# Traditional WAN Deployments

- Individual device configuration
- Configuration is not standardized organization wide
- Focus is on link connectivity, not the required performance for applications
- Typically difficult to migrate to another WAN service

# SD-WAN

- Cisco acquired Viptela in 2017 to enhance their SD-WAN solution (previously called ‘IWAN’)
- It provides automated setup of WAN connectivity between sites
- Monitoring and failover is automated
- Traffic flow control is application aware

# SD-WAN Benefits

- Automated, standardized setup of connectivity between sites
- Transport independent
- Simplified, integrated operations
- More flexibility and easier to migrate WAN services
- The required, predictable performance for important applications
- Integration with the latest cloud and network technologies
- Lower cost

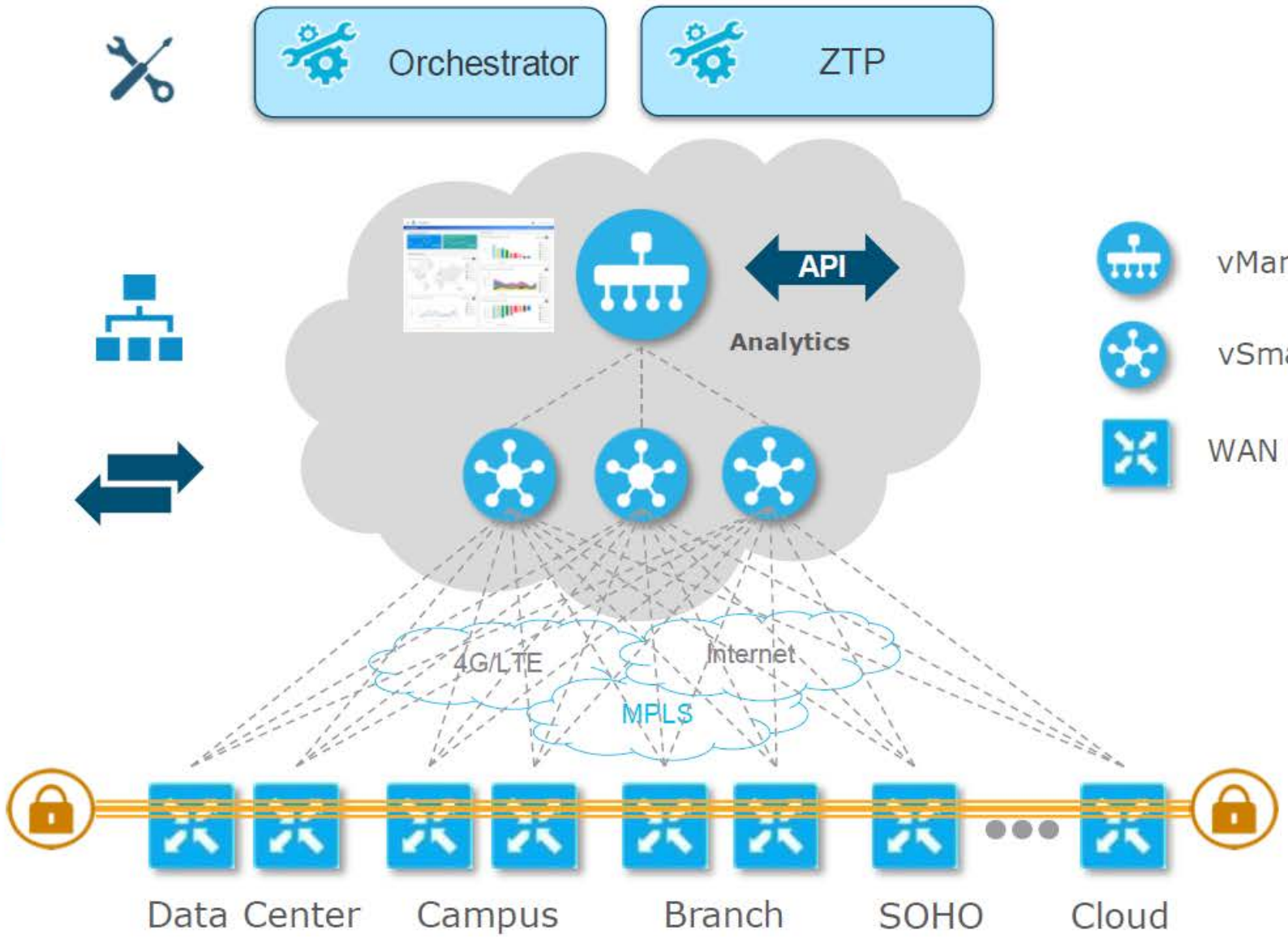
# SD-WAN Architecture – Horizontal Scaling

**Orchestration = vBond**

**Management = vManage**
(Multi-tenant or Dedicated)

**Control Plane = vSmart**
(Containers or VMs)

**Data Plane = Edge**
(vEdge or Cisco ISR/ASR)



# Data Plane - vEdge Routers

- vEdge routers run the data plane.
- They are physical or virtual routers.
- They form an IPsec encrypted data plane between each other.
- A site can have 2 vEdge routers for redundancy.

# Control Plane - vSmart Controllers

- vSmart controllers run the control plane.
- They are the centralized brain of the solution.
- They run as virtual machines.
- They distribute policy and forwarding information to the vEdge routers inside TLS tunnels.
- Each vEdge router connects to two vSmart controllers for redundancy.

# Management Plane – vManage NMS

- The vManage NMS provides the management plane GUI.
- It enables centralized configuration and simplifies changes.
- It provides real time alerting.
- It runs as a virtual machine.
- Multiple vManage NMS are clustered for redundancy.

# Orchestration – vBond orchestrator

- The vBond orchestrator authenticates all vSmart controllers, vManage NMS and vEdge routers that join the SD-WAN network.
- It enables vEdge routers to discover each other, vManage and vSmart.
- It has a public IP address and is deployed in the DMZ.
- It runs as a virtual machine (can also run on a router in smaller deployments.)
- Multiple vBond orchestrators can be deployed with round robin DNS.

# ZTP Zero Touch Provisioning service

- Cloud based shared service hosted by Cisco.
- Utilized on first boot of vEdge router only.
- Directs it to vBond to orchestrate joining it to the network.

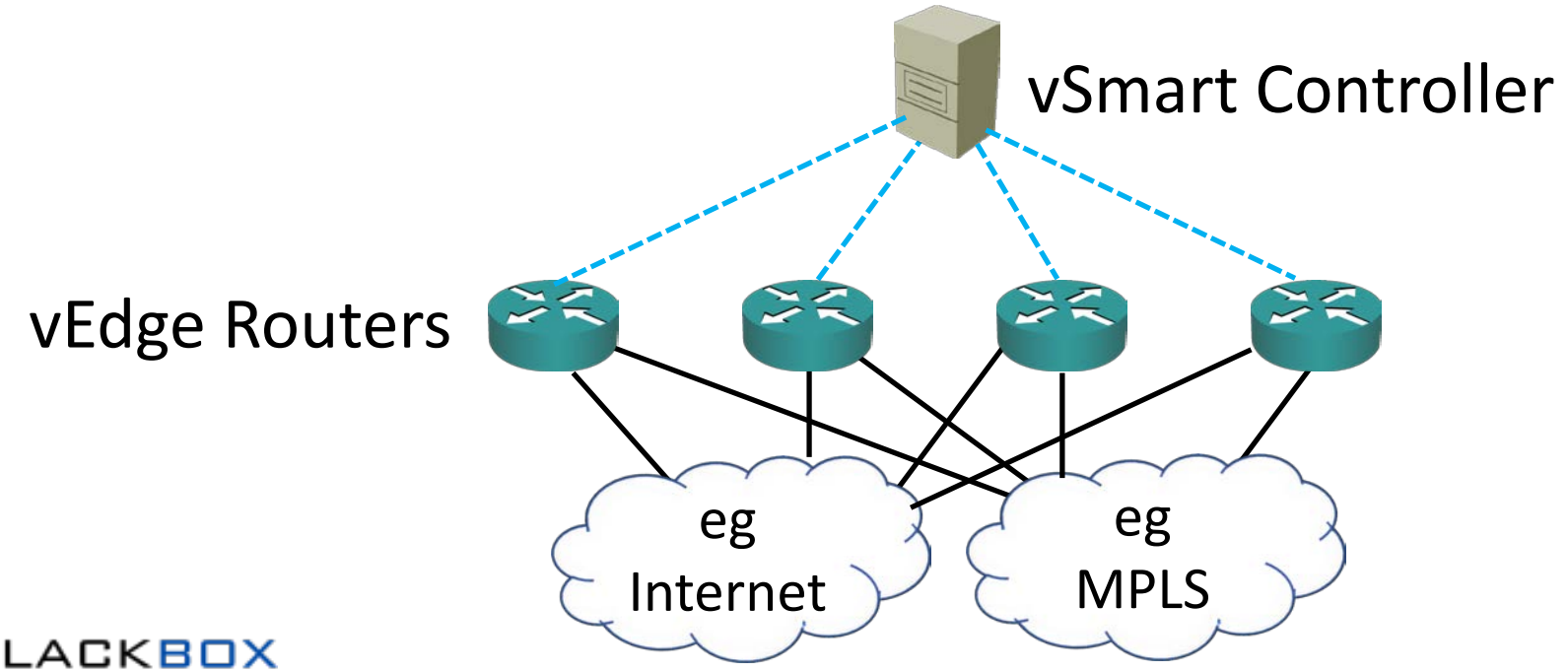
# On Premises and Cloud

- vBond, vSmart and vManage can be deployed:
  - On premises
  - Hosted in Cisco (or partner) cloud

- Most deployments are in the cloud

# Building the Data Plane

- The vSmart controller directs the vEdge routers to build a full mesh (by default) of IPsec VPN tunnels between themselves.
- vSmart propagates policy and routing information to the vEdge routers with OMP Overlay Management Protocol.



# BF VPN Tunnel Monitoring

- Bidirectional Forwarding Detection packets are sent over all VPN tunnels
- This detects if a tunnel goes down, and also provides latency, jitter and loss statistics

# Traffic Forwarding Options

- If multiple tunnels are available (for example over MPLS and Internet) traffic can be load balanced over the tunnels:
- Active/Active
- Weighted Active/Active
- Application pinning Active/Standby
- Application Aware Routing

# Application Aware Routing

- BFD monitors the latency, jitter and loss across the VPN tunnels
- You can set minimum requirements for an application with Service Level Agreement SLA Classes
- SD-WAN ensures the application is sent over a link which meets its SLA requirements
- By default traffic will fall back to another link if no suitable link is available