Implementing Gateway

This chapter contains the following sections:

Linux Gateway

This is the default gateway and it provisions the appropriate firewalls and NAT rules on the VM.

Cisco Adaptive Security Appliance Gateway

Cisco UCS Director provides the ability to create an application container that makes use of a physical Adaptive Security Appliance (ASA) gateway.

This physical gateway allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.

Cisco Adaptive Security Virtual Appliance Gateway

Cisco UCS Director provides the ability to create an application container that makes use of an Adaptive Security Virtual Appliance (ASAv) gateway. The Cisco ASAv supports both traditional tiered data center deployments and the fabric-based deployments of Cisco Application Centric Infrastructure (ACI) environments. The ASAv provides consistent, transparent security across physical, virtual, application-centric, SDN, and cloud environments.

The ASAv brings firewall capabilities to virtualized environments to secure data center traffic within multi-tenant architectures. As it is optimized for data center environments, the ASAv supports vSwitches. The ASAv can therefore be deployed in Cisco, hybrid, and even non-Cisco data centers, significantly reducing administrative overhead and improving flexibility and operational efficiency.

For ACI deployments, the Cisco Application Policy Infrastructure Controller (APIC) provides a single point of control for both network and security management. APIC can provision ASAv security as a service, manage policy, and monitor the entire environment for a unified view of the entire distributed infrastructure. Many

APIC functions can be controlled through Cisco UCS Director, including creation and deletion of ASAv gateways.