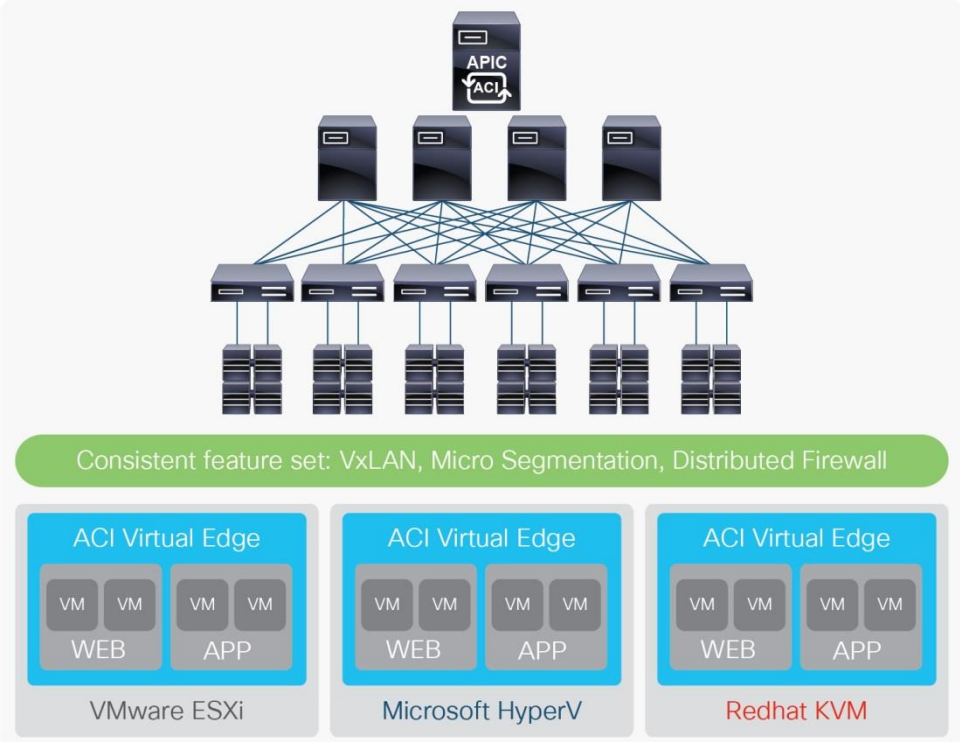
White Paper

# Introducing the Cisco Application Centric Infrastructure (ACI) Virtual Edge

## Product overview

Cisco® Application Centric Infrastructure Virtual Edge is a hypervisor-agnostic virtual node that handles switching and policy enforcement for the Cisco Application Centric Infrastructure (Cisco ACI™) solution. Virtual Edge is architected to run on any hypervisor and offer a consistent feature set with no dependency on proprietary vendor APIs. Cisco ACI Virtual Edge is the next generation of Cisco Application Virtual Switch.

Virtual Edge brings the Cisco ACI policy model, security, and visibility to virtual infrastructure and provides policy consistency for the virtual domain. Virtual Edge also allows you to extend the Cisco ACI policy model to existing infrastructure, providing outstanding investment protection. In future, Virtual Edge enables Cisco ACI to be extended to bare-metal clouds, offering consistent policies across on-premises and cloud applications.



## Product benefits

Cisco ACI Virtual Edge is a distributed virtual node that resides in the hypervisor user space of a virtualized host, providing switching and policy enforcement. Here are some of the advantages of Virtual Edge:

- **Hypervisor independence:** Cisco ACI Virtual Edge is architected from the ground up to be hypervisor agnostic, enabling customers to get a consistent feature set across physical and virtual workloads independent of which hypervisor they have chosen. Virtual Edge utilizes APIs published by hypervisor vendors without any need for proprietary-API access. The current version of Virtual Edge is targeted for the VMware ESXi hypervisor. In future, Virtual Edge will be available for the Microsoft Hyper-V, Red Hat KVM, and other hypervisors.
- **Security:** Cisco ACI Virtual Edge enables you to configure granular security policies for your virtualized applications. Policies can be defined based on network and virtual machine attributes, providing flexibility for both network and server administrators. Virtual Edge also integrates with the Cisco Next-Generation Intrusion Prevention System (NGIPS) security solution to dynamically detect threats based on predefined business policies or know signatures and dynamically enforce security policies.
- **Application visibility:** Cisco ACI Virtual Edge has in-built modules to track, secure, and report well-known Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) based protocol activity, providing insights into applications. These modules make it easier for admins to discovery application ports that assist in the definition of granular security policies. These application visibility modules are tightly integrated into the security modules, providing dynamic protection when a security breach occurs.
- **Investment protection:** Cisco ACI Virtual Edge is architected to transport and deploy Cisco ACI policies over any vendor's existing network infrastructure. Using Virtual Edge, customers can—at their own pace—seamlessly migrate their applications running on existing infrastructure to Cisco ACI with minimal disruption.

## Cisco ACI Virtual Edge use cases

Cisco ACI Virtual Edge can be deployed with the Cisco ACI solution to address a variety of uses cases to simplify configuration, reduce operational burden, enhance security, and provide visibility into the data center. The following are some popular use cases:

- **Simplify blade server deployments:** Typically, in blade server deployments, the blade switch in the server chassis needs to be configured separately from rest of the Cisco ACI infrastructure. Also, most blade switches support only VLAN, which needs to configured and managed. Depending on your scale, you could have multiple blades with different scopes of VLANs that need to configured, presenting a configuration and management challenge. Cisco ACI Virtual Edge eliminates these two problems by avoiding the need to configure and manage VLANs. With Virtual Edge, you can configure Virtual Extensible LAN (VXLAN) from the server directly to the Cisco ACI leaf switch, and then you just need to define an infrastructure VLAN on the blade switch. This capability greatly simplifies the initial deployment, reduces the operational burden on day-to-day operations, and is agnostic to the addition of new or the migration of existing applications.

- **Microsegmentation:** Cisco ACI Virtual Edge enables you to configure policies by identifying your applications using both network and virtual machine attributes. This capability gives both server and network admins the flexibility to identify an application or a workload based on desired attributes. You can use these attributes to address a variety of uses cases. For example, you can move an application through various lifecycle stages, such as development, testing, and production, just by changing the policies. Or, if all servers running a certain software version have a security vulnerability, the microsegmentation supported by Virtual Edge would enable you to easily identify those servers and perform maintenance without affecting the rest of your applications.
- **Auto Quarantine:** The Cisco Next-Generation Intrusion Prevention System (NGIPS) integrates with Virtual Edge, giving you the ability to identify attacks with known signatures and dynamically isolate affected workloads from the rest of your network by placing them in a quarantine group. Admins can perform security patches or maintenance on these affected systems and bring them back into production without disrupting rest of the applications. As attackers create new security vulnerabilities, the NGIPS will continue to add signatures to identify these new attacks, keeping your network aware of and safe from any new attacks.
- **Distributed firewall:** Cisco ACI Virtual Edge tracks well-known protocols like TCP and UDP and applications that run on top of these protocols. This functionality can be used to prevent spreading of insider attacks that have bypassed the north-south firewall. Once a system is compromised inside your data center, it is difficult to detect the breach until it is too late. Virtual Edge can be deployed with Cisco ACI to prevent these insider attacks before they start spreading. As you add more compute nodes to scale your applications, the firewall functionality scales with it, because Cisco ACI Virtual Edge runs on each compute node. In future, the firewall capability will include features like application-level gateways, which let you filter traffic coming from a node to strictly adhere to a specification, giving you granular policy definition.
- **Application discovery:** The Cisco ACI solution is, by default, a whitelist policy–based solution, meaning everything is denied until you open up ports to allow your specific applications. Sometimes you might not know all the ports being used by an application, or when you perform an upgrade or add additional modules to your existing applications, they might start using additional ports that might not be open. In such cases, your applications might not function properly or may even fail. Cisco ACI Virtual Edge has built-in functionality to log both permit and deny traffic. You can turn on permit logging when you add a new application and simply discover the ports being used. Once you discover the ports, you can change your whitelist policy to open up specific ports for your application. Deny logging can be used to prevent unauthorized access and provide information on the intruder.

## System requirements

Cisco ACI Virtual Edge is compatible with any server hardware listed in the VMware Hardware Compatibility List. It requires:

- 2 virtual CPUs
- 4 GB of RAM
- 8-GB hard drive

Cisco ACI Virtual Edge is supported with VMware ESXi Hypervisor release 6.0 and later.

## For more information

Cisco Application Centric Infrastructure


**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.





Printed in USA C11-740220-00 02/18