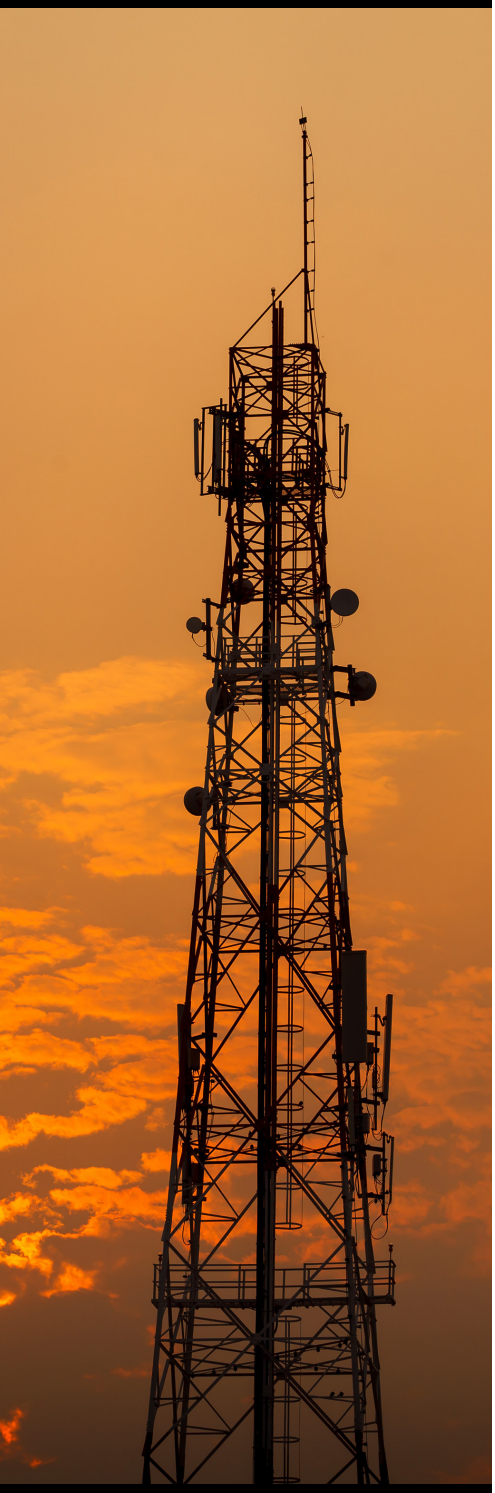
efficient iP™

White Paper



Telco/ISP: High Performance DNS Infrastructures In Three Case Studies

Three contexts, three ways of optimizing DNS infrastructure for greater security, performance, simplicity, and a drastic reduction in TCO.

efficient iP™

White Paper

Outline:

Case 1
Get rid of useless server farms

Case 2
Get rid of unsuitable intermediary security layers

Case 3
Decentralize DNS architecture

By 2022, global IP traffic will have multiplied elevenfold from 2012 figures, reaching an annual run rate of 4.8 zettabytes per year (Cisco Visual Networking Index 2020). This explosion in traffic is due to the rapid increase of mobile applications, mass video use, the Internet of Things, and cloud services. To remain competitive, companies in the Telecom sector must meet this demand by guaranteeing the availability, performance and security of critical services such as the DNS.

Unfortunately, there is one drawback: traditional DNS architecture has reached its limit. The stacking of DNS servers, load balancers and security layers create a structure that is complex to deploy, costly to maintain and unsuitable for correctly protecting DNS services. Such architecture is ineffective against most attacks such as DDoS, zero-day failures or data exfiltration.

A new approach is necessary to meet the challenges of performance, security and costs. With its SOLIDserver™ range of appliances, EfficientIP offers a DNS solution dedicated to the telecom sector, which unites high performance and intelligence to guarantee advanced security.

- SOLIDserver DNS Blast- a DNS cache server capable of absorbing up to 17 million DNS requests per second
- DNS Guardian- the adaptive security component integrated into DNS Blast, which performs in-depth analysis of the DNS traffic and is protected against all types of attacks (DDoS, DNS tunneling, sloth domain attack)

SOLIDserver provides enterprises the chance to rethink and simplify their DNS architectures to reduce TCO, improve security and guarantee a service suited for future needs.

Based on real situations, this document illustrates how SOLIDserver meets the challenges of performance, security, simplicity and reduction of costs, in three different environments and contexts:

I. Case 1: Get rid of useless server farms

II. Case 2: Get rid of unsuitable intermediary security layers

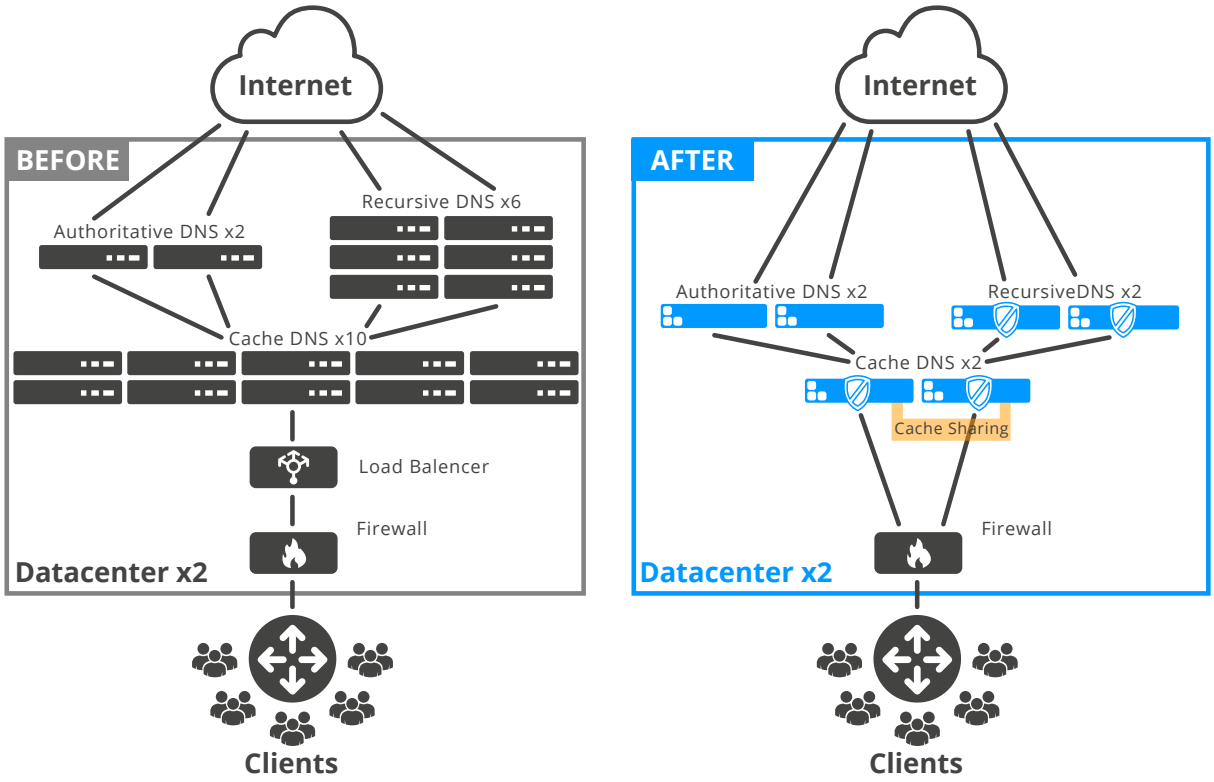
III. Case 3: Decentralize DNS architecture

Case 1

Get rid of useless server farms

The first case shows an initial architecture deployed in two data centers, with each utilizing ten DNS opensource (BIND) servers dedicated to the cache function. Two load balancers distribute traffic among these ten servers. Authoritative and recursive functions are performed by other DNS servers, also installed in the two data centers.

In each data center location, the ten cache servers and two load balancers are replaced by two SOLIDserver DNS Blast appliances with high availability. The Cache Sharing function (real time synchronization of cache data) is activated between all SOLIDserver DNS Blast appliances, including between the data centers. A management platform centralizes DNS management between the two data centers and the different functions (authoritative, recursive, cache).



Benefits:

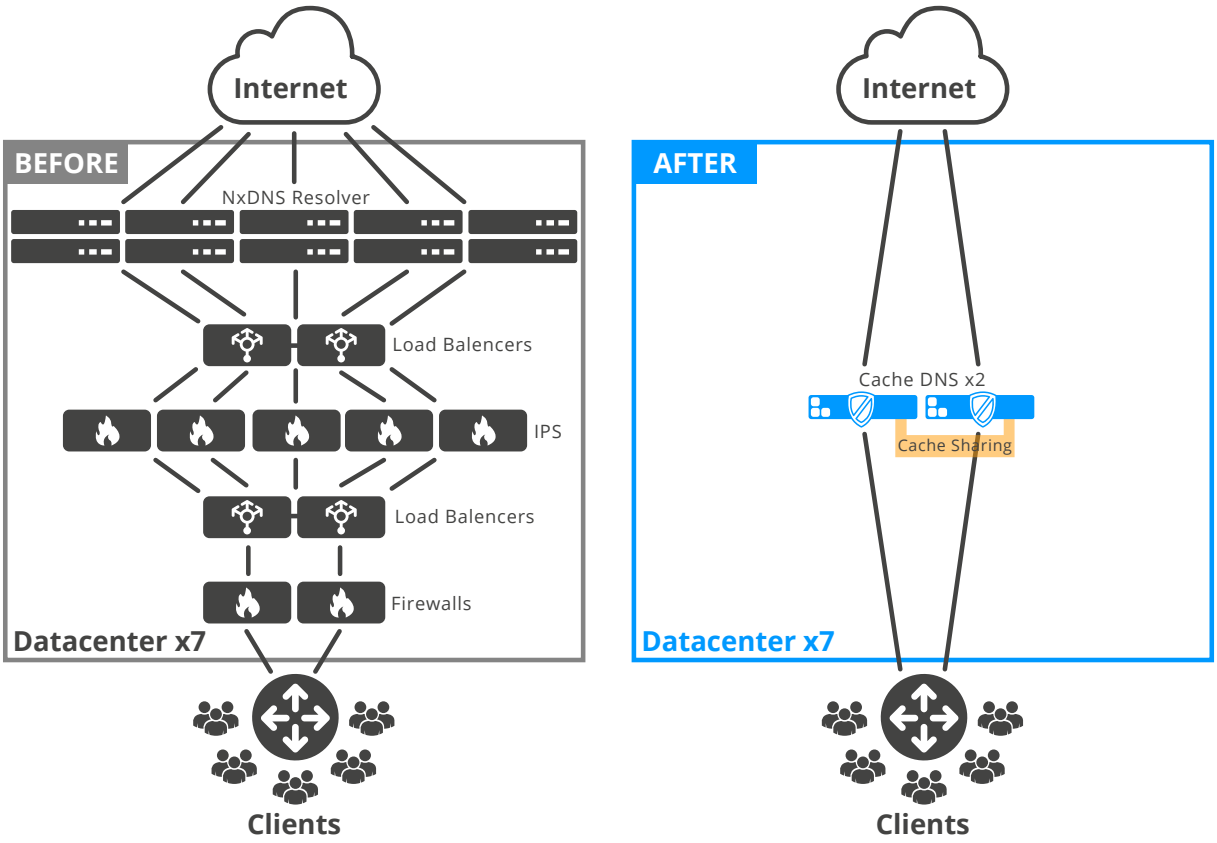
1. Performance: Twenty DNS BIND servers are replaced with four SOLIDserver DNS Blast appliances.
2. Reduction of costs: Increases space within the data center; reduces energy and operating and maintenance costs.
3. Security: In addition to the initial performance objective, the architecture benefits from the advanced security functionalities of SOLIDserver.

Case 2

Get rid of unsuitable intermediary security layers

The second case shows a DNS architecture distributed among several regional sites. Each site is equipped with ten DNS servers, protected by two firewall layers (applicative and network) and load balancers.

A DNS Blast server including DNS Guardian replaces the group of DNS servers on each site, as well as the two layers of firewalls and load balancers. The performance of DNS Blast allows it to absorb significant traffic or DDoS-type attacks. The advanced security mechanisms of DNS Guardian replace the firewalls, protecting against all types of attacks and ensuring continuity of service with legitimate traffic, even when the source of the attack is not identifiable.



Benefits:

1. Security: The placement of an adaptive security solution dedicated to the DNS guarantees availability of the service.
2. Performance: The performance of a single SOLIDserver DNS Blast is five times greater than that of ten connected servers.
3. Reduction of costs: Eliminates purchase, administration and maintenance costs for all technologies removed.

DNS security is ensured directly by SOLIDserver appliance servers, and does not require any further external security layers. In this way, the DNS service benefits from a dedicated solution, adapted to the DNS protocol and its function. This is not only much more effective for attack protection, but also drastically reduces the complexity of the infrastructure, its maintenance and associated costs.

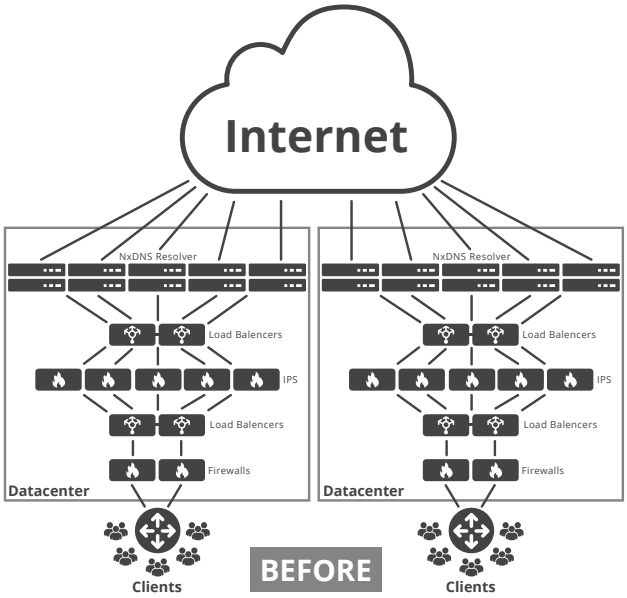
Case 3

Decentralize DNS architecture

The last case focuses on DNS traffic analysis. In recent years, operators identified a significant rise in DNS traffic. To deal with this heavy growth, new DNS servers were regularly added to the infrastructure.

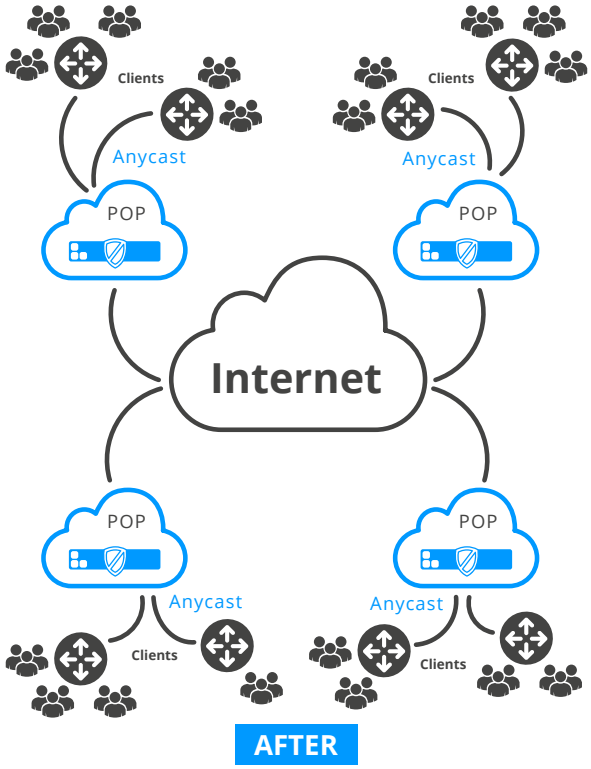
Initially, the project's main objective was to significantly increase the service's performance to deal with the increase in traffic, and be capable of protecting it against any DDoS attack. During the solution evaluation phase, the operator benefited from the advanced analysis functions of DNS Guardian to find out more about the nature of incoming traffic. This analysis showed that much of the traffic was in fact illegitimate, that the operator was regularly under attack, and consequently that the accumulation of services was mainly intended to deal with attacks.

The operator had initially envisioned centralizing DNS services in two data centers, with fifty DNS servers for each.



With the performance and security functions of DNS Blast, the operator was able to significantly rethink their architecture. Two SOLIDserver DNS Blast appliances were deployed in ten Points of Presence (PoP). While most DNS servers have an intrinsic latency of 0.035 seconds, . SOLIDserver DNS Blast enables a latency of 0.000027 seconds.

In addition to improving the general performance of service and security, the operator was able to get the DNS service closer to customers, reduce latency to improve the user experience, and block the clustering of traffic in the network core during attacks.



Benefits:

1. Performance: Deployment of a more powerful and smarter DNS infrastructure eliminates illegitimate traffic.
2. Security: Improved detection and protection against high volume or furtive attacks or security failings.
3. Reduction of costs: Optimizes the infrastructure, from one hundred DNS servers to twenty SOLIDserver DNS Blast.

The traditional method of adding servers as traffic increases is no longer the only option. All optimization projects begin with an analysis of the current situation. In this specific case, the analysis of the DNS traffic makes it possible to cut unnecessary expenses and deal with the problem directly at source.

Furthermore, deploying DNS servers in the periphery of the network to delocalize the service towards regional points provides three major benefits:

- Most traffic remains in the periphery and no longer encumbers the internal bandwidth of the network.
- The risk of service unavailability is divided between regional points and does not concern the entire service.
- Operators can offer a much more powerful and secure service at the local level, as well as a better user experience.

Conclusion

The three situations covered in this document present a real alternative to the accumulation of DNS servers and security solutions not adapted to the DNS service, to ensure the service level required by the market. They also present an opportunity to rethink DNS architecture and make it a competitive advantage. The DNS service becomes its own security solution; performance and security are focused on a single point. Once simplified, the DNS infrastructure can be visualized differently, as shown in the third case.

EfficientIP offers a 360° security solution which protects DNS infrastructures against specific threats to the DNS (high volume and furtive attacks and exploits). It integrates patented innovative technologies that guarantee unrivalled availability of DNS services, without a risk of blocking legitimate requests, and without the need for complex configurations or the irritating setup of filtering rules. This unique security solution is quick to roll out and maintain, as well as very economical. It includes the following solutions: SOLIDserver™ DNS Blast, DNS Guardian, Hybrid DNS Engine, DNS Cloud, and DNS Firewall.

Thanks to this dedicated technology, it is possible to improve the performance of the DNS infrastructure, guarantee protection against all types of attacks, and drastically reduce costs with a rationalized architecture.

efficient iP™

REV: C-200629

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
33 Ubi Avenue 3
08-25 Vertex Building, Singapore 408868
+65 6678 7752