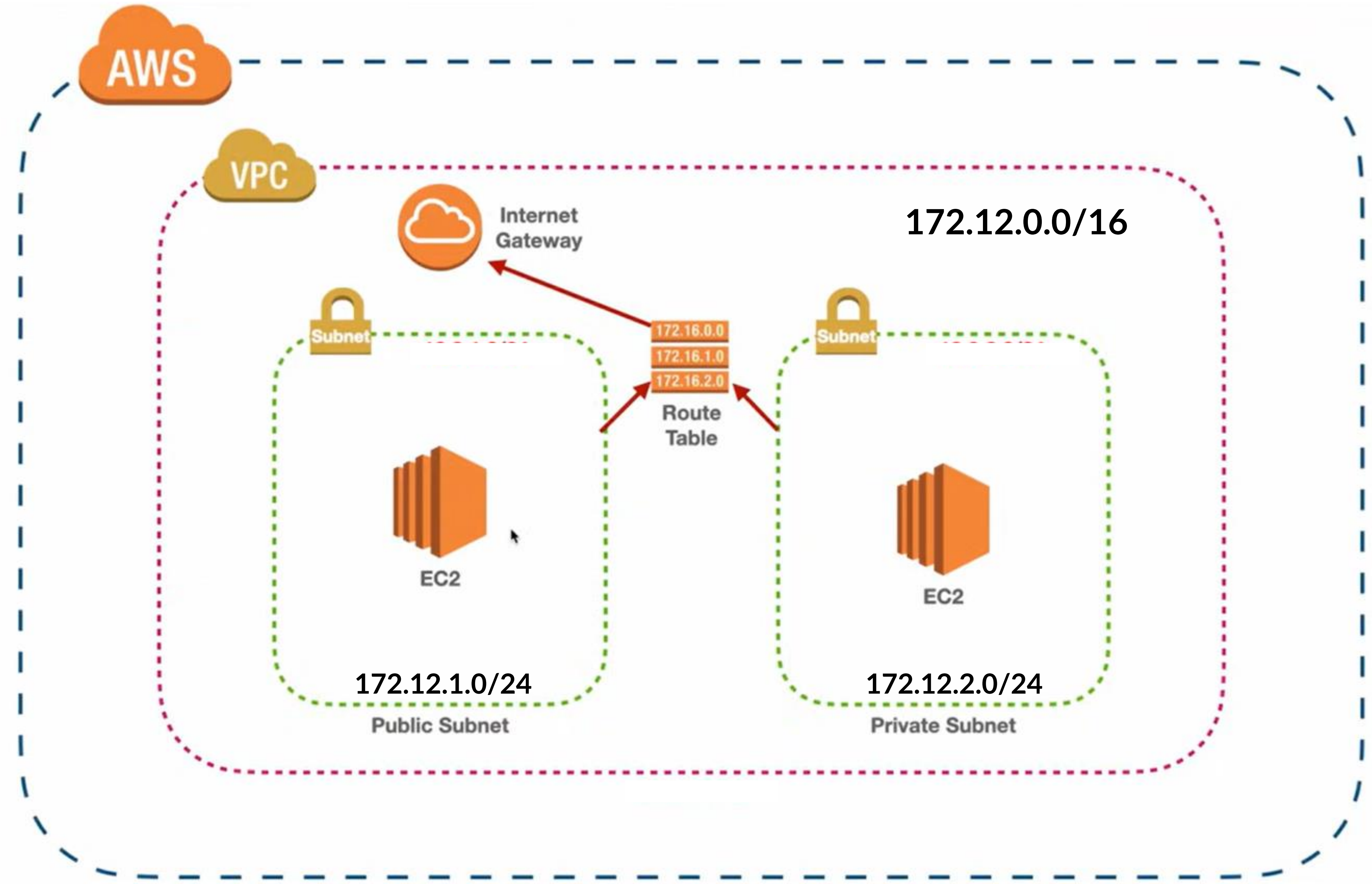
Creación de laboratorio de infraestructura para Pruebas de Penetración

Componentes de infraestructura AWS

3 instancias AWS EC2
1 instancia 8GB RAM

2 contenedores con servicios vulnerables

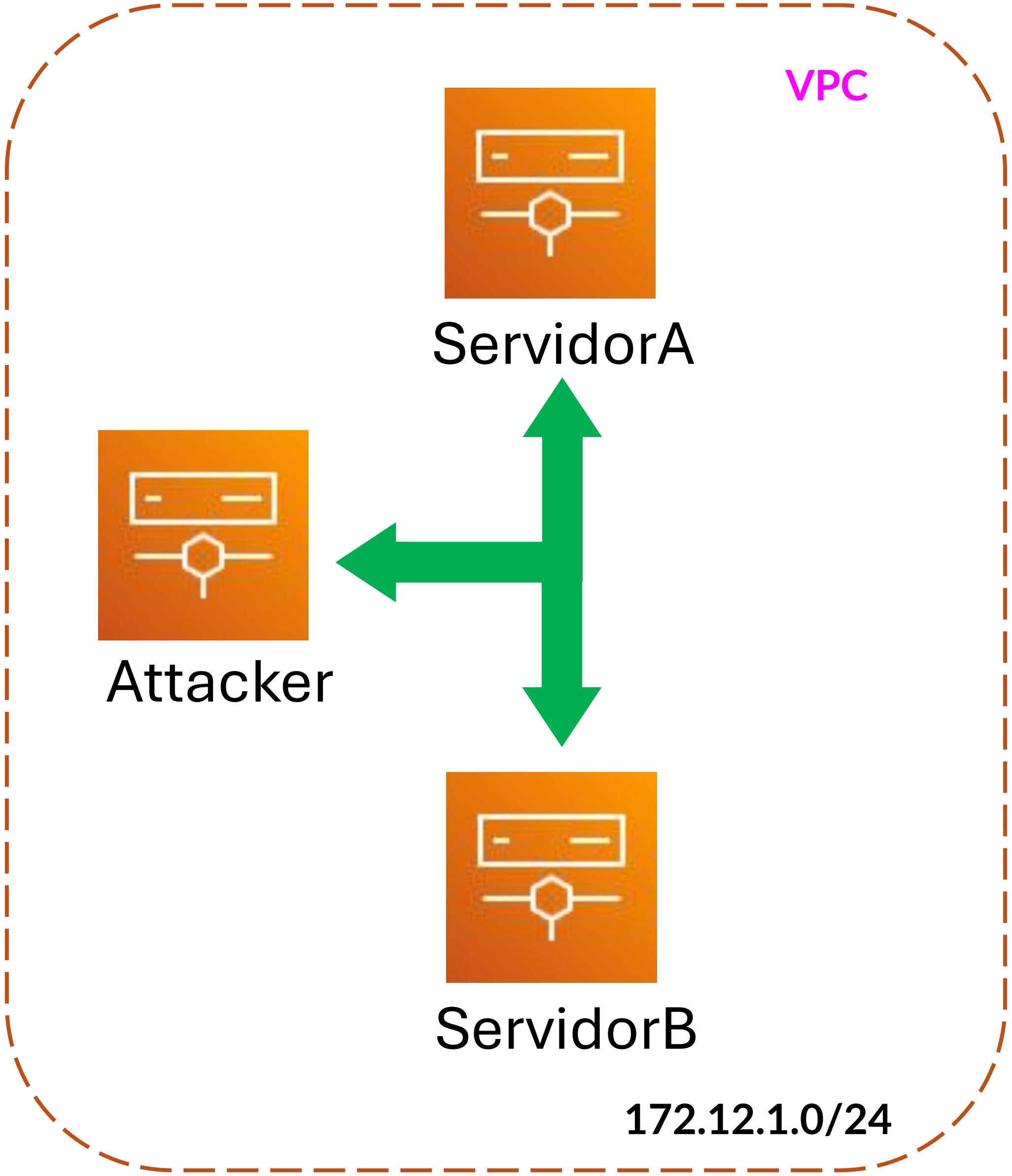
1 instancia adicional como máquina atacante

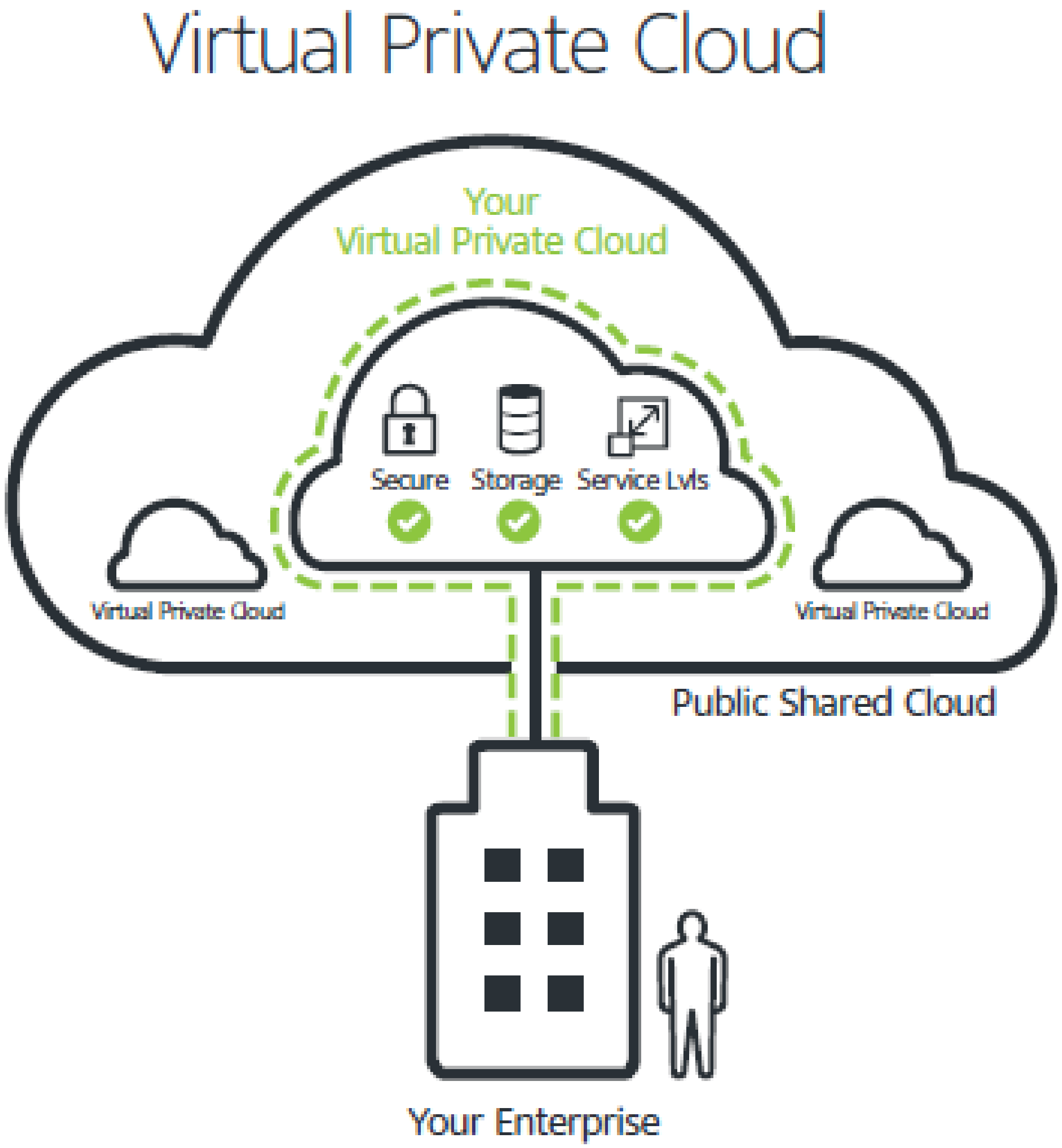


172.12.0.0/16

172.12.1.0/24

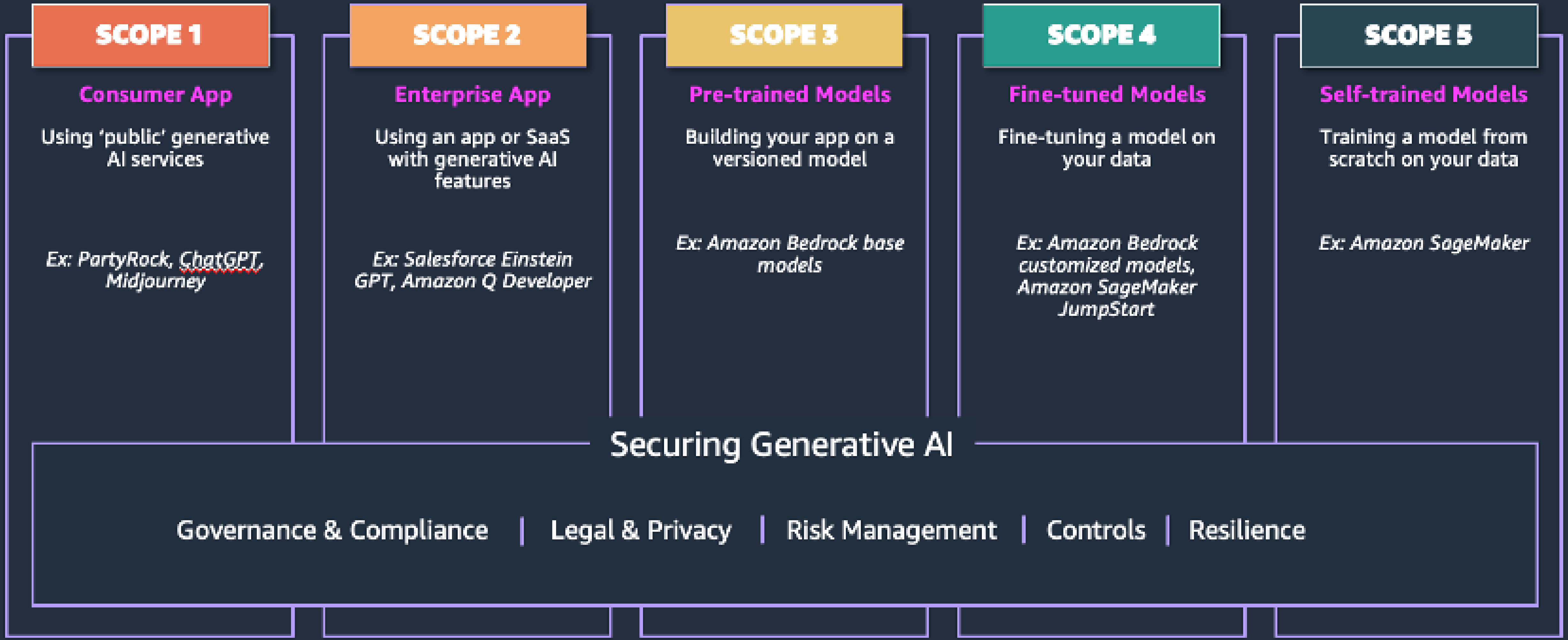
172.12.2.0/24


VPC
ServidorA
Attacker
ServidorB
172.12.1.0/24


Virtual Private Cloud
Your
Virtual Private Cloud
Secure
Storage
Service Lvls
Virtual Private Cloud
Virtual Private Cloud
Public Shared Cloud
Your Enterprise

AWS Generative AI Security Scoping Matrix

WHICH MODEL IS RIGHT FOR YOUR USE CASE?



SCOPE 1

Consumer App

Using 'public' generative AI services

Ex: PartyRock, ChatGPT, Midjourney

SCOPE 2

Enterprise App

Using an app or SaaS with generative AI features

Ex: Salesforce Einstein GPT, Amazon Q Developer

SCOPE 3

Pre-trained Models

Building your app on a versioned model

Ex: Amazon Bedrock base models

SCOPE 4

Fine-tuned Models

Fine-tuning a model on your data

Ex: Amazon Bedrock customized models, Amazon SageMaker JumpStart

SCOPE 5

Self-trained Models

Training a model from scratch on your data

Ex: Amazon SageMaker

Securing Generative AI

Governance & Compliance | Legal & Privacy | Risk Management | Controls | Resilience