efficient iP™
DEFINING SMART DDI

White Paper

Mitigating DNS Zero-Day Exploits With Hybrid Architecture

Key Benefits

- Protect against zero-day vulnerabilities
- Improve security risk management
- Eliminate Single Point of Failure (SPoF)
- Apply best practices to strengthen DNS security foundations
- Enhance upgrade agility

Exec Summary

The Domain Name System relies on pieces of software and protocols that are not exempt from current IT ecosystem risks, and therefore can be subject to security breaches. The difference with most of the available internet services is that without the DNS, many other services will fail.

If taking down the entire Domain Name System is considered mission impossible given its worldwide distribution, taking down or diverting companies's public or private DNS services is far easier for an attacker, and can seriously impact a business.

DNS is essential to every network and must be carefully secured to ensure IT services availability, communications and general business activity. Nevertheless, it's security is rarely a reality and much more could be done to ensure DNS service reliability.

Considering server-related attacks, patches are rarely applied in a timely fashion due to testing processes or lack of time and resources. Fixing critical services vulnerabilities quickly puts immense pressure on operational teams, often resulting in high risk errors. Worse, even when carefully updated, software remains vulnerable to zero-day exploits available on the black market which can easily be bought by hackers in order to reach their goal.

As recommended by the Network Testing Labs, the most secure approach to address these kinds of vulnerabilities is the hybrid use of different software. Correctly managed, this allows a quick and easy switch from one to another in a matter of minutes. Even better, running both pieces of software simultaneously within the DNS architecture can reduce the risk of the service falling under the exploitation of a single daemon's security hole. However, this best practice implementation can quickly become complex, expensive and risky if DNS services management are not properly addressed.

This white paper aims to present the challenges and benefits of hybrid DNS architecture, and how this best practice should be handled to ensure reliability, manageability and security of DNS services.

Most DNS Platforms Suffer From SPoF

Your network is vulnerable to cyber attacks in ways you likely have not heard of, or ever even imagined. The possibilities offered by a successful takeover of DNS servers are tremendous, allowing traffic redirection, malware control or simply arbitrary service outages. This should make DNS security a top priority among IT professionals.

Yet, there are many who still do not invest much into their DNS platform, leaving it on the backburner of their overall company's security strategy. Lack of understanding about this core network service leads to the ubiquity of BIND as the main name server software used by an IT department, making it a common target for attackers, and one of the Single Points of Failure for an entire IT infrastructure.

Despite the fact that known exploits are generally fixed quickly (10 patches were released for BIND in 2015), they are still rarely applied in time. The resulting risk is not negligible, with the latest and best example being CVE-2015-8704 affecting BIND. This vulnerability, referenced as requiring very little knowledge to exploit, could be easily used by any malware to take down any unpatched DNS server or service depending on it, such email or web-based applications.

As an average of 6 identified vulnerabilities per year since 2010 have affected BIND software (most of them related to DOS weaknesses), applying the appropriate patches while following quality procedures becomes a challenge. Upgrade processes should be carried out quickly and effortlessly without putting the reliability of DNS services at risk.

Even more problematic, software often contains unidentified programming errors that may be exploited by underground hackers. Looking for such vulnerabilities has become a growing business that offers big profits, as many are willing to pay for useful exploits. In this context, open source projects can benefit from transparency (even if some claim that this also exposes them). But what to say about proprietary software that are more likely subjected to hidden threats ?

Relying on a single piece of software to deliver such a critical network service leaves an entire infrastructure highly vulnerable to DoS attacks based either on unpatched bugs or zero-day exploits. Such software exposure must be addressed appropriately.

What is Hybridization?

A common strategy to mitigate the software exposure of a specific service is to hide the sensitive information that could be used to identify its version and configuration properties. Unfortunately, this is rarely sufficient to protect a service, as advanced fingerprinting techniques often allow for the easy identification of software by considering its behavior. That is why more advanced setups rely upon a hybrid approach that mixes different software edited by different vendors with complex clusters on top, which run the protected service. This setup ensures that the resulting behavior will be varied enough to complexify the attacker's task.

Hybrid architectures are certainly the most secure approach to stand against zero-day attacks, as it is highly unlikely to find the same weakness at the same time in different software maintained by different editors. Therefore, only one subset of a platform can be impacted at a time, ensuring DNS service availability and integrity.

Hybrid architectures also deliver another important benefit for smooth quality upgrade procedures: giving IT teams the capability to switch from one software to another. Engineers are given time to carefully validate each code release before pushing it into production, preventing undesired side effects on the service's dependencies.

DNS Hybridization Challenges

The hybrid approach has many advantages, yet is rarely deployed. This is mainly due to the underlying costs of deployment, and maintenance being such a complex setup within itself. Managing different software configuration formats while dealing with the differences and limitations of each product is challenging. It requires specific expertise on each DNS engine, and careful management to maintain consistency over the various DNS configurations to ensure quality and continuity of the service. Additionally, it consumes more time and resources, as mixing software will increase the number of patches required to follow validation and upgrade processes.

What is the appropriate solution to get all of the advantages of a hybrid DNS architecture without the associated challenges and risks?

How to Deploy Manageable, Secure and Reliable Hybrid DNS Architectures

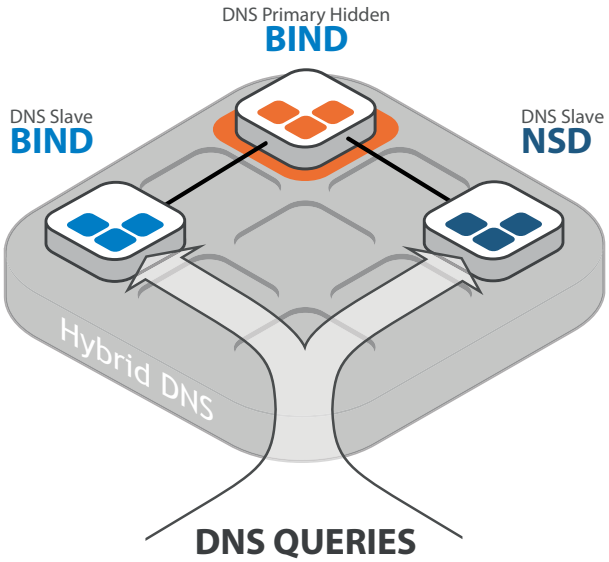
Managing a hybrid DNS architecture requires four components to ensure proper deployment, easy configuration and reliable upgrade processes.

First, a hybrid DNS platform must rely on servers embedding at least two different sets of DNS engines (only one active at a time) that are easily managed as a single entity. This implements an abstraction layer, automatically ensuring the consistency between a software's specific configurations.

The second major requirement is the ability to switch instantaneously from one active DNS software platform to an alternate one. This provides an effective way to mitigate the risk resulting from disclosed, yet unpatched vulnerabilities which otherwise may leave your DNS service (and thusly your business) exposed to security threats. It is only once a patch has been tested, validated and applied that the same mechanism can be used to resume normal operations, reverting to the original DNS engine in use.

The third is to provide the necessary tools to easily and quickly apply patches, and transparently keep the overall DNS platform up-to-date. This upgrade process must check and ensure the continuity of compatibility between the different DNS software.

The last requirement is to go beyond unitary DNS server management, and instead manage the architecture of servers. Managing DNS service at the architecture level enables IT teams to centrally and automatically configure distributed DNS platforms according to their respective role within the architecture (e.g., master, slave), regardless of the DNS software code. It provides an abstraction layer that manages name resolution as a service running on top of a distributed yet coherent platform, simplifying the deployment and administration of a hybrid DNS architecture.



Hybrid DNS Technology Benefits

Advanced hybrid DNS technology providing the required key components has several significant and unique advantages:

- Protects against zero-day vulnerabilities by giving network administrators the agility to switch from one name server technology to another for immediate vulnerability remediation
- Eliminates Single Point of Failure (SPoF) by mixing different technologies
- Strengthens the security foundation to fool hackers that are attempting to analyze the architecture design
- Improves security risk management by enabling users to run advanced patch testing before installing

EfficientIP is the only DDI vendor providing state-of-the-art hybrid DNS technology. SOLIDserver™ appliances are equipped with an embedded hybrid DNS engine (BIND and NSD/Unbound) and SmartArchitecture™ templates. This combination provides a unique solution to easily design, deploy and centrally manage hybrid DNS architectures mixing servers that are running different technologies, to ensure compliance with fundamental security best practices.

EfficientIP could be one of the competitive advantages.

About EfficientIP:
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.
17 Wilmont Mews, Suite 400
West Chester, PA 19382
+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
16 Raffles Quay #38-03
Hong Leong Building
Singapore 048581