efficient iP™
DEFINING SMART DDI

Product Documentation

Hybrid DNS Engine
THE Answer Against DNS Zero-Day Vulnerabilities

Hybrid DNS Benefits

- Mitigate risk before attacks take down your business
- Protect against zero-day vulnerabilities
- Eliminate single point of failure (SPoF)
- Strengthen DNS security in a way that baffles hackers
- Improve security risk management

Name servers can be particularly vulnerable to cyber attack. The need for DNS security has never been greater. Because DNS is such a critical service on your network, the testing and verification are absolutely necessary. You want to avoid the risk of continuing to use the vulnerable name server software, but you also want to avoid the risk of installing the name server software update until you know the update is thoroughly tested.

Hybrid DNS technology provides the highest-level security for your name servers. When a security alert or actual cyber attack affects your currently-running name server software (BIND for example), Hybrid DNS technology gives you alternative name server software that you can switch to with a single click. Your data center operations continue normally. And you revert to using the original name server software only after its vulnerability has been patched, tested and verified.

The result is greater security. Less risk. Faster performance (the alternative name server software is highly responsive). And easier administration.

EfficientIP is the only DDI vendor to provide state-of-the-art, high-quality, truly effective hybrid DNS security.

Why a Hybrid DNS Engine

Without Hybrid DNS technology, a security alert or actual cyber attack that targets the name server software you're currently running leaves you with few options and dramatically increases your risk of data loss or network downtime. A DNS vulnerability exposes your network to attacks, can reveal confidential internal information about your company and can turn your entire network into one huge botnet. Having the ability to easily and painlessly switch to a different name server program – unaffected by the DNS vulnerability – eliminates these risks.

DNS security breaches happen when hackers exploit DNS software and DNS protocols. The stateless nature of DNS lends itself to exploitation by hackers, criminals and industrial spies. A hacker determines which DNS software you're using by sending your name server malformed, invalid DNS requests and noting the nature of your name server's response. Each different name server software product has a unique "footprint" – a unique pattern of responses that it sends when the name server receives incorrectly-formatted DNS requests. The hacker probes your network, analyzes the responses and then attacks. When you switch to alternative name server software, you thwart the attack and leave the hacker wondering what happened. You've baffled and confused the hacker. Hackers will never be sure which name server software is running.

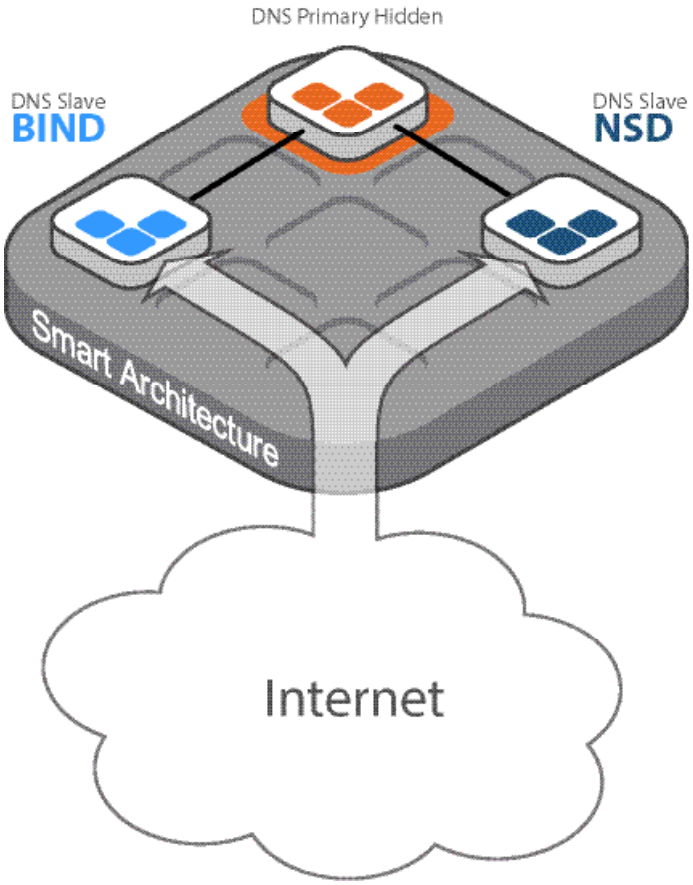
They'll find that analyzing DNS network packet footprints to discover name server flaws, fissures and openings is a daunting, complex and nearly impossible task. The hybrid approach of having two alternative software technologies within the same architecture makes the name server's security footprint (its apparent behavior in terms of network requests and responses) baffling to hackers because the DNS engines do not have the same types of algorithms. They thus present hackers with different responses when probed with incorrect DNS request formats or DNS attacks.

Hybrid DNS Engine: How It Works

The most commonly-used name server software is BIND. Therefore, cybercriminals can, with some impunity, assume that your network uses BIND.

BIND is an excellent compromise between speed and security, between ease of administration and robustness and between RFC integration and universal applicability. However, its very popularity makes it a common target. BIND's known flaws and bugs have all been fixed. However, like any other computer program, BIND contains some remaining but unknown and unidentified programming errors that hackers will find and take advantage of.

EfficientIP SOLIDserver appliances embody advanced Hybrid DNS Technology. The EfficientIP Hybrid Technology incorporates a second DNS engine, in addition to BIND, in a single DNS appliance. This increases the security and reliability of critical DNS services in case of attack or security threats. The alternate DNS engine is based on two different name server products, Unbound and NSD. Unbound is a validating, recursive, and caching DNS resolver designed for high performance. NSD is an authoritative only, high performance name server. (NSD is about twice as fast as BIND, which means that NSD offers a more robust environment in case of a DoS attack).



At any moment, one DNS engine is active (running) on a SOLIDserver DNS appliance and the other is in standby mode. EfficientIP's SmartArchitecture automatically ensures that configuration changes are synchronized between the two DNS engines.

With a single click, you switch from running name server software that's been hacked to alternate name server software that's unaffected by a security breach. The alternative name server software can remain in place while DNS programmers patch, test and validate a security upgrade to the vulnerable name server product.

Furthermore, EfficientIP's SmartArchitecture enables effortless deployment of hybrid DNS architectures. For instance, designing, deploying and managing a Master/Slave architecture with Master servers running BIND and Slave servers running NSD is easy with SmartArchitecture templates.

Hybrid DNS Engine Key Benefits

EfficientIP's Hybrid DNS engines protect against zero-day vulnerabilities by giving network administrators the agility to switch from one name server technology to another for immediate vulnerability remediation.

The Hybrid DNS architecture eliminates single point of failure (SPoF) following security alerts and strengthens DNS security in a way that baffles hackers.

And EfficientIP improves your security risk management by giving you the option of switching name server technologies when you decide, not when someone else decides. The result is transparent to you and opaque to hackers.

EUROPE

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

USA

EfficientIP Inc.
17 Wilmont Mews, Suite 400
West Chester, PA 19382
+1 888-228-4655