Issue 1

On Demand Diversified External DNS is Here.

"With a few clicks of a mouse from a single pane of glass, TCPWave gives you the power to provision and manage any number of virtual DNS servers, on demand, on any or all major clouds, to absorb a large-scale DDoS attack"

Mitigate a DDoS Attack

Enterprises face a new challenge with greater DDoS attacks that can take down the largest organizations, and even the largest carrier ISP service providers, thus effecting thousands of customers at once. Anytime a solution is found to resolve a DDos attack, the assaulters will create a new and larger intrusion. The only true way to mitigate all DDos attacks is to acquire the DNS horse power to absorb the attack.

When it comes to external DNS, customers have two choices. A) They can host their own; which may save money but increases OpEx, expensive idle servers and has the risk of limited access that can be easily be targeted by hackers. Or, B) They can outsource to an external DNS provider which could have a higher cost, but offers more security with a much higher availability.

Cloud Diversification using TCPWave DDI

However, there's a new problem with the second option. What if an attack on a customer is so large, it takes down the customer and the carrier hosting that customer, hence the attack effects all the other customers? Well that is exactly what happened in October 2016. An attack on one

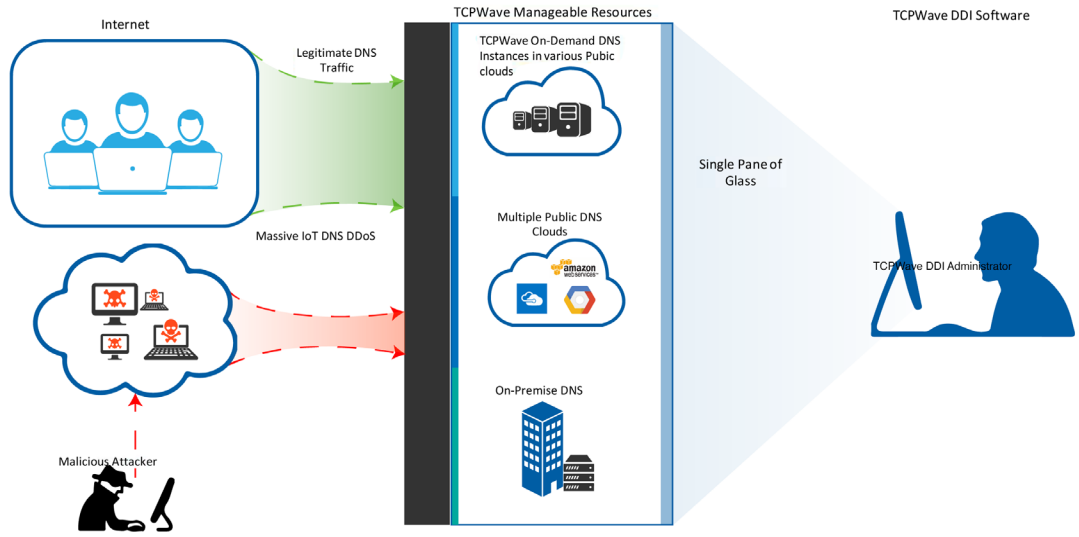
customer took down several others that were simply using the same external DNS carrier. A whole new risk the industry was not prepared for. Now customers are faced with a new challenge of diversifying their external DNS over several diverse external DNS providers and cloud options. That option may solve the problem; however, it becomes the difficult challenge of managing several networks as one.

TCPWave is the first DDI company that built a product for exactly that. They leverage a unique solution which combines cloud automation and REST API to protect their clients' digital resources from the largest DDoS attacks. Now customers can easily diversify their external DNS and instantaneously add redundancy, with a click of the mouse. TCPWave can nullify the effects of a DDoS attack by dynamically spooling up multiple virtual DNS servers, as needed, over any or all major public and private clouds as well as their private networks, from one single pane of glass. with diversification, automation, redundancy, and the ability to spawn multiple DNS instances on demand, the customer can absorb any DDoS attack, no matter how large it is.

Extending DNS to multiple public and private clouds for diversity and resiliency is too challenging to manage for most enterprise organizations. The resources needed to manage and mesh independent cloud providers is cumbersome, expensive, and risky if done incorrectly. That's why many rely on a large independent external DNS provider to advertise their DNS. Today's larger DDoS attacks make that single source solution risky as well.

TCPWave offers a unique solution to this problem. They allow their clients to build, manage, and instantaneously grow their external DNS network from one dash board; that leverages their REST API to manage most major cloud providers. The same dashboard manages the customer's private cloud DNS and internal DNS as well; automatically and securely keeping everything in sync. The result is one, easy to manage, secure diverse dynamic network spread out over several unique public and private cloud providers.

FIGURE 1 On Demand Diversified External DNS



Source: TCPwave

External DNS Options

Manage External DNS internally

This may protect your company from attacks targeted at other companies however it poses the following:

- Requires additional unnecessary DNS hardware increasing CapEx.
- Severely limits the points of presence of DNS into the Internet.
- Dedicated DNS resources for monitoring DNS performance

Contract with an external provider

This will resolve the issues of managing DNS internally but will open your company to other issues. If an attack on any of the companies managed by the external provider is successful, then your company's DNS performance is compromised as well.

Contract with multiple external DNS providers (DNS Diversification)

This will allow companies to withstand and mitigate the largest DNS attacks and is the new recommended standard for external DNS. However, DNS diversity creates the following Issues:

- Use a different management GUI for each DNS provider.
- No verification that the data typed in each GUI is in sync.
- No central view of DNS configuration across DNS providers.
- No central External DNS performance monitoring.

TCPWave DDI for External DNS

This solution resolves all of the above issues by managing external DNS from a single pane of glass by your company's DNS/Cloud administrator. Below are the benefits of the TCPWave IPAM

- Single GUI to manage all external and internal DNS.
- Updates all external DNS providers in parallel.
- Increased security of input data from a single GUI.
- Preconfigured REST interface out of the box communicates to all popular cloud providers such as AWS, DYN, Google, Azure, Verisign etc.
- One tool to manage external and internal DNS as well as DHCP and IP Management.
- Capacity planning metrics in a central spot for distributed cloud DNS infrastructure.
- Scalability on demand to auto provision additional DNS cloud instances to absorb a DDOS attack.
- Integration of fault management metrics from multiple cloud providers to the enterprise's command center.
- Reinforced data integrity checks to ensure that the data served across multiple cloud providers is in sync.
- Eliminates the necessity to add user accounts in each cloud provider for performing DNS administration.
- Provides audit reports for each DNS change in any cloud provider.

Source: TCPWave

Research From Gartner:

If External DNS Fails, So Does Your Digital Business

Without properly functioning external DNS, Internet-based resources may "disappear" without warning. For enterprises with Web and cloud-based applications and content, external DNS solutions offer reliability, performance and traffic management beyond that of traditional opensource-based solutions.

Foundational Document

This research is reviewed periodically for accuracy. Last reviewed on 15 September 2016.

Key Findings

- DNS is mission-critical to all organizations that connect to the Internet. DNS failure or poor performance leads to applications, data and content becoming unavailable, causing user frustration, lost sales and business reputation damage.
- The increased trend toward dynamic, fragmented and distributed cloud-based applications complicates the task of maintaining visibility and availability of key resources, or — in cases where multiple endpoints may be suitable — routing to the "best resources" based on constantly changing attributes.
- An externally sourced, managed and focused DNS as a service (DNSaaS) solution can be cost-effective, and offer greater resilience, reliability and performance, while evolving to keep pace with the needs of cloud and digital business applications.

Recommendations

- Don't assume that internal and external DNS should be treated or supported the same.
- Take an inventory of existing DNS practices, noting the cost to support, feature set provided and ability to evolve in support of increasingly distributed and Internet/cloud-based solutions.
- Perform a risk analysis of the criticality of external DNS in support of both customer-facing content and distributed applications.
- Don't assume your current DNS solution is optimized for reliability or cost. Perform a feasibility study of DNSaaS options and the business benefits of the greater reliability, markedly improved performance and dynamic traffic management (and associated routing decisions) that such solutions provide.
- Conduct a head-to-head analysis of existing, on-premises and cloud-based DNS solutions.

Analysis

What DNS Is

The Domain Name System, or DNS, maps the names commonly used by users and applications to the numeric Internet Protocol (IP) address that the Internet and associated networking systems use. The technology and concept itself are decades-old, and are often implemented using open-source technology such as BIND. Enterprises often implement their own authoritative DNS servers and manage the mapping of their names to resources. It is important to distinguish internal from external DNS services. DNS services are often described as being "internal" to the enterprise — that is, enterprise-facing, or "external," or public-facing (see Note 1). This research will focus on the external service offerings, although several leading vendors in each category are moving to support both.

The visibility and apparent availability to the public of enterprise content and applications rest completely on DNS services functioning properly.

DNS Threats and Opportunities

At the highest level, DNS can be looked at in terms of business threats and opportunities. The threats come from the risk of Internet and cloud-based applications and resources being rendered "invisible" or nonexistent, by the failure of the name service that identifies them. Invisible websites (or simply slow ones), malfunctioning e-commerce applications, and faulty distributed applications can be directly tied to lost revenue, competitive disadvantage and business reputation damage. From a security stance, Managed DNS can offer the scale and technology to mitigate distributed denial of service (DDoS) attacks

against the DNS infrastructure, as well as outright hijacking of the DNS servers themselves. The opportunities come from the ability to improve resilience and performance of access to those DNS-named resources, and improved business value of applications and content by directing users to the optimal resources, based on attributes such as global load balancing, application availability, application performance, user location, time of day, etc.

At a simple operational level, the cost of managed DNS should be compared against the cost of enterprises managing DNS themselves, including the cost of people, platforms and technologies, such as DNS servers in multiple geographic locations. As we will outline in this research, however, it would be difficult, if not impossible, for those enterprises using open-source DNS technology, as is often the case, to keep up with the evolution and advancements in DNS-related services offered by managed providers (see Note 2).

Why DNS Matters

Why It's Important

Failed or poorly performing DNS can cause applications, data and content to disappear and become "not available" to the end user. In the event of a DNS failure, an application or resource is still accessible if the user or application knows the exact IP address of the resource he or she wishes to access, but the practical effect is that host name resolution failure equates to an effective lack of availability.

What's at Stake? What Are the Downsides?

Complete Failure — Externally-Facing Resources Disappear

In the event of a complete failure, external resources disappear to those users initiating a request for them. A message such as "This Web page is not available" or "Error resolving name" leaves users wondering if they mistyped the address, or whether the site is down or perhaps has even been taken out of service. For all intents and purposes, the resource is gone:

- **Website content or resources are not visible** — 404 or "fail whale": This is not a DNS response, but a byproduct of poor management and, in fact, an HTTP response; in this case, the site itself may respond, but links or content on the page cannot be resolved, triggering a "404" or fail whale response. While the user isn't left wondering about the business viability or existence of the site, the content is unavailable.

- **Applications written to names, including those using multiple sources of data fail:** Rather than Web page users receiving a 404 message about a broken link, they find that their application fails. Given the increasingly distributed and modular approach to application development, the opportunities for a DNS failure to render applications out-of-service are increasing.

- **IOT "breaks"** — the Internet of Things (IoT): Things make DNS requests just as users and applications do. A failure of DNS will render a sensor or module (or thing) unable to communicate upstream with the systems collecting data or triggering action. Given the explosive growth in the number and reliance on such things, DNS failure is an increasingly undesirable outcome.

Poor Performance

More common than complete failures, poorly performing DNS systems will increase latency between sources and sinks of resources, with users unsure of where the delay is being inserted, but frustrated overall. Performance may be slowed by an inability to mitigate DNS-based DDoS attacks, or simply by an insufficient number or geographic dispersion of DNS servers. In the case of distributed applications calling on any number of external resources, delays are accretive — that is, they stack up:

- Pages found slowly, or time out — Users experience a delay, or even a timeout, when making a request. In such cases, it is common for users to simply give up and go to an alternative site, where possible.

- Content on pages paints slowly, or doesn't appear — While the requested resource may initially appear, the content on the page is delayed long enough for the user to become frustrated and abandon the request. Users routinely abandon pages and shopping carts.

In both of these cases, user frustration will lead to brand damage, loss of purchase conversions, reduced revenue and users switching to a competitor.

Should You Do External DNS Yourself?

DNS that is responsible for outward-from-the-enterprise service (e.g., to customers, partners and the public) is normally provisioned through two to four or more servers running an implementation of BIND or some other open-source-based software. While this has functioned well enough for the past few decades, the growing importance of Internet and cloud-based content and the increase in name-using distributed applications is placing greater degrees of criticality on the performance and reliability of the DNS service. Given the relatively low cost, increased performance and reliability, and rich value-added feature set of externally provided services, we expect DNSaaS to increase in deployments and importance. The point here is not so much why enterprises shouldn't do it themselves, but, given the alternative, why would they, unless their specific configuration made an external solution cost prohibitive? Below, we highlight seven key advantages of sourcing DNS externally from a managed DNS provider.

Reasons to Source Externally

- **Reliability/resiliency** — design of platform and features: The first and foremost reason to source DNS externally with a managed service provider is to ensure the reliability and resiliency of the system — in other words, the likelihood of DNS "staying up." Without resilience and availability, all other features and capabilities are moot points. Users should look for a provider that offers an Anycast network, geographically distributed points of presence or pops, and the use of multiple carriers to avoid failure based on network outages. Other services beyond the scope of strictly managing DNS per specification are capabilities such as load balancing and advanced failover, which provide an added layer of resilience to application delivery.

- **Scale and scope/breadth of platform** — number of POPs; it's a numbers game, and tough(er) to overload: This ties into the reliability, resilience and availability we just discussed. Rather than two or a small handful of servers, providers can offer dozens or more servers spread across geographies utilizing many different carrier connections. This scale and scope, or breadth of platform, underlies the fact that resilience is a numbers game. The more distributed and redundant the network of pops, and the greater the size of the pipes between them, the greater the bandwidth to absorb disturbed DDoS attacks against DNS servers and the greater the capability to survive regional disasters.

- **Performance:** After availability, the next most important benefit of using a managed DNS service can be the improvement in performance both in terms of the DNS system itself and the observed performance of the website and/or applications by the end user. The performance of the servers themselves, which may be based on proprietary extensions, open-source technology or a complete proprietary stack, is one obvious performance attribute of all good DNSaaS implementations. Layering on top of a distributed high-bandwidth network with multiple points of presence places DNS resolution closer to users wherever they may be in the world. Above the DNS layer, services such as load balancing and geodirection further improve the performance as experienced by the end user. Shaving latency off of DNS queries can become even more pronounced in cases of content and applications that will call upon multiple destinations.

- **Expertise, technical depth and constant evolution:** DNS network design and architectures can be extremely complex to get right. Much like any "as a service" offering, one advantage of DNSaaS over internally designed and hosted open-source solutions is leveraging the expertise, technical understanding and constant attention to the latest features and threats that a specialist brings. While basic, RFC-compliant DNS functioning may not change that frequently, higher-layer functionality, particularly in the areas of telemetry-driven routing and security responses to attacks such as DNS-based DDoS attacks and hijacking, will continue to evolve rapidly.

- **Responsiveness/continuous management:** Continuing the theme of leveraging external expertise, having DNS-expert system engineers on duty and available to both predict and react to failures and attacks can be advantageous. In essence, this takes DNS from being a task and/or risk and places the risk and response on the shoulders of external experts.

- **Advanced features:** These are service capabilities not part of core DNS, but integrated with it in advanced solutions. While some of these have become common (such as failover and load balancing), others (such as routing based on rules, telemetry, filters, and even API calls) extend the usefulness and business benefits of a managed DNS platform. The vision here includes using the traffic awareness, system and application state, and rules to provide automation extending to other platforms, including cloud. (For a representative list of DNSaaS vendors, see Note 3.)

The Contrarian View

It is important to note that some organizations may have very specific and valid reasons for keeping control of DNS in-house, such as mandates for isolation, security, flexibility or control (for example, running redundant hidden master DNS name servers inside the firewall) that cannot accommodate giving such a function to an outside, cloud-based provider. Enterprises may be using an internal DNS solution that includes other DDI services, such as DHCP and IP address management that provide adequate external security. Also, some organizations simply may not want to pay the monthly fee for something they believe they can adequately support with their own staff. We do expect to see a blending of some of the more sophisticated solutions, both internal solutions extending externally and external providers that offer internal, on-premises solutions. There may also be configurations with frequent changes on such a massive scale that a "pay-per-change" model isn't as attractive.

Recommendations

- Don't assume that internal and external DNS should be treated or supported the same.
- Take an inventory of existing DNS practices, noting both cost to support and ability to evolve in support of increasingly distributed and Internet/cloud-based solutions.
- Perform a risk analysis of the criticality of DNS in support of both customer-facing content and distributed applications.
- Perform a feasibility study of external options and the business benefits that leading DNS solutions with greater reliability, markedly improved performance, and dynamic traffic management (and associated routing decisions) can provide.
- Conduct a head-to-head analysis of both on-premises and cloud-based DNS solutions.

Note 1. Internal Versus External DNS

Internal DNS solutions are increasingly described as DDI solutions, referring to a combination of DNS DHCP and IP address management. The DDI market is composed of solutions that provide and/or manage internal DNS and DHCP services, along with IP address management. DDI helps improve the availability of critical IT infrastructure, while reducing operational expenditures.

The external DNS market consists of Internet service providers (ISPs), Web hosting providers and, for the topic of this research, managed DNS service vendors (such as Dyn, Neustar, NSONE and Verisign) that provide cloud-based primary and/or secondary authoritative DNS servers with degrees of reliability, security and additional features. Although many DNS servers can be used for internal or external DNS, the administrative and operational requirements for internal and external DNS are quite different.

Note 2. Threats and Opportunities Associated With External DNS Management

Threats:

- Lack of resilience — 404 (fail whale)
- Poor performance — simple slow response
- Poor performance — routing to a suboptimal resource
- Poor load balancing
- Inefficient asset allocation
- Low website sales conversion rates
- Lost sales
- Damaged business reputation
- Increased security exposure

Opportunities:

- Risk mitigation — avoidance of DNS failure, poor performance or security events
- Improved user experience for Web-based content
- Improved performance for distributed applications
- Improved visibility into DNS usage and traffic patterns
- Increased revenue through commerce site conversions
- Dynamic routing solutions and new business opportunities based on telemetry and traffic management
- Improved security stance
- Ease of use/improved manageability compared to legacy zone file management

Note 3. DNSaaS — Representative Vendors

- Akamai
- Amazon (Route 53)
- Dyn
- Neustar (UltraDNS)
- NSONE
- Verisign

Source: Gartner Research Note G00276917, Bob Gill, Foundational Refreshed: 15 September 2016 Published: 25 August 2015

TCPWave Solution: Advanced Cloud Integration + Robust REST Framework

Extending DNS to public cloud increases reliability and performance. TCPWave takes this one step further to include multiple clouds with its unique cloud and REST API technology. TCPWave also provides the ability to launch and destroy any number of DNS instances in any cloud. Thus, organizations can truly diversify their cloud options thereby enabling absorption of DNS DDoS attack of any scale.

TCPWave provides a single pane of glass through which IT admins can manage DNS zone data across various public clouds and always keep them in sync with on premise DNS instances. TCPWave DDI comes with inbuilt cloud hooks which can be used to extend the infrastructure operations into the cloud.

TCPWave provides prebuilt DNS cloud images for various clouds like Amazon Web Services, Microsoft Azure, Google Cloud etc. These images can be launched on demand from the TCPWave DDI interface whenever required. Thus, it becomes easy to scale up or scale down the DNS instances in the cloud in accordance with the DNS query traffic. This kind of instantaneous spinning up DNS instances as needed across multiple clouds helps absorb even massive IoT based DDoS attacks.

Conclusion

With TCPWave DDI, customers can perform the following tasks with few simple mouse clicks from a single interface:

- Create DNS zones in any public cloud.
- Keep the DNS zones in sync, no matter where they are hosted.
- Launch or destroy DNS instances on any cloud based on the DNS queries volume.

Although the TCPWave technology is relatively new to the cloud market, it provides features that are more suited for the DevOps, Nextgen Cloud, SMB and IoT deployments as well as large enterprise deployments. Customers now have the power to defend against any kind of DNS based DDoS attacks using TCPWave DDI. Enterprises interested in increasing their internal and external DNS resiliency should consider TCPWave as a strong positive.

BENEFITS OF TCPWave

Eliminate Downtime and Business Risk – With TCPWave's On-Demand DNS instances on various clouds, and with automation that reduces mistakes

Absorb Massive DDoS Attacks – With on-demand diversified and redundant zone data on several public clouds, possible with TCPWave single pane of glass

Reduce Costs – By allowing their customers to right size their DNS networks, and by reducing the time, human error, and costs normally associated with managing large diverse network.

As an innovator in cloud related services, TCPWave provides state of the art public and private cloud visibility and operations for DNS, DHCP and IP address(DDI) management, apart from traditional on premise DDI services. The company's advanced REST API end points for managing its break through services like Dual DNS, IPv4, IPv6, public clouds extensions etc. are revolutionizing the way enterprises are automating forward into the future of public clouds. To learn how TCPWave and its team of cloud experts are helping enterprises in their cloud endeavors, for further information visit www.tcpwave.com