WHITE PAPER

Rethinking Software-Defined Networks

F5 and Cisco enable enterprises to build an SDN that reduces application delivery time, operational costs and risk of downtime by "operationalizing" the network.

Software-defined networks (SDNs) represent a step forward in networking technology, but it's now become clear that it's going to take some new thinking about how to implement SDNs if they are to support enterprise requirements and gain traction.

Few, if any, organizations have deployed SDNs beyond a pilot phase, and for good reason. While SDNs hold promise in terms of improvements in flexibility, agility and ease of management, in practice companies are not convinced they can deliver at enterprise scale. Device configuration quickly becomes too difficult and expensive to perform, particularly for Layer 4–7 stateful services such as firewalls, load balancers and Web performance optimization. What's more, the layering of virtual network services—in effect disconnecting them from the underlying physical infrastructure—can lead to a lack of end-to-end visibility that makes SDNs difficult or impossible to manage and troubleshoot.

"There's been a lack of clarity in terms of the SDN value proposition, with much of the SDN industry focused on reducing the cost of hardware," says Zeus Kerravala, principal analyst with ZK Research. "I don't think many customers really care about that. They want environments that are easier to manage and enable applications to perform better. That hasn't really been the top priority for SDN pure-play companies."

BUILDING A TRULY EFFECTIVE SDN

Addressing the issues starts with an approach to SDNs that places policy control in a centralized controller, but with distributed policy implementation and execution. That makes it possible for companies to centrally determine the level of service each application should receive, but automate the chore of ensuring the policies are carried out.

Today the network can become a bottleneck when delivering applications because human beings have to configure the Layer 4–7 devices that ensure proper application performance, security and availability. "Historically, it can take months to deploy applications and services, and a lot of the reason is human latency," Kerravala says.

For an SDN to be effective on an enterprise scale, it has to be built on an open architecture to support multivendor implementations. It also needs to be able to work with both the physical network infrastructure and the virtual servers and storage systems deployed on top of it.

> "Historically, it can take months to deploy applications and services, and a lot of the reason is human latency."
>
> —Zeus Kerravala, principal analyst
> ZK Research

And it has to be manageable. "People will not put SDNs in place if they can't manage them," says Jim Metzler, principal with Ashton, Metzler & Associates. "Say you're running an SDN solution on top of a hypervisor and you can't map between the two of them. Suddenly your application is running badly and you don't know why. That's really bad. You certainly need effective end-to-end management."

F5 AND CISCO DELIVER

Delivering on all of these requirements requires an SDN solution that is at once open, scalable, programmable, secure and manageable. F5 has teamed with Cisco to deliver just such a solution, one that enables customers to "operationalize" the network—meaning, automate numerous tasks that are done manually today. The result is the ability to automate end-to-end application delivery across a flexible, application-aware network fabric, providing the speed, reliability and security that businesses need.

A focus on applications

The joint F5 and Cisco solution marries the Cisco Application Centric Infrastructure (ACI) architecture with F5's deep expertise in an area that's been missing from the SDN discussion: application-layer services.

F5 Synthesis fills the gap by delivering Software Defined Application Services (SDAS). Just as virtual server technology enables the abstraction of server software from the underlying hardware, Synthesis enables abstraction of application services such as application access control, Web and mobile application acceleration, and more. It enables these Layer 4–7 services to be provisioned as services across any combination of physical, virtual and cloud platforms rather than as individual devices.

Cisco ACI is a data center architecture that combines a high-performance network fabric with centralized, policy-based control to enable automated application provisioning without sacrificing scalability, security and full end-to-end management.

The joint F5 and Cisco solution simplifies and automates end-to-end application delivery across an integrated and elastic data center fabric, providing each application with an appropriate level of speed, reliability and security.

"Other than F5 and Cisco, the rest of the network industry hasn't focused much on the impact of SDNs on applications," Kerravala says. "If your value proposition is to make applications run better, you have to focus on applications."

Open and programmable

The combined F5 and Cisco solution is built on open, published APIs that enable rapid integration of components from various vendors. The solution also embraces open source software and open standards and protocols, including the OpenStack cloud computing platform, along with multiple hypervisors.

The solution supports the idea of programmability, which enables switches and other network components to react to events in real time as they happen in the network and route traffic accordingly—a feat statically programmed switches simply can't accomplish.

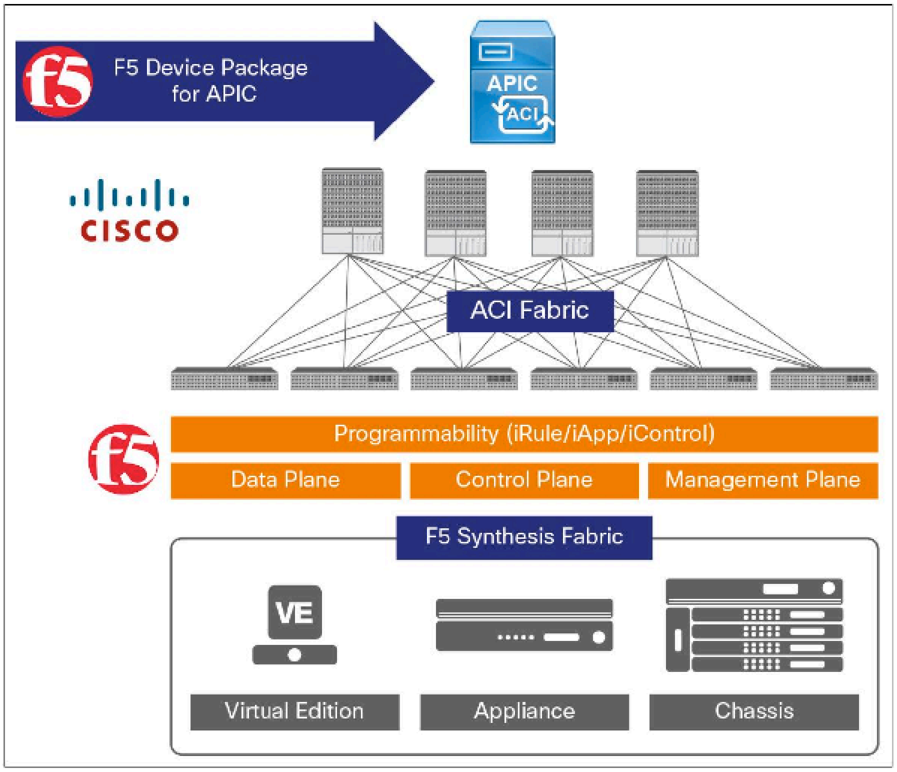
Scalable, manageable, secure

The central policy controller (Cisco APIC) helps the solution deliver on both scalability and enterprise-level performance. It automates the process of configuring the various Layer 4–7 services responsible for ensuring quality of service across the enterprise.

"If you automate that application provisioning process, you can make changes a lot quicker," Kerravala says. "There's a lot of value in that."

The solution also ensures secure multitenancy with respect to virtualized servers, software instances and virtual network overlays. That's another crucial requirement for SDNs given enterprises and carriers will likely want to have multiple different business units or customers sharing some of the same physical infrastructure in their SDN environments.

"Those networks have to be kept completely separate from one another from a security perspective," Metzler says, such that a breach on one won't affect the other. Kerravala says that can be difficult to achieve with a virtualization overlay model, where the physical and virtual infrastructure are invisible to one another. "There needs to be greater awareness," he says.



Finally, the combined F5 and Cisco solution includes detailed telemetry, or instrumentation of various components, to enable the end-to-end monitoring and management that Metzler says is a must-have.

BENEFITS OF AN EFFECTIVE SDN

The net result is an SDN that brings benefits in three general categories: improved time to market, reduced costs and reduced risk.

Time to market

The automation capabilities inherent in the F5 and Cisco solution mean companies can deploy applications much more quickly. The network is no longer a bottleneck because the "human latency" to which Kerravala refers is removed. That means improved time to market for applications, which translates into improved business performance and agility.

Reduced costs

More automation also means fewer tasks for humans to perform, which reduces complexity and results in substantial savings. "Of the total cost of ownership in a data center, people costs are about 40%," Kerravala says. "If you can reduce people costs through automation, you get big savings."

Less risk

Automating tasks once performed by humans also reduces risk. "The largest cause of downtime in a data center is human error," Kerravala says. "If you can automate what humans do, the number of human errors goes down." And with a reduced number of errors, the risk of downtime likewise goes down.

Operationalizing the network

What it all adds up to is "operationalizing" the network, with the end result being simplified operations and troubleshooting, less downtime and faster deployment of new services.

"Another value proposition that has gone underappreciated is a shift to more of a Dev/Ops model," Kerravala says. Today, application development and network operations teams have no knowledge of one another, so developers may create applications that he says "wreak havoc on the network. If I can bring them together, I'll have an underlying IT infrastructure that'll run more smoothly."

To learn more about the F5 and Cisco alliance and how they are rethinking SDNs, click here to visit the F5 page and here for the Cisco page.