Cisco ACI Virtual Edge:

Organizations that have deployed the Cisco® Application Centric Infrastructure (Cisco ACI™) platform in their data centers, can now use the Cisco ACI Virtual Edge to extend VXLAN and advanced features like micro EPGs or distributed firewall all the way up to the vSphere hosts.

Overview

The Cisco Application Policy Infrastructure Controller (APIC) can integrate with a number of virtualization domain managers, such as vCenter, Microsoft SCVMM/Azure Pack, etc. to provide management of the virtual networking layer connected to the fabric. This is accomplished through the use of Cisco ACI Virtual Machine Manager (VMM) domains, whereby APIC can provide consistent management of physical and virtual, with automatic correlation of both domains.

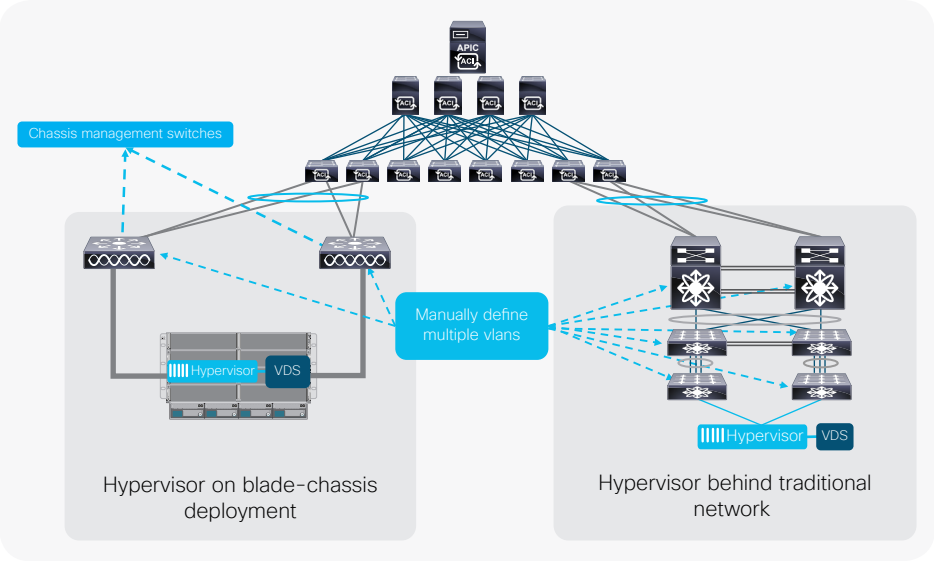
You can configure Cisco ACI VMM Domains with VMware vCenter using the native vSphere Distributed Switch (VDS). This configuration uses VLAN pools to assign encapsulation to EPGs mapped to the VMM domain, allowing customers to realize virtual and physical network automation from the APIC inclusive of applying distributed security policies.

One of the challenges network administrators face when the physical servers are inside blade-chassis or connected to legacy networks that represent switching hops between the hypervisor virtual switch and the Cisco ACI fabric leafs is shown in the Figure 1. In either of these cases, APIC does not automate the configuration of the VLANs corresponding to each EPG on blade-switch devices or on the traditional network devices. This introduces complexity by adding the need for some external automation and may have further issues related to the scale and limitations of to the blade switch or legacy switch type. Cisco ACI Virtual Edge provides extra benefits building on top of a VDS VMM domain to overcome these issues and more.

Benefits

- Hypervisor Independent
- Simplify integration of ACI Fabric with existing infrastructure
- Reduced operating expense
- Enhanced security
- Investment protection
- Simplify legacy infrastructure migration to ACI

Figure 1. VDS Integration showing manul configuration of VLANS over existing infrastructure



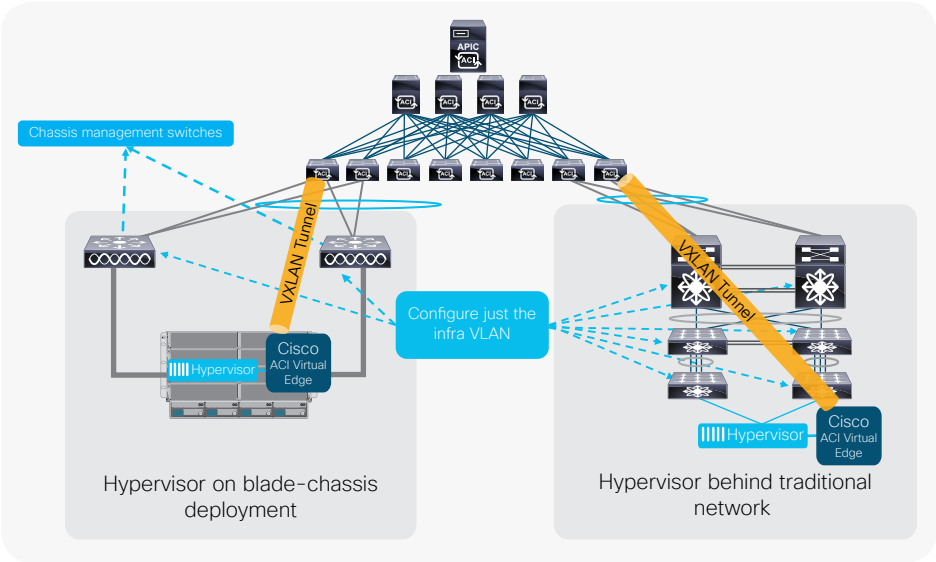
Cisco ACI Virtual Edge solution

The Cisco ACI Virtual Edge is a hypervisor-independent virtual service appliance that is designed to implement Cisco ACI policies using modern software network libraries such as Data Plane Development Kit (DPDK). It leverages the native distributed virtual switch that comes with the vSphere hypervisor and builds a distributed, APIC controlled service layer on top of VDS to extend its functionality.

Virtual Edge extends virtual extensible LAN (VXLAN) overlay, micro-segmentation, and distributed firewall functions to virtual hosts deployed in the Cisco Application Centric Infrastructure (Cisco ACI).

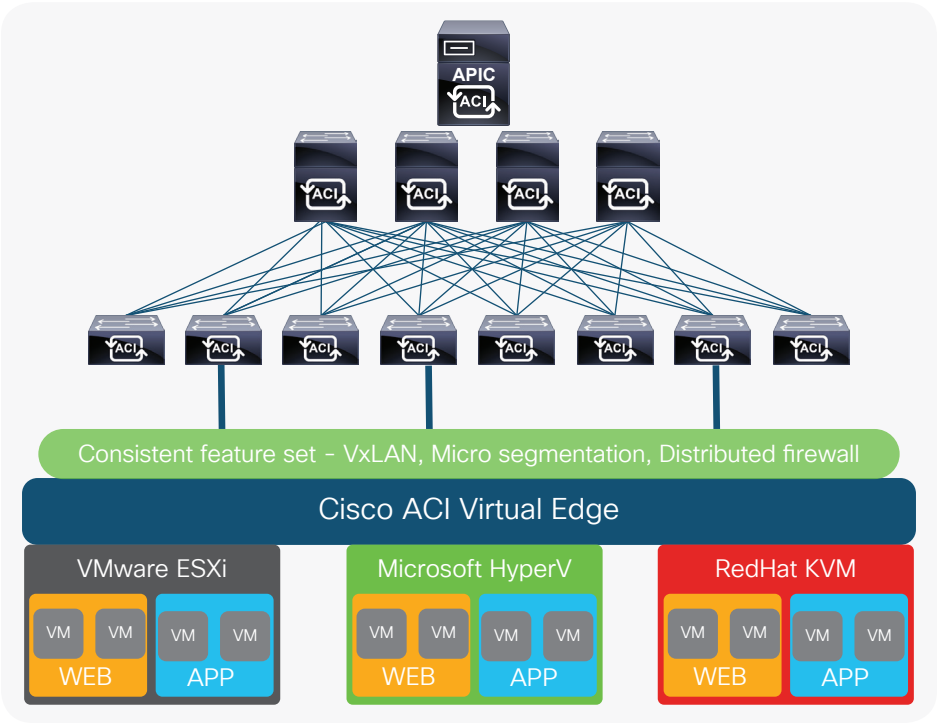
Cisco ACI Virtual Edge eliminates many of the complexities and limitations of manual configuration of VLANs in intermediate devices by using a VXLAN to connect virtual endpoints on the hypervisor to the Cisco ACI fabric. In this scenario, the administrator needs to define only one VLAN –the Cisco ACI infra-VLAN–on the blade switch management devices or throughout the traditional network. By running the Cisco ACI Virtual Edge with VXLAN, customers can easily map ACI networking and policies to hypervisors running on blade switches or connected to legacy networks (Figure 2). This will also help customers migrate virtual work load from the legacy infrastrcutre to ACI fabric.

Figure 2. Simplified deployment of ACI polcies with ACI Virtual Edge over existing infrastructure using VXLAN



Cisco ACI Virtual Edge runs in the user space, free from hypervisor kernel dependencies and operational limitations, and functions as a virtual leaf, managed by Cisco Application Policy Infrastructure Controller (APIC) software. Because ACI Virtual Edge is implemented in user-space, it can be extended to run in any hypervisor (Figure 3).

Figure 3. ACI Virtual Edge distributed Service running across multiple hypervisors



Virtual Edge integrates with the Cisco ACI fabric using the open source protocol OpFlex, enabling APIC to communicate policy to be rendered on its specific data path, much like it does with Nexus-based ACI leafs. The Cisco ACI Virtual Edge can enhance distributed security policies programmed from APIC. For instance, using Virtual Edge customers can benefit from a distributed stateful firewall when implementing contracts. Virtual Edge also enables customers to implement Micro EPGs without hardware dependencies on the leafs, thus enabling granular micro segmentation for all ACI customers. Finally, because AVE can report statistics and metrics to the APIC via OpFlex, it also provides better visibility into virtual workloads.

Cisco ACI Virtual Edge provides investment protection by extending ACI policy enforcement capabilities to virtual hosts attached to existing infrastructure (such as Nexus 2K-7K or any other vendor infrastructure), and allows for seamless migration from legacy infrastructure to ACI.

As the newest member of the Cisco Application Virtual Switch family, Cisco ACI Virtual Edge supports all current features that Cisco Application virtual switch supports as well as newly added features. Cisco ACI Virtual Edge is introduced and supported with Cisco ACI 3.1 for VMware vSphere 6.0 and later releases and has a very minimal resource requirements of the server that it is hosted on interms of CPU and RAM.

Cisco ACI Virtual Edge Integration with vSphere

The Cisco APIC integrates with the VMware vCenter instances to transparently incorporate the Cisco ACI policy framework into vSphere workloads. The APIC works with a native vSphere distributed switch mapped to a VMM domain. The APIC manages all application infrastructure components and constructs on the VDS. The server administrators leverage the Cisco ACI vSphere Plug-in to deploy the Cisco ACI Virtual Edge service appliance on each of the hosts to implement an APIC-controlled distributed virtual edge.

Network connectivity and policy is then created through APIC by defining application network profiles and Endpoint Groups (EPGs), and the APIC pushes them to vCenter as port groups on the distributed virtual switch. When mapping an EPG to the VMM Domain, administrators can select whether its traffic will be handled by Cisco ACI Virtual Edge or not. This allows administrators to connect interfaces such as vmkernel ones to bypass the AVE, in order to ensure that best practices are observed for traffic such as vMotion or IP Storage. Most EPG however will be configured so that the traffic from the virtual network interface cards assigned to corresponding port groups goes through Cisco ACI Virtual Edge.

Virtual Edge can be deployed both in VLAN and VXLAN mode. Figure 4 depicts the process of integrating Cisco ACI with Cisco ACI Virtual Edge.

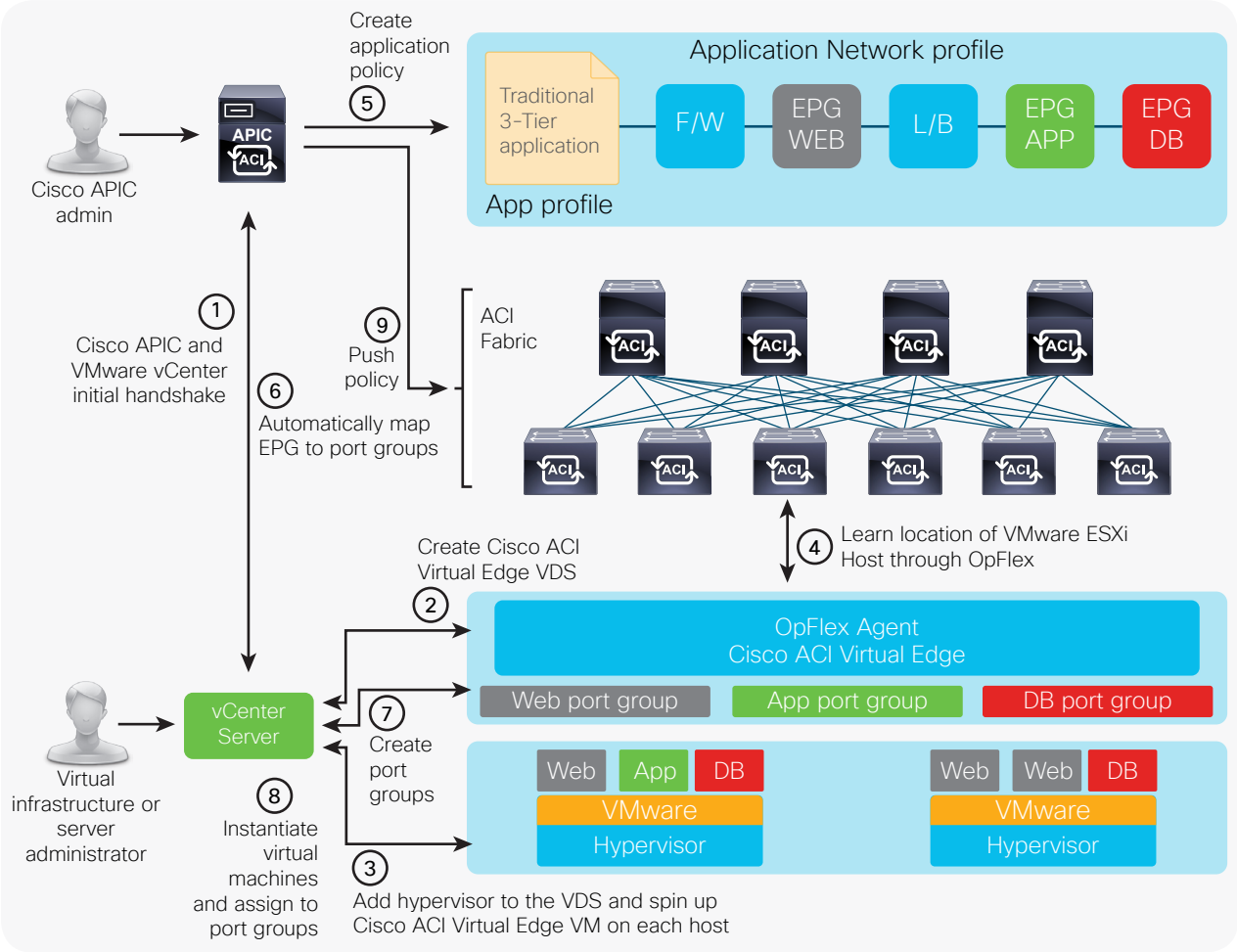
Conclusion

Cisco ACI Virtual Edge provides investment protection by extending ACI policy enforcement to virtual hosts attached to non-Nexus 9000 infrastructure and allows for seamless migration from legacy infrastructure to ACI. It simplifies the deployment of ACI in blade chassis environments and also provides enhanced security and visibility into the traffic that is being switched at the hypervisor level.

For more information

www.cisco.com/go/aci

Figure 4. Using Cisco ACI Virtual Edge in the Cisco ACI fabric



C11-740131-00 02/18