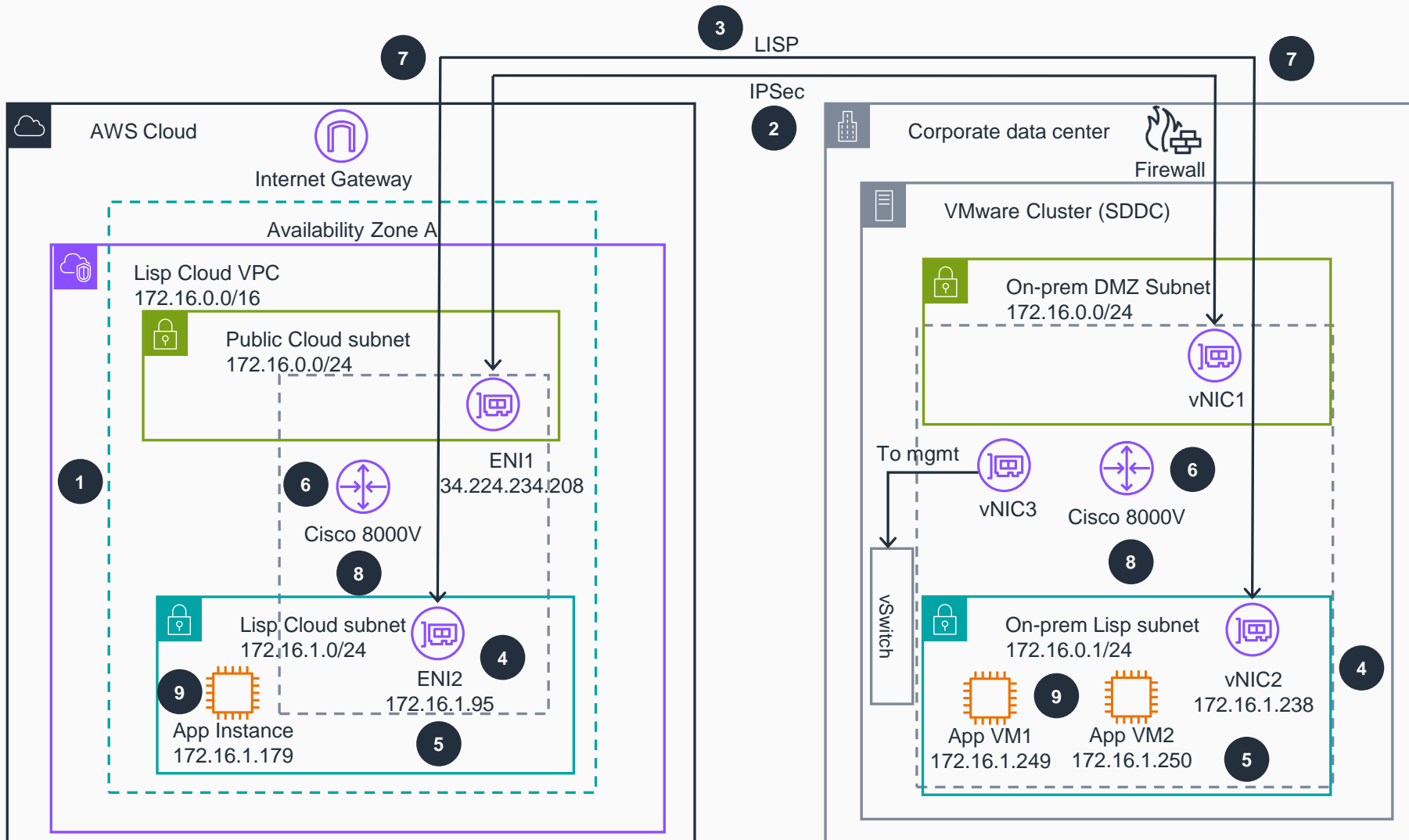


# Guidance for Automated Deployment of Layer 2 Stretch Network Extensions with Cisco 8000v on AWS

This architecture diagram illustrates how to effectively deploy and support Layer 2 Network extension with Cisco 8000V on AWS



- 1 AWS CloudFormation deploys the infrastructure, provisioning both the AWS Cloud and on-premises Cisco Catalyst 8000V routers with pre-configured LISP, IPsec, and OSPF settings.
- 2 A secure IPsec tunnel is established between the on-premises Cisco Catalyst 8000V via Virtual Network Interface Card 1 (vNIC1) and the AWS Cisco Catalyst 8000V via Elastic Network Interface1 (ENI1) through the **AWS Internet Gateway**.
- 3 The LISP protocol initializes on both routers, separating endpoint identifiers (EIDs) from routing locators (RLOCs) to enable Layer 2 network extension.
- 4 Secondary IP addresses are configured on router interfaces, Elastic Network Interface2 (ENI2) on the AWS side. vNIC2 on-prem learns hosts directly through ARP broadcasts. This activates the Layer 2 extension capability.
- 5 Traffic originates from either environment, whether from on-premises application virtual machines (App VM1: 172.16.1.249, App VM2: 172.16.1.250) or from the AWS Cloud (App Instance: 172.16.1.179).
- 6 The Cisco Catalyst 8000V (either on-premises or in AWS Cloud) encapsulates Layer 2 frames with LISP headers to enable transport across Layer 3 networks.
- 7 The encapsulated traffic is encrypted using IPsec and transmitted through the secure tunnel via the **AWS Internet Gateway** on the AWS Cloud side and Firewall on the Corporate data center.
- 8 The destination Cisco Catalyst 8000V (either in AWS Cloud or on-premises) decrypts and decapsulates the traffic, then routes it to the appropriate subnet via ENI2 or vNIC2.
- 9 The packets reach their destination application, maintaining the original Layer 2 addressing throughout the entire flow regardless of traffic direction.

