Enterprise Strategy Group | **Getting to the bigger truth.™**

ESG Lab Validation

Cisco Application Centric Infrastructure (ACI)

Scalable, Automated, Secure, and Open Software-defined Networking to Support Digital Transformation

By Tony Palmer and Kerry Dolan, Senior IT Validation Analysts

October 2017

This ESG Lab Report was commissioned by Cisco Systems
and is distributed under license from ESG.

Contents

ESG Lab Reports

The goal of ESG Lab reports is to educate IT professionals about information technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

Introduction

ESG conducted thorough, hands-on testing of Cisco's Application Centric Infrastructure (ACI) with focus on performance, availability, security, and operational simplicity, conducting the same tests against a software-only software-defined network (SDN) solution for comparison.

Executive Summary

Organizations today are challenged to keep pace with ever changing customer demands and ever present competitive threats. To succeed, organizations need to be much more agile and focused on delivering a superior customer experience. This will require fine tuning and in many cases upgrading processes, culture, and technology; this is commonly referred to as a digital transformation. It will be critical to ensure that all applications are deployed rapidly, perform optimally, remain highly available, and are secure. To make this transformation, organizations need to deploy technologies that take advantage of software-defined capabilities, yet also remain simple to operate and automate. Cisco has designed ACI to be a key enabler of digital transformation.

ESG Lab Validated

In VM to bare metal server testing, ESG Lab found that Cisco ACI provided up to 80% lower latency, up to 600% higher throughput, and up to a 40% improvement in large file transfers between a VM and a bare metal server.

Overall, ESG Lab found Cisco ACI performance to be consistent and predictable across all tests. In realistic scenarios, where traffic flows throughout the environment are dynamic and often unpredictable, involving both virtualized and non-virtualized applications and systems, ACI delivered consistently lower latency and better throughput, with the predictable performance required by mission-critical applications.

Cisco ACI leverages an active-active architecture for high availability on all network paths, with sub-second convergence on failure conditions. ESG Lab noted that in the competing solution, active-active availability was limited to using equal-cost multi-path routing (ECMP), which works for routing, but not for other critical network services, like security and NAT. Active-standby availability schemes are suboptimal for modern mission- and business-critical applications. Examining the working elements of the two solutions tested, ESG Lab observed that ACI possesses 50% fewer failure vectors as compared with the competitive solution. ESG Lab testing also confirmed zero impact or sub-second failover convergence times in all availability tests. In ESG Lab's opinion, ACI is an excellent choice for mission- and business-critical applications.

Data center breaches often occur from within the data center itself. With its whitelist security model, ACI provides a ubiquitous micro-segmentation solution. Applying security rules and policies at the network level is complicated by the fact that IT professionals must ensure that all network elements within the data center network apply rules and policies consistently for all types of network traffic. ESG Lab tested the ability of Cisco ACI to provide consistent micro-segmentation support to workloads in multiple hypervisors, bare metal endpoints, and containers—across data centers connected via a WAN. Cisco ACI provided granular endpoint security enforcement across both data centers, with policies defined using objects from VMware vCenter. We conducted the same test with the software-only SDN solution and found that when we attempted to apply the same firewall policies to the same workloads across data centers with different vCenter servers, those policies were not enforced.

ESG was particularly impressed by how easy it is to deploy multi-tier applications using out of the box Ansible playbooks provided by Cisco ACI. In addition, the integrated overlay network virtualization model allows ACI to deliver automation much faster than the software-only SDN solution tested by ESG while consuming fewer resources. ESG Lab automated provisioning of a private cloud environment using Ansible with ACI more than 40 times faster than would be possible with the software-only SDN. ESG Lab also confirmed a significant compute and storage capacity savings since ACI does not require additional VMs to execute routing and gateway services.

Cisco ACI technology worked seamlessly regardless of the virtualization or application packaging technologies employed. Customer environments are often a mix of multiple hypervisors and the ACI test setup could have easily included Hyper-V, KVM, and Kubernetes containers and achieved the same operational and functional results—even between VMs on different hypervisors. However, to ensure the fairness of the comparison with the software-only SDN solution, which does not support such functionality, those tests were excluded.

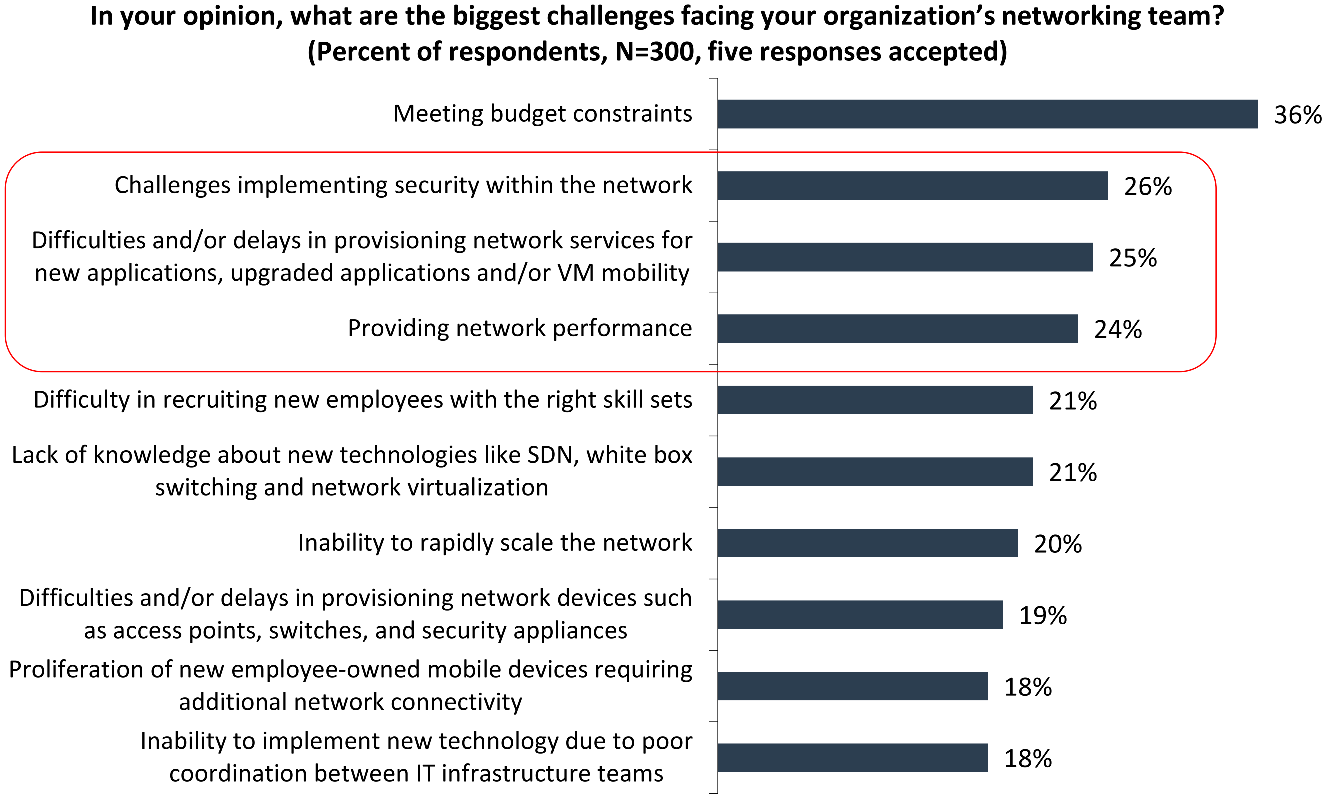
ESG found that Cisco ACI provides a simple, scalable, and highly available network that is well-suited to mission-critical workloads. If your organization is interested in improving the automation, agility, security, and availability of your networks across multiple hybrid data centers, ESG Lab recommends taking a close look at Cisco ACI.

Background

An agile, consistently high-performance network is essential for data center computing. Every part of business—and, some would argue, almost every part of life today—is impacted by network health and functionality, as employees access data and applications from multiple locations, on multiple devices. As networks expand to handle today's web-scale business, however, they become more complex and difficult to manage, leading to performance and uptime problems, and frustrating users. Also, a constant threat of network intrusion can result in irreparable harm including data loss, compliance failure, and reputation damage, keeping network security top-of-mind for IT professionals.

Recent ESG research underscores these realities. When asked about their biggest networking challenges, ESG research respondents cited network security implementation, provisioning network services for applications and mobile virtual machines (VMs), and performance among the top challenges, putting them just behind budget constraints (see Figure 1).[1]

Figure 1. Top Ten Networking Challenges



Source: Enterprise Strategy Group, 2017

[1] Source: ESG Survey, *Network Modernization Trends*, July 2017.

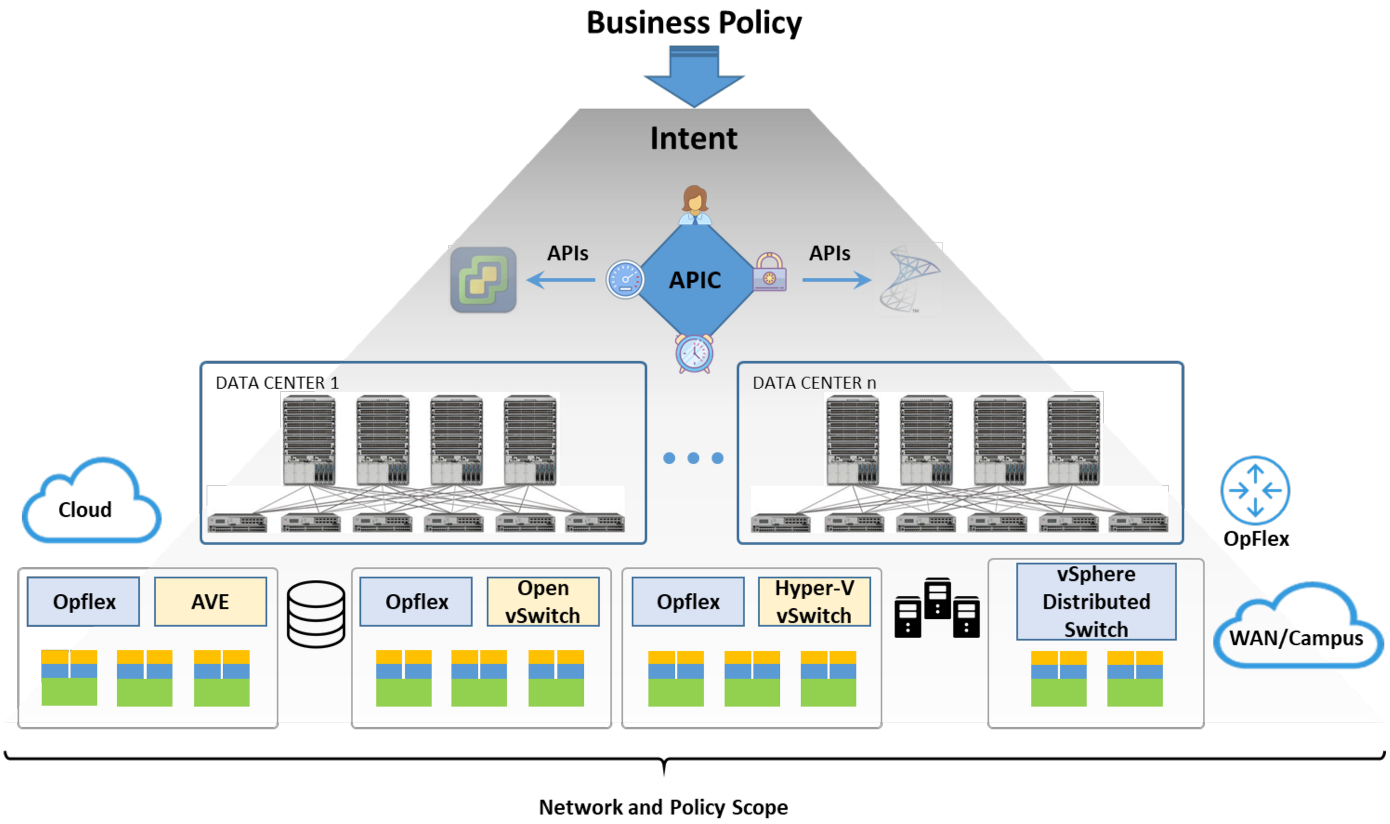
Software-defined networking can simplify network control and operations by abstracting the control and data planes from the underlying hardware. By creating dynamic, programmable, logical network components based on high-quality physical ones, SDN can deliver more dependable network services that are faster and easier to design, manage, and troubleshoot.

Cisco ACI

Cisco ACI is a software-defined networking solution that combines physical and virtual elements with the goal of simplifying network operations and management while delivering application-focused network services. Cisco ACI is designed to scale up to 400 switches and 180,000 endpoints. With ACI's integrated overlay model, customers can automate common network tasks to simplify their work, while also enabling them to evolve toward application-based, policy-driven network services. With a common platform for physical, virtual, and cloud environments, Cisco ACI provides centralized visibility and control so that administrators can manage and troubleshoot network services across their environment. ACI provides micro-segmentation for any workload. In virtualized environments, ACI micro-segmentation seamlessly scales across hypervisors and across data centers based on VM attributes; in addition, it simplifies the process of deploying and scaling the network, and improves security. The Cisco ACI architecture presents fewer failure vectors than software-only SDN solutions, enabling it to fail less often and recover faster from common network failures (i.e., link or network node failures). In addition, Cisco ACI provides visibility into the hardware to understand traffic flows so that administrators can better understand faults and remediate them.

As seen in Figure 2, the Cisco Application Policy Infrastructure Controller (APIC) integrates with the physical and virtual switching layers, including third-party and open source options to create the foundation for a policy model that tailors network and security services to applications and ensures alignment with business policies.

Figure 2. Cisco Application Centric Infrastructure



Source: Enterprise Strategy Group, 2017

Application Policy Infrastructure Controller (APIC)

The Cisco APIC[2] provides centralized access to and control of all fabric information and managed virtual switches with the goal of optimizing the application lifecycle for scale and performance. To this end, the APIC supports flexible network and policy provisioning across physical and virtual resources. It consists of a minimum-three-node controller cluster that manages and operates the ACI fabric and connected virtual switches. The APIC cluster enables synchronization and management of endpoint network state seamlessly across multiple Virtual Machine Management (VMM) and physical domains. The Cisco ACI fabric software provides an object-based switch operating system—programmable through an open REST API—that can manage the underlying components using the OpFlex protocol; this creates an open framework that enables application-aware network and policy automation.

Cisco Nexus 9000 Series Switches

The Nexus 9000 Series[3] are designed to deliver high performance, high density, low latency, and power efficiency in a range of form factors with 1/10/25/40/50/100G Ethernet configurations. The switches can operate in Cisco NX-OS Software or Application Centric Infrastructure (ACI) modes with Cisco's Cloud Scale ASIC technology. They are a good fit in both traditional or fully automated data center deployments.

Cisco Application Virtual Switch (AVS) / Application Virtual Edge (AVE)

The Cisco AVS and AVE—the upcoming next generation of the AVS—are software components of the Cisco ACI framework. They comprise a purpose-built, distributed virtual switch that is integrated with the ACI management and orchestration platform to automate virtual network provisioning. AVS/AVE are designed to offer different forwarding and encapsulation options, traffic steering to application services, and stateful inspection across many VMware vCenter virtualized hosts and data centers. Cisco's AVS and AVE are integrated with the Cisco ACI architecture as a virtual leaf and are managed by the Cisco APIC. The Cisco AVS implements the OpFlex protocol for control plane communication with the APIC.

Cisco recently announced that Cisco ACI will be available within public cloud environments. The new offering, called Cisco ACI Anywhere, will leverage the Cisco AVE, the next generation of the Cisco AVS. The premise of Cisco ACI Anywhere is to provide Cisco customers with the flexibility to run applications across their own private clouds, as well as the public clouds of their choice, while maintaining consistent network policies across their entire multi-cloud domain.

OpFlex and Third-party Virtual Switching

Cisco ACI uses a declarative control model based on scalable control of intelligent objects. Declarative control dictates that each object is asked to achieve a desired state and makes a promise to reach this state, without being told precisely how to do so. This differs from the more traditional imperative model which must specify every element of low-level configuration to reach the desired state. Cisco ACI leverages declarative control to separate out application, operation, and infrastructure requirements and allow each to be specified independently. The OpFlex Protocol is the mechanism used by Cisco ACI to implement declarative control in order to transfer abstract policy from a network policy controller to a set of smart devices capable of rendering abstract policy.

In addition to Cisco's AVS and AVE, Cisco ACI uses the OpFlex protocol to work with Open vSwitch (OVS) and the Microsoft Hyper-V virtual switch. APIC also leverages northbound APIs to interface with other third-party vSwitches, like VMware VDS. OpFlex is also used to interact with certain Cisco routers and switches, like the Nexus 7000, ASR 1000, and ASR 9000.

[2] To learn more about the APIC, visit: https://www.cisco.com/c/en/us/products/cloud-systems-management/application-policy-infrastructure-controller-apic/index.html

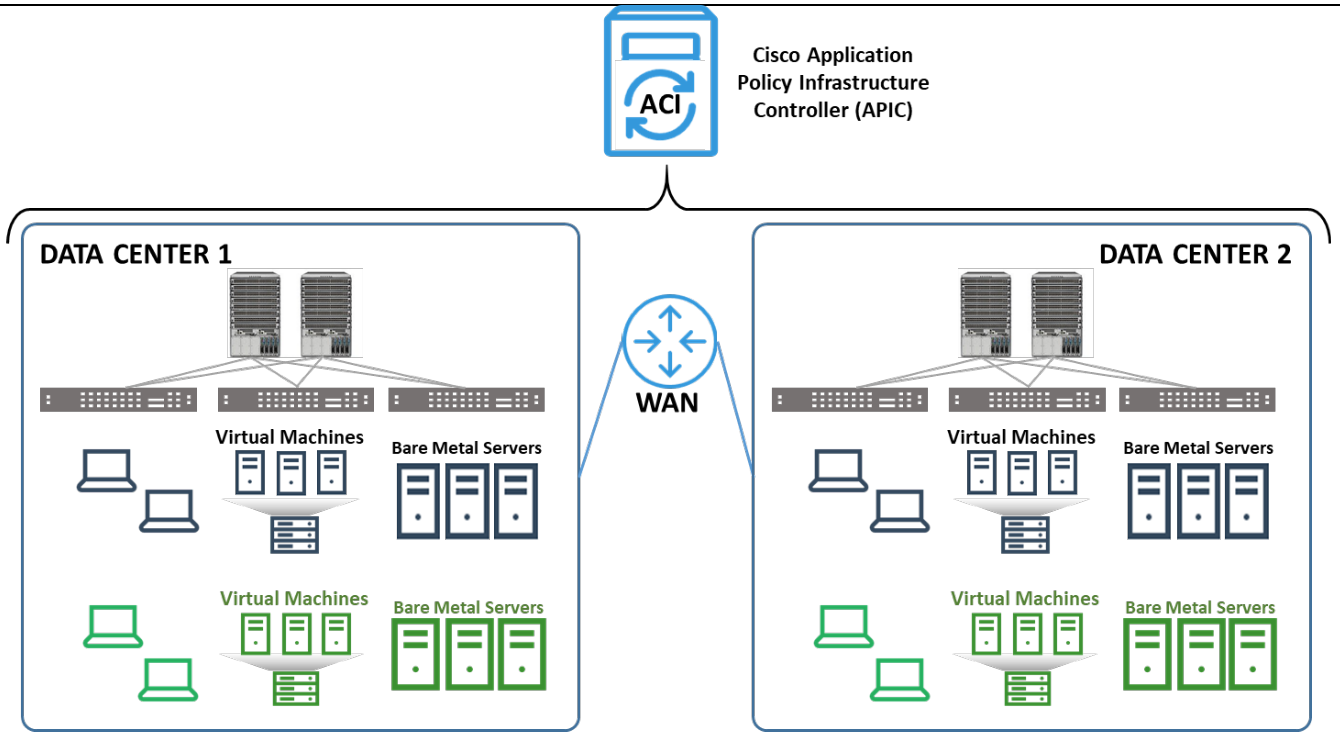
[3] To learn more about the Nexus 9000 series, visit: https://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html?stickynav=1

ESG Lab Validation

ESG Lab performed hands-on evaluation and testing of Cisco ACI and compared results with a software-only SDN solution. Testing was designed to demonstrate the performance, availability, security, and automation provided by ACI in a modern, distributed enterprise environment with physical and virtual servers spanning multiple data centers.

The test bed was designed to emulate a customer environment with multiple data centers and a mix of virtualized and bare metal servers supporting production and development environments (see Figure 3). Customer environments often host a mix of multiple hypervisors and the ACI test setup could just as easily have included VMware, Hyper-V, KVM, and Kubernetes/containers to demonstrate the same operational and functional results—even between VMs on different hypervisors. However, to ensure a fair comparison to the other SDN solution, which does not support such functionality, those tests were excluded.

Figure 3. The ESG Lab Test Bed



Source: Enterprise Strategy Group, 2017

Performance

ESG Lab tested the performance of Cisco ACI as compared with a software-only solution in multiple scenarios designed to emulate common use cases deployed by organizations in the real world: workload running between virtual machines hosted in a hypervisor on a single host, between virtual machines on different hosts, and between virtual machines and bare metal servers.

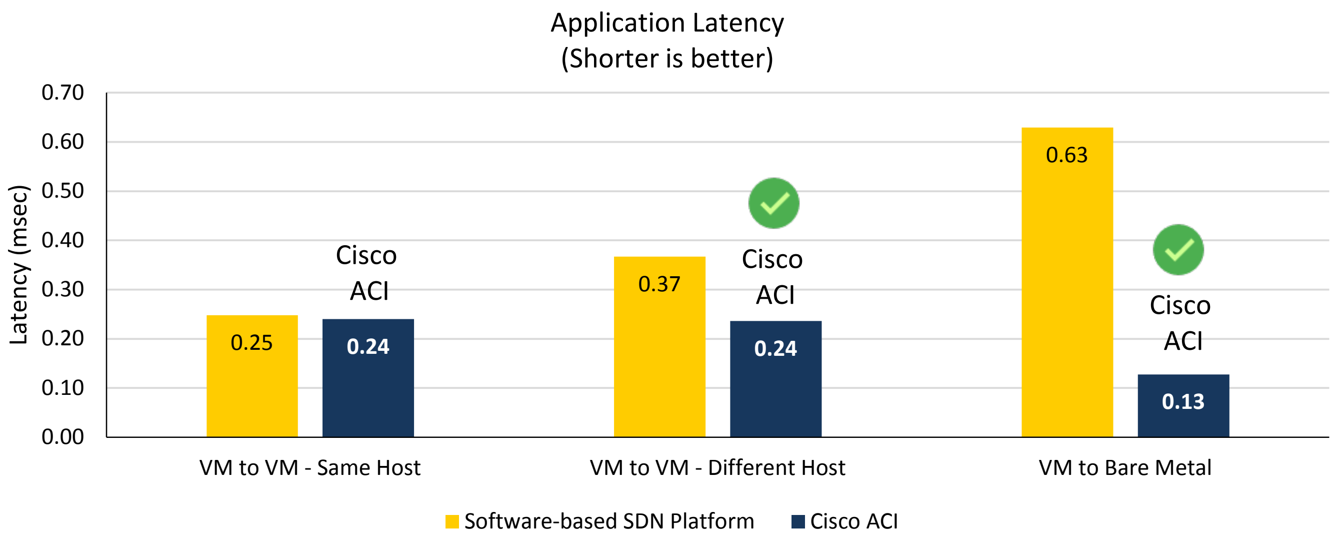
ESG Lab Testing

Performance testing is largely application-dependent, and many factors contribute to understanding the results. Network infrastructure, storage throughput and latency, application software, and the hypervisor scheduler are all factors that can impact performance in some way. ESG Lab selected three simple metrics to measure performance of Cisco ACI as compared with a software-only SDN platform.

Application latency was measured using Linux nmap version 6.40. Network throughput was tested using Linux iPerf3 using maximum segment sizes (MSS) of 250, 500, and 1,448 bytes. Application throughput was tested by downloading a 7GB file using two different protocols: an HTTP file transfer using *wget* from Apache running on CentOS. All tests used Cisco C220-M4L servers with dual Xeon E5-2650, 10-core CPUs. Large receive offload (LRO) and TCP segmentation offload (TSO) were enabled at the host and guest levels, and receive side scaling (RSS) was enabled on all hosts with VXLAN-capable NICs. All VMs used for testing were created from a single template with identical vCPU, memory, and network configurations. Because test results on virtualized x86 platforms can vary slightly across individual iterations, each test was executed ten times and the results were averaged to make the results more accurate and consistent.

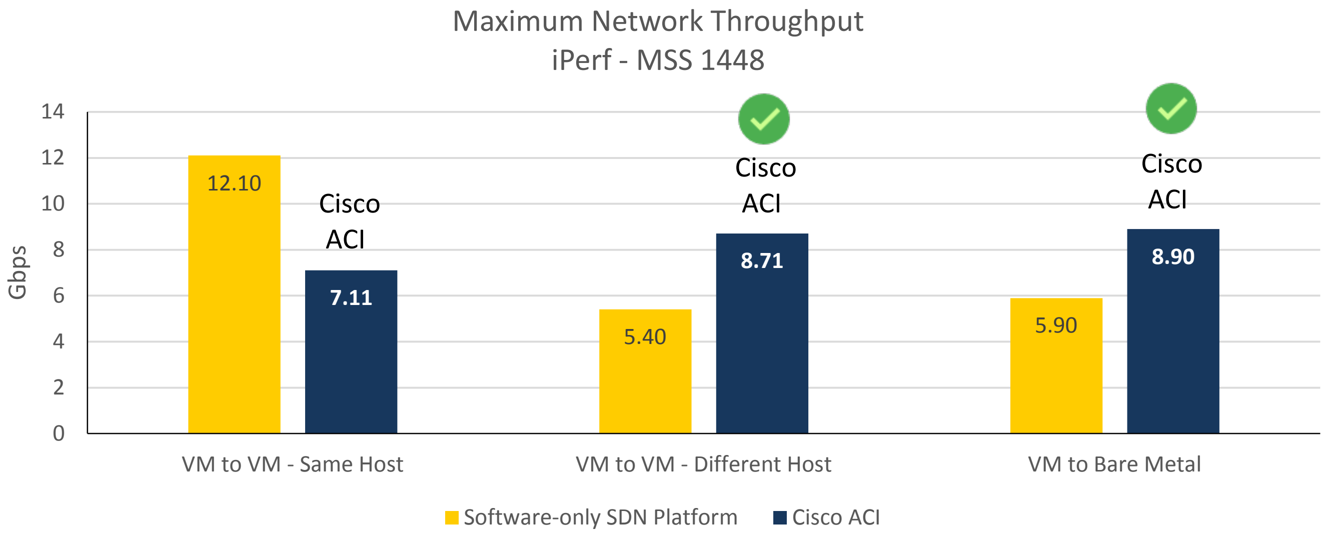
Figure 4 shows the latency between VMs in the same hypervisor, in different hypervisors, and from a VM to a bare metal. In all cases, Cisco ACI showed an advantage, with ACI providing 80% lower latency than the software-only SDN solution running in virtual machines.

Figure 4. Application Latency



Next, network throughput was tested using iPerf3. In these tests, the software-only SDN platform provided better performance when both VMs were on the same host, but when traffic had to cross to a different host, or using a non-virtualized bare metal server, Cisco ACI showed the advantage. Figure 5 shows the results with MSS set to 1,448, where ACI's performance advantage was 61% for VM to bare metal server traffic. In the tests with smaller segment sizes, the difference was more pronounced. At an MSS of 500 bytes, ACI's throughput for the same VM to bare metal test was 3.8 times that of the software-only SDN. With an MSS of 250, ACI's throughput between a VM and bare metal server was 6 times the software-only solution.

Figure 5. Network Throughput using iPerf3



It's important to note that in the VM-to-VM tests in the same host, the 10Gbps network uplink was a bottleneck for ACI as traffic between the VMs flows through the leaf switch. Cisco maintains that a 25Gbps uplink would have enabled ACI to achieve comparable throughput.

Finally, we looked at transfers of a 7GB file using *wget* to transfer files over HTTP.

Figure 6. Transfer of a 7GB File Using wget

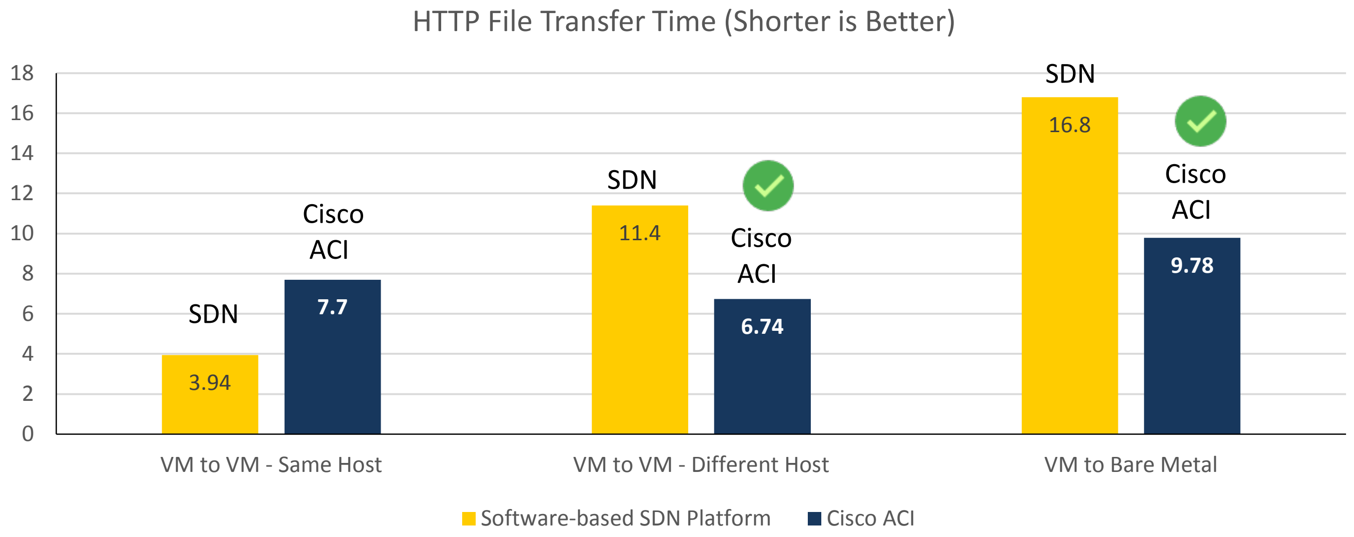


Figure 6 shows that while the software-only solution could transfer files between VMs in the same host faster, ACI provided better performance for transfers that crossed between hypervisors or to bare metal servers.

Why This Matters

Consistently high-performance networks are essential for modern enterprise computing. Every aspect of business is impacted by network health and functionality, as employees and customers access data and applications from multiple locations, on multiple devices. When asked to name the biggest challenges networking teams are facing today, nearly one in four cited providing network performance. Maximizing application performance was cited by 23% of respondents as a capability that would have the most impact helping organizations to grow their business.[4]

Through hands-on testing, ESG Lab found that Cisco ACI provided consistently better performance than a software-only SDN where overlay routing and gateway functions were provided in virtual machines. ACI provided 40-50% lower latency in tests between VMs on different ESXi hosts and up to 80% lower latency between VMs and bare metal servers.

While the software-only solution provided higher raw throughput between VMs in the same host, it is important to note that in real-world applications, most traffic will be between VMs on different hosts or from VMs to bare metal servers. Cisco maintains that using 25GbE NICs will eliminate the bottleneck and the performance for VM-to-VM communication on the same hosts will be comparable. For workloads between VMs on different ESXi hosts, ACI delivered comparable throughput and between VMs and bare metal servers, ACI delivered 33% higher throughput.

For file transfers, the type of application had an impact on the results for VMs in the same hypervisor, but when traffic had to traverse hypervisors or get to bare metal servers, ACI provided consistently better transfer times.

In simulated real-world environments, where traffic flows are dynamic and often unpredictable, flowing throughout the environment and involving both virtualized and non-virtualized applications and systems, ACI delivered consistently lower latency and better throughput, with predictable performance appropriate for mission-critical applications.

Network Availability

For modern, “always-on” businesses, disaster recovery and business continuity plans are of paramount importance given the high costs of downtime. ESG Lab examined availability in the Cisco ACI architecture as compared with a software-only SDN running in virtual machines.

ESG was interested in testing the active-active nature of ACI and looking at the convergence times users can expect relative to the various failure vectors of the different architectures and approaches. Examining the ACI architecture reveals just six fundamental failure vectors. ESG tested those failure vectors and documented the impact of both failure and recovery in Table 1.

[4] Source: ESG Survey, *Network Modernization Trends*, July 2017.

Table 1. ACI Failure Vectors

Failure Vector	Redundancy Mode	Impact on Failure	Impact on recovery
APIC node failure	scale-out cluster	none	none
APIC cluster failure	hot standby node	loss of access to the management plane	none, with a configuration backup
spine node failure	ECMP	sub-second	none
leaf node failure	ECMP, vPC	sub-second	none
leaf/spine link failure	ECMP, vPC	sub-second	none
Server link failure	vPC	sub-second (dependent on the server stack)	dependent on the server stack

Failing an APIC node and even the whole cluster had zero impact on performance, micro-segmentation, or SDN routing. All other failures had sub-second impact. ESG Lab also examined the architecture of the software-only SDN platform and found additional failure vectors based on the configuration of virtual machines as overlay routers and gateways.

Table 2. Software-only SDN Solution Failure Vectors

Failure Vector	Redundancy Mode	Impact on Failure	Impact on recovery
management VM	none (relies on hypervisor HA)	management plane, firewall	none, with a configuration backup
controller VM failure	scale-out cluster	none	none
controller cluster failure	vSphere HA, SRM	loss of access to the management plane, loss of ARP suppression	none, with a configuration backup
overlay router control VM single failure	HA (heartbeat)	30-32 seconds downtime	none
overlay router control VM double failure	none (vSphere HA)	total outage	none
gateway active/standby mode	ESG HA (heartbeat)	24 seconds downtime	none
gateway active/active mode	ECMP	24 seconds downtime	up to 12 seconds
underlay spine node failure	ECMP	sub-second (depends on underlay)	none
underlay leaf node failure	ECMP, vPC	sub-second (depends on underlay)	none
underlay leaf/spine link failure	ECMP, vPC	sub-second (depends on underlay)	none
server link failure	vPC	sub-second (depends on server stack)	depends on server stack

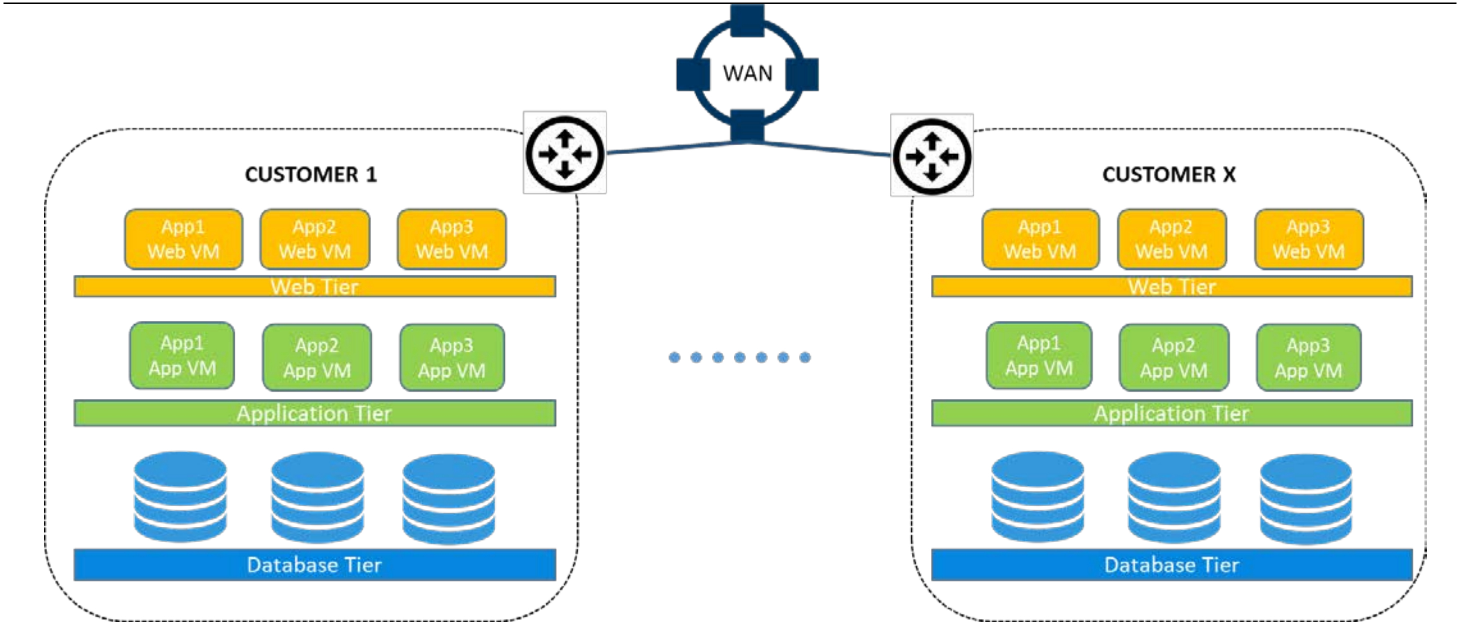
In testing, ESG Lab saw outages ranging from 24 seconds when a single gateway node failed to a complete outage of the SDN overlay network when multiple overlay router VMs were failed. The results of testing are detailed in Table 2. The failure vectors that have no approximate equivalent in ACI are highlighted in red. It is worth noting that some of these scenarios also apply to planned maintenance. Based on this analysis, ESG Lab concluded that Cisco ACI exposes fewer failure vectors than the software-only solution tested, and those failure vectors have a much lower impact on the environment.

Network Automation

ESG Lab also looked at automation options for ACI. Network automation is a key enabler of value for SDN technologies. Automation can speed up the delivery of network-based services while reducing costs. Network automation abstracts configuration information for network services from the physical infrastructure, which enables users to set up services with automated software orchestration tools.

ACI supports a wide variety of automation/orchestration tools, including Cisco UCS-D, Cisco Cloud Center, VMware vRealize Automation/Orchestrator, Microsoft Windows Azure Pack, OpenStack Neutron (multiple distributions), Ansible, Python SDK, and the ACI toolkit. ESG Lab used Ansible[5] to automate the creation of a three-tier topology with Internet/WAN access in both the ACI and software-only SDN environments for any number of applications or tenants, as seen in Figure 7. For this configuration, each customer gets her own routable subnets, customers must be isolated from one another, the web-tier subnet must be automatically announced to the WAN device, connections to bare metal subnets must be automatic, and the network control and the data plane must be redundant.

Figure 7. Creating a Three-tier Topology with Internet and WAN Access



Source: Enterprise Strategy Group, 2017

There were multiple challenges in implementing this scenario with the software-only SDN, including a couple of items that could not be automated, and one step that would require the DevOps engineer to have enough of an understanding of routing to be able to create static routes from the tenant gateways into OSPF, a complex prospect. The deployment of ten topologies for the software-only SDN took approximately 60 minutes to complete. In addition, the VM-based routers and gateways required 40 vCPU, 30 GB of RAM, and 60 GB of storage. The ACI deployment required zero routing expertise, automated every activity, required 20% fewer lines of code, and deployment of ten topologies completed in just 1.5 minutes. There were no new resources required for the ACI deployment.

[5] You can find Cisco ACI Ansible modules here: http://docs.ansible.com/ansible/devel/list_of_network_modules.html#aci

Why This Matters

In modern environments with highly distributed resources and workforces, network availability is both business- and mission-critical. If the network fails, everything fails. As networks expand to handle today's web-scale business, they become more complex and difficult to deploy and manage, leading to performance and uptime problems, which frustrates users and alienates customers.

Software-defined networking was invented to simplify network control and operations by abstracting the control and data planes from the underlying hardware. By creating dynamic, programmable, logical network components based on high-quality physical ones, SDN can deliver more dependable network services that are easier to design, manage, and troubleshoot.

Not all SDNs are created equal, though. Software-only SDN solutions where routing and gateway functions run in VMs can be problematic when it comes to supporting mission-critical applications that require sub-second convergence like voice, video, or financial services.

ESG Lab validated that Cisco ACI provides a highly available, active-active SDN suitable for mission- and business-critical applications. ACI's architecture has fewer failure vectors and all the network failure events ESG tested showed zero or sub-second traffic impact. With the software-only SDN, ESG saw higher complexity and more failure vectors, along with up to 32 seconds of downtime on single failure events, due to the active-passive nature of the architecture.

ESG Lab leveraged Ansible to automate provisioning of a private cloud environment with ACI more than 40 times faster than would be possible with the software-only SDN. ESG Lab also confirmed a significant compute and storage capacity savings since ACI does not require additional VMs to execute routing and gateway services.

Security

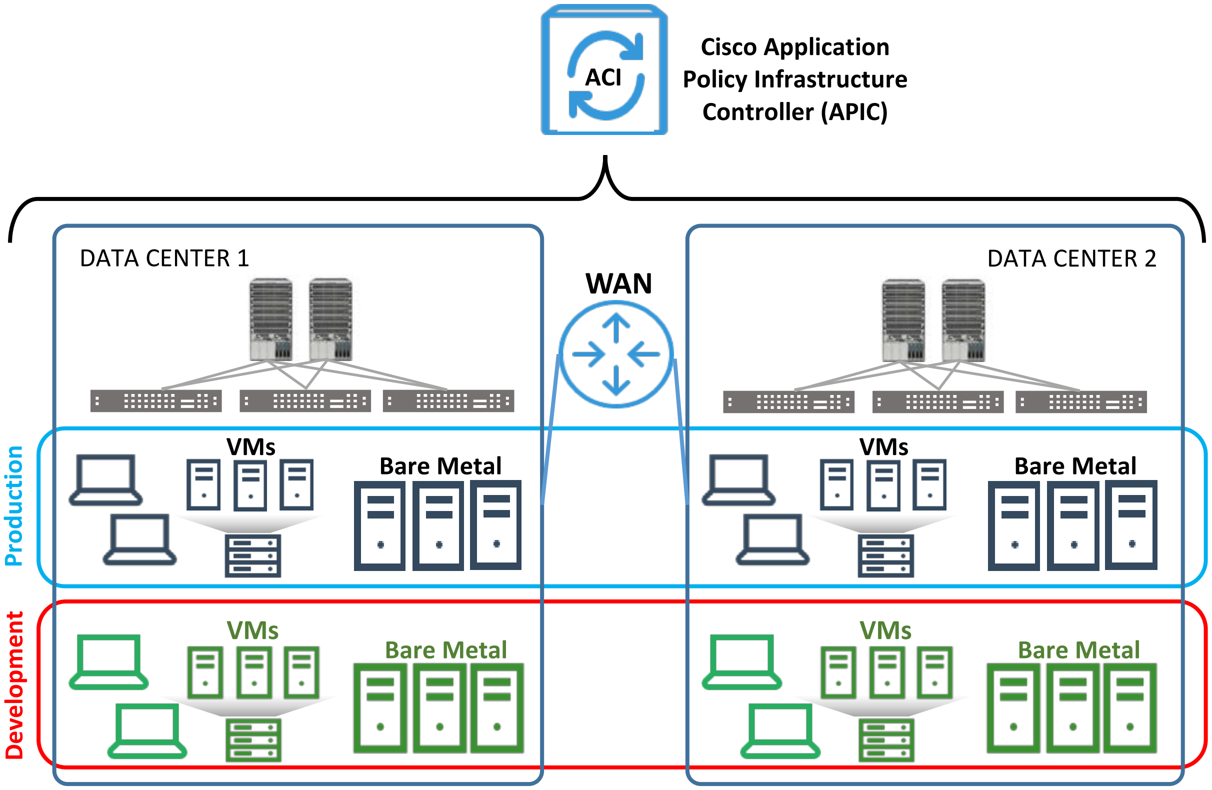
Cisco ACI is designed to provide consistent micro-segmentation support for multiple hypervisors, bare metal endpoints, and containers, which enables granular endpoint security enforcement. Micro-segmentation enables security policies to be applied at the workload level, rather than depending on other network elements (e.g., firewalls) to provide end-to-end network security at the network traffic level alone. To enact security policies, Cisco ACI will construct a contract specific to each type of workload. The contract dictates the data and endpoint(s) a workload can access, regardless of its placement in the data center. If a workload is moved within or between data centers, Cisco ACI maintains that contract. ACI contracts define security rules up to Layer 4. Contracts in ACI can also define other parameters like QoS.

ESG Lab Testing

ESG Lab first examined how Cisco ACI applies security rules consistently across workloads located in two data centers and under different vCenters. The data centers were connected to each other by an IP-routed WAN. Figure 8 depicts the test topology. We set up two clients in separate WordPress production and development sites in one data center. We then used Cisco ACI to enable micro-segmentation to span both data centers and apply the following firewall rules:

- Allow the production client in the WAN to communicate with the production WordPress sites in both data centers while preventing communication with the development sites.
- Allow the development client in the WAN to communicate with the development sites in both data centers while preventing communication with the production sites.

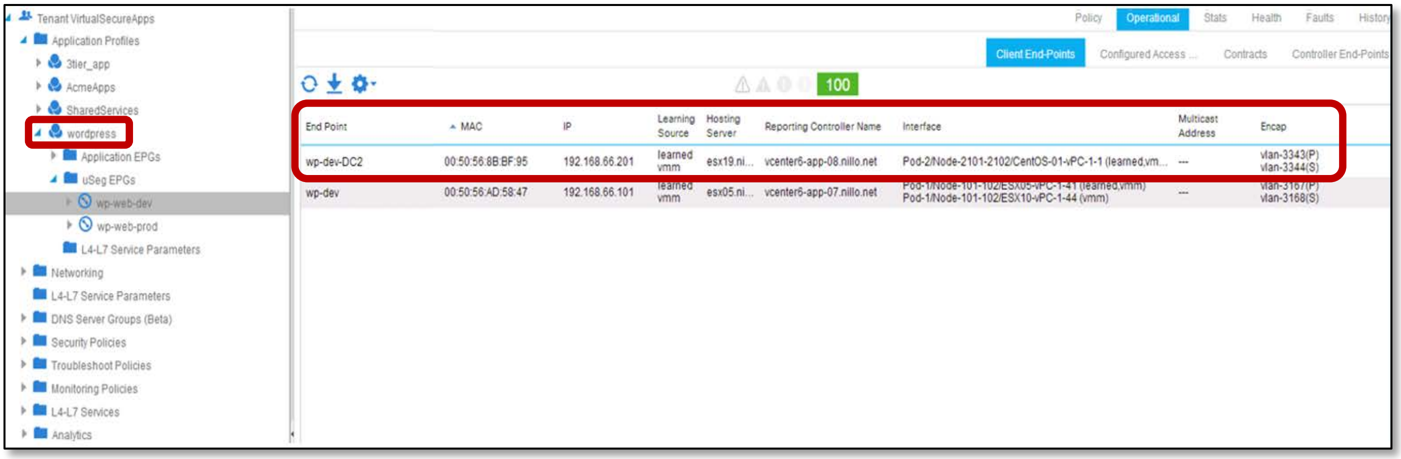
Figure 8. Lab Topology: Micro-segmentation Across Data Centers



Source: Enterprise Strategy Group, 2017

Critically important, the VMs were classified into the correct security policies using vCenter objects, in particular a combination of vSphere Tags. We then confirmed that the firewall rules were observed, as each client communicated with the sites as defined in its individual contract. More importantly, we saw that Cisco ACI applied the same firewall rules to both production and development sites in both data centers, even as VMs were moved across different vCenters using vMotion. ESG Lab also reviewed the details of individual VMs under micro-segmentation across both data centers. Workload details included IP address, MAC address, and server host. Figure 9 shows the details for the development VMs in both data centers. In addition to VM details, contract details can be viewed to ensure that Cisco ACI is enforcing the correct policies.

Figure 9. Individual Workload Details in the ACI GUI



End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Encap

wp-dev-DC2	00:50:56:8B:BF:95	192.168.66.201	learned vmm	esx19.ni...	vcenter6-app-08.nillo.net	Pod-2/Node-2101-2102/CentOS-01-vPC-1-1 (learned,vm...	---	vlan-3343(P)
								vlan-3344(S)

wp-dev	00:50:56:AD:58:47	192.168.66.101	learned vmm	esx05.ni...	vcenter6-app-07.nillo.net	Pod-1/Node-101-102/ESX05-vPC-1-41 (learned,vmm)
						Pod-1/Node-101-102/ESX10-vPC-1-44 (vmm)
							---	vlan-3167(P)
								vlan-3168(S)

Source: Enterprise Strategy Group, 2017

ESG also conducted the same test with the software-only SDN solution using a similar topology. We observed that unlike Cisco ACI, this software solution could not maintain firewall policies across the two data centers when the VM migrates between different vCenters. We found that the policies broke when attempting to apply the rules consistently across data centers.

Why This Matters

When asked to name the networking capabilities that would have the greatest impact on helping organization to grow their business, 46% of respondents to a recent ESG survey cited ensuring network security, making it the most cited answer by a wide margin.[6]

As enterprises continue to virtualize their applications, enforcing data center network security becomes increasingly complex, especially when VMs can be moved to different hosts both within and between data centers. Applying security rules and policies at the network level can become complicated as IT professionals must ensure that all network elements within the data center network apply rules and policies consistently for all types of network traffic. Inconsistency in policy enforcement can result in data loss, network vulnerabilities, and unplanned outages, all of which can lead to brand erosion and revenue loss.

ESG Lab tested the ability of Cisco ACI to provide consistent micro-segmentation support to workloads in multiple hypervisors, bare metal endpoints, and containers—across data centers connected via a WAN. We applied a contract to a production workload and to a development workload, which provided granular endpoint security enforcement across two data centers. We saw that both workloads could communicate only with the sites defined in the contract. We conducted the same test with a software-only SDN solution and found that the policies broke when attempting to apply the same firewall policies to the same workloads across data centers.

[6] Source: ESG Survey, *Network Modernization Trends*, July 2017.

Customer Interview

ESG Lab spoke with Indranil Sengupta, the head of Product Engineering and Operations for NTT America, about their use of Cisco ACI in NTT America's cloud data center. NTT America serves North, South, and Central America as part of NTT Communications, a global Fortune 500 company. This division of NTT America provides managed infrastructure services for global enterprise customers with complex requirements.

NTT America provides infrastructure platforms and ongoing management for both test/dev and production needs. To be successful in this competitive industry, they must provide consistent, secure services that scale, while constantly focusing on improving efficiency. Cisco ACI's software-defined networking automates the deployment and ongoing management of networking services, enabling NTT America to manage with less effort and cost, and to quickly and easily adjust services as customers' needs change and grow.

Multi-tenancy is essential to keeping managed service platforms cost-effective, but because of the complexity of NTT America customers' requirements, each tenant infrastructure is different. Typical hyper-scale web services support multi-tenancy using a cookie cutter approach, with all services essentially the same—not an option with the complex requirements of NTT America's customers. Cisco ACI makes it possible to leverage the efficiency of multi-tenancy while providing tailored networks for each customer. Without Cisco ACI, NTT America engineers would have to individually create each tenant environment—disruptive to customers and costly for NTT America.

With Cisco ACI, NTT America can more easily scale their service delivery, reducing costs. Cisco ACI has also enabled the company to reduce time to service. "We deployed a solution for a financial customer—it was complex, with stringent compliance and security parameters," commented Sengupta. "Cisco ACI enabled us to deploy it in half the expected time, and the customer was thrilled."

NTT America plans to continue expanding its Cisco ACI deployment to more customers and leveraging the increased efficiency and flexibility it provides. Said Sengupta, "This is a very competitive industry, so every quarter we need incremental improvement in reducing effort and costs. With Cisco ACI, we can provide more and better services to customers without increasing the price."

The Bigger Truth

Keeping up with the pace and scale of business today is demanding on IT. Administrators are stretched to the limit, often handling hundreds of applications with different requirements, as well as users in multiple locations with numerous endpoints. In addition, the consumerization of IT has resulted in users having not only higher expectations, but also enhanced standing. In this context, a sophisticated SDN solution is not just a "nice to have," but rather an underpinning of a successful and profitable business. Operational simplicity and automation capabilities are futile if not supported with consistent high performance. A superior and seamless customer experience demands a highly available, "always-on" ecosystem for modern applications supporting throughput- and latency-sensitive mission-critical applications like video, voice, and financial services. To provide a viable security model, an SDN solution must bind and protect applications across multiple data centers both vertically and horizontally.

As more organizations look to embrace the hybrid cloud movement and expand application execution across the on-premises and multi-cloud domains, they must shift from infrastructure-focused management to application-centric management to leverage modern IT systems, including public cloud services and technologies such as containers and microservices. This does not mean that infrastructure management is no longer important, but it does show that the focus for hybrid cloud is the abstraction of the underlying infrastructure to support applications. As companies continue to leverage new technologies to support their IT transformations, hybrid cloud will become a driving technology, and a rock-solid SDN strategy to support those dynamic applications is a requisite for a successful hybrid cloud strategy.

Cisco ACI offers such a solution, creating an ecosystem that delivers application-focused networking services for efficiency, simplicity, security, high performance, and high availability. It includes physical, virtual, and cloud elements, and scales easily along with an organization's growing environment. Leveraging software-defined networking from a controller cluster and Nexus 9000 Series switches, Cisco ACI discovers and manages the network fabric across multiple hypervisors and data centers, and its open framework makes it easy to integrate with solutions from network management and orchestration vendors.

ESG validated that ACI delivered consistent, high performance that translates well to real-world environments, where traffic flows are dynamic and often unpredictable, involving both virtualized and non-virtualized applications and systems. In ESG testing, ACI delivered consistently lower latency and better throughput, with predictable performance appropriate for mission-critical applications. ESG Lab validated that Cisco ACI provides a highly available SDN suitable for mission- and business-critical applications. All network failure events ESG tested showed zero or sub-second traffic impact.

ESG Lab leveraged Ansible to automate provisioning of a private cloud environment with ACI more than 40 times faster than would be possible with a software-only SDN. ESG Lab also confirmed a significant compute and storage capacity savings since ACI does not require additional infrastructure VMs to execute routing and gateway services. ESG also validated that Cisco ACI can apply micro-segmentation and security policies consistently within and between data centers.

Organizations are increasingly challenged to build networks that can respond to the business needs of highly virtualized data centers and public and private clouds with a mix of virtualized and physical infrastructure. ESG found that Cisco ACI provides a simple, scalable, and highly available network that is well-suited for mission-critical workloads. If your organization is interested in improving the automation, agility, security, and availability of your networks across multiple hybrid data centers, ESG Lab recommends taking a close look at Cisco ACI.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.