WHITE PAPER

The Benefits of a Virtualized Approach to Advanced-Level Network Services

Sponsored by: Cisco

Lucinda Borovick

February 2011

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

EXECUTIVE SUMMARY

Advanced-level network services are an integral component of today's scalable virtual datacenter design. These services provide application acceleration and load balancing that improve user productivity, ensure optimal resource utilization, and monitor quality of service. They also provide security services to isolate applications and resources in consolidated datacenters and cloud environments that ensure compliance and reduce risk.

Deploying advanced-level network services in a virtualized datacenter environment has traditionally been extremely challenging. Typical deployments of services such as load balancing, WAN optimization, application security, and network monitoring and control have been performed using dedicated hardware in static network topologies. These deployments typically do not provide sufficient flexibility to support virtualized workloads, and enterprises are challenged to support on-demand virtual machine (VM) provisioning, workload mobility, and public or private cloud deployments. Perhaps worst of all, deploying advanced-level network services using a traditional appliance-centric approach does not provide for consistency of features and policies across the entire network in an automated fashion because policies are applied at the level of the individual device and not necessarily at the level of the entire network.

IDC defines *network services* as services that are designed to facilitate and optimize network operations, primarily at the network level. Examples include the ability to set up VLANs and security at the network level (IPsec).

This inability of advanced-level network services to flexibly accommodate large-scale virtualization limits organizations' ability to efficiently deploy new applications, increases operational costs, and acts as a roadblock to wider-scale adoption of virtualization and cloud computing. While enterprises have been rapidly adopting server virtualization and cloud computing in order to realize the benefits of reduced server sprawl, reduced operating costs, and greater levels of application availability, they have often done so in spite of — and not because of — the flexibility, or lack thereof, provided by their underlying network.

IDC defines *advanced-level network services* as network services that are primarily concentrated at the application levels of the OSI stack, consisting of services such as load balancing, WAN optimization, application security, and network monitoring and control.

One solution is to implement virtualized advanced-level network services (i.e., services that are deployed as software) in a virtualized manner and not as point appliances in the network. Such virtualized services can provide the same set of features and functionality available previously, but in a more scalable, unified, and cost-effective manner. Yet this is only a partial solution because the virtual services must also have visibility and support for the virtual applications and allow for application mobility and on-demand capacity expansion.

Vendors and IT organizations have been taking piecemeal approaches to this by cobbling together homegrown solutions, focusing on vendors' point solutions, and implementing siloed virtualization deployments. This is because few vendors have offered virtualized network services in a standardized, holistic way until now. Cisco Unified Network Services (UNS) represents one of the industry's first approaches to incorporating virtualized advanced network services to more fully and seamlessly support virtualization/cloud technologies and enable enterprises to more widely realize their benefits while still incorporating advanced-level network services such as load balancing, WAN optimization, network security, and network monitoring and control into their networks. And because these services are implemented in a virtualized manner and are not dependent on point appliances, organizations can ensure that features and policies can be applied in a consistent manner across their environment, even in multitenant environments found in application hosting providers or enterprises supporting private cloud deployments for multiple business units.

SITUATION OVERVIEW: CURRENT NETWORKS LIMIT VIRTUALIZATION AND CLOUD ADOPTION

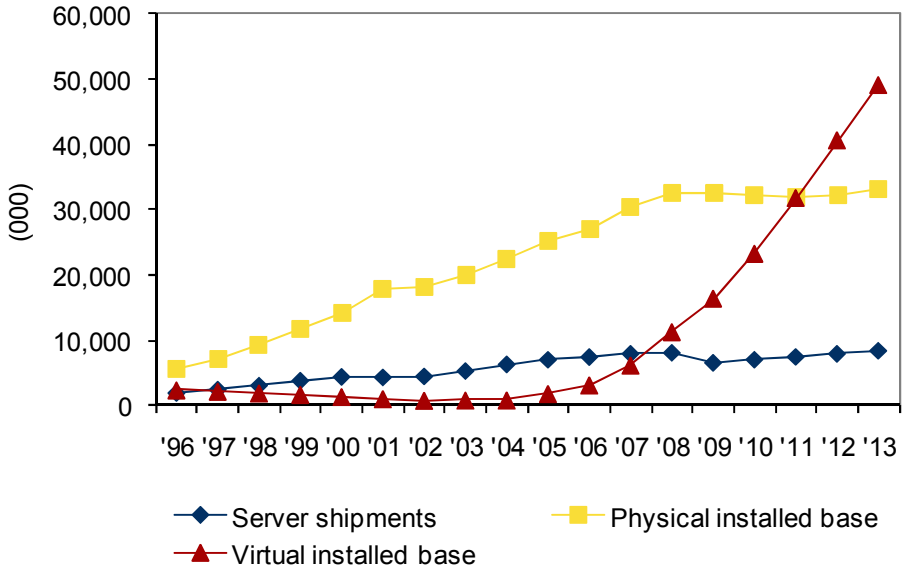
Growth in Server Virtualization

Previous-generation application infrastructures were built using dedicated server hardware in the enterprise datacenter, usually with one or more physical servers per application. As the number of applications grew, so too did the server, network, and management infrastructure required to support them. Beginning several years ago, enterprises addressed this physical server sprawl by introducing virtualization, consolidating the workloads that had been previously scattered on multiple servers down to a single server.

This trend has accelerated in recent years to the point where the worldwide installed base of physical servers has largely leveled off since 2008, while the virtual server installed base continues to grow at more than 30% per year. IDC expects that the installed base of virtual servers will be approximately equal to the installed base of physical servers by the end of 2011 (see Figure 1). Further, IDC estimates that only 9% of workloads and 2.1% of physical servers were virtualized in 2005. IDC expects over 22% of physical servers and a full 69% of workloads to be virtualized by 2013.

FIGURE 1

Worldwide Server Shipments and Installed Base



Source: IDC, 2011

Virtualization has helped enterprises reduce physical server sprawl, drive consolidation, and increase server utilization. This has helped reduce up-front capital costs, reduce operating costs in power and cooling, extend the life of many datacenters, and drive greater levels of application availability. It has also yielded benefits in flexibility, agility, and control by introducing a virtual layer between the OS/application layer and the underlying hardware. However, even as virtualization has helped reduce the number of physical servers, the number of virtual servers continues to rise, resulting in increased complexity and server personnel management costs.

Adoption of Cloud Computing

Cloud computing builds on and extends the benefits of virtualization while addressing some of the issues with virtualization in terms of complexity and server personnel management costs. Cloud computing enables higher levels of automation, orchestration, provisioning, and deployment, and it can help IT departments more rapidly scale their compute resources to more flexibly adapt to changing business requirements. It also provides elasticity: It helps organizations put the right amount of resources in the right place at the right time.

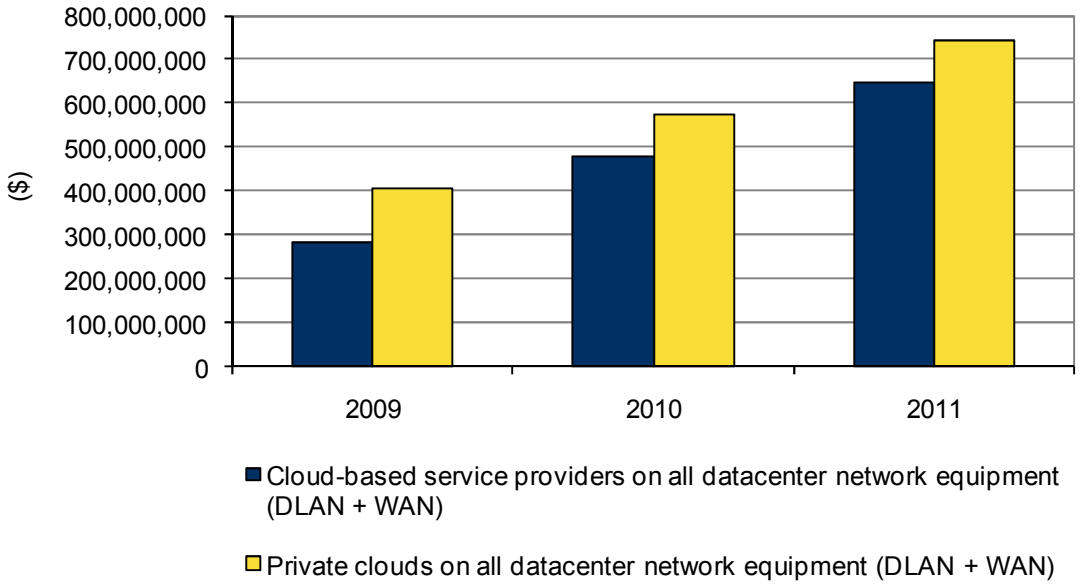
Cloud computing allows IT organizations to reduce complexity in their environment, ease workload for internal IT staff, and reduce the number of skills that need to be maintained in their organization. It can help IT departments more rapidly scale their compute resources to more flexibly adapt to changing business requirements. In fact,

IDC is predicting that cloud computing will be moving from a talking point to just another normal way to deliver IT in 2011 as one of the key transformation technologies in the marketplace.

IDC is forecasting growth in cloud computing over the next five years. In a January 2010 IDC survey of IT decision makers, fully 44% stated that they are "considering private clouds," reflecting both user interest in cloud technology and the early stages of cloud adoption. Looking at the projected network buildout to support cloud deployments, IDC expects network infrastructure investments to more than double over the next three years, growing to over $1 billion each by 2013 for the public and private cloud segments. Figure 2 shows the positive rate of growth for worldwide public and private cloud network spending for 2009–2011.

FIGURE 2

Worldwide Public and Private Cloud Network Spending, 2009–2011



Source: IDC, 2011

Cloud also addresses one of the key economic challenges of datacenter infrastructures. By reducing the number of labor hours required by the enterprise to manage its infrastructure and application layer, organizations can scale out their infrastructure without having to scale IT staff, and they can maintain their existing investments in infrastructure with a leaner IT staff and save on IT staffing costs. Finally, because cloud can be quickly scaled up — and even more importantly, down — nearly in real time, it can deliver an infrastructure that can more flexibly adapt to changing business requirements.

Current Enterprise Networks Inhibit Flexibility, Virtualization, and Cloud Adoption

Unfortunately, realizing the benefits of virtualization and cloud computing does require some investment on the part of the IT organization, in terms of both investment in infrastructure and staff hours. One of the areas that requires some of the most attention to "virtualization enable" the infrastructure is the network.

In the early stages of server virtualization, there is limited use of virtual machine mobility. The majority of customers rarely migrate virtual machine workloads. As customers look to provide greater agility to their datacenter, seamless virtual machine mobility is required. The ability to quickly and easily move and redeploy virtual machines on other physical hardware is required to meet fluctuations in capacity and utilization demand. The problem is that most enterprise networks assume a static application topology. Not designed to be virtualization aware, enterprise networks need to evolve with automation in mind in order to support wide-scale virtualization deployment.

For example, many enterprise networks today do not support seamless deployment of VMs between clusters of servers within a single datacenter or across multiple datacenters. With network services implemented as point solutions, migrating VMs from one end of the datacenter to another requires breaking quality-of-service and network policies and manually reestablishing them at the other device, which is both risky to the business and time consuming and expensive to implement.

A key challenge to implementing virtualization and cloud computing with today's networks is providing security and application-level services. This is particularly important given the varying requirements and policies of different applications and organizations. It is difficult to deploy, provision, and maintain services in a modular, scalable, and easily customized fashion. For example, while one datacenter application may require one set of security policies and application control characteristics, another application may require a completely different set of services and policies, arranged in a different order on the network.

Traditional Appliance-Centric Network Service Deployments Limit Growth and Flexibility

To date, most enterprises have deployed advanced-level network services using an appliance-centric approach: Services such as WAN acceleration, security, and network monitoring have each relied on the deployment of one or more appliances in the network to handle those functions. Unfortunately, this approach limits the growth and flexibility of the organization, especially as virtualization and cloud deployments come into play. Reasons include:

- **Resource requirements to support devices.** As the number of appliances in the network grows, they stretch the organization's ability to support them, from the perspective of both operational expenses and staff capacity.

- **Limited ability to replicate services.** Deploying services through point appliances can restrict the mobility of those services and features and can limit the ability to extend and replicate the services easily across one or more datacenters or across a multitenant environment.

- **Limited disaster recovery capabilities.** Many organizations looking for high levels of resiliency and disaster recovery choose to build active-active datacenters that provide backup for each other. In such organizations, seamless service replication is a key enabler, and by limiting the ability to easily replicate services across datacenters, point appliances can act as a hindrance to disaster recovery capabilities.

- **Lack of feature consistency across the infrastructure.** Perhaps most important, by implementing advanced-level network services in a virtualized manner and not as appliances, organizations can ensure that they have complete consistency of features and policies across their entire network, without having to implement each at an appliance-by-appliance level. This not only reduces operational costs and headaches but also can provide greater consistency and scalability to the organization.

Advanced-Level Network Services Break When Deploying Virtualization

To optimize their network and application performance, many enterprises have adopted advanced-level network services such as load balancing, WAN optimization, network security, and network analysis and monitoring. While such advanced-level services provide great benefits in terms of network and application performance, security, and control, they have traditionally been applied in a "fixed" manner in the network. The introduction of virtualization has typically disrupted these networks, and the ability to deploy new applications or to virtualize applications and services has been limited.

Devices providing advanced-level network services such as load balancers, WAN accelerators, and firewalls have typically been deployed "in line" with the application servers they are supporting. Such a topology can become a bottleneck with large numbers of applications, each of which may have different policy requirements, especially as an organization attempts to introduce virtualization into the datacenter. Organizations that have deployed advanced-level network services find they make the networks inflexible and act as barriers when deploying virtualization and cloud computing.

Network services that are "virtualization aware" and that can provide support for migrating application and security policies among the shifting workloads are a critical step in providing a virtualization-aware network.

Multitenancy and Enterprise Private Clouds Bring Particular Challenges

One of the advantages of virtualization and cloud computing is the ability for multiple clients to share in an IT infrastructure in a multitenant environment. This is true for both hosting service providers and enterprises looking to support private cloud computing for multiple business units.

Advanced-level network services that support multitenancy enable the IT department or service provider to offer application performance, security, and monitoring and control for individual virtual workloads in the datacenter. The ability to enable segmentation of specific services to individual user groups or customers is the foundation for a rich business-oriented datacenter design.

IT ORGANIZATIONS PURSUING PIECEMEAL APPROACHES TO VIRTUALIZATION-AWARE NETWORK SERVICES

Clearly, enterprises have been working to deploy network topologies that support virtualized environments and to implement technologies to make their virtualized deployments more seamless to provision and manage. In many instances, they have striven to introduce advanced-level network services such as load balancing, WAN optimization, security, and network monitoring into these environments with varying degrees of success, primarily supported with one-time technology integrations and implementation of one specific advanced-level network service, lacking integration with the full spectrum of virtualization-aware services demanded.

Unfortunately, most advanced-level service technologies have only limited virtualization awareness built into their products, and many customers have solved the problem in siloed portions of their datacenter and only after a great degree of customization, manual workarounds, and trial and error. But clearly the industry is headed in this direction, and future advancements should make it much simpler for organizations to deploy advanced-level network services into their virtualized environments.

Importance of Virtualization-Aware Network Services to the Enterprise

Advanced-level network services bring a great number of benefits to the network and application layer, including network optimization, cost reduction, security, and control. These are clearly important technologies for enterprises to adopt into their networks. But virtualization and cloud also bring a large number of benefits in terms of reduced operating costs, increased flexibility, and control, and network managers need reliable technologies that enable them to implement both into their networks.

Fortunately, the first generation of virtualization-aware network services is beginning to hit the market. These services are designed to enable easy adoption and management of a virtualized infrastructure and can help address the bottlenecks described earlier. Recognizing this, forward-thinking IT managers are beginning to evaluate these technologies as part of their virtualization enablement efforts. Technologies being introduced include network and virtualization support, load balancing and application controllers, WAN acceleration, network security, and network analysis and monitoring.

Virtualization-Aware Network Services Enable the Dynamic Datacenter

With virtualization-aware network services, organizations are able to treat their datacenter as a single, dynamic unit, even if it consists of disparate physical datacenters located around the world. VMs can be automatically migrated to underutilized portions of the datacenter or to other datacenters without requiring manual IT involvement, and all quality-of-service and network policies, etc., remain intact.

Some of the specific capabilities that customers should look for when considering introduction of an end-to-end suite of virtualization-aware network services offerings into their network include a virtualization-aware network and a fabric that allows the dynamic insertion of services as needed.

The products and services should be designed from the ground up to accommodate virtualization; they should not be afterthought add-ons. IT departments need to deploy a network architecture from the ground up that is virtualization aware. This is true for all network services, but it becomes exponentially important when deploying advanced-level network services.

IT departments should deploy a network fabric that provides flexibility to "insert" advanced-level network services as required, including for production-level application deployments that occur in a phased approach. For many organizations, a subset of the user base is the first to use a new business application, very often users who are local to the datacenter/headquarter location. In the first phase, given the smaller user population and the availability of local bandwidth, the need for advanced-level network services is a "safety net." As deployments rise in scale, scope, and distance, the need to add advanced-level network services quickly and without disruption to the network architecture is critical. This flexibility to adapt to new business use can be achieved only with a virtualization-aware fabric in place.

Plans for supporting a full spectrum of advanced-level network services should include the following:

- **Load balancers and application controllers.** Load balancers and application controllers are fundamental building blocks in datacenter design and should be included in any end-to-end advanced network services deployment.
- **WAN acceleration.** WAN acceleration enables organizations to improve application performance, user experience, and user productivity; optimize their bandwidth usage; and reduce operating costs, and it is usually included in large enterprise network deployments.
- **Network security.** Network security is one of the most critical network services. One of the key security challenges in a virtualized environment is enforcing security policies at the granular level of individual VMs or groups of VMs, and organizations should ensure they have the appropriate security services in place to do so.

- **Network analysis and monitoring.** Because organizations cannot optimize what they cannot measure, good network analysis and monitoring services are a fundamental building block of the network. Network analysis and monitoring is particularly challenging in a virtualized environment, with services that can provide visibility down to the VM level.

A More Holistic Approach Is Required

Unfortunately, many of the approaches enterprises and vendors have taken to date are one-off approaches and workarounds, as many network vendors have yet to come to market with holistic, end-to-end approaches to providing virtualization-aware network services in their solutions. Point solution vendors have typically not integrated service routing frameworks into the hypervisor/virtual switch, so the service is not truly independent of the application location and network topology.

Instead, the problem has been solved in a piecemeal fashion, creating isolated islands throughout the datacenter, and in individual silos. What is required is for vendors to bring to market an entire suite of advanced network services offerings designed from the ground up to be virtualization aware and to support virtualization and cloud computing in the enterprise. This network foundation will be a fundamental building block of a private cloud infrastructure.

CISCO UNIFIED NETWORK SERVICES

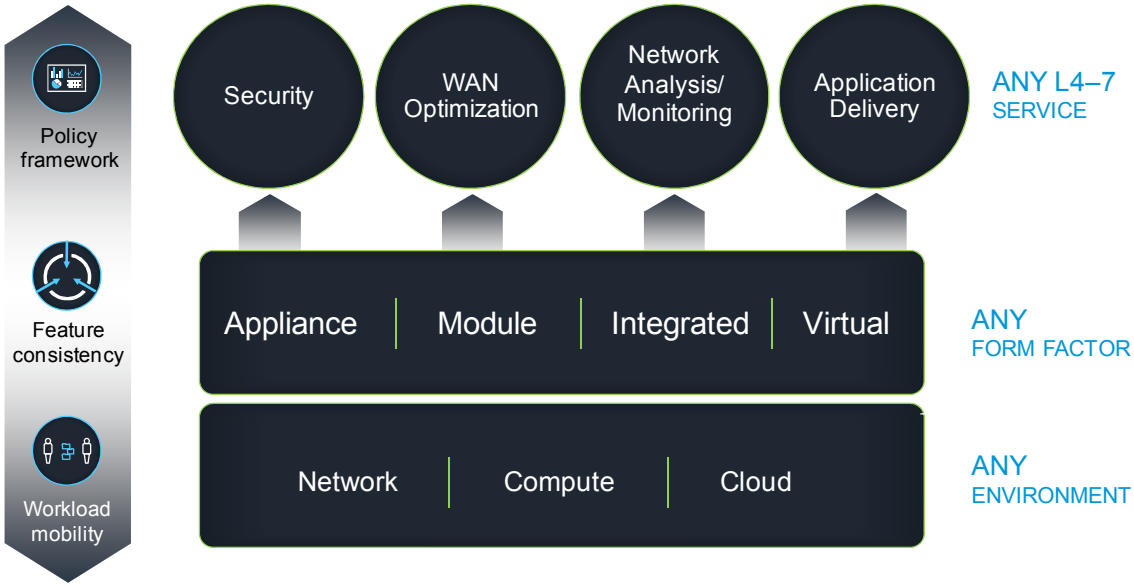
In September 2010, Cisco announced a new pillar in its Business Advantage datacenter architecture: Unified Network Services (UNS). This pillar adds to Cisco's unified fabric and unified computing initiatives; with Business Advantage, Cisco now offers the following pillars:

- Unified Fabric
- Unified Network Services
- Unified Computing

UNS brings virtualization-aware advanced-level network services into the Cisco networking portfolio. It is designed to shorten the otherwise long and painful transition from a physical infrastructure to a virtualized or cloud-based infrastructure by extending current investments in physical infrastructure while paving the way for services that will support the migration to a virtualized environment. UNS does this by extending Cisco's strength in integrating with the existing network while adding key requirements for policy-based elastic provisioning, scale-out, virtual machine mobility, and multitenancy (see Figure 3).

FIGURE 3

Cisco Unified Network Services



Source: Cisco, 2011

Specific virtualization-aware differentiators and architectural features built into Cisco UNS include:

- **Virtualization-aware services.** Probably the signature aspect of Cisco UNS products is that they are designed to adapt to the needs of highly virtualized datacenters and cloud infrastructures and to provide visibility into virtual machines and mobile workloads. They include a portfolio of application delivery controllers, WAN acceleration devices, security services, and network management solutions designed to support virtual hosts, mobile workloads, and on-demand provisioning.

- **On-demand service deployment with flexible deployment options.** UNS includes a framework to create and expand service workloads to allow organizations to adapt to the needs of rapidly changing business environments. With a variety of deployment options including dedicated physical appliances, network-integrated service modules, software, and virtual machines, enterprises have the option to deploy the form factor that best meets their scalability and deployment requirements.

- **Policy-based provisioning and integrated management.** Services can be defined and expanded on demand based on defined policies for quality-of-service and security requirements. Policies associated with a virtual machine are location independent and migrate with the VM. UNS incorporates a consistent management approach between form factors (physical and virtual), with the goal of providing a common, centralized platform for all virtualization-aware advanced-level network services.

- **Transparent service insertion.** UNS is designed to simplify the insertion of security and application service delivery into enterprise networks by removing the requirements that services be deployed at specific points of the networks; instead, they can be implemented as virtual machines themselves and can be transparently and instantly inserted into the network on demand.

- **Traffic steering (service routing) framework.** UNS can route network traffic between the source and destination IP through required network services, such as through the Virtual Security Gateway (VSG) for security policy enforcement. This allows services to be deployed and provisioned quickly as new applications and hosts come online and allows policies to follow VMs as they are moved throughout and between datacenters.

- **Integrated orchestration across service offerings.** With UNS, administrators can consolidate and centralize policy-based orchestration across multiple service offerings, including security, application controllers, and WAN acceleration. Whereas in the past instrumentation and monitoring had to be done on a service-by-service basis, UNS provides administrators with a single, consistent view of traffic patterns and packet counts across these services.

Cisco UNS Services

Cisco UNS creates a framework for multiple services that can be configured and provisioned dynamically/on demand to suit the needs of virtualized enterprise deployments and cloud computing. It is designed to unify the way application services and security services are provided in enterprise datacenters by providing consistent and flexible services delivery using policy-based provisioning across different service types, form factors, and environments.

UNS consists of a set of dedicated network services products (appliances and modules) as well as virtual services running on virtual machine platforms. Dedicated services include the Cisco Application Control Engine (ACE) and Wide Area Application Services (WAAS), both of which provide application acceleration in appliance and module form factors, and the Adaptive Security Appliance (ASA), which provides application security at both the network aggregation layer and the WAN edge. ASA provides an integrated suite of security services in a single datacenter-class appliance, including firewall, IPS, VPN, and NAT. The Network Analysis Module (NAM), which provides application performance monitoring, can be deployed as a dedicated appliance, an embedded module, or a virtual blade on the Nexus 1010 management platform.

Virtual services include the Virtual Security Gateway, a multitenant virtual server security solution that enforces security policies at the granular level of the VM, and Virtual WAAS (vWAAS), a virtualized application acceleration solution. Both are available as software on VMware servers and Cisco Nexus 1000V virtual switches.

By offering a choice of services delivered as virtual service nodes or dedicated appliances or servers, Cisco provides enterprises with the flexibility to leverage existing resource investments and to scale easily as new capacity is required. Features and management platforms for each product area are consistent across the physical and virtual form factors for greater efficiency and ease of deployment.

Cisco UNS Use Case Scenarios

Cisco has already had experience with customer use case scenarios demonstrating how UNS has been deployed in enterprise environments and the specific benefits that can be attained with each.

Two early use cases include:

- **Cisco virtual desktop infrastructure (VDI).** UNS can work in conjunction with Cisco VDI to provide greater scalability, low client latency, and security between client operating environments within virtual servers. The Cisco UNS vWAAS works as part of the VDI environment to accelerate desktop applications to clients while running as a virtual service that can be dynamically created and provisioned on demand. The Cisco VSG virtual firewall provides logical isolation for client environments, visibility for VMs and applications to the virtualization layer, and enforcement of policies that migrate along with the VMs.

- **Enterprise private cloud.** Cisco UNS provides integrated services that can help reduce the costs of managing and provisioning private clouds with integrated services that can be provisioned on demand and deliver the application performance and security that the deployment requires. The Cisco NAM provides centralized visibility to application performance, while the Cisco ACE application controller and server load balancer ensure server utilization and application acceleration in virtualized environments while supporting logically isolated applications between organizations in the private cloud. The VSG and ASA firewall appliances enforce security policies and create trust zones between virtual machines and applications.

In both cases, policies governing security, quality of service, and application performance can be implemented and enforced at the granular level of individual VMs, overcoming the challenges to widespread application virtualization.

FUTURE OUTLOOK

IDC believes that the best practices of network architectures of the past are being rewritten in order to support the overarching trend of virtualized IT and an agile, efficient datacenter design. This new network foundation will include virtualization-aware advanced-level network services that address not only the availability requirements of today but also the agility and efficiency demands of private cloud deployments.

OPPORTUNITIES AND CHALLENGES

IDC sees a number of opportunities and challenges for customers as they look to adopt and for Cisco as it brings to market products that take advantage of virtualization-aware network services. Opportunities include:

- **For customers: realizing the full benefits of the agile datacenter.** Customers who rearchitect their networks to take full advantage of these features can achieve the many benefits described earlier as they migrate applications to virtualized environments and the cloud. Benefits include increased flexibility in their networks, better application performance, reduced operating costs, and faster application deployment.

- **For IT: adding value to business by adding much needed intelligence to cloud services.** This is an opportunity for IT to demonstrate its value to the business by adding much-needed intelligence to virtualized environments and cloud services.

- **For Cisco: establishing new differentiated, value-added offerings.** The network equipment market is highly competitive, with vendors competing on both the need to bring to market innovative new technologies and the need to develop solutions that reduce companies' total cost of ownership and drive attractive return on investment (ROI). By addressing the needs of networks as they relate to virtualization and cloud computing, Cisco is again pushing the boundaries of its current offerings and is working to differentiate itself from other vendors in the market.

Challenges include:

- **For customers: redesigning the network.** Nearly by definition, enterprises today that could benefit from deploying virtualization-aware network services have networks that are static and inflexible. Introducing the required technology can be expensive and difficult. Further, network managers are measured on uptime of network, and they are conservative and hesitant to make changes to the network. All of this makes it challenging for organizations to incorporate significant changes into their network.

- **For Cisco: demonstrating value in implementing the entire framework.** Cisco is coming to market with a number of products under the UNS umbrella and will need to ensure that customers derive maximum benefit by deploying the entire framework and not just individual point products.

- **For Cisco: demonstrating the ROI of the entire solution.** Implementing these new technologies will require new capital expenditures for many enterprises and may have an effect on ongoing operational expenditures as well. Cisco will have to demonstrate how the benefits and savings to the broader business will yield an attractive ROI to make the change worthwhile.

CONCLUSION

Advanced-level network services, such as load balancing, WAN optimization, network security, and network monitoring and control, are essential elements of today's datacenter network. These services enable organizations to run their networks more efficiently, reducing their overall operating costs while ensuring application security, scalability, and control. Unfortunately, until recently, most advanced-level network service solutions have been incompatible with virtualization and cloud computing, meaning that IT organizations have had to rely on cobbled-together, piecemeal approaches when incorporating virtualization into their environment. In fact, the lack of foundational architecture has been an inhibitor to cloud computing deployments.

With its Unified Network Services solutions, Cisco is bringing to market one of the industry's first end-to-end, holistic approaches to providing advanced-level network services that are designed to support the needs and requirements of virtualized and cloud computing environments. By incorporating VM-aware technologies such as on-demand service deployment, policy-based provisioning, and transparent service insertion, UNS supports the deployment and management of VMs across or even between enterprise datacenters. And with deployment options from dedicated hardware to services that are themselves virtualized, UNS provides enterprises with the flexibility to leverage their existing network investments while providing the window to scale new capacity as required.