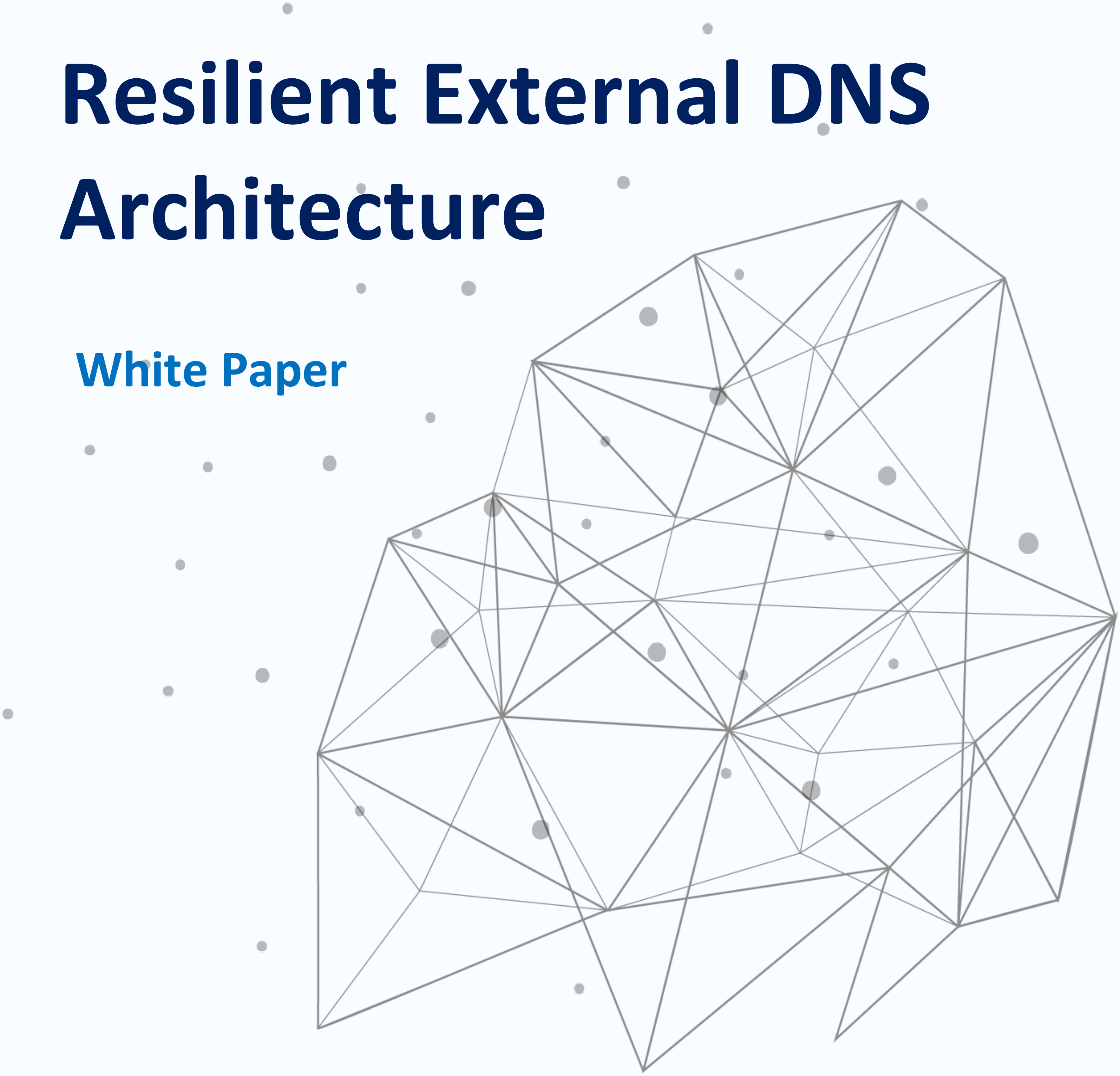
# Resilient External DNS Architecture

## White Paper

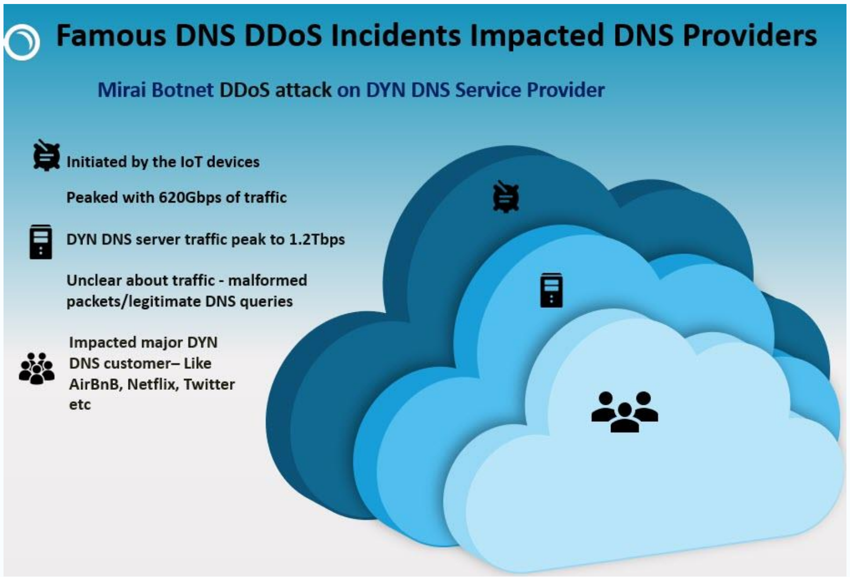


# 1 INTRODUCTION

In the systems and networking environment, the growth and stability of an organization mainly depend on factors such as network infrastructure, system, data security, product scalability, and reliability. Regardless of the size of the business, to effectively manage the increasingly complex environments these factors are important but often ignored leading to compromised infrastructure. While free or open source solutions can provide minimal services to run the business, they can be maintenance exhaustive and lack the robustness to be considered "Enterprise Grade" in today's modern network technology. Therefore, businesses are seeking automated environments and are ready for customized solutions to adapt to the expected level of automated solutions.

## 1.1 Problem Statement: External DNS

Enterprise deploys a multi-tier security solution to mitigate every possible cybersecurity risk for all the public-facing applications hosted in data centres and cloud. To achieve 100% uptime, the enterprise also needs to focus on possible DNS DDoS outages which can lead to a complete outage of the public infrastructure across the globe. Many a times enterprise opt for cloud centric DNS solution provider for the public facing DNS records. Let us look at some of the prominent outages in recent years.



Famous DNS DDoS Incidents Impacted DNS Providers

Mirai Botnet DDoS attack on DYN DNS Service Provider

Initiated by the IoT devices

Peaked with 620Gbps of traffic

DYN DNS server traffic peak to 1.2Tbps

Unclear about traffic - malformed packets/legitimate DNS queries

Impacted major DYN DNS customer– Like AirBnB, Netflix, Twitter etc

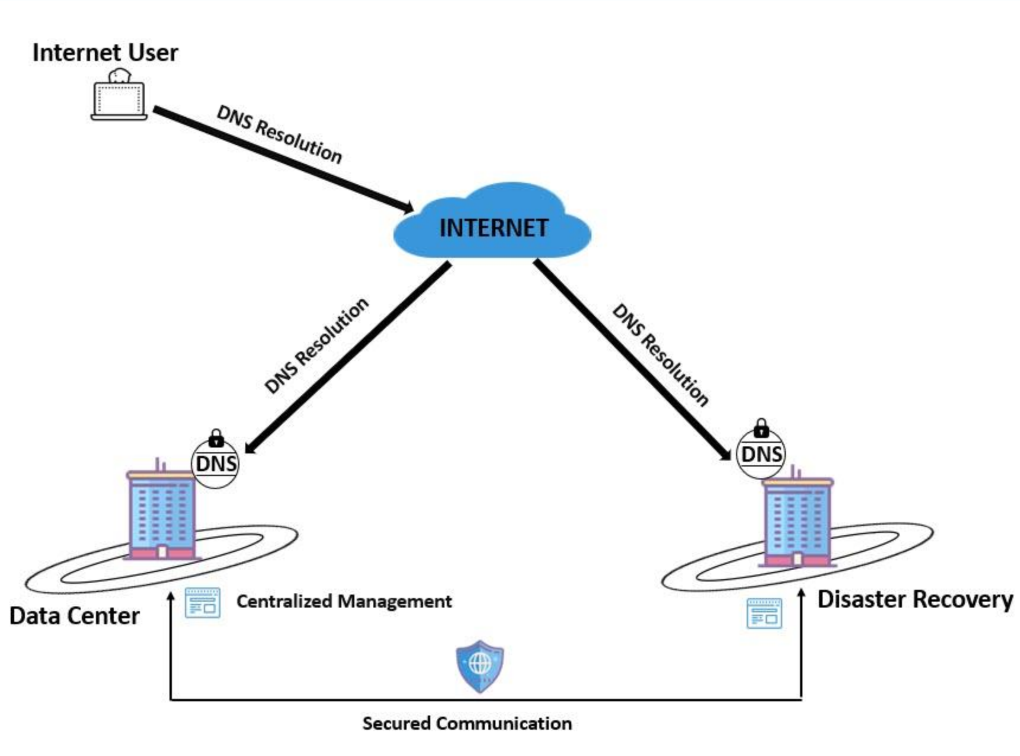
### Cloud Provider Outage Incidents

- Cloud DNS provider said its morning outage affecting numerous websites was due to an IP outage by the internet service provider – **August 2020**
- A configuration error in the backbone network caused an outage for Internet properties and DNS service providers that lasted 27 minutes. – **July 2020**
- For about 30 minutes, visitors to Cloud DNS provider sites received 502 errors caused by a massive spike in CPU utilization on network – **July 2019**
- Dotcom-Monitor tracked a Cloud DNS outage today. Dotcom-Monitor clients that utilize DNS provider may have received error messages associated with the DNS outage lasting from 5-7 minutes starting at approximately – **August 2013**

# 2 Recommended Approach

## 2.1 Take Control: On-Premise DNS solution

Considering the current security solutions which are deployed on-premise, TCPWave recommends opting on-premise DNS solution for the complete control of the DNS infrastructure. With the current approach, Enterprises can have complete control of the DNS infrastructure and mitigate the possible risk of DNS outages. By having on-premise DNS, the enterprises have complete control of the zone configurations and service availability.



## Key Security Features

The following are the Key Security Features delivered as base solution:

### DNS Anycast

Anycast DNS is a traffic routing algorithm used for the speedy delivery of website content that advertises individual IP addresses on multiple nodes. User requests are directed to specific nodes based on routing decisions.

### DNSSEC viz

This tool displays the DNSSEC key validation from Root zone to the Authoritative zone in a visual and interactive graph and below the graph it will display validation in plain text format for easy read.

### DNS Response Rate Limiting

Response Rate Limiting (RRL), is an enhancement to the DNS protocol which serves as a mitigation tool for the problem of DNS amplification attacks. Recommended by ISC. By implementing rate limiting configurations, enterprise can mitigate the possible DNS DDoS attacks like – DNS amplification, reflection, nxdomain, flooding and cache poisoning attacks.

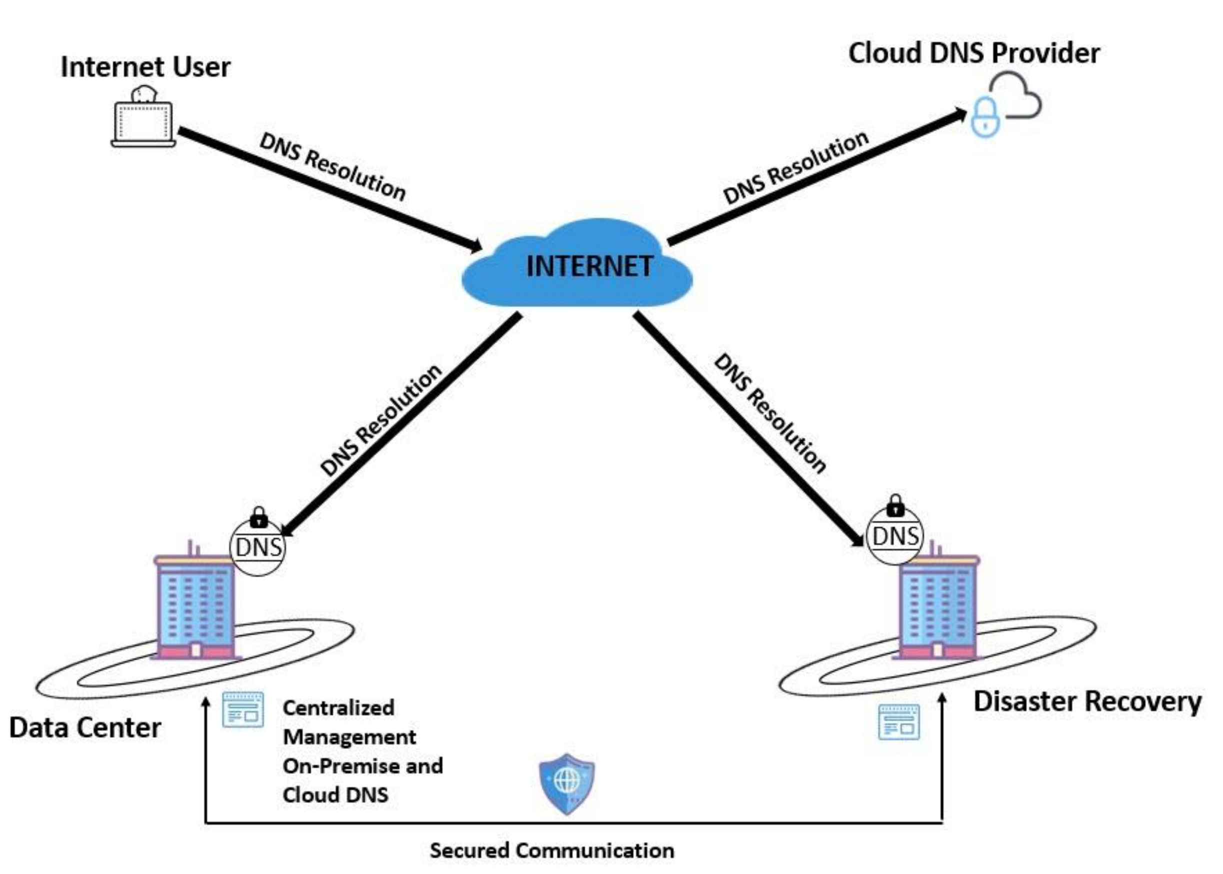
### DNS Tunnel Detection

The DNS Tunnel Detection logic is built into the TCPWave DNS appliance. DNS tunnels are used for malware infiltration and Data exfiltration.

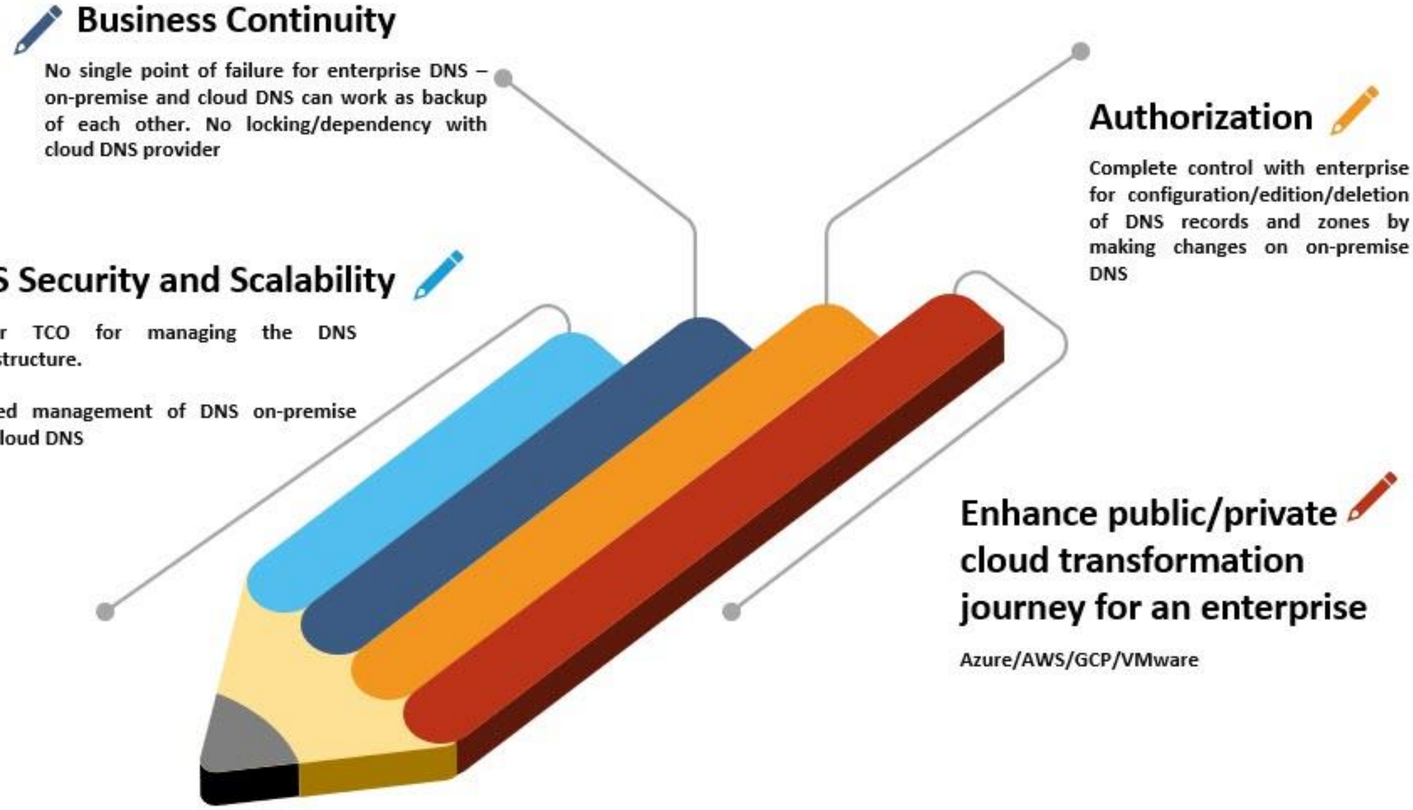
## 2.2 Best of Breed: Hybrid Approach in Future

In the later phase, if the Enterprise opts for cloud-based DNS solutions from cloud DNS solution providers, can fully integrate with cloud providers for centralized on-premise management. TCPWave provides a unique advantage of simplified management of the cloud and on-premise DNS solution.

By opting for the best of the breed, customers can keep control of the DNS zones/resource records by placing the DNS on-premise. The cloud DNS provider will continue to function as "secondary authoritative DNS".



# Key Advantages



### Business Continuity

No single point of failure for enterprise DNS – on-premise and cloud DNS can work as backup of each other. No locking/dependency with cloud DNS provider

### Authorization

Complete control with enterprise for configuration/edition/deletion of DNS records and zones by making changes on on-premise DNS

### DNS Security and Scalability

Lower TCO for managing the DNS infrastructure.

Unified management of DNS on-premise and cloud DNS

### Enhance public/private cloud transformation journey for an enterprise

Azure/AWS/GCP/VMware

# Conclusion

## TCPWave DNS Features

TCPWave was built with native cloud, automation, and virtual computing in scope. Most competing products have been designed and built before any of these robust technologies were born. Using agile engineering, REST as the core, and Java for the GUI, TCPWave is positioned to quickly adapt to today and tomorrow's rapidly advancing technology

### The Next Steps

When growing, upgrading, migrating, or evaluating the network components, TCPWave has the experience, and global reach, to help you efficiently deploy your network and the skills to help you smoothly install a global network, as well as the ability to leverage partnerships to reduce deployment costs. By opting TCPWave, you can make improvements in:

- Reliable uptime
- Integration to automated systems
- Ease of migration
- Redundancy and or fast recovery times
- Real-time Endpoint and topology visibility

### Want to connect

Contact the TCPWave Sales Team to discuss the customized deployment and migration strategies.