

CloudStack NYC

Networking Overview

Current as of Apache CloudStack 4.4/Citrix CloudPlatform 4.5

Introductions

Thanks to BWG Strategy and ShapeBlue

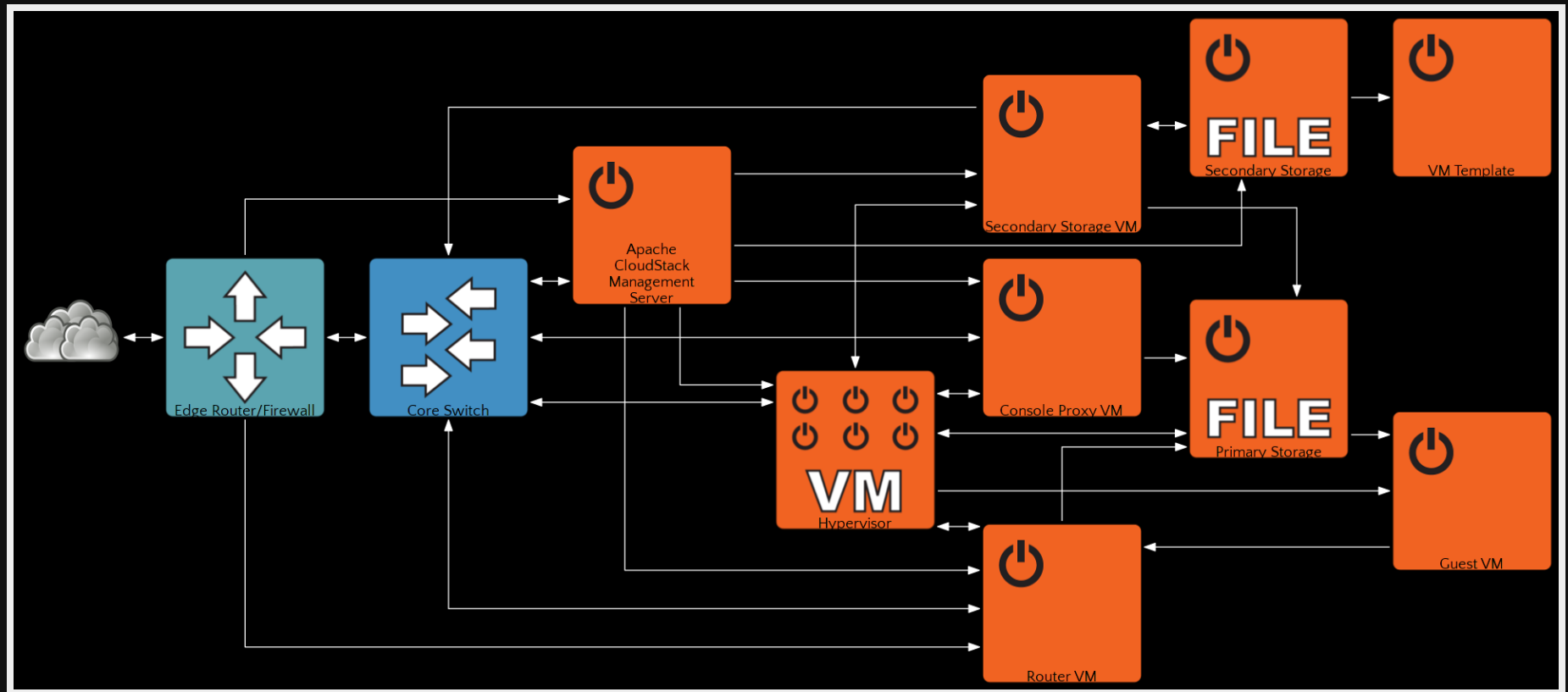
CloudStack Zone Types

- **Basic**
- **Advanced**
 - **Security Groups**
 - **Isolated**
 - **VPC**

Basic

- Flat Network
 - Single VLAN
 - Consecutive IP blocks
 - Security and Isolation handled by Security Groups
 - Security Groups supported on:
 - KVM
 - XenServer
 - LXC
 - Bare Metal
- Compare to AWS Classic

Basic Zone



Advanced Security Groups

- Only supported on **KVM**
- Like Basic but allows VLAN Isolation between Guest, Management, and Storage Traffic

Advanced

Isolated

- VLAN isolation between Networks and Domains
- Requires Advanced Networking
 - Hypervisor Support:
 - KVM
 - XenServer
 - VMware vSphere
 - LXC
 - Hyper-V
 - Bare metal
 - Requires 802.1Q capable hardware (switch/router/firewall)

Advanced Isolated

- A single VM can live in one or more network(s)
- Each Isolated Network is a VLAN (even within a Domain)
- Cross-Network traffic can be routed via a VM in both networks or VPN.

Advanced VPC

- VLAN isolation between VPCs and Domains
- Requires Advanced Networking
 - Hypervisor Support:
 - KVM
 - XenServer
 - VMware vSphere
 - LXC
 - Hyper-V
 - Requires 802.1Q capable hardware (switch/router/firewall)

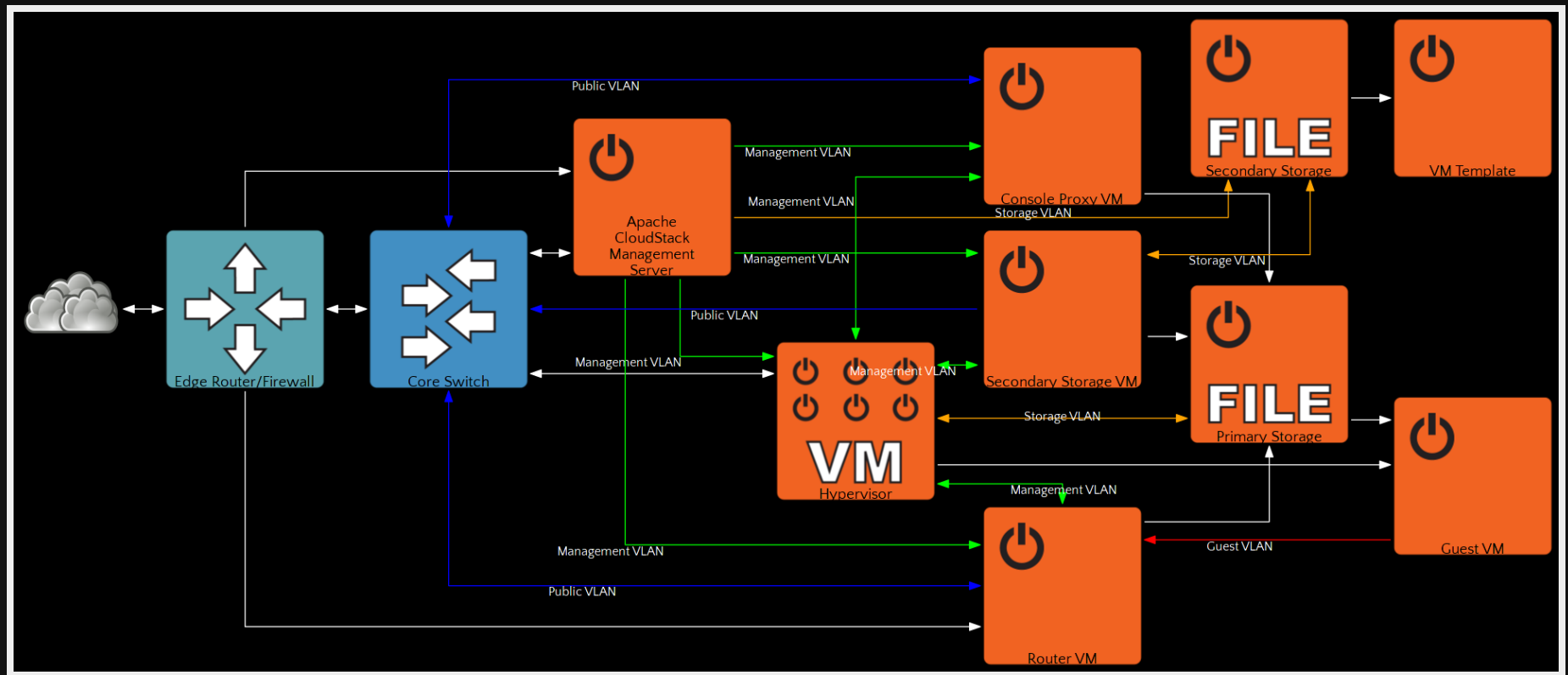
Advanced VPC

- Domain VPC defines a SuperNet and Networks are created as Subnets of this SuperNet.
- A single VM can live in only one tier (Subnet)
 - (But it can live in a VPC tier and an isolated network)

Network Service Offerings

- Means of defining what Network Services you want to offer to your Domains
- Defaults provide *most* services for a given Network Type
- New offerings can be created to tie into other Network Devices:
 - Netscaler
 - Nicera NVP
 - Brocade
 - BigSwitch VNS
 - F5
 - OpenDaylight (Experimental)
 - Cisco VNMC
 - Midonet
 - Nuage VSP
 - Juniper SRX
 - Palo Alto
 - ...and so many more...

Advanced Zone



Virtual Router

- One per-CIDR block for Basic and Advanced with Security Groups
- One per-network for Advanced Isolated
- One per-VPC for Advanced VPC
- Provides:
 - Routing
 - Firewalling
 - NAT
 - Load Balancing
 - VPN
 - Road-Warrior for Advanced Isolated
 - Site-to-Site for Advanced VPC
 - DHCP
 - DNS
 - PXE (for BareMetal)

Networking Concerns

- IP Addresses/VLANs
 - Must hold at least 3 IP addresses for System VMs (more for Advanced)
 - IP addresses for "Public" IPs
 - "Public" IPs are held by Router VMs on their "outside" interface
 - Guest Space
 - VLAN range used by Guest Networks in an Advanced Isolated/VPC Zone
 - Default CIDR block can be set in Zone creation
 - ...but Default CIDR block can be overridden
 - Management Space
 - VLAN/IP space used to manage Hypervisors
 - Also used for "link-local" (System VM) management on VMware
 - Storage Space
 - Used for communication from Hypervisor to Primary and Secondary Storage

Wrap-Up

**Network Diagram Icons (c) Node-Nine,
Inc.**

(ciscomentor.com)

Thank you BWG Strategy and ShapeBlue