White Paper

Cisco ACI and Citrix NetScaler: Opening the Way to Data Center Agility

Business Agility Requires Data Center Agility

Today's successful enterprises innovate and respond to change faster than their competitors. They deploy new products and services faster, leverage new technologies faster, and respond to marketplace changes faster. They demonstrate business agility.

Information technology departments have made great strides in supporting business agility. “Agile” software development methods speed up application delivery. “DevOps” practices streamline software releases. Virtualization technology allows application processing to be moved and expanded in minutes. Mobile technologies give customers and employees new choices for interacting with applications.

However, some data center technologies have become barriers to flexibility and responsiveness. Much of the networking and security infrastructure that supports applications remains “hardwired.” Networking and security devices must be configured individually. Processes to modify configurations and add new devices are slow and laborious. Highly skilled experts are needed to make even small changes.

In fact, in most enterprises today data center agility, or more accurately the lack of it, is a major drag on business agility. Applications themselves have become far more flexible, but many of the promised business advantages cannot be realized while the infrastructure is rigid.

Fortunately, leading-edge technology companies are developing products, methods and standards that support flexible, application-centric infrastructures.

In this white paper we will discuss:

- Why data center limitations are restricting business agility.
- How Cisco Application Centric Infrastructure (ACI) supports frequent changes in applications and infrastructure.
- How Cisco and Citrix® have integrated NetScaler® with ACI to improve data center agility.

Why Data Center Limitations are Restricting Business Agility

Most data center technologies and tools are blind to applications and application requirements. When application developers and business managers define infrastructure requirements for applications, those requirements must be translated by highly skilled experts into detailed configurations for the building blocks of the infrastructure, including servers, storage systems, networking devices and security devices. Those detailed configurations need to be laboriously implemented on the infrastructure components.

When applications need to be modified, expanded or deployed differently, the new requirements need to be re-translated into detailed configuration changes, and these changes need to be manually applied to all of the affected systems and devices.

To see how this “failure to communicate” can slow the delivery of new applications and impede a business from responding to changing market and operational needs, let’s look at a two-part scenario.

Scenario Part 1: Rolling out a new e-commerce application

The CEO of a manufacturing company has set a goal to increase online sales 30% in the coming year, driven primarily by the introduction of an innovative new product line. To accomplish this, the company needs to roll out an enhanced three-tier e-commerce application that allows web site visitors to simulate the use of the products under conditions set by the customer.

Timing is critical. The company’s major rival has announced that a competitive product line will be launched in three months. Every week of lead-time over the competitor will increase revenue and help the company lock in new customers.

The application development group has finished coding and testing the application. They hand it over to the operations and networking group to deploy it in the data center.

Determining the basic structure of the data center infrastructure to support this application is not difficult. The operations team determines that the application could be handled by a pair of routers, a switch, a firewall for security, and an application delivery controller (ADC) to increase application performance and reliability, as shown in Figure 1.

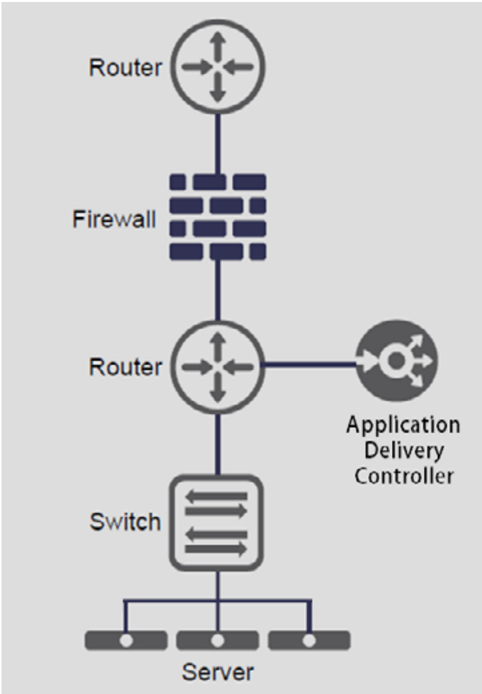

Figure 1: Infrastructure components to support th application

Unfortunately, the process of installing and configuring the security and networking components ("service insertion"), is much more complex. Figure 2 shows a subset of the tasks involved.

Preparing the infrastructure for the application requires:

- Staff with detailed knowledge of how to translate application requirements into infrastructure details, and how to configure network equipment, firewalls and load balancers.
- Painstaking work to set parameters on each individual device.
- Extensive testing, because the manual configuration process is so error-prone.

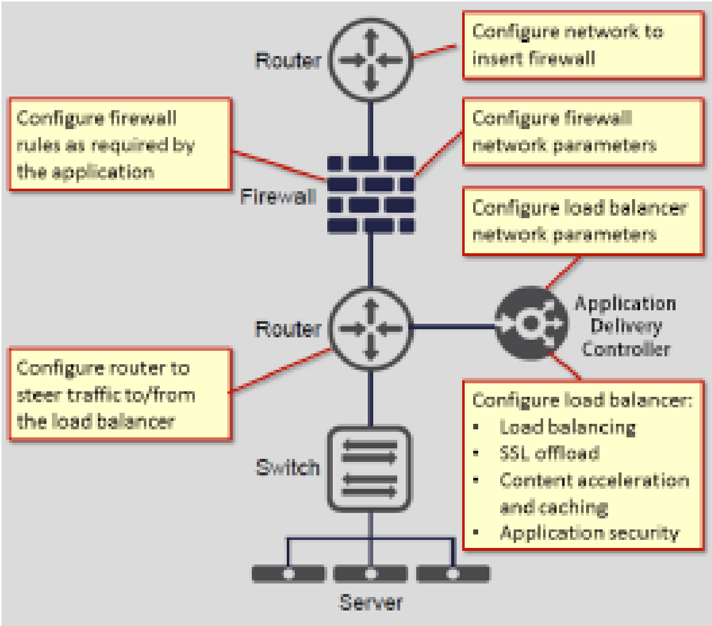

Figure 2: The "services insertion" process involves setting rules and parameters manually on many devices

In the end, the service insertion process will take several days. Not only is this expensive in terms of the valuable time of the operations staff, the delay might cost tens of thousands of dollars in current and future revenues. There is also a risk that not everything will work right when the application is launched, resulting in customer dissatisfaction and additional lost sales.

Scenario Part 2: Responding to change

Good news!

The new products are a huge hit! Everyone in the industry wants to try them. The reviews are ecstatic. Web site visitors also love the new simulation feature on the web site; they play with it for hours.

Bad news!

The spike in traffic has brought the application to its knees. Customers are using the new simulation feature more than forecast, and the feature requires more processing power than anticipated. Several large customers want to link to the application via SSL VPNs, which would further overload the current infrastructure. If the company can't fix these problems, customers will become frustrated and wait to see the competitor's version, costing the company hundreds of thousands of dollars in revenue and customer good will.

The solution is not difficult in theory: add more servers and an SSL VPN appliance, activate more performance optimization features in the application delivery controller – and replicate the entire application infrastructure at a second data center in Asia.

But service insertion becomes a bottleneck once again:

- The SSL VPN appliance needs to be installed and configured.
- The routers and the firewall need to be reconfigured to include the SSL VPN appliance.
- The switch and the application delivery controller need to be reconfigured to accommodate the new servers, and the new features must be activated on the ADC.
- The entire time-consuming manual configuration process needs to be repeated at the Asian data center.

These steps might delay the company's response for several more days.

Beyond the Scenario

The situation in today's data centers is actually much more complex than implied in the scenario described above. In a typical enterprise:

- The infrastructure includes hundreds or thousands of servers and devices.
- Applications are deployed in virtual environments, or split between physical, virtual and cloud-based systems.
- Applications with very different networking and security share the same infrastructure.
- Applications and infrastructure are continually being enhanced and upgraded.

In this complexity, even trouble-shooting problems and implementing minor changes requires extensive expertise and painstaking attention to detail, making infrastructure the least agile part of the information technology environment. These conditions explain why more than 80% of data center spending goes to operational tasks, leaving less than 20% available for enabling innovation.[1]

So what can enterprises do to enable true data center agility? The next sections of this white paper will look at how the Cisco Application Centric Architecture (ACI) changes the way networking and data center services are provisioned for applications, and at how Citrix NetScaler fits into ACI. It will then return to the scenario described above and show how ACI and NetScaler can change completely how enterprises respond to changing business needs.

1 IDC: "New Economic Model for the Datacenter," 2011

Cisco ACI: Letting Applications Drive Infrastructure

Cisco Application Centric Architecture (ACI) is a data center technology initiative designed to radically simplify and accelerate the entire application deployment lifecycle. It allows enterprises to create application-centric policy models, then use those models to provision computing, networking, storage and other data center services from a central location.

In short, ACI allows applications to drive networking behavior, instead of the reverse. Benefits of ACI include:

- Reducing service insertion times from days to hours, or even minutes.
- Simplifying the process of translating application requirements into infrastructure configurations, so service policies can be defined in terms of application components instead of network elements like VLANs, IP subnets and Layer 4 ports.
- Enabling networking and data center services to be configured and managed from a central point of automation and control, so application policies can be applied consistently and reliably across the enterprise.
- Reducing costs, by automating manual operations to free up staff resources, and by minimizing downtime caused by errors and misconfigurations.
- Simplifying the management of applications that cross physical, virtual and cloud environments, and multi-tenant environments where several applications share the same infrastructure.
- Allowing servers and service appliances to be grouped into resource pools, so services to applications can be scaled up and down quickly to meet changing demands.

In this white paper we provide a high-level view of Cisco ACI with a focus on how it increases data center agility by enabling rapid service insertion. For more detailed information on ACI, please see the documents listed in the Resources section at the end of the paper.

Creating an Application-Centric Policy Model

Cisco ACI provides very powerful concepts and tools for creating policy models of applications and the infrastructure elements that support them. The three most important are Endpoint Groups, Policies and Application Network Profiles.

“Endpoint Groups” (EPGs) are a collection of similar endpoints that represent an application tier or a set of services. The endpoints themselves are typically physical servers or virtual machines, but they can also be systems such as network storage systems and security and network devices.

ACI “policies” define connections and services between EPGs. These include access rules and security parameters, quality of service (QoS) settings, and rules and filters for Layer 4 through Layer 7 services.

An “Application Network Profile” (ANP) is the combination of EPGs and the policies that define their interaction for a specific application (Figure 3).

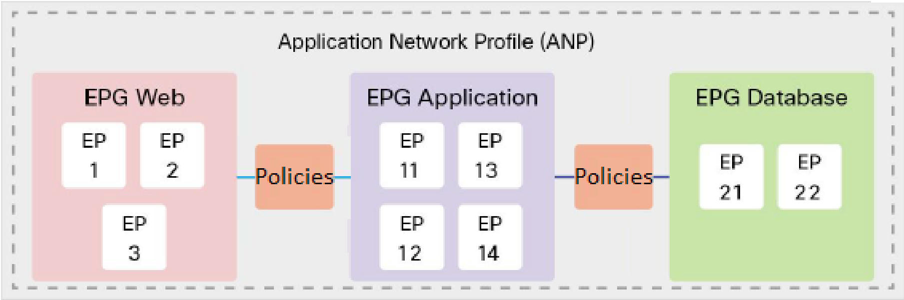

Figure 3: An Application Network Profile (ANP) is made up of endpoint groups (EPGs) and the policies that define thier interaction

In the scenario discussed earlier, the e-commerce application might be modeled as having three EPGs, one providing the front-end web services, a second running the application logic, and a third supporting the database, as shown in Figure 3. The endpoints within an EPG can be varied, including combinations of physical servers and virtual machines, but they perform functions for the same tier of the application, and the policies connecting them with other tiers are the same. For the e-commerce application the policies between the web tier and the application tier might include access control lists and rules for the firewall, QoS rules giving some types of transactions priority over others, and rules governing how transactions from the web tier will be balanced across resources in the application tier.

This model provides many benefits for an agile data center. Most importantly, EPGs act as a single policy enforcement point for a group of contained objects. Policies can be defined once for the entire EPG rather than individually for each endpoint. Those policies then control interactions between all the members of the first EPG and all the members of the second. In Figure 3, a single set of policies governs transactions between EP1 in the web tier and EP11, EP12, EP13 and EP14 in the application tier, between EP2 and all of the endpoints in the application tier, and so forth.

Figure 4 illustrates the impact of this approach. In a standard networking model, linking five endpoints in a web tier to four endpoints in an application tier, with five filter rules between each pair, would require 100 policy entries (5x5x4=100). In the ACI model, linking one source EPG to one destination EPG, with five filter rules between, requires only five policy entries.

The same ratio applies to changing one of the rules. In this example, changing filter 3 would require 20 entries in the standard model (changing filter 3 between source 1 and destination 1, between source 1 and destination 2, between source 1 and destination 3, etc.), versus one entry with ACI.

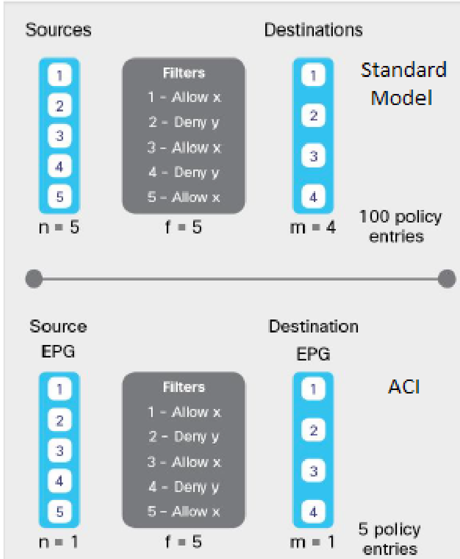

Figure 4: Defining policies once between endpoint groups dramatically reduces the number of policy entries needed

Similar benefits apply for adding, removing and moving endpoints. As shown in Figure 5, when an endpoint is moved from one EPG to another, the policies for the new EPG are automatically applied to the endpoint. There is no need to make a complete set of policy entries for the endpoint in its new location to manage how it communicates with endpoints in other tiers.

The ACI model also provides for reusability and policy consistency. Application Network Profiles can be reused, for example to replicate the same set of application policies in different data centers. Policy sets can be reused between similar applications. Reusing policy sets not only accelerates the deployment of new applications, it also simplifies maintenance and reduces errors, because network and system administrators will be able to work with the same settings across the enterprise.

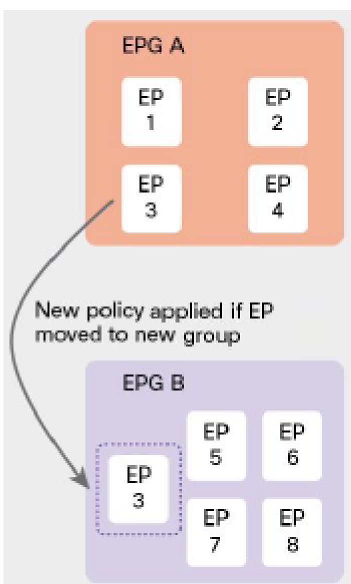

Figure 5: ACI reduces the work needed to add, remove and move endpoints

Managing the ACI Fabric: the Cisco APIC

The Cisco Application Policy Infrastructure Controller (APIC) serves as a single point of control and a central data repository for the Cisco ACI. It is where administrators define the endpoint groups, policies, application network profiles and other components of the ACI. As illustrated in Figure 6, it also provides the mechanisms to communicate the relevant policies to data center resources, including those used for:

- Physical networking
- Hypervisors and virtual networking
- Layer 4 to Layer 7 services
- Wide Area Network and cloud services
- Storage
- Computing

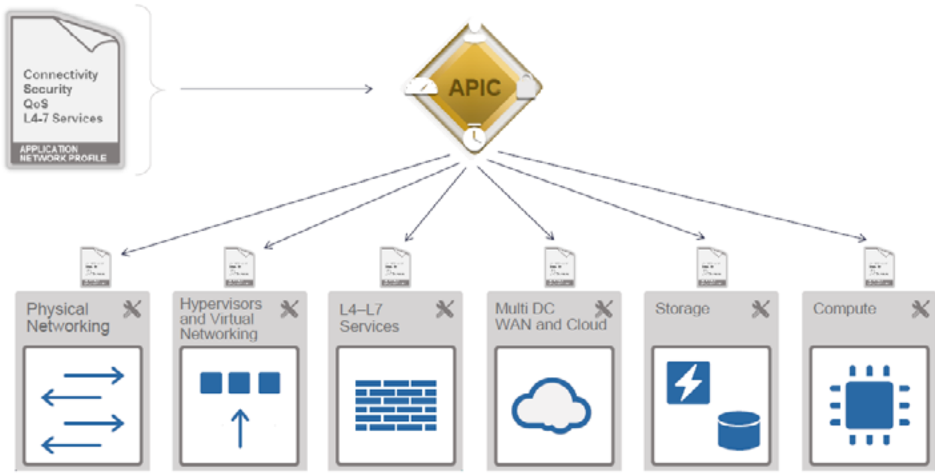

Figure 6: The Cisco Application Policy Infrastructure controller (APIC) serves as a single point of control and a central data repository for Cisco ACI

APIC includes a Policy repository that maintains all of the ACI policies and rules for the enterprise, and an Endpoint registry that includes information on all of the endpoints known to the ACI.

Policies are distributed to endpoints when the endpoints attach to the ACI, through other triggers, or by an administrative static binding.

APIC also includes an Observer subsystem that monitors the operational state, health and performance of hardware and software related to ACI. This gives administrators visibility into network behavior as it relates to applications, including real-time metrics and detailed resource consumption statistics.

One of the great strengths of APIC is that it offers a graphical drag and drop GUI to create Level 4 to Level 7 "Service Graphs" (Figure 7). A Service Graph makes it easy to specify the security, networking and other devices that provide services between two EPGs, and then to set policies to configure those devices. Service graphs can then be assigned to application profiles. This means that the policies of the ACI model can be created and deployed in minutes, rather than hours or days.

But how does the APIC translate policies into specific configuration settings used by security and networking devices? The white paper will now discuss how that works with Citrix NetScaler.

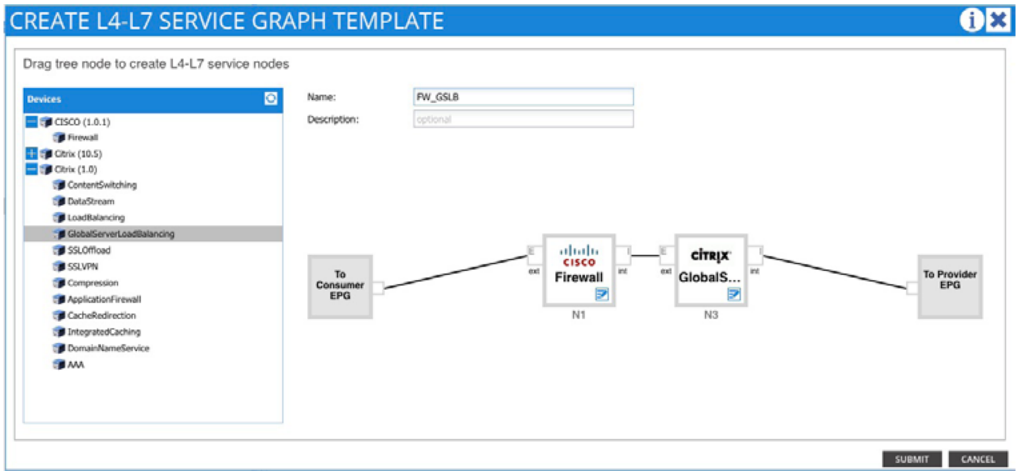

Figure 7: A Service Graph makes it easy to specify devices and policies between EPGs

Citrix NetScaler and ACI

NetScaler is the world's most advanced Application Delivery Controller for mobile and web applications. Key capabilities of NetScaler include:

- Load balancing, to distribute workloads across multiple servers in order to achieve optimal resource utilization, maximize throughput, and minimize response times.
- SSL offload and acceleration, to speed up the handling of the encryption and authentication requirements of Secure Socket Layer (SSL) web traffic.
- SSL VPN, to terminate SSL VPN connections without using the resources of a web server.
- Content-aware switching, to send requests to different servers based on the URL being requested.
- TCP offload, to reduce traffic by consolidating multiple HTTP requests from multiple clients into a single TCP socket to the back-end servers.
- Compression, to reduce the volume of HTTP web traffic.
- Caching, to speed up performance by storing static content so that some user requests can be handled without contacting the web servers.
- Application firewall, to scan network traffic and protect against a broad range of web-based threats, including SQL injection attacks, cookie and session poisoning, buffer overflows, form filed manipulation, and cross-site scripting (XSS).
- Authentication, authorization and auditing for application traffic.

Citrix and Cisco have worked together to provide comprehensive integration between ACI and NetScaler. Most of the features listed above, and others, will be configurable based on ACI policies managed by the Cisco APIC.[2]

Figure 8 illustrates how policies created in APIC can be translated into configuration settings used by Citrix NetScaler.

2 APIC support for NetScaler features is being implemented over time. Check with your Citrix representative for a current list of supported features.

A NetScaler Device Package contains an XML file that defines a Device Configuration Model for NetScaler. After the APIC administrator imports this package NetScaler functions and parameters can be configured in APIC. Policies are created in APIC using the Service Graph GUI described above.

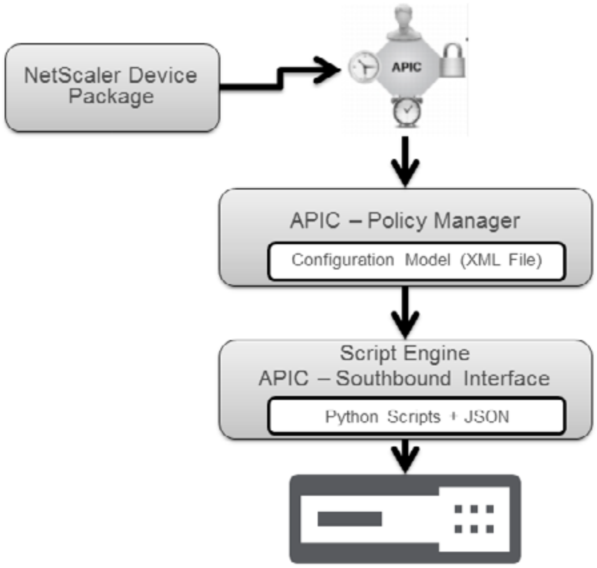

Figure 8: APIC creates an XML model of policies and configuration settings, then generates Python scripts to implement the policies on NetScaler devices

The APIC Policy Manager then generates an XML configuration model that includes the NetScaler functions and parameters that were defined. The APIC Script Engine then uses this information to generate a series of Python scripts. APIC distributes the Python scripts to the relevant NetScaler devices, where they are executed to manage NetScaler functions and set parameters based on the policies defined in the APIC.

This high level of integration provides several key benefits:

- NetScaler appliances and virtual appliances can be configured from one location, with less time and effort.
- Changes to configurations are automatically pushed out to all appropriate NetScaler appliances.
- Customers can utilize the advanced capabilities of NetScaler, and are not restricted to “lowest common denominator” ADC features
- NetScaler appliances participate in all of the advantages of Cisco ACI, including the ability to roll out and change applications quickly and reliably, with far less work than using manual methods.

The integration preserves existing NetScaler deployment topologies and Layer 2-Layer 3 interoperability. No network redesign is required, and no NetScaler model or license upgrades are needed.

Citrix and Cisco working together

Citrix is one of Cisco's closest and most active partners in the ACI ecosystem and in the development of open standards designed to accelerate the development of ACI. The two companies are jointly guiding the IETF Network Service Header (NSH) protocol standard, are co-authors of the IETF draft standard for the OpFlex Protocol, and are co-contributors to the OpenDaylight project.

Data Center Agility: Back to the Scenario

How would Cisco ACI and Citrix NetScaler help with the e-commerce application scenario described earlier in this paper?

The initial application rollout would be greatly accelerated. Rather than configuring the firewall and application delivery controller manually (Figure 2), a network or system administrator could create a Service Graph using APIC's drag and drop GUI (Figure 7), then let APIC do the work of pushing the configurations to the firewall and the NetScaler device. Not only would this process involve less work, it would also be more reliable, and therefore require less testing.

In all, ACI and NetScaler would probably cut "service insertion" time for the new application from days to hours, or even minutes.

The effect on addressing the changes to the application would be even more dramatic. Configuring the new SSL VPN appliance would be as simple as dragging and dropping the new device and selecting parameters on a service graph (Figure 9). Changes to the configurations of the firewall and NetScaler device could be made on the same service graph. The APIC would automatically push out the changes to the VPN appliance, the firewall and NetScaler.

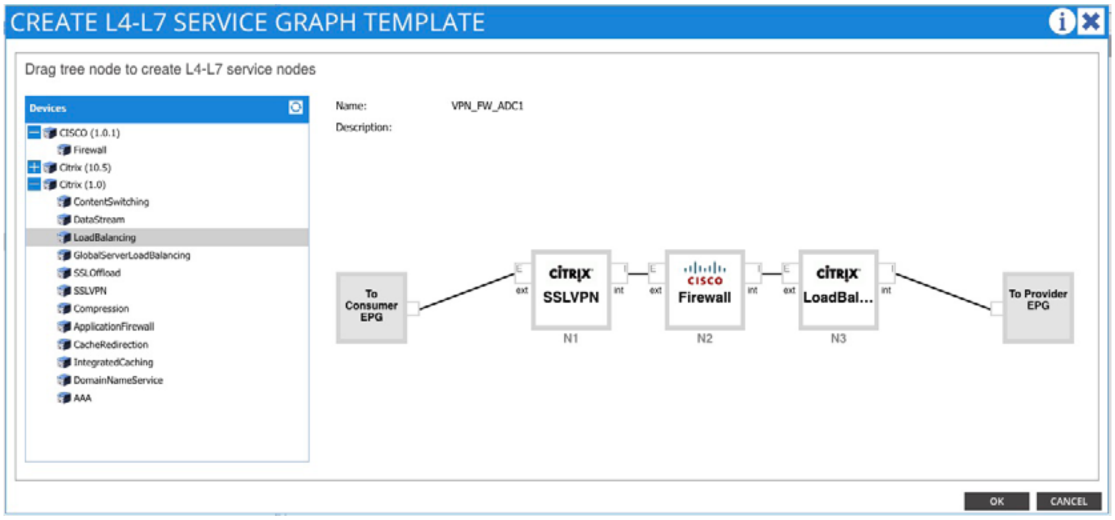

Figure 9: A new SSL VPN appliance can be inserted and configured in a few minutes

In addition, the Application Network Profile created for the first data center could be applied with only a few minor adjustments to the second data center. The time-consuming, error-prone, manual configuration process would be eliminated at that location.

These advantages would be magnified in a real data center environment, because ACI would help keep track of and manage the thousands of servers and devices, mixture of physical and virtual environments, and constant changes to applications and infrastructure elements.

Summary: Increasing Data Center Agility to Increase Business Agility

The scenarios described above illustrate how Cisco ACI and Citrix NetScaler can work together to increase business agility.

The company described in the scenarios was able to introduce a new application quickly, with a robust, high-performance, secure infrastructure. The organization was then able respond to change quickly, with much less effort than would otherwise have been required.

The benefits of deploying ACI with NetScaler and other devices include:

- Faster reaction to business needs, including rolling out new applications, upgrading applications with new features and technologies, and responding to sudden changes in customer and operational requirements.
- Freeing network and system administrators from repetitive, time-consuming configuration tasks.
- Improving security and service levels to users through the consistent and accurate application of policies to multiple devices.
- The ability to manage one set of policies, from one location, for applications that span physical, virtual and cloud environments and use a wide variety of networking and security devices.

For more information on Cisco ACI, Citrix NetScaler, and how they work together, please visit: www.citrix.com/netscaler/Cisco.

Appendix: Resources

Cisco and Citrix: Building Application Centric, ADC-enabled Data Centers

Cisco Application Policy Infrastructure Controller Data Center Policy Model

Cisco Application Policy Infrastructure Controller (Cisco APIC) At-A-Glance

The Cisco Application Policy Infrastructure Controller

What is an Application Delivery Controller (ADC)?

Cisco and Industry Leaders Will Deliver Open, Multi-Vendor, Standards-Based Networks for Application Centric Infrastructure with OpFlex Protocol

Towards Standards-based Automation

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. An integral part of our DNA is creating long-lasting customer partnerships and working with them to identify their needs and provide solutions that support their success. John T. Chambers is the Chairman and Chief Executive Officer of the $47 billion company. For more information about Cisco, visit www.cisco.com.

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.