TECHNICAL WHITE PAPER

Unified Communications and Collaboration as a Service

Maintaining Security, Availability, and Reliability in the Private Cloud

Overview

Enterprise organizations around the world are increasingly turning to managed network and cloud services to reduce capital and operational expenses (CapEx and OpEx); enhance workforce productivity; increase agility; achieve more predictable costs; and simplify operations throughout the application lifecycle. Today's managed cloud-based services deliver high levels of reliability, availability, and security, which are all traditional, core attributes of carrier-class service provider infrastructures.

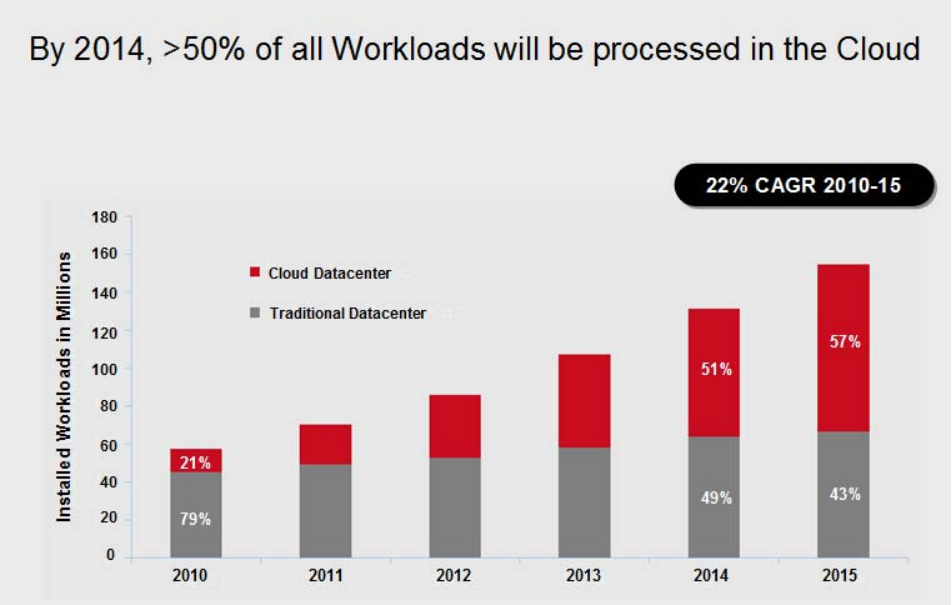
But not all cloud services are alike. Public cloud services can be vulnerable to Internet intrusions.

Private and dedicated cloud services – available from service providers to individual organizations – are far more secure and reliable. This reality is due to a variety of factors, including:

- A defense-in-depth security strategy with overlapping layers of protection
- The use of a customer specific virtual routing and forwarding (VRF) environment, allowing each customer to have their own unique instance of an application that is not shared
- Firewalls to control traffic as it travels to and from private cloud services and protect against threats from inside or outside an enterprise
- Use of purpose-built management systems as well as syslogs for system monitoring and management, security auditing, and generalized informational analysis, debugging, and troubleshooting to remediate failures and help reduce downtime
- The ability for customers to assign addresses utilized behind the cloud-based firewall to create a "demilitarized zone" (DMZ) for the service

The popularity of cloud services is driving massive increases in data center and network traffic, with global cloud traffic expected to grow by a factor of 12 between 2010 and 2015, reaching 1.6 zettabytes a year in 2015, according to the Cisco Global Cloud Index: Forecast and Methodology, 2010-2015. The same study predicts that by 2014 over 50 percent of computing workloads in data centers will be cloud based (Figure 1), resulting in a compound annual growth rate (CAGR) of 22 percent.

Figure 1. Growth of Cloud Workloads



Source: Cisco Global Cloud Index: Forecast and Methodology, 2010-2015

The IDC Worldwide Managed Network Services 2010-2014 Forecast predicts global cloud services revenue to grow at a CAGR of 11.5 percent, expanding from $45.2 billion in 2009 to $77.9 billion by 2014. An April 2011 study by Forrester Research entitled “Sizing the Cloud” predicts that private cloud services revenue will grow from $7.8 billion in 2011 to $15.9 billion by 2020. The overall cloud services market will grow by nearly a factor of six, from $40.7 billion in 2010 to more than $241 billion, by 2020.

According to a recent Cisco Internet Business Solutions Group study, 50 percent of enterprises began cloud migrations in 2011 and at least 12 percent of all enterprise workloads will run on clouds globally by 2013. This underscores the confidence many organizations have in the integrity of cloud services.

The combination of private, hosted and managed cloud services with unified communications and collaboration services can reduce or eliminate the need to install, maintain, and upgrade onsite PBX equipment and applications. Each customer is provided with dedicated, virtual instances of each application, including software and hardware redundancy and availability.

Beyond the cost and operational benefits, private, hosted and managed unified communications help organizations increase teamwork and productivity, improve speed to market, enhance business process flexibility, increase customer satisfaction, and reduce travel expenses. The ability to deliver unified communications applications (including presence, IP voice, instant messaging, desktop and Web conferencing, and collaboration workspaces) to both fixed and mobile clients further adds to the overall value.

When it comes to private, hosted, and managed cloud environments, there are various approaches to security, reliability, and availability – some far superior to others. This is especially true for unified communications, where information confidentiality may be required and where the absence of reliable, available services may lead to the failure of business operations.

Security, Availability, and Reliability Challenges

In an era where business happens in an instant, the confidentiality of trade secrets, sales and customer information, and communications between employees, customers, partners, and suppliers is especially vital. Strategic advantage can be won or lost based on the availability and security of information – and reliable unified communications and collaboration services and information can often form the basis of entirely new business models.

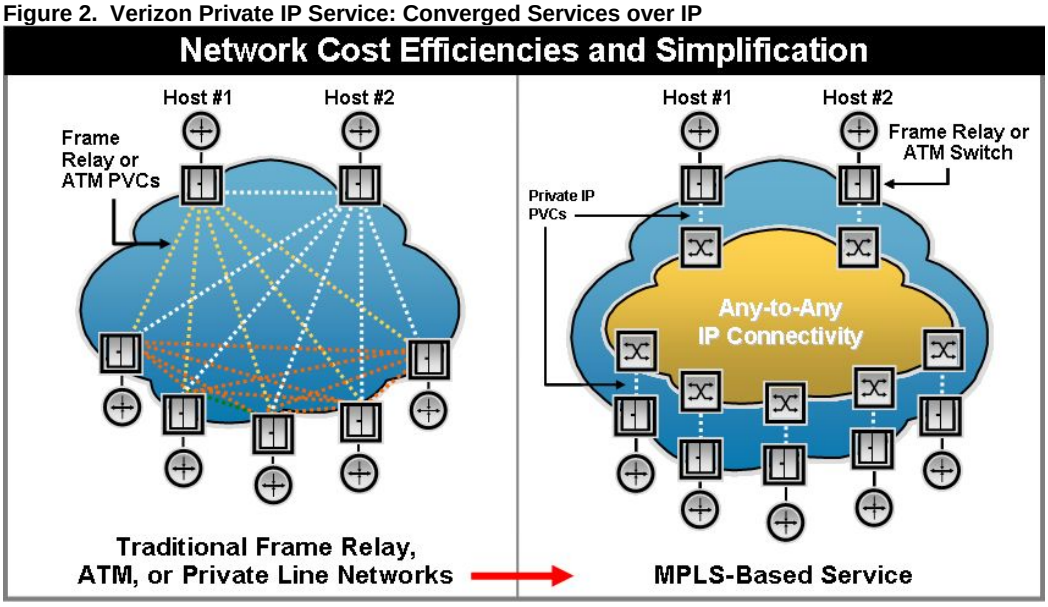
Services provided over the Internet and public clouds, moving from large collocation data centers and out to insecure fixed and mobile devices, lack the rigid security and reliability of enterprise network and private cloud services. For enterprise unified communications and collaboration, these shortcomings are unacceptable.

By contrast, world-class, private, hosted and managed cloud services incorporate proven industry best practices, architectures, platforms, and technologies, and adhere to enterprise data center standards. These services also enable many new features based on virtualization and other more recent innovations.

Private IP and UCCaaS

Verizon's Global Private IP Service infrastructure is a private, hosted and managed cloud services environment that offers a carrier-class approach to the most mission-critical enterprise business services. Customers obtain services via a Layer 3 MPLS (Multiprotocol Label Switching) VPN, getting the security and quality of service (QoS) of older ATM and Frame Relay, the flexibility and scalability of IP, and the convergence of voice, data, and video applications over an integrated network infrastructure (Figure 2).

Figure 2. Verizon Private IP Service: Converged Services over IP



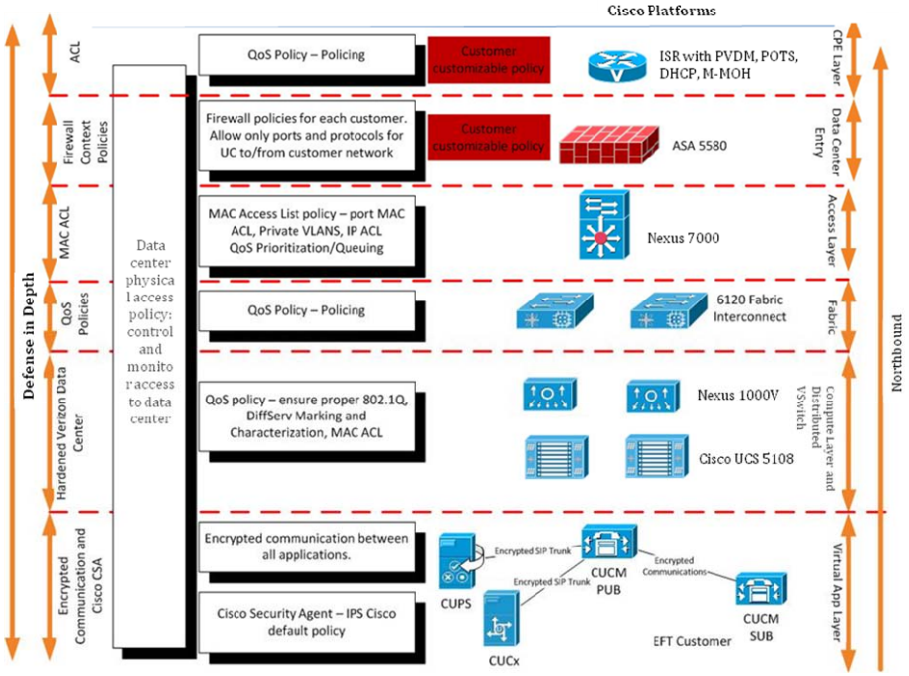
Verizon's UCCaaS (Unified Communications and Collaboration as a Service) provides an extensive roster of unified communications and collaboration applications to users in varied work environments and scenarios, packaging the entire suite of Cisco Hosted Collaboration Solution applications into a single user license. The package includes client and server software access rights, service and support, and software upgrades.
The solution is based on Cisco Unified Communications Manager and VMware vSphere Hypervisor for virtualization. Applications include:

- Cisco Unified Communications Manager: Delivers call control, voice services, and plug & play provisioning of IP phone features
- Cisco Unity Connection: Provides voice messaging features and services such as Web voicemail, Internet Message Access Protocol (IMAP) integration for Microsoft® Outlook® and Cisco Unified Personal Communicator client, and IMAP integration for Cisco Unified Mobile Communicator (CUMC) client integrated with Cisco Jabber on-premise and cloud-based collaboration services. Cisco Jabber provides a single interface across presence, instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing
- Cisco Jabber/Cisco Unified Personal Communicator: Allows customers to bring together all their communication applications in a single, easy-to-use interface for PC or Mac. Users can stay connected virtually anywhere they are and quickly find people they need to reach. Cisco Unified Personal Communicator brings secure soft phone capabilities, presence, instant messaging, visual voicemail, video, Web conferencing, and more to the desktop.
- Cisco Jabber Instant Messaging: Enables users to instantly connect and collaborate with colleagues across locations and time zones. Using online presence, users can find, connect, and collaborate with practically anyone, from virtually anywhere.
- Cisco Jabber Mobile Client: Extends communication and collaboration capabilities to the smart phone or tablet, providing remote or mobile workers the ability to connect and collaborate across any network and via preferred devices.
- Verizon Audio and Net Conferencing: Offers users a virtual meeting room, allowing them to collaborate instantly or schedule events in advance.

Two key differentiators of UCCaaS include:

- **Multi-customer versus multi-tenant computing infrastructure**: While multi-tenant computing infrastructures feature a single set of applications in one IP address space on a server that then supports multiple different customers, the multi-customer infrastructure behind UCCaaS provides each customer with dedicated, virtual instances of each individual application through the use of virtualization technology. Each instance of software is thus completely isolated from every other instance. Applications run in their own address spaces, with dedicated server processing provided to each customer. There is no routing between VRFs and individual instances of firewalls at the edge of the network, enabling customers to set up their own filter rules. Data stores on the storage area network (SAN) feature a logical unit number (LUN) dedicated to each separate customer. The multi-customer environment is more secure than multi-tenant, allowing customers to enjoy the benefits of dedicated software while taking advantage of shared hardware, with carrier-class security, flexibility, and resiliency.
- Defense-in-Depth security model: This industry proven best practice features multiple layers of security and different security techniques that provide overlap protection should any one layer or technique or component fail [Figure 3]. UCCaaS utilizes a variety of technologies and techniques to protect the core network and customer networks. This includes the use of stateful and redundant firewalls; Deep Packet Inspection (DPI); individual server and component hardening; and physical security at Verizon data centers.

Figure 3. Defense-in-depth Security Layers and Corresponding Cisco Platforms



Security, availability, and reliability features at each network layer for UCCaaS include:

Customer premises equipment (CPE) and access security focuses on the PCs, phones, media players, gateways, routers, and other devices that connect to the network. The devices themselves have the ability to encrypt data, voice, or video traffic, but this can become resource intensive. Instead, separate virtual LANs (VLANs) for voice and data with QoS and the use of access control lists (ACLs) help ensure that only end points are permitted to communicate to on-premise service routers and media routers. Security features protect VoIP devices that must interconnect with the public switched telephone network (PSTN).

Switch ports must be protected from Media Access Control (MAC) content-addressable memory flooding attacks, where the switch is flooded with so many MAC addresses that it cannot determine which port an end station or device is attached to. In this case, it broadcasts the traffic to the entire VLAN and the attacker is able to see all traffic coming to all the users in the VLAN. Security tools limit the number of MAC addresses allowed to access individual ports, based on the connectivity requirements for those ports.

Phones on the network are also vulnerable to data attacks. Gratuitous Address Resolution Protocol (GARP) on the phones helps to prevent man-in-the-middle (MITM) attacks involving an attacker who tricks an end station into believing that he or she is the router and tricks the router into believing that he or she is the end station. This scheme makes all the traffic between the router and the end station travel through the attacker, thus enabling the attacker to log all of the traffic or inject new traffic into the data conversation. GARP on an IP phone protects against an attacker's ability to capture the signaling and RTP voice streams from the phone.

A partial list of other access security measures includes:

- Port security: It is important to prevent access to all switch ports. An exception is those devices allowed to connect to the port via their MAC addresses. This form of device-level security authorization enables a network administrator to authorize access to the network by using MAC addresses as device credentials.

- Dynamic Host Configuration Protocol (DHCP) snooping: When enabled, this feature treats all ports in a VLAN as untrusted by default and prevents a non-approved DHCP or rogue DHCP server from handing out IP addresses on a network by blocking all replies to a DHCP request unless that port is allowed to reply.
- Dynamic ARP Inspection (DAI): This feature is used on the switch to prevent GARP attacks on the devices plugged into the switch and on the router. Here the GARP feature prevents all devices on the LAN, not just IP phones.
- IEEE 802.1X Port-based Authentication: Used to identify and validate the device credentials of an IP phone before granting it access to the network, the 802.1X feature is a MAC-layer protocol that interacts between an end device and a RADIUS server. It encapsulates the Extensible Authentication Protocol (EAP) over LAN to transport the authentication messages between the end devices and the switch.
- Phone authentication and encryption: Cisco Unified Communications Manager can be configured to provide multiple levels of security to phones within a voice system, including device authentication plus media and signaling encryption using X.509 certificates.

A virtualized instance of a data center firewall deployed between the customer's VRF instance of their applications and the applications themselves provides an access control and monitoring point to the unified communications and collaboration applications. The firewall is an important best practice, protecting the unified communications services from attack from the customer's enterprise environment. It also helps prevents denial of service (DoS) attacks and polices access from the voice and data VLANs based on the customer's application environment and policies. With UCCaaS, customers have access to data via syslog which can be used in place of security log gathering. Firewall rules may be customized to meet customer security practices that may already be in place. [Note: Customers may customize their firewall policies for firewalls that extend and further harden their security posture but Verizon's baseline security policy cannot be modified.]

The fabric interconnect to the SAN—the ports and backplane used to communicate between VM instances and the SAN—is segmented like the virtual LANs that carry voice and data and distributed switching further isolates customer traffic. While cloud services that provide infrastructure-as-a-service (IaaS) such as Amazon's Elastic Compute Cloud (EC2) are transactional, bursty services, UCCaaS cannot tolerate even a few seconds of latency, since this will cause parties in a phone conversation to hang up. Therefore, QoS features are needed to protect against latency while also serving to protect against a DoS attack.

The distributed switching architecture in the Verizon data centers isolates customer data, with each customer VRF extended through the switched architecture. Redundant switching infrastructure prevents a single point of failure from disrupting service. Verizon uses extended features of Cisco Nexus 1000V switches to extend QoS features inside the virtual distributed switch environment to ensure signaling and media are given the correct priority from end to end.

At the compute layer within the servers that run the VMs, CPU cores are dedicated to specific customers for the separation of applications and data. Multiple servers are supported by different processors to enable failover.

At the application layer, the virtual Linux environment has been hardened. Linux by design is not subject to virus attacks. All unnecessary services and ports have been disabled. The OS is not accessible to the customer. The applications are only accessible through the management applications portal. Additionally, the entire application environment is monitored and logged.

Physical security for the UCCaaS environment at Tier 1 Verizon data centers includes multiple layers of physical isolation requiring a combination of biometric scans, an ID card, and ticket/notification to enable access and work on data center infrastructure. All servers and

network components are protected by a two form factor access method, to restrict and actively control access to components. Additionally, the data centers do not have direct Internet access, only dedicated interconnects to the individual customers. Cisco provides management via secure dedicated connections into Verizon data centers, terminating in the Cisco Remote Operations Services Center. This provides isolation of the UCCaaS Core and protects customers by isolating their network from the Internet.

The UCCaaS architecture, utilizing a multi-customer computing infrastructure and defense-in-depth security, has been shown to deliver better than 99.999% uptime, fault tolerant reliability, and a service provisioning methodology that features scalability for even the largest enterprises.

UCCaaS Business Benefits

For the enterprise user, solutions such as UCCaaS provide an array of measurable benefits that impact individual productivity and the organization's bottom line. These include:

- Improved time-to-value through rapid deployment since UCCaaS is ready for adoption immediately, enabling collaboration in real-time with a broad set of individuals across multiple geographies. UCCaaS can save time over do-it-yourself PBX deployments. The service is customizable for employees and does not require a large capital investment, making it an excellent low-risk alternative to rolling out new technology solutions. Easy integration of existing services reduces the complexity and timeframe required for deploying a hybrid model.
- Extensibility. UCCaaS integrates into Enterprise software fabric – ERP, CRM and custom applications. It integrates with and delivers desktop and immersive video and is able to grow to meet your organization's changing needs.
- Better cost control through the reduction of capital outlays for communications solutions. With UCCaaS, companies can move to a predictable expenditure that can be scaled up or down based on business cycles. As a service instead of a product, UCCaaS protects companies from technology obsolescence and allows IT to focus their resources on more strategic projects.
- Exceptionally high reliability for more predictable business operations, based on carrier-class availability, management, monitoring, and multi-layered security.

Conclusion

Service providers offering services via the private, hosted and managed network cloud are incorporating stringent security, availability, and reliability features developed over decades in the most sophisticated enterprise environments and Tier 1 data centers. Computing architectures utilizing virtualization and based on multi-customer instead of multi-tenant infrastructure provide software and information isolation for each enterprise deployment. The defense-in-depth security strategy protects bare metal and virtualized assets, embedding security throughout all layers of the network to maintain the confidentiality, integrity, and availability of data, applications, endpoints, and the network itself.

UCCaaS is a carrier-class offering that provides these features to enterprises through numerous individual technologies, platforms and devices delivered through Private IP network connectivity. Beyond providing an array of CapEx and OpEx benefits, it is easily and flexibly deployed and swiftly brings demonstrable benefits from the use of unified communications and collaboration services by fixed and mobile assets in today's enterprises.

For More Information

Verizon UCCaaS Fact Sheet
http://www.verizonbusiness.com/resources/factsheet/fs_unified-communications-and-collaboration-services_en_xg.pdf

Verizon Private IP Service
http://www22.verizon.com/wholesale/solutions/solution/private+ip.html

Cisco Unified Communications Manager Security Guide
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/8_5_1/secugd/sec-851-cm.html

Cisco Unified Communications System Solution Reference Network Design
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8x.html

For more information, please contact your account representative or visit
verizonbusiness.com/products/communication

About Verizon Business
Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world's most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today's extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world's largest businesses and governments—including 96 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at www.verizonbusiness.com.

verizonbusiness.com