Cloud Networking Services

By Dr. Jim Metzler
Ashton Metzler & Associates
Co-Founder, Webtorials Analyst Division

Blue Coat®

Fonality
Talking Business

Virtela™

VYATTA®
Open Networking

Webtorials™

Table of Contents

Executive Summary

The two primary forms of public cloud computing, Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS), are both growing dramatically in popularity. Up until recently, the primary challenges that public cloud computing solutions presented to an IT organization were managing, securing and ensuring acceptable performance of the solutions. While those challenges still exist, recently a new class of solutions has begun to be offered by Cloud Computing Service Providers (CCSPs). These are solutions that have historically been provided by the IT infrastructure group itself and include WAN and application optimization, VoIP, Unified Communications (UC), security, network management and virtualized desktops. This new class of solutions will be referred to in this report as ***Cloud Networking Services*** (CNS). Relative to the use of public cloud computing, IT organizations have a new challenge – determining when it makes sense to use a CNS.

IT organizations are showing significant interest in CNS solutions and their adoption potentially represents a fundamental shift in terms of how IT services are provided. The factors that are driving and inhibiting the adoption of CNS solutions are the same factors that are driving and inhibiting the adoption of any public cloud computing offering. As a result, when evaluating a CNS solution, IT organizations need to determine if the solution delivers on the promise of public cloud computing while also eliminating, or at least minimizing, the negative aspects of a public cloud computing solution such as concerns that IT organizations have over the security and confidentiality of their data. Part of the promise of public cloud computing is lower cost, which is relatively easy to evaluate. Another part of the promise of public cloud computing is increased agility, which can be difficult to evaluate. One measure of the agility of a CCSP is the degree to which they have virtualized their entire data center, not just their servers.

IT organizations have expressed more interest in ***VoIP*** and in ***UC*** than they have in any other form of CNS. In addition, as described in *The 2011 Sourcebook for VoIP and UC Services*, there are over 200 providers of cloud based VoIP and Unified Communications services. While having that many providers can result in benefits to consumers, it also creates some challenges. These challenges include the fact that providers tend to use different names for their services, have notably different business models and offer a very wide range of functionality – everything from basic telephony to call center support to HD voice.

The primary role of a CNS that offers ***WAN and application optimization*** functionality is to provide functionality similar to what is provided by premise based WAN optimization controllers (WOCs). There are three distinct use cases for this class of CNS. As with any CNS, one use case is that the CNS provides all of the promised benefits of public cloud computing. The second use case is that the utilization of this class of CNS enables an IT organization to optimize the performance of applications delivered to mobile users without having to deploy software on each mobile device. The third use case is that this class of CNS enables an IT organization to optimize the performance of services obtained from a CCSP.

One of the key focus areas for a ***security oriented CNS*** is to provide firewall and/or IPS functionality. Such a service should support equipment from the leading vendors and should offer predictive analytics whereby the CNS can diagnose the vast majority of potential enterprise network and security issues before they can impact network health. Given the risks associated with Web based applications, a key focus area for a security oriented CNS is to provide sophisticated Web content filtering and granular policy controls that can leverage dynamic rating algorithms and that can accurately identify and categorize web content in real time. Another

important security concern is the rapid growth of malware. For example, a recent report from Cisco[1] identified almost 290,000 unique instances of malware on the Web in June 2011. That number is almost triple the number of unique instances of malware that Cisco found on the Web in March 2011 (105,536). To protect against malware, a CNS should be able to identify suspicious content or sites that are either suspicious or are known to distribute malware. In order to be effective, a CNS that provides Web content filtering or malware protection needs a source of intellectual capital that identifies known and suspected vulnerabilities.

As is the case with security, ***network management*** is a very broad topic. Because of the breadth of the topic, it is possible to find network management focused CNSs that provide a wide range of functionality. For example, it is possible to find a CNS that manages security functionality such as IPS and firewalls or basic networking functionality such as routers. When evaluating any of these solutions, IT organizations need to determine how wide a range of vendors' products the solution can manage and how much expertise the CCSP has with those products.

A recent report from IBM[2] identified the fact that most IT professionals view the data stored on mobile devices and how that data can be misused or lost as the main security threats associated with these devices. That view creates a marketplace opportunity for a CNS that provides mobile device management. The need for such a service is reinforced by another market research report[3] that concluded that many IT organizations are struggling to support the growth in mobile employees.

In contrast to functionality such as VoIP, security and management, ***desktop virtualization*** is a topic that has received a lot of attention in the trade press, but has not been widely implemented. A cursory look at the market research data contained in this report seems to indicate that there is not much interest in a CNS that offers desktop virtualization functionality. However, given the wide disparity between the existing and planned deployment of functionality such as VoIP and the existing and planned deployment of desktop virtualization, another way to look at that market research data is that IT organizations are actually relatively more interested in using a CNS to provide desktop virtualization functionality than they are to use a CNS to provide more traditional IT functionality.

One of the reasons why there is such a relatively high interest in a CNS that provides desktop virtualization functionality is that desktop virtualization is both new and highly complex. For example, there are two fundamental forms of desktop virtualization: server-side and client-side. Each form of desktop virtualization has its own strengths and weaknesses[4] based in part on the type of employee and the type of user devices that the IT organization intends to support. Choosing the right type or types of desktop virtualization is only part of the challenge. Ensuring acceptable performance presents some significant challenges. One way that an IT organization can overcome the performance challenges that are associated with using desktop virtualization, whether the IT organization supports desktop virtualization themselves or uses a CNS solution, is to utilize a CNS that optimizes the traffic flow that is associated with desktop virtualization.

[1] Cisco Annual Security Report

[2] http://www-935.ibm.com/services/us/iss/xforce/trendreports/

[3] http://www.csoonline.com/article/683735/mobile-workers-not-being-supported-by-it-survey-says

[4] http://www.cio.com/article/504348/Desktop_Virtualization_5_Most_Popular_Flavors_Explained

Background

Introduction

As recently as a couple of years ago there was wide disagreement relative to what was meant by the phrase ***cloud computing***. In the current environment there is general agreement that there are three classes of cloud computing solutions: public, private and hybrid. Cloud Computing Service Providers (CCSPs) such as Salesforce.com and Rackspace that provide their services either over the public Internet or over other WAN services are offering a class of solution that is often referred to as a public cloud computing solution. Some IT organizations have decided to implement the characteristics of public cloud computing solutions[5] within their internal IT environment. These solutions are referred to as private cloud computing solutions. In those instances in which an enterprise IT department uses a mixture of public and private cloud services, the result is often referred to as a hybrid cloud computing solution.

The two primary forms of public cloud computing are Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS). According to Gartner[6], the Software as a Service (SaaS) market had worldwide revenues of $10.0 billion in 2010 and is projected to reach $21.3 billion by 2015. To date, the focus of the SaaS providers has been on enterprise applications such as Customer Relationship Management (CRM), Enterprise Resource Planning (ERP) and communications and collaboration. The current SaaS marketplace is comprised of a small number of large players and thousands of smaller players.

When most industry analysts discuss the IaaS market they focus on the basic compute and storage resources that are required to run applications. With this as the definition of IaaS, the barrier to enter the IaaS marketplace is notably higher than is the barrier to enter the SaaS marketplace. That is one of the primary reasons why there are significantly fewer vendors in the IaaS market than there are in the SaaS market. Representative IaaS vendors include Amazon, AT&T, CSC, GoGrid, IBM, Joyent, NaviSite (recently acquired by Time Warner), NTT Communications, Orange Business Services, Rackspace, Savvis (recently acquired by CenturyLink), Terremark (recently acquired by Verizon) and Verizon. The IaaS market is expected to exhibit significant growth in the next few years. For example, Gartner[7] estimates that the IaaS market will grow from $3.7 billion in 2011 to $10.5 billion in 2014.

Up until recently, the primary challenge that public cloud computing solutions presented to the infrastructure group within an IT organization was around support. One way that challenge manifests itself is that the typical IT infrastructure group struggles to manage, secure and ensure acceptable performance of public cloud computing solutions. While that challenge still exists, recently a new set of solutions has begun to be offered by CCSPs. These are solutions that have historically been offered by the IT infrastructure group itself. In addition to the communications and collaboration services already mentioned, this includes WAN and application optimization, security, optimization and virtualized desktops. Throughout this report this new class of solutions will be referred to as Cloud Networking Services (CNS). The introduction of CNS presents the IT infrastructure group with a new challenge. That challenge is

[5] These characteristics are described in the report entitled A Guide for Understanding Cloud Computing,

[6] SaaS Revenue Growth

[7] Qas.com

to determine which of the traditional IT services it should continue to provide itself, which ones it should acquire from a CNS provider and which ones it should provide in a hybrid fashion.

One goal of this report is to create a focus on this new set of public cloud computing solutions-CNS. Another goal of this report is to identify some of the representative classes of CNS solutions and discuss the functionality that IT organizations should look for when evaluating these solutions. A third goal of this report is to identify some of the key enabling technologies that enable effective CNS solutions. Given that the deployment of CNS has just begun, it is not a goal of this report to be exhaustive; i.e., to define all of the possible classes of CNS solutions that either already are, or soon will be provided by a CCSP.

CNS: The Next Wave of IaaS Solutions

In May 2011, one hundred and sixty four IT professionals completed a survey in which they were asked to indicate how likely it was over the next year that their company would acquire a CNS. Their responses are shown in Table 1.

Table 1: Interest in Cloud Networking Services

	Will Not Happen	Might Happen	50/50 Chance	Will Likely Happen	Will Happen
VoIP	34.3%	17.5%	12.6%	15.4%	20.3%
Unified Communications	26.1%	26.8%	16.9%	14.8%	15.5%
Network and Application Optimization	33.8%	22.1%	14.7%	14.0%	15.4%
Disaster Recovery	30.8%	23.8%	20.0%	11.5%	13.8%
Security	39.0%	16.9%	16.9%	14.0%	13.2%
Network Management	38.8%	26.6%	7.2%	17.3%	10.1%
Application Performance Management	35.8%	28.4%	15.7%	12.7%	7.5%
Virtual Desktops	40.7%	24.4%	18.5%	9.6%	6.7%
High Performance Computing	41.9%	24.8%	16.3%	10.1%	7.0%

The data in Table 1 shows that the interest in CNS is quite broad, as over twenty-five percent of the survey respondents indicated that over the next year each of the services listed in the top six rows of Table 1 would either likely be acquired or would be acquired. This represents the beginning of what could be a fundamental shift in terms of how IT services are provided.

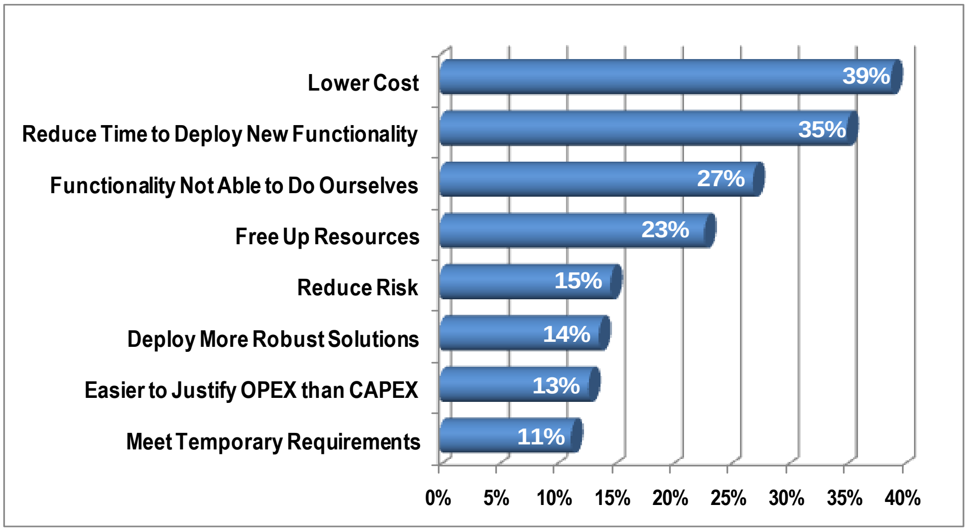
The most appropriate way to classify CNS solutions is to classify them based on how IT organizations are structured and hence how IT organizations would consume these solutions. Most IT organizations have an applications organization whose primary role is to develop, acquire and maintain enterprise applications such as CRM, ERP and SCM. Most IT organizations also have an infrastructure organization whose primary role is to provide, manage, secure and optimize the networks and servers that support the applications that enable the company's business processes. In most cases, services such as voice, collaboration, disaster recovery, management, security, optimization and virtual desktops are provided by the infrastructure organization – not the applications organization. Because of the way that IT organizations are typically structured, throughout this report CNS solutions will be considered to be the next wave of IaaS solutions.

The Drivers and Impediments of Public Cloud Computing Solutions

Drivers

The market research report entitled *Cloud Computing: A Reality Check and Guide to Risk Mitigation* reported on the results of a survey in which one hundred and eighty six IT professionals were asked to indicate the two primary factors that are driving, or would likely drive their company to use public cloud computing services. Their responses are shown in Figure 1.

Figure 1: The Drivers of Public Cloud Computing



One of the observations that can be drawn from Figure 1 is that the primary factors that are driving IT organizations to use public cloud computing solutions such as CNS are the same factors that drive any IT organizations to adopt any form of out-tasking. In particular, the primary two factors that drive an IT organization to use public cloud computing solutions is if CCSP can provide the needed functionality faster and more cost effectively than the IT organization can.

Impediments

IT organizations that are evaluating CNS need to be concerned with the issues that impede the use of any public cloud computing solution. Those impediments are discussed in the report entitled *Cloud Computing: A Reality Check and Guide to Risk Mitigation*. As that report indicates, three of the primary impediments to the adoption of cloud computing are security, performance and management.

Security

Some insight into the shifting nature of security vulnerabilities in general and the risks of public cloud computing services in particular was provided in a report published by IBM in March 2011 that was entitled *X-Force 2010 Trend and Risk Report*[8]. The report documents a 27% increase in security vulnerabilities in 2010 vs. 2009 and stated that, "Web applications accounted for nearly half of vulnerabilities disclosed in 2010 -- Web applications continued to be the category of software affected by the largest number of vulnerability disclosures, representing 49 percent in 2010. The majority represented cross site scripting and SQL injection issues."

Given the concerns that IT organizations have relative to the security of public cloud computing solutions it was not surprising that the IBM report dedicated a new section to the security trends and best practices that are associated with cloud computing. However, while highlighting some of the security concerns that are associated with public cloud computing, the IBM report also discusses some of the ways in which today's public cloud computing solutions can actually make an organization more secure. Even more interesting is that in the report IBM predicts that over time that the market will drive public cloud computing providers to provide access to security capabilities and expertise that is more cost effective than in-house implementations. The IBM report concluded that "This may turn questions about cloud security on their head by making an interest in better security a driver for cloud adoption, rather than an inhibitor."

Performance

The next section of this report contains a discussion of a CNS that focuses on WAN and application optimization and how such a CNS can serve as an alternative to the onsite deployment of products such as WAN Optimization Controllers (WOCs)[9]. Such a CNS can be leveraged to solve traditional optimization challenges such as transmitting large files between offices or improving the performance of a chatty protocol. As is discussed below, such a CNS can also be used to improve the performance of services that are delivered to mobile workers or are acquired from a CCSP.

Management

One of the fundamental issues relative to managing either a public or hybrid cloud computing service is that the service has at least three separate management domains: the enterprise, the WAN service provider and the various cloud computing service providers. For the sake of example, consider two of the alternative cloud computing approaches that an IT organization might take to support a hypothetical application that will be referred to as BusApp. Those approaches are:

- Public Cloud Computing

  The IT organization accesses BusApp from a Software-as-a-Service (SaaS) provider. The employees of the company that work in branch and regional offices use an MPLS

[8] http://www-935.ibm.com/services/us/iss/xforce/trendreports/

[9] An even more detailed discussion of the topic of network and application optimization can be found in The 2011 Application and Service Delivery Handbook.

service from a network service provider (NSP) to access BusApp, while home office workers and mobile workers use the Internet.

- Hybrid Cloud Computing

  The IT organization hosts the application and data base servers in one of their data centers and the web servers are provided by a cloud computing service provider (CCSP). All of the users access BusApp over the Internet and the connectivity between the web server layer and the application server layer is provided by an MPLS service.

In order to monitor and manage either deployment of BusApp, consistent and extensive management data needs to be gathered from the cloud computing service provider(s), the MPLS provider(s) and the provider(s) of Internet access. In the case of the first option (public cloud computing) similar management data also needs to be gathered on the components of the on-site infrastructure that are used by the company's employees and supported by the IT organization. In the case of the second option (hybrid cloud computing) similar management data also needs to be gathered on both the on-site infrastructure as well as the web and application servers that are supported by the IT organization. In either case, effective tools are also necessary in order to process all of this data so that IT organizations can identify when the performance of BusApp is degrading before end users are impacted and can also identify the root cause of that degradation.

Evaluating CNS Solutions

The use of public cloud computing solutions such as CNS is just the latest example of IT organizations using a third party to provide needed functionality; a.k.a., out-tasking. Hence, IT organizations that are evaluating CNS solutions should have the same vendor management concerns that they have for any form of out-tasking. This includes:

- Understanding the financial viability of the provider
- Understanding the provider's commitment to providing this class of service
- Building into the contract how business and technology changes will be handled over the life of the contract

When evaluating a CNS solution, IT organizations also need to understand the breadth of functionality that it provides. For example, as explained in a subsequent section of this report, VoIP and Unified Communications (UC) oriented CNS solutions provide a very wide range of functionality – everything from basic telephony, to call center support to HD voice. As could be expected, not all of the providers offer the same functionality. As a result, IT organizations that are evaluating these solutions need to determine if the solutions that they are considering provide the required functionality.

Evaluating whether or not a given solution provides the required functionality is standard operating procedure for IT organizations. In addition, there is not much difference in terms of how an IT organization would evaluate the functionality provided by an on premise based hardware solution vs. how it would evaluate the functionality provided by a solution offered by a CCSP. What is different about evaluating CNS solution stems from the fact that they are cloud based. As such, IT organizations need to closely look at the vendor management issues that were previously discussed as well as the impediments to the use of public cloud computing solutions that were also previously discussed. One of these impediments is security. According to many market research reports, including the market research report entitled *Cloud Computing: A Reality Check and Guide to Risk Mitigation*, concern about security is the primary impediment to the adoption of public cloud computing solutions and hence evaluating the security of the CNS provider's facilities is a critical component of evaluating a CNS solution.

One part of evaluating the security of a CNS provider's facilities is to evaluate the security provided for any communication that transits a wide area network. For example, does the CCSP support 256-bit AES encryption for site-to-site VPNs? Another part of evaluating the security of a CNS provider's facilities is to evaluate whether or not the CCSP's implementation of a multi-tenant environment has compromised security. For example, IT organizations need to determine if the CCSP can enable the IT organization to maintain compliance with the necessary corporate and regulatory standards while still leveraging the CCSP's shared infrastructure model's cost benefits and improved operational efficiency. For this to happen, each tenant must have their own private, isolated and secure virtual network security infrastructure. This requires that the CCSP implement an enterprise class virtual firewall that enables IT organizations to be able to define and enforce access control policies and to be able to segment departments while isolating the multi-tenant virtual infrastructure. In addition, if zone-based deployments are possible, this preserves existing PCI compliance, and also enables the organization's DMZ servers to be hosted securely in the virtual environment without the need to restructure IT policy or firewall architecture.

However, just as important as whether or not the CNS solution provides adequate security is whether or not the solution actually provides the benefits (Figure 1) that drive IT organizations to use public cloud computing solutions.

The primary benefit of using a public cloud computing solution is lower cost. While it can be a little tricky to compare the usage sensitive pricing of the typical CNS solution with the fully loaded cost of a premise based solution, the cost information provided by the CCSP should give the IT organization all the information about the CNS solution that it needs to do that analysis.

The second most important benefit of using a public cloud computing solution is being able to reduce the time it takes to deploy new functionality. Evaluating the agility of a CCSP is notably more difficult than evaluating their cost structure. One way for an IT organization to evaluate the agility of a CCSP is to identify the degree to which the CCSP has virtualized their infrastructure. This follows because a virtual infrastructure is notably easier to initialize, scale and migrate than a physical infrastructure is. Since the vast majority of CCSPs implement virtualized servers, server virtualization is unlikely to distinguish one CCSP from another. What can distinguish one CCSP from another is the degree to which they have virtualized other components of their infrastructure. One such component, firewalls, was previously discussed. Another such component is networking. By implementing routing software that runs on top of the most common hypervisors, CCSPs increase their ability to quickly provision and configure capacity. This approach to providing routing functionality also maps more closely to the usage sensitive pricing that most CCSPs offer. In addition, as will be discussed in the sub-section of this report entitled *Virtual Desktops*, virtualized networking also enables a CCSP to scale their service offering in a very cost effective manner.

Representative CNS Solutions

WAN and Application Optimization

Unlike some of the other CNS provided functionality discussed in this report (e.g., security, management), WAN and application optimization is a relatively narrowly defined function. This function has traditionally consisted of implementing devices, either at a branch office or in a data center, the goal of which is to optimize performance.

There are two principal categories of WAN and application optimization products. One category is an Application Delivery Controller (ADC). An ADC improves application performance by sitting in front of a server farm and delivering service requests to the members of the server farm based on criteria such as the load that each server is currently processing. Another way that an ADC improves application performance is by performing computationally intensive tasks, such as SSL or TCP processing, and hence freeing up server resources. An ADC can also accelerate the performance of applications delivered over the WAN by implementing optimization techniques such as compression and reverse caching. While the functionality provided by an ADC is often incorporated into a public cloud computing solution, it does not readily lend itself to being part of a stand-alone CNS.

The second category of WAN and application optimization products is WAN optimization controllers (WOCs). The goal of WOCs is to mitigate the negative effect that WAN services such as the Internet or MPLS have on application performance. Table 2 lists some of WAN characteristics that impact application delivery and identifies WAN optimization techniques that a WOC can implement to mitigate the impact of the WAN. The WAN optimization techniques are explained in detail in the *2011 Application and Service Delivery Handbook*.

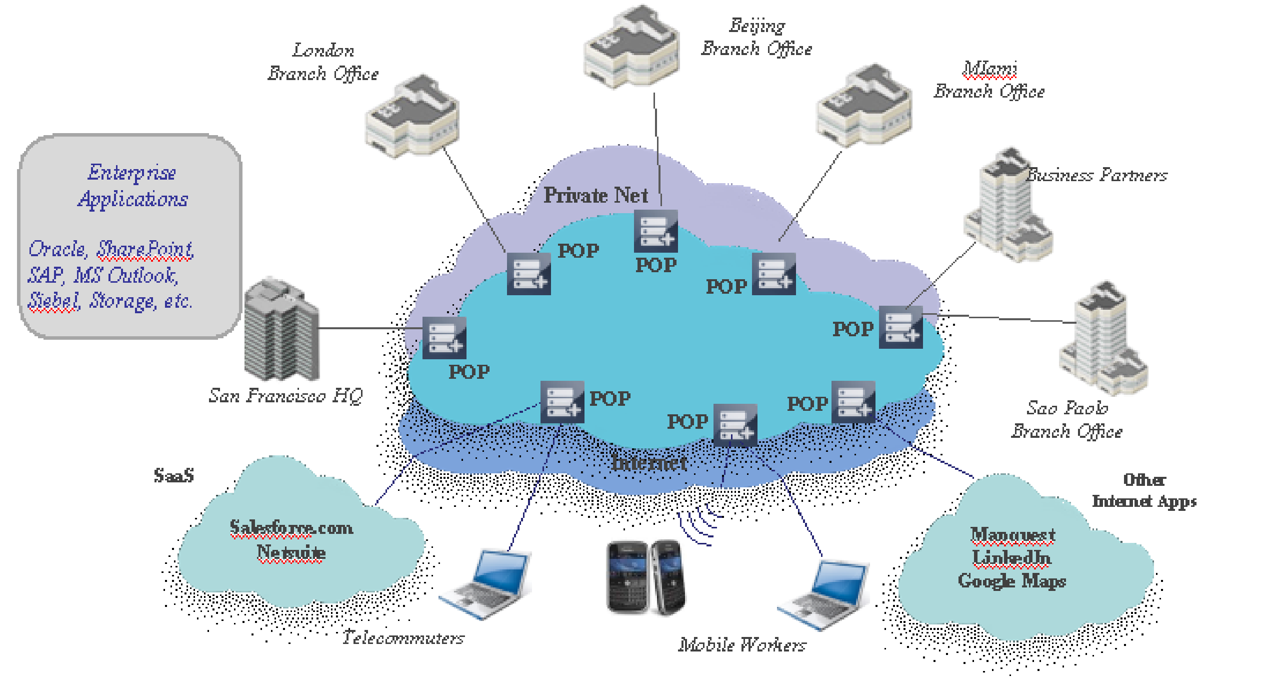
Table 2: Techniques to Improve Application Performance

WAN Characteristics	WAN Optimization Techniques
Insufficient Bandwidth	Data Reduction: Data Compression Differencing (a.k.a., de-duplication) Caching
High Latency	Protocol Acceleration: TCP HTTP CIFS NFS MAPI Mitigate Round-trip Time Request Prediction Response Spoofing
Packet Loss	Congestion Control Forward Error Correction (FEC) Packet Reordering
Network Contention	Quality of Service (QoS)

WOCs are typically deployed in a symmetric fashion – with a WOC in the branch office and another in the data center. When WOCs were first deployed several years ago, they were always deployed as hardware-based appliances. In most cases, the enterprise IT organization has implemented WOCs on a Do-It-Yourself (DIY) basis. However, over the last couple of years, a significant percentage of enterprise IT organizations have acquired WOC functionality as a managed service. In the last couple of years, some IT organizations have begun to implement a virtual or soft WOC. The phrase soft WOC refers to running WOC software in a virtual machine (VM). In part due to the resistance that most IT organizations have for putting additional software on end devices, there has been only a very small deployment to date of WOC functionality running on laptops.

More recently, IT organizations have begun to be able to gain access to WAN and application optimization as a CNS. As shown in Figure 2, to be effective the CCSP that provides the CNS needs to have enough cloud data centers (CDCs) or points of presence (POPs) so that there is a CDC/POP in close proximity to the users. The CCSP has to implement WAN optimization techniques, such as those listed in Table 2, and potentially other value added functionality at each POP. Ideally the CCSP would support a wide variety of WAN access services to give users the broadest possible set of alternative methods for accessing the services provided by the CCSP.

Figure 2: WAN and Application Optimization CNS



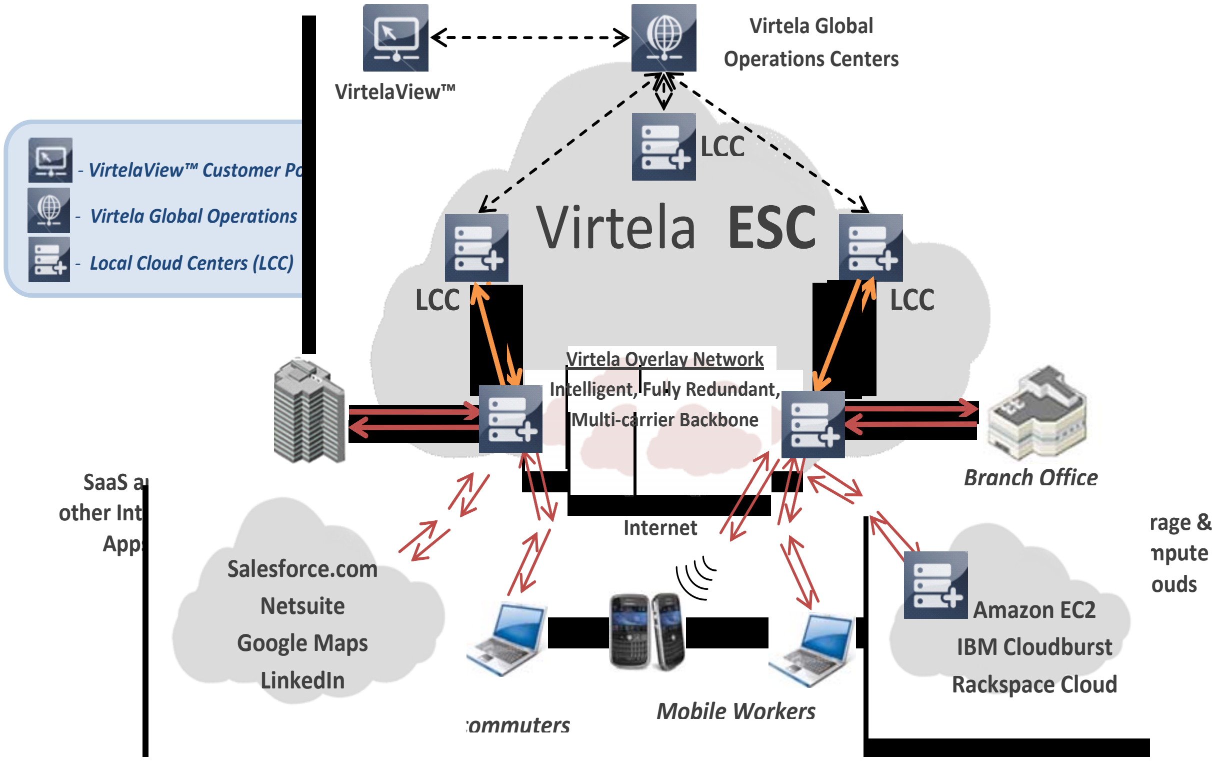
There are three distinct use cases for a CNS that provides WAN and application optimization functionality. One such use case was already mentioned - a CNS can be leveraged to solve traditional optimization challenges. In this case, the factors that would cause an IT organization to use such a CNS are the same factors that drive the use of any public cloud based services; e.g., cost savings.

Virtela ESC

The Virtela Enterprise Services Cloud (ESC) is the world's first open platform purpose-built for cloud networking services (CNS) – enabling a broad array of enterprise networking, security, and mobility capabilities to be delivered from the cloud.

Virtela ESC provides seamless communications between enterprise end users using any device (i.e. desktop, laptop, smartphone), private data centers, private and public clouds over any mix of underlying transport networks or network service providers.

The core architecture of Virtela ESC:



Virtela ESC has breakthrough architecture for cloud network services – locally distributed around the world via 50 Local Cloud Centers (LCCs), and optimized for virtual devices to support a wide range of IT services and applications. These innovations unlock core benefits for enterprises faced with supporting increasingly distributed workforces/locations that need fast and secure access to increasingly centralized applications from anywhere in the world.

Additionally, many companies often face decreasing IT budgets and staff. Virtela ESC frees enterprises from common IT constraints:

- The increasingly expensive “do-it-yourself” approach to capital-intensive hardware/software solutions at each site
- Closed 3rd party platforms that tie cloud services to a single network or service provider

The key unique attributes of Virtela ESC are as follows:

- **Open Architecture**
  Virtela ESC is independent of the underlying network, carrier, and technology. As a result, it delivers the best service to any location, using any network anywhere in the world. This infrastructure independence gives customers the freedom to choose the best mix of carriers, network and security services, and geographic locations for delivery.

- **Locally Distributed**
  Virtela ESC effectively brings services to the end user's doorstep via its highly distributed network of 50 Local Cloud Centers (LCCs) in major cities centers around the world. By pushing service delivery to the network edge, Virtela accelerates applications immediately, near the content source, and instantly mitigates security threats near the source of attack. Conventional clouds follow a centralized hosting model that may take end user traffic halfway around the world before reaching desired content. Virtela ESC offers the deepest geographic reach of any cloud platform available today.

- **Optimized for Virtual Devices**
  Virtela ESC changes the "One Device, Per Service, Per Location" status quo model. Virtela has de-coupled service delivery from hardware, virtualizing cloud network services to eliminate the complexity and expense of deploying multiple physical devices at your offices. This results in an order of magnitude cost savings and ease of use. Virtela ESC services can be activated within minutes and feature a consumable pay-as-you go pricing model.

Virtela delivers cloud network services using its Overlay Network multi-carrier backbone network. The Virtela Overlay Network uses VirtelaRoute™ intelligent routing and QoS mapping capabilities to deliver highly reliable service across multiple best-of-breed carrier networks around the world. This backbone can withstand the smallest performance issue to major infrastructure outages, including complete carrier network failures. Virtela ESC also leverages predictive analytics technology called VirtelaPredict™ to diagnose over 95 percent of potential network and security issues before they can impact network health.

The combination of Virtela multi-carrier Overlay Network and VirtelaPredict ensures ESC's industry-leading service performance and availability.

Virtela ESC supports a wide variety of services including:

- **Managed Cloud-based Application Acceleration.** The service makes applications such as email, web-based collaboration, backup and storage, ERP/CRM and windows file sharing run 5-25x faster with a 250% money-back guarantee. The service works regardless where the applications are hosted – within the enterprise headquarters or office locations, private cloud or public cloud such as Amazon EC2, IBM Cloudburst, and Rackspace cloud. If end users do not experience faster application response time, Virtela pays the customer 250% of the service charge. Virtela's cloud-based application acceleration interactive model show how much performance improvement by application customers can achieve based on their locations and remote access speed around the world.

- **Managed Cloud-based SSL VPN.** This service provides reliable and secure remote access for mobile and remote workers around the world using a simple web interface and Internet access. It offers the highest remote access availability SLA-up to 100%-in the industry with Virtela's global load balancing, global redirect capabilities, as well as Virtela's resilient, multi-carrier backbone. The service also offers a seat reservation feature that allows IT managers to reserve seats in the event of traffic spikes or in a disaster recovery situation.

- **Managed Cloud-based Security.** Virtela's portfolio of cloud-based security services includes cloud-based firewall, Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), web filtering, Security Event and Information Management (SIEM), and malware services. This suite of services allows customers to save on upfront hardware while getting the benefits of a fully managed service. With a layered security approach, Virtela's Managed Cloud-based Security detects and blocks malware coming from the Internet, WAN, or LAN and offers an extra layer of defense with protection purpose-built for bots.

- **Managed Cloud-based SIEM.** Virtela's SIEM service tracks traffic events on a multitude of network devices, including routers, switches, firewalls, and IDS/IPS. This service helps companies strengthen their security posture, protect their intellectual property, and facilitate the collection, management, and analysis of log data that is integral to meeting SOX, GLBA, HIPAA and PCI audit requirements. This service is also wholly integrated within the security services that Virtela offers.

- **Cloud-based Mobile Device Management.** As smartphones become more common in the workplace, IT managers now need to manage these devices as part of their IT infrastructure. This service helps with mobile expense and security management. Companies will be able to control costs by getting alerts when usage limits are reached, blocking when roaming occurs and by setting different policies by user group, as examples. IT managers also have the ability to locate lost or misplaced phones, remotely wipe/selective wipe applications, prevent access to corporate data if rogue applications are detected, and more. Virtela's service is mobile operator and OS platform independent. Offered for a low per-device monthly fee and no upfront charges, the service can be activated quickly from the cloud, includes a unified management portal called Virtelaview™, and offers the industry's first real-time notification SLA.

Virtela ESC's managed cloud network services, enabled by the Virtela Overlay Network, complement our managed CPE-based services, giving you the flexibility to choose the best solution on a location-by-location basis and allowing you to leverage our in-depth experience and expertise in deploying, managing, and maintaining global networking, security, and mobility services.

About Virtela
Virtela Technology Services Incorporated is the world's largest independent managed network, security and cloud services company. Virtela offers an award-winning suite of services – including managed networks, security, application acceleration and proactive infrastructure management – to mid-market and Fortune 500 customers around the world. Virtela offers unparalleled geographic reach to more than 190 countries through its partnerships with more than 500 carriers.

Virtela is headquartered in Denver, Colorado, with global support centers around the world. For more information, please call +1 (720) 475-4000 or visit www.virtela.net.

The second use case is the ongoing requirement that IT organizations have to support mobile workers. According to IDC[10], there will be 1.2 billion mobile workers by 2013 and the results of a recent survey[11] (The Survey) showed that many IT organizations are struggling to support the growth in mobile employees. Part of the challenge associated with supporting mobile employees is to provide these employees with high performance access to the Internet. This challenge is becoming even more difficult because the types of devices used by mobile workers are changing. Until this year, the most common device used by a mobile worker was a PC. However, according to Deloitte[12], in 2011 more smartphones and tablets will be sold than PCs. Given that few IT organizations to date have loaded optimization software onto laptops, it is highly unlikely in the foreseeable future that many IT organizations will load optimization software onto less powerful devices such as smartphones and tablets.

Another challenge that is associated with supporting mobile workers is how the applications that these workers access has changed. At one time, mobile workers tended to primarily access either recreational applications or applications that are not delay sensitive; e.g., email. However, in the current environment mobile workers also need to access a wide range of business critical applications, many of which are delay sensitive. This shift in the applications accessed by mobile workers was highlighted by SAP's recent announcement[13] that it will leverage its Sybase acquisition to offer access to its business applications to mobile workers.

The cumulative effect of these challenges is the lack of satisfaction on the part of remote workers. For example, according to The Survey, more than a quarter (27 percent) of CIOs said that their workers experience network performance problems when they work remotely, while 11 percent have problems with application performance.

The third use case for utilizing a CNS that provides WAN and application optimization functionality is the ongoing requirement that IT organizations have to support access to cloud services. As previously mentioned, in some instances it is possible for an IT organization to host a soft WOC at the CCSP's site. For example, an IaaS provider such as Rackspace might allow an IT organization to host a soft WOC at their data centers, but a SaaS provider such as Salesforce.com is unlikely to allow that. In those instances in which it is not possible to host a soft WOC at the CCSP's site, a CNS can improve the users' access to cloud services by providing to the users the type of functionality shown in Table 2.

As is the case with each class of CNS that is discussed in this report, in many situations the most appropriate solution is a hybrid solution. Using optimization as an example, a hybrid solution could consist of optimization functionality that is provided to all mobile workers by a CNS and is provided to branch office workers by a combination of hardware based WOCs, software based WOCs and a CNS.

[10] http://www.ciozone.com/index.php/Mobile-and-Wireless/IDC-Mobile-Workers-Will-Pass-1-Billion-in-2010.html

[11] http://www.csoonline.com/article/683735/mobile-workers-not-being-supported-by-it-survey-says

[12] http://www.deloitte.com/view/en_GX/global/industries/technology-media-telecommunications/tmt-predictions-2011/technology/fd19b1b06ef6d210VgnVCM1000001a56f00aRCRD.htm

[13] Wall Street Journal, May 17, 2011, page B7

VoIP & Unified Communications[14]

As was shown in Table 1, IT organizations have expressed great interest in acquiring cloud based VoIP and UC services. In addition, as described in *The 2011 Sourcebook for VoIP and UC Services* (The Sourcebook), there are over 200 providers of cloud based VoIP and Unified Communications services. While having that many providers results in benefits to consumers, it also creates some challenges. One such challenge is that providers tend to use different names for their services; i.e., cloud VoIP, hosted VoIP, virtual PBX and communications as a service (CaaS). Throughout this report, the breadth of cloud based VoIP and UC services will be referred to as CaaS solutions.

Another challenge that is associated with having such a breadth of providers is that the various providers don't all have the same business models. They have a number of business models including a:

- Service where the provider owns the hardware, software, network and has the staff that implements and maintains the service.
- Service that is a collection of dedicated or shared servers that run customer owned software, i.e. a private cloud.
- Provider that uses a third party's communications software to enable the service and that bundles the network access, management and possibly an SLA into a total package.
- Provider that develops their own software and hosts the service on their site.
- Provider that locates the requisite system on the enterprise premises, charges by a metric such as the number of phones supported and manages the system remotely.
- Reseller that owns little if any resources (e.g., hardware, software or network) but that resells cloud services from one or more, usually wholesale, providers.

As noted, there are over 200 providers of CaaS solutions. As pointed out in The Sourcebook, these providers offer a wide range of functionality including:

- Basic Telephony: Just the features expected for small business and consumer phone service.
- IP Telephony: The common features and functions found on a legacy PBX and the newer generation of IP PBXs are offered.
- Unified Messaging: A messaging service that typically includes a single storage and delivery of voice mail, e-mail, and fax messages.

[14] The material in this section is based in large part on *The 2011 Sourcebook for VoIP and UC Services*

Advertorial

Industry: Technology

Employees: 200

Headquarter: San Diego

> The deciding factor in choosing Fonality was the robust telephony features and the cost savings their solution provided.
>
> - Greg Harvey, IT Director

About the Customer:

The Overland Storage vision is to deliver effortless storage solutions for data management and data protection across the data lifecycle.

Challenges:

As a growing business Overland Storage faced many roadblocks that affected their choice in a solution that would meet their current and future communication needs.

- Move off multiple legacy systems, including Nortel and ShoreTel, that required a site visit and fees any time a system change was required

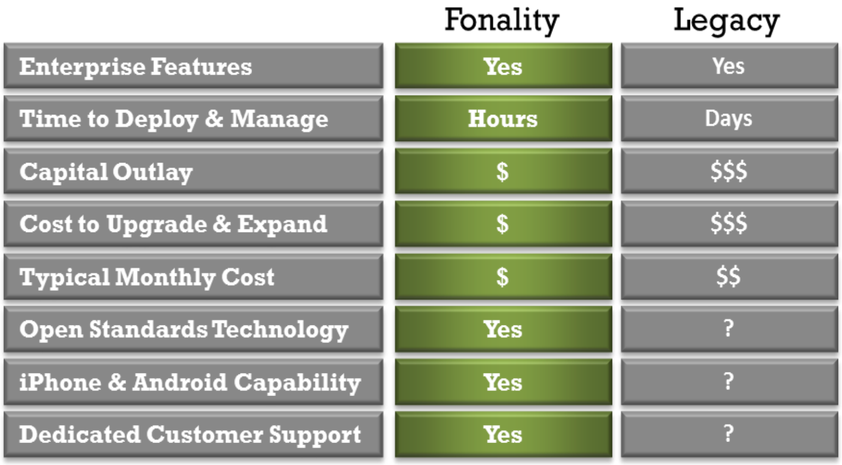
- Provide real-time presence information to employees both in the office and mobile

- Provide rich contact center features and the opportunity to auto-generate key performance reports

- Improve internal employee communications

The Solution:

A purpose built Fonality communication solution with the award winning Heads Up Display Unified Communications client was able to provide Overland Storage with the features and functionality suited for their growing business needs. Not only were they able to communicate internally with effiecency, they were able to ultimatley provide a better customer service experience. The company will save more than $14,000 a year in system maintenance costs alone with the Fonality communication solution.



	Fonality	Legacy
Enterprise Features	Yes	Yes
Time to Deploy & Manage	Hours	Days
Capital Outlay	$	$$$
Cost to Upgrade & Expand	$	$$$
Typical Monthly Cost	$	$$
Open Standards Technology	Yes	?
iPhone & Android Capability	Yes	?
Dedicated Customer Support	Yes	?

- Presence: A system for collecting and managing an individual's status, ability to communicate and preferences for mode of communication.

- Conferencing: Typically this includes voice/audio, video and web conferencing services.

- Call Center Support: This would include individual or combined functions such as:

    - Auto Attendant
    - Automatic Call Distribution (ACD)
    - Interactive Voice Response (IVR)
    - Auto/predictive Dialing

- Unified Communications: A communications service that includes several of the following elements: voice, unified messaging, video, mobility, web/data collaboration, and presence.

- HD Voice: This service uses broadband IP phones to deliver very high quality voice.

As The Sourcebook also points out, 75% of CaaS providers offer basic telephony while only 58% offer unified communications.

Some IT organizations will choose to use a CaaS solution to fulfill all of their collaboration requirements. However, as was the situation with WAN and application optimization, some organizations will want a hybrid solution in which the organization fulfills some of the requirements themselves and the organization utilizes a CaaS provider for the remainder of the requirements. Based on this requirement, a critical component of a CaaS solution is that it can be deployed in such a way that it complements the other collaboration solutions that potential customers already have, or intend to deploy. Another critical component of a CaaS solution is that it can support a broad range of user devices including desktops, laptops, tablets and smart phones. The importance of supporting a broad range of devices was highlighted in the previous section when it was mentioned that in 2011 the sales of smartphones and tablets will exceed the sale of PCs. One of the difficulties with supporting smartphones is that these devices run on a variety of operating systems and no operating system to date has become the *de facto* standard.

One of the primary factors that is driving users to adopt CaaS are the general advantages of public cloud computing that have been previously discussed in this report. As was the case with WAN and application optimization, the growth in the number of mobile workers is another key factor driving adoption. In particular, in order to increase the effectiveness of the growing number of mobile employees, companies are adopting unified communications functionality such as messaging and conferencing. Cloud based services provide an effective way of doing this, particularly for small to medium sized companies.

As previously mentioned, the material in this section is based in large part on *The 2011 Sourcebook for VoIP and UC Services* that was authored by Delphi and Webtorials. IT organizations that are evaluating cloud based VoIP and/or Unified Communications services may want to consider utilizing a consulting service provided by Delphi and Webtorials[15].

[15] Webtorials UC Consulting Services

Security

As previously noted, the scope of what is meant by WAN and application optimization is somewhat limited and the scope of what is meant by VoIP and unified communications is only slightly broader. In contrast, the scope of what is commonly meant by *security* is extremely broad. For example, in many cases IT organizations are extending their security perimeter and are also implementing a defense in depth approach to security. For the sake of this report, the focus of the discussion of security will be constrained to some of the primary aspects of security that were detailed in the previously mentioned IBM report entitled *X-Force 2010 Trend and Risk Report*.

As previously noted, the IBM report stated that, “Web applications accounted for nearly half of vulnerabilities disclosed in 2010.” One way that IT organizations can protect themselves against the growing number of security threats associated with the use of the Web is by creating detailed acceptable use policies and by driving compliance to those policies by leveraging a CNS that offers sophisticated Web content filtering and granular policy controls. The phrase *sophisticated Web content filtering* refers to the fact that static ratings of known web threats are not rigorous enough to protect against security vulnerabilities that are constantly changing and becoming increasingly more sophisticated. As a result, in order to ensure the most up to date Web content filtering, the CNS should implement dynamic rating algorithms that can identify and categorize web content accurately and in real time. In addition, comprehensive antivirus scanning provides additional protection from malware that can be contained in any type of file attachment.

Part of the growing security challenge associated with Web based applications is the continually increasing business use of social media sites such as facebook and of major Web mail services such as Yahoo. A company could implement a simple acceptable use policy that either allows or denies access to these sites. However, such a policy ignores the fact that these sites typically provide a variety of functions, some of which fall into the acceptable use policies of a growing number of organizations. To deal with the evolving use of multi-faceted social media sites, a CNS needs to be able to allow access to a social media site such as facebook, but block specific activities within the site, such as gaming or posting. Analogously, the CNS needs to have the granular controls to be able to allow users to send and receive mail using Yahoo, but block email attachments. This means that a CNS must be able to categorize these multifaceted sites in multiple categories, so that the different content is accurately represented. This functionality is necessary in order to enable effective and accurate acceptable use policy enforcement.

Another one of the security challenges associated with the use of Web based applications that is rapidly increasing in importance is the growth of malware. For example, in their Q2 2011 Global Threat Report[16], Cisco identified almost 290,000 unique instances of malware on the Web in June 2011. That number is almost triple the number of unique instances of malware that Cisco found on the Web in March 2011 (105,536). In Blue Coat’s 2011 Mid-Year Security Report[17] they stated that in the first half of 2011 that search engine poisoning was the most popular form of malware. According to Blue Coat, in nearly 40 percent of all malware incidents, search engines and/or portals were the entry point into malware delivery networks. According

[16] http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html
[17] http://www.bluecoat.com/doc/16622

Advertorial

COMPREHENSIVE WEB SECURITY AS A SERVICE

The Web Security Module of the Blue Coat Cloud Service provides market-leading web protection to organizations of all sizes without updating appliances, servers or user desktops. The Web Security Module is an Internet-delivered service that leverages Blue Coat's proven technology and collaborative, cloud-based community of over 70 million users to ensure real-time protection against known and unknown web-borne threats. With extensive web application controls and detailed reporting features, the Web Security Module enables administrators to create and enforce granular policies that are instantly applied to all covered users, including fixed locations and roaming users.

Reduced cost and complexity

Large and mid-sized enterprises must defend themselves against sophisticated web-borne malware, while reducing IT costs and boosting productivity for an increasingly distributed workforce. The Web Security Module of Blue Coat's Cloud Service allows customers to realize significant cost savings, eliminating the need to purchase, deploy and maintain on-premise hardware or software. Intuitive tools make it easy to create, enforce, and monitor effective web use policy. And because the service leverages a user-based subscription, customers pay only for what they need, and can seamlessly scale their web threat protection as required.

Real-time, dynamic malware protection

The Web Security Module delivers the best malware protection, using a combination of sophisticated, real-time web ecosystem analysis and inline malware scanning, including AV technology from leading vendors. Blue Coat's sophisticated web traffic behavioral analysis system inspects all parts of the web ecosystem to determine suspicious and malicious sites, and also examines malware-prone file types in detail. It even identifies "phone-home" or botnet traffic, enabling IT to quickly find and clean infected assets. By leveraging real-time web ratings and the web activities of millions of users in the WebPulse™ cloud community, the Web Security Module offers comprehensive web threat protection.

Market-leading web content filtering

The Web Security Module includes Blue Coat's comprehensive web filtering capabilities, which enable customers to achieve compliance by consistently enforcing their acceptable use policies. These features also allow IT to accurately filter web traffic by assigning multiple categories to any given URL, based on ratings from the global WebPulse user community.

Because static ratings of known web threats cannot protect against highly agile sources of malware, the service provides dynamic rating algorithms that identify and categorize web content in real time, ensuring the most up-to-date URL filtering. Blue Coat also maintains Blue Coat Labs to augment rating accuracy of web pages or domains.

Granular web application controls

The Web Security Module provides the industry's most effective controls for managing Web 2.0 applications, including the ability to control the use of leading social media applications such as Facebook, MySpace, Twitter, Flickr, YouTube, LinkedIn and more. IT can apply policies based on a wide range of criteria, including user, group, applications, postings, and media transfer controls:

-> Allow access to social media sites such as Facebook, but block specific activities within the site, such as gaming or posting.

-> Enforce SafeSearch and keyword search controls for all major engines, including media search engines.

-> Control whether users can send or receive messages and attachments for all major webmail services, such as Yahoo, MSN, AOL, and more.

IPSec VPN

-> Users behind firewall; traffic forwards to service transparently.

-> Authentication agent on AD domain manager

Proxy Chaining

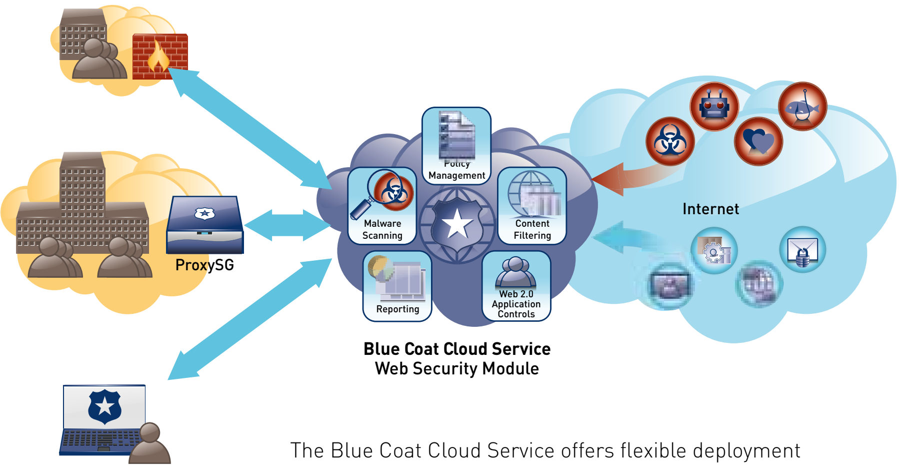
-> Forward from existing ProxySG, Squid or ISA

-> Authentication based on proxy

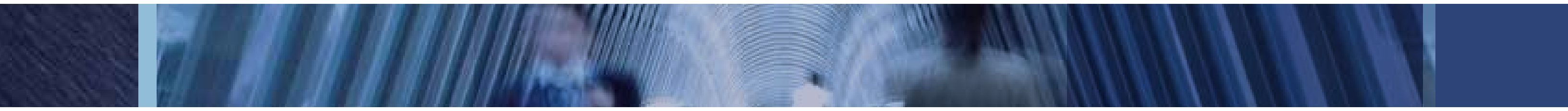
Desktop Agent

-> Client software forwards to service transparently

-> Authentication based on system credentials



The Blue Coat Cloud Service offers flexible deployment options for any size organization



Powerful, intuitive policy management and reporting

The Blue Coat Cloud Service incorporates industry-leading proxy and policy technologies, which have become the global standard for network security architectures. Administrators can quickly and easily enforce broad-based or detailed policies for network access and use – from small groups to hundreds of thousands of users – all in one simple configuration.

Through seamless integration with customers' existing authentication systems, Web Security Module administrators can instantly report on web activity by user, group or across the organization. Organizations of any size can leverage the rich, enterprise-level reporting features of the Web Security Module, including dashboards, drill-down, and custom reports.

Flexible deployment options

The Cloud Service was architected to ensure flexibility and instant interoperability with existing network infrastructures. A simple configuration change to firewall, router, or proxy solution allows administrators to instantly protect and enforce Internet use policies for all users connected behind the device. An optional lightweight desktop agent ensures that roaming users are protected regardless of their location.

A web security service for any size business

The Cloud Service is built on a secure, high-performance, multi-tenant architecture. Data center deployment is geographically dispersed, with multi-network vendor locations and extensive redundancy. Individual components of the service are built on highly secure foundations.

As a testament to its reliability, the service infrastructure has been in production for over six years without a major outage, with over 70 million users regularly accessing it.

BENEFITS

Market-leading web threat protection and control

-> Sophisticated web intelligence and inline malware scanning

-> Identify and categorize new web content in real time with >99% accuracy

-> Manage Web 2.0 applications with granular controls

Reduce cost and complexity

-> No upfront costs – pay as you go

-> Integrates seamlessly with existing network infrastructure

-> Less downtime, higher user productivity

-> Service architecture provides infinite scalability

Easy to configure and manage

-> Quickly enforce policies for network access and use

-> Instantly report on web threats and user activity

-> Support cloud-only or hybrid deployment models

-> Transparent AD integration

Built on a robust, scalable infrastructure

-> Deployed globally on a purpose-built, multi-tenant architecture

-> Over 70 million users regularly access the service

-> In production for over six years without a single major outage

-> Backed by a guaranteed 99.999% uptime SLA

Connection Methods

IPSec VPN (Site to Site)		
Proxy Chaining		
Desktop Connector Agent	Operating Systems • Microsoft Windows XP (32-bit) with Service Pack 3 or later • Microsoft Windows Vista (32-bit and 64-bit) Service Pack 2 or later • Microsoft Windows 7 (32-bit and 64-bit)	Minimum Hardware Requirements • Must meet minimum operating system requirements for Microsoft Windows XP/Vista/Win7 • x86 or x86-64 compatible processor • 100 MB of available hard disk space for software installation and logging • High-speed Internet connection (Ethernet or Wi-Fi network adapter required)

Supported Authentication Services

Active Directory	Operating Systems • Windows 2003 SP2 or later	Minimum Hardware Requirements • Must meet minimum hardware requirements for Windows 2003 SP2 and later • X86 or x86-64 compatible processor • 100MB of available hard disk space for software installation and logging • High speed internet connection

to the report, in 2011 email and pornography were the third and fourth most popular way to lure users to malware[18].

The Blue Coat report concluded that:

- Malware hosting is often found within categories that companies typically allow in their acceptable use policies; e.g., online storage and software downloads.
- Businesses should block pornography and online gaming.
- A single defense layer, such as a firewall or anti-virus software, is insufficient against the dynamic nature of malware and the extensive infrastructure of malware delivery networks.

To protect against malware, a CNS should be able to identify suspicious content or sites that are either suspicious or are known to distribute malware. In order to be effective, a CNS that provides Web content filtering or malware protection needs a source of intellectual capital that identifies known and suspected vulnerabilities. This source needs to be both dynamic and as extensive as possible.

One part of the value proposition of a CNS that provides security functionality is the previously discussed value proposition of any cloud based service. For example, a security focused CNS reduces the investment in security that an organization would have to make. In addition, a security focused CNS reduces the amount of time it takes to deploy new functionality. The speed at which changes can be made to a CNS adds value in a variety of situations, including providing better protection against zero-day attacks[19]. As discussed below, the IBM report also discussed the growing security risks that are associated with the dramatic growth of mobile workers. Another part of the value proposition of a security focused CNS is that unlike a traditional security solution that relies on the implementation of a hardware based proxy, a CNS can also protect mobile workers. The CNS does this by leveraging functionality that it provides at its POPs as well as functionality in a software agent that is deployed on each mobile device.

This report previously made the observation that in many instances, the most appropriate solution is a hybrid solution. That observation certainly applies to a CNS that provides security functionality. In some cases, the IT organization already has functionality such as web filtering or malware protection deployed in CPE at some of their sites. In this case, the IT organization may choose to implement a CNS just to protect the sites that don’t have security functionality already implemented and/or to protect the organization’s mobile workers. Alternatively, an organization may choose to implement security functionality in CPE at all of their sites and to also utilize a CNS as part of a defense in depth strategy.

Other situations in which a security centric CNS can serve to either be the only source of security functionality, or to compliment CPE based implementations include cloud-based firewall and cloud-based IPS services. Such a service should support equipment from the leading vendors. Given the previously mentioned importance of hybrid solutions, the service should allow for flexibility in terms of whether the security functionality is provided in the cloud or from CPE as well as for flexibility in terms of who manages the functionality – a CCSP or the enterprise IT organization. These options are shown in Table 3.

[18] The second most popular way that users were lured to malware was a collection of ways that didn’t fit into any other category.

[19] http://en.wikipedia.org/wiki/Zero-day_attack

Table 3: Management and Delivery Options

CPE Based Security Functionality Managed by a CCSP	Cloud Based Security Functionality Managed by a CCSP
CPE Based Security Functionality Managed by the IT organization	Cloud Based Security Functionality Managed by the IT organization

Table 3 illustrates how a given CNS can be regarded as providing multiple classes of solutions. For example, if a CNS offers the option of providing security functionality such as a firewall, it is reasonable to classify it as a security solution. However, if the same service offers the option of managing firewalls that are provided by an enterprise IT organization, it is reasonable to classify the service as a management solution.

In addition to the specific security functionality provided by the CNS, the CNS should also:

- Provide predictive analytics whereby the CNS can diagnose the vast majority of potential enterprise network and security issues before they can impact network health.

- Incorporate expertise, tools, and processes to ensure that the service that is provided can meet auditing standards such as SAS-70 as well as industry standards such as ITIL.

- Integrate audit and compliance tools that provide the necessary event-correlation capabilities and reporting to ensure that the service meets compliance requirements such as Sarbanes-Oxley, HIPAA, GLB and PCI.

- Provide the real-time notification of security events.

Network Management

As is the case with security, ***network management*** is a very broad topic. Because of the breadth of the topic, it is possible to find a CNS that provides almost any possible form of management functionality. For example, the preceding section of this report discussed CNS solutions that manage security functionality such as that provided by IPSs and firewalls. There are also CNS solutions that manage basic networking functionality such as routers. When evaluating any of these solutions, IT organizations need to determine how wide a range of vendors' products the solution can manage and how much expertise the CCSP has with those products.

Analogous to the preceding section on security, the scope of what will be covered in this section will be constrained to some of the primary issues that were detailed in the IBM report entitled *X-Force 2010 Trend and Risk Report*. As previously mentioned, the IBM report concluded that most IT professionals view the data stored on mobile devices and how that data can be misused or lost as the main security threats associated with these devices. That view creates a marketplace opportunity for a CNS that provides mobile device management. The need for such a service is reinforced by the previously referenced market research report that concluded that many IT organizations are struggling to support the growth in mobile employees.

In order to be an effective, a CNS that provides mobile device management should:

- Offer a portal that provides a comprehensive view into the mobile device environment.

- Given the ongoing consumerization of IT, the portal should provide visibility into both corporate and employee-owned mobile devices.

- Enable the organization to implement security policies through simple click configuration and provisioning.

- Control access to key network resources and applications by specific user groups or by lines of business.

- Detect if a mobile device has been lost and, if so, delete the data from the device.

- Detect when roaming, data, voice, or SMS usage thresholds have been reached, and provide real-time alerts to prevent unwanted billing overages.

In addition to managing specific pieces of network hardware or mobile devices, another focus area for a management centric CNS is managing services provided by a CCSP. As is the case with the deployment of most new technologies and services, there was at best a minimum of management capability associated with the initial wave of CCSP services. For example, the initial wave of CCSP services came with little if any commitment on the part of the service provider relative to an SLA. The SLAs that were provided were based strictly on the availability, and not the performance, of the CCSP's service. These SLAs required the customer to use primitive techniques such as logging to prove that the CCSP's solution didn't meet the promised level of availability. Few if any IT organizations had the ability to monitor and manage the end-to-end performance of this initial wave of CCSP provided services.

At the same time that CCSPs were deploying services that had little if any commitment to an SLA, IT organizations were beginning to respond to internal pressure by offering performance-based SLAs to the company's business unit managers. However, the majority of IT organizations have found that conducting the end to end performance monitoring that is necessary to support SLAs for delay-sensitive applications such as VoIP is very difficult. For example, as documented in *The 2011 Application and Service Delivery Handbook,* over two thirds of IT organizations stated that getting better at ensuring acceptable performance for VoIP traffic over the next year was either very or extremely important to their organization.

A strong case can be made for a CNS that manages a VoIP solution that an IT organization acquires from a CCSP. The value proposition for this type of CNS has three major components:

- There is great interest on the part of IT organizations to acquire VoIP from a CCSP.

- Few IT organizations currently do a good job of end-to-end management of a service that they acquire from a CCSP.

- IT organizations are under increasing pressure to ensure acceptable performance for VoIP traffic.

.

Virtual Desktops

Most of the functionality that has previously been discussed (e.g., optimization, management, VoIP, security) has already been broadly implemented. As such, the question of using a CNS to provide this functionality centers around using a CNS to either support a relatively small number of employees who don't currently have access to the functionality, reducing the cost of providing the functionality or using a CNS to support new requirements; i.e., mobile employees or cloud computing.

In contrast to that situation, desktop virtualization is a topic that has received a lot of attention in the trade press, but has not been widely implemented. *The 2011 Application and Service Delivery Handbook* reported on the results of a survey in which the survey respondents were asked to indicate the percentage of their company's desktops that have either already been virtualized or that they expected would be virtualized within the next year. Their responses are shown in Table 4.

Table 4: Deployment of Virtualized Desktops

	None	1% - 25%	26% - 50%	51% - 75%	76% - 100%
Have already been virtualized	55%	36%	3%	1%	4%
Expect to be virtualized within a year	30%	51%	8%	4%	7%

One conclusion that can be drawn from the data in Table 4 is that to date less than half of IT organizations have implemented desktop virtualization and the ones that have implemented it, have only done so sparingly. Another conclusion that can be drawn from the data in Table 4 is that over the next year, there will be a modest increase in the use of desktop virtualization.

Comparing the data in Table 1 and Table 4 leads to another interesting conclusion.   As shown in Table 1, between a quarter and a third of IT organizations stated that the adoption of a CNS to provide functionality such as VoIP, security or network management either will likely happen or will happen. That contrasts to the sixteen percent of IT organizations that said that the adoption of a CNS to provide desktop virtualization either will likely happen or will happen.   Just based on those percentages, it appears as if IT organizations are not very interested in using a CNS solution for desktop virtualization. However, given the wide disparity between the existing and planned deployment of functionality such as VoIP and the existing and planned deployment of desktop virtualization, another way to look at that data is that IT organizations are actually relatively more interested in using a CNS to provide desktop virtualization functionality than they are to use a CNS to provide more traditional functionality.

One of the reasons why there is such a relatively high interest in a CNS that provides desktop virtualization functionality is that desktop virtualization is new and highly complex. For example, there are two fundamental forms of desktop virtualization. They are:

- Server-side virtualization
- Client-side virtualization

With server-side virtualization, the client device plays the familiar role of a terminal accessing an application or desktop hosted on a central presentation server and only screen displays, keyboard entries, and mouse movements are transmitted across the network. This approach to virtualization is based on display protocols such as Citrix's Independent Computing Architecture (ICA) and Microsoft's Remote Desktop Protocol (RDP).

There are two primary approaches to server-side virtualization. They are:

- Server Based Computing (SBC)
- Virtual Desktop Infrastructure (VDI)

IT organizations have been using the SBC approach to virtualization for a long time and often refer to it as Terminal Services. Virtual Desktop Infrastructure (VDI) is a relatively new form of server-side form of virtualization in which a VM on a central server is dedicated to host a single virtualized desktop.

Client-side application virtualization is based on a model in which applications are streamed on-demand from central servers to client devices over a LAN or a WAN. On the client-side, streamed applications are isolated from the rest of the client system by an abstraction layer inserted between the application and the local operating system. In some cases, this abstraction layer could function as a client hypervisor isolating streamed applications from local applications on the same platform. Application streaming is selective in the sense that only the required application libraries are streamed to the user's device. The streamed application's code is isolated and not actually installed on the client system. The user can also have the option to cache the virtual application's code on the client system.

Each form of desktop virtualization has its own strengths and weaknesses[20] based in part on the type of employee and the type of user devices that the IT organization intends to support. As a result, one criterion that IT organizations can use when evaluating a CNS that provides desktop virtualization functionality is the classes of desktop virtualization that they support. In addition, IT organizations should determine if the CNS offers delivery options analogous to what is depicted in Table 3.

Choosing the right type or types of desktop virtualization is only part of the challenge. Ensuring acceptable performance for VDI presents some significant challenges. For example, the ICA and RDP protocols employed by many hosted application virtualization solutions are somewhat efficient in their use of the WAN. However, these protocols have significant limitations with graphics-intensive applications, 3D applications, and applications that require audio-video synchronization. Compared with hosted applications, streamed applications are far less efficient as they typically use the same inefficient protocols (e.g., CIFS) that are native to the application. Furthermore, streamed applications create additional bandwidth challenges for IT organizations because of the much larger amount of data that must be transmitted across the WAN when the application is initially delivered to the branch. One way that an IT organization

[20] http://www.cio.com/article/504348/Desktop_Virtualization_5_Most_Popular_Flavors_Explained

can overcome the performance challenges that are associated with using desktop virtualization, whether the IT organization supports desktop virtualization themselves or uses a CNS solution, is to utilize a CNS that optimizes the traffic that is associated with desktop virtualization.

A preceding section of this report (*Evaluating CNS Solutions*) provides some insight into how IT organizations should evaluate CNS solutions. Two of the criteria that were discussed in that section were security and scalability. Relative to a CNS solution for desktop virtualization, those criteria are tightly inter-related. A CCSP that offers a desktop virtualization solution must provide secure access to their data centers using Virtual Private Network (VPN) tunnels. However, if the CCSP uses a traditional approach to networking based on physical appliances, it will require a network appliance for each customer to support the required VPN functionality. If, however, the CCSP uses a virtual networking solution, it can run tens of instances of the routing software in a single high end server and hence scale notably more efficiently.

Summary & Recommendations

Over the last few years, IT organizations have begun to make a broad adoption of SaaS and IaaS solutions and numerous market research reports indicate that the adoption of these solutions will increase significantly over the foreseeable future. However, with the exception of communications and collaboration, to date the SaaS solutions that have been adopted have been enterprise business applications such as CRM or ERP and the IaaS solutions that have been adopted have been basic compute and storage.

The research contained in this report indicates that the market is potentially approaching a fundamental shift in terms of how IT services are provided. That market research indicates that IT organizations have strong interest in obtaining many traditional IT services from a CCSP. Those services include VoIP, UC, WAN and application optimization, security, management and desktop virtualization.

Given the potential shift in terms of how IT services are provided, IT organizations need to develop a strategy that identifies which of the traditional IT services it will continue to provide itself, which ones it will acquire from a CNS provider and which ones it will provide in a hybrid fashion. As part of developing this strategy, IT organizations need to evaluate the burgeoning set of CNS solutions. When evaluating these solutions, the bare minimum that an IT organization needs to understand is the functionality that the solution provides. However, since CNS is just another form of public cloud computing, IT organizations also need to determine if the CNS solution delivers on the promised benefits of public cloud computing while also eliminating, or at least minimizing, the negative aspects of a public cloud computing solution.

The key promised benefits of public cloud computing are shown in Figure 2 and include:

- Lowering cost
- Reducing the time it takes to deploy new functionality
- Being able to acquire functionality that was not previously available
- Freeing up resources

Concern about security is the primary impediment to the adoption of public cloud computing solutions and hence evaluating the security of the CNS provider's facilities is a critical component of evaluating a CNS solution. One part of this evaluation is determining how the CCSP secures any transmission over the WAN. Another part of the evaluation is to determine whether or not the CCSP's implementation of a multi-tenant environment has compromised security.

As noted, part of developing a strategy for the use of CNS solutions is to determine where an IT organization will use a CNS as part of implementing a hybrid solution. Using optimization as an example, a hybrid solution could consist of optimization functionality that is provided to all mobile workers by a CNS and is provided to branch office workers by a combination of hardware based WOCs, software based WOCs and a CNS. Another part of the strategy is to determine if the IT organizations will also use multiple CNS solutions in an inter-related fashion. For example, an IT organization that uses a CNS for virtual desktops or VoIP may also use a CNS to provide optimization to ensure acceptable performance.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

Published by
Webtorials
Editorial/Analyst
Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of Steven Taylor and Jim Metzler.