White Paper

The Emerging Role of a CDN in Facilitating Secure Cloud Deployments

Sponsored by: Fastly

Robert Ayoub
August 2017

IDC OPINION

The ongoing adoption of cloud services and the desire for anytime, anywhere connectivity will require further evolution in how security services are delivered. Continued growth in application-layer attacks, fraud exposure, and nefarious actors targeting end users is making security a key consideration when moving to the cloud. In particular, there is an even more pressing need to block threats where attackers meet users at the edge of the network.

Content delivery networks (CDNs) have been early proponents of pushing IT-related services closer to the end user. Acting as a reverse proxy, a CDN is designed to speed up web and application delivery for a better user experience. CDNs can also provide core security services to protect traffic running across their networks. These services typically include distributed denial of service protection (DDoS), web application firewall (WAF), bot protection, and Transport Layer Security (TLS) encryption. Because CDNs facilitate scalable infrastructure and natural proximity to users at the network edge, they can be an appealing option for offloading critical security functions.

As enterprises of all sizes move to the cloud, IDC recommends that they consider the security implications of adopting these architectures and determine whether additional security controls are required. By placing edge compute power closer to end users, a CDN can effectively act as a network-level and application-level enforcement point. This can complement existing cloud-oriented architectures and even accelerate an enterprise's transition to the cloud.

IN THIS WHITE PAPER

This white paper looks at how the use of a CDN can complement cloud deployment models. We explore how a CDN works in conjunction with a public cloud, a private cloud, and a hybrid cloud while highlighting key security considerations of each model. In light of these considerations, we detail the potential advantages of leveraging a CDN to deliver a low-latency, scalable managed approach to security policies. Finally, the white paper touches on some key features to look for when considering a CDN for cloud security.

August 2017, IDC #US43005617

SITUATION OVERVIEW

Cloud deployments are becoming increasingly mainstream and mission critical. IDC predicts that by 2018, 60% of enterprise IT workloads will have moved off-premise and into a cloud architecture. IT spending is following suit. IDC estimates that by 2020, 67% of total enterprise IT infrastructure and software spending will be designated for cloud offerings.

As production workloads move to cloud architectures, security remains a top concern for most enterprises. In a 2016 IDC survey of over 11,000 respondents, 53% of respondents indicated that security was an inhibitor for moving to the public cloud. Cloud-based applications need security controls that span the breadth of traditional network security to web-oriented application security. However, decisions regarding where to deploy security controls and who should manage them require considerable analysis.

A CDN can help with some of the previously discussed challenges by providing a network-level and application-level enforcement and compute point to enhance different kinds of cloud architectures. Three distinct cloud architectural models that can benefit from the use of a CDN are on-premise private cloud, public cloud, and hybrid cloud. The sections that follow explore the three cloud deployment options in more detail.

On-Premise Private Cloud

In the on-premise private cloud usage model, the enterprise essentially rebuilds its on-premise datacenter in a dedicated, private cloud environment. While cloud services may be in use for auxiliary IT services, the main business typically expands by scaling physical infrastructure or virtual machines. A number of things could prevent these organizations from moving their entire business systems to the public cloud, including deeply ingrained operational business practices, risk intolerance, or historical inertia.

From a security point of view, these organizations need to switch from securing physical on-premise assets to virtualized assets at the private cloud host. This can be done a number of different ways. Application-level security controls are typically coded in at the application server, middleware, or the application itself, using language features or security libraries. Network-level security controls are generally deployed as "software" versions of appliances such as network intrusion detection system (IDS), intrusion prevention system (IPS), firewalls, and load balancers (which terminate and accelerate TLS). Software-defined versions of these controls can take several forms, such as software appliances, virtual appliances, or containers.

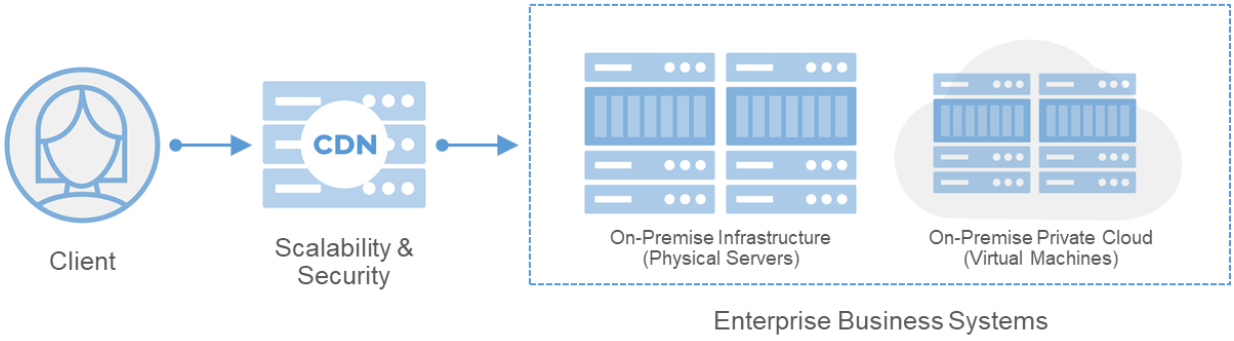
Compared with public cloud environments, the private cloud approach provides more control and elasticity over which security services are deployed. Enterprises can more rapidly scale software variations of these controls in a cloud environment. However, control typically comes at a financial and performance cost. All traffic needs to pass through a combination of security software appliances and workload tools, all of which may impact performance over a purpose-built hardware-oriented architecture.

A CDN can help address some of the previously mentioned challenges of a private cloud. Sitting between an enterprise's end users and business systems, a CDN acts as a reverse proxy to accelerate and secure all web and application-level traffic passing between both points. CDNs can offload expensive security processing, accelerate core content (including video and streaming), and even provide additional functionality such as load balancing (see Figure 1).

Here, the CDN essentially acts as a cloud enabler, allowing the enterprise to take advantage of the benefits of a public cloud deployment while addressing several key security concerns.

FIGURE 1

On-Premise Private Cloud



Source: Fastly, 2017

Public Cloud

In the public model, the enterprise makes a wholesale move to a public cloud architecture and migrates applications, data, and business systems to infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) providers. By essentially recreating an entire datacenter in a public cloud environment, an enterprise can leverage the services of public cloud providers at a lower price point.

From a security perspective, organizations take on different levels of responsibility depending on the service model being used. With an IaaS model, organizations assume data, application, and system management security risks, while the service provider assumes network, hardware, and physical security risks. When organizations move toward a PaaS or software-as-a-service (SaaS) model, service providers typically take on the additional security risks associated with owning more of the stack.

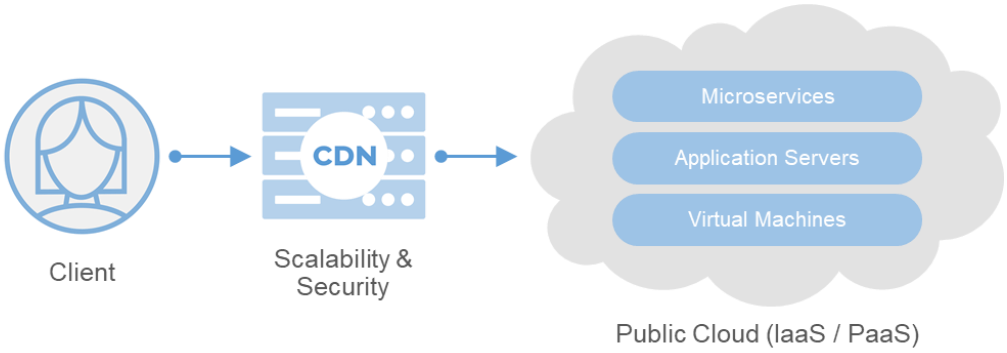
There are a number of potential concerns with this deployment model. Accessing public cloud services across the internet can introduce latency. Public cloud providers build out a small number of very large datacenters to scale their operations, which means that traffic has to travel long distance to access services. While dedicated leased lines or Layer 2/Layer 3 VPNs can help address these latency issues, both bring additional network complexity and operational costs. Another potential concern is the reduction in visibility and control across the IT stack. From a security perspective, this can be particularly challenging if the enterprise is working with multiple cloud vendors. The fact that not all cloud providers support the same security controls could potentially result in fragmented security policies and operational complexity.

A CDN can offer an additional layer of security to enhance the public cloud model. Enterprises can scale their business systems and applications using public IaaS/PaaS functionality to complement their public cloud architecture. The CDN can then be used to centralize and enforce consistent security policies across disparate microservices and applications running on various cloud-instantiated operating systems. For example, a CDN can enforce a specific version of TLS and cipher suite, irrespective of differences in downstream web servers, application servers, or TLS libraries. A CDN can also enforce a baseline set of application-level rules that protect against code injection, malicious web requests, or brute-force log-in attempts, irrespective of this support (which may be fragmented) in the applications themselves (see Figure 2).

A CDN can also reduce the amount of customization involved in switching cloud providers. Using a CDN for security helps an enterprise more easily migrate or move to a different public cloud provider while maintaining its existing security configurations.

FIGURE 2

Public Cloud



Source: Fastly, 2017

Hybrid Cloud

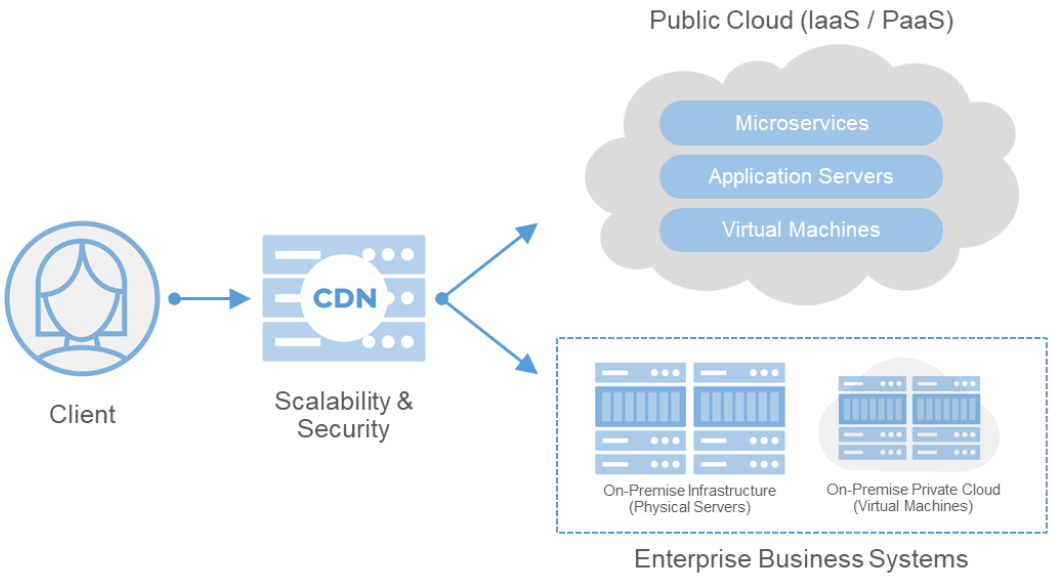
Moving to the cloud is often an iterative process. Many enterprises start by moving test and development assets, saving mission-critical assets for later phases of the migration. A hybrid approach typically involves a combination of some on-premise infrastructure, some private cloud deployments, and some public deployments via an IaaS or PaaS provider.

Often in a hybrid scenario, an enterprise keeps some application security controls in place while outsourcing network security to the cloud. This leads to a less cohesive security posture while also failing to take advantage of the full cost savings and scalability of the public cloud.

For organizations moving through or looking to maintain a hybrid cloud model, CDNs can play an important role in ensuring common security controls across on-premise deployments and public or private cloud instances (see Figure 3).

FIGURE 3

Hybrid Cloud



Source: Fastly, 2017

FUTURE OUTLOOK

Extending Security to the Edge

CDNs are well positioned to help enterprises securely migrate to the cloud. When CDNs are located closer to end users, they can both deliver and secure web and application content. Most CDNs offer a broad range of security solutions, including authentication, data integrity protection, bot mitigation, application firewalling, rate limiting, availability threat protection (anti-DDoS), and network security. With high-bandwidth, globally distributed networks, CDNs also have the performance and availability needed to handle volumetric DDoS attacks. This is especially critical in light of the growing size and frequency of these attacks.

IDC notes that a more advanced CDN can deliver even greater functionality by moving additional logic to the edge. From a security perspective, this means having near-real-time visibility into the latest threats and vulnerabilities through real-time streaming of logs and metrics to multiple logging and analytics platforms. In turn, such visibility means being able to react to those threats and vulnerabilities by quickly adjusting DDoS, WAF, and bot protection rules or creating new rules as needed. This also means having the ability to roll out (or roll back) security policies globally in milliseconds for rapid edge enforcement – and doing all this without negatively impacting web or application performance. A CDN that can offer these capabilities effectively complements the core cloud by extending security policies out to the edge.

IDC recommends that organizations choosing a CDN for cloud security ask the following questions to determine whether a CDN has true edge cloud capabilities:

- **Real-time insights.** How quickly can the CDN provide insights into the latest security events and notifications? Some CDNs provide these insights from the network edge in milliseconds; others can take seconds, minutes, or even hours.

  Real-time insights apply to both security incidents and the impact of rule changes. If an organization makes a change to its WAF or DDoS rules, how quickly can it see the impact of this rule change? How quickly can the organization roll back a change if needed?
- **Control.** Does the CDN give an organization the option to make its own configuration changes to security policies? Can the security team push out new WAF rules, update ACLs, or alter DDoS rules instantly based on active attacks? Most CDNs require a professional services engagement to alter security rules with no ability for customers to make these changes themselves.

  A more advanced CDN can also enhance control by pushing application logic to the edge. For example, users can be authenticated at the edge of the network, eliminating any latency associated with having to send this traffic back to the point of origin.
- **A fully integrated platform.** Does the CDN offer all security capabilities on one compliant (PCI-certified) high-performance platform? Can the CDN protect from DDoS attacks on the same platform used to accelerate web and application delivery? Having these capabilities on separate platforms impacts performance because a separate DDoS platform will not perform as well as a core delivery platform. It also introduces complexity associated with coding to two different APIs and having different functionality across platforms.

CHALLENGES/OPPORTUNITIES

Securing cloud workloads can introduce unique concerns and challenges. Some are operational challenges around monitoring workloads across cloud assets. These challenges typically result from having assets dispersed across a hybrid architecture or multiple public cloud providers. For private cloud deployments, challenges can occur around provisioning the appropriate security controls with each new workload in the cloud. These controls, of course, also need to move dynamically with workloads. Risk management can also be challenging because it can be difficult to assess the overall security status of cloud infrastructure. This in turn can make it difficult to document regulatory compliance.

Regulatory compliance in the cloud can be a particularly thorny issue for organizations. Besides having to navigate specific regulations that may or may not be cloud friendly, end users themselves have serious reservations about meeting regulatory compliance in the cloud. In the 2016 survey mentioned previously, over 25% of cloud users reported that regulatory compliance was a significant inhibitor to moving to the public cloud.

CONCLUSION

As enterprises continue to embrace the cloud, they cannot lose sight of the need to secure their applications and network. With a growing number of today's attacks taking place at the network edge, there is also a need to think about how to enforce security policies at the edge, without negatively impacting performance. IDC believes that enterprises should consider augmenting cloud security using a CDN that can function as an edge cloud, providing visibility and control of traffic without sacrificing performance. This will allow organizations to enforce security policies and controls in real time from the edge, ensuring a more dynamic response to today's rapidly emerging threats.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2017 IDC. Reproduction without written permission is completely forbidden.