

DNS Blast

World's Fastest and Most Advanced DNS Cache Security Solution

Highlights:

- Absorb extreme Denial of Service (DoS) attacks with the world's fastest DNS cache performance
- Protect service continuity and data confidentiality with DNS Transaction Inspection (DTI) and behavioral threat detection
- Prevent users from accessing malicious content
- Augment application access control with domain filtering per user
- Improve user experience with ultra-low latency
- Simplify infrastructures with purpose-built DNS security technology and reduce Total Cost of Ownership (TCO)
- Enhance architecture agility with actionable scalability

A New Security Context For Extreme DoS Attacks on DNS Services

Recent months have shown a dramatic increase in the scale, frequency, and sophistication of DNS Distributed DoS (DDoS) attacks. Domain name services are the most targeted application layer for many years and commonly used by malware to build among the largest volumetric attacks ever seen. At the same time, the latest reports also demonstrated the insidious approach of hackers in building DNS stealth assaults that are not possible to detect with traditional protection systems, aiming to exfiltrate confidential data or causing huge disruption to business operations.

The fast-growing deployments of unsecured Internet of Things (IoT) devices, user mobility, and Bring Your Own Device (BYOD) amplify these threats calling for a drastic rethink of the DNS security approach through high-performance and purpose-built advanced analytics. Only by understanding these risks and integrating new solutions can you efficiently and proactively strengthen business continuity, data confidentiality, and user experience that your company deserves.

DNS Blast™: World's Fastest and Most Advanced DNS Cache Security Solution

DNS Blast from EfficientIP is a game-changing technology offering a revolutionary approach to DNS security, in all aspects: cache, recursive and authoritative. DNS Blast innovations combine the world's fastest cache appliance with the most advanced built-in security systems, protecting against the largest spectrum of threats.

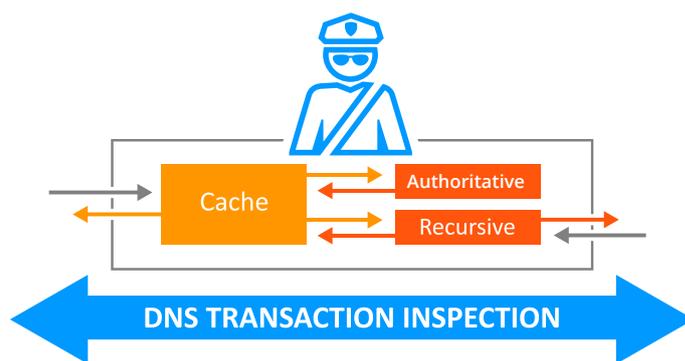
Outstanding Performance for DNS Service Delivery and Protection

DNS Blast cache appliance suite is a unique market solution delivering up to 17 million queries per second (QPS) to absorb large volumetric DoS attacks while offering unprecedented robustness, actionable scalability, and ultra-low latency. More importantly, built-in advanced security features are delivered at record speed to ensure the integrity and continuity of mission-critical DNS services, even during the most critical attacks.

Advanced Security Technologies to Protect Business Continuity and Data Confidentiality

DNS Blast is a purpose-built hardened security cache appliance with embedded patented innovations to intelligently protect against DNS security threats, regardless of the attack type: exploits and zero-day, data exfiltration, DGA (Domain Generation Algorithms), volumetric and stealth attacks. It includes the following advanced security components:

DNS Guardian: it is the first DNS security product that enables complete DNS Transaction Inspection and advanced analytics for real-time behavioral threat detection. DNS Guardian overcomes the limitations of signature-based security systems that only offer limited peripheral traffic visibility. Patented smart countermeasures provide unique adaptive security to protect data confidentiality and guarantee unmatched continuity of DNS services, even if the attack source is impossible to identify (such as during a distributed weak signal attack). DNS Guardian can also be configured to act as a transparent proxy - ideal for global RPZ filtering or deep behavioral client traffic analysis in order to filter or quarantine malicious IPs. DNS security policies can be applied on DNS Guardian appliances to enforce behavioral threat detection settings and mitigation configurations over the entire network.



DNS Guardian Innovative Security Framework

Hybrid DNS Engine: The SOLIDserver Blast solution incorporates two DNS cache engines (BIND & Unbound), managed transparently as a single unit. It provides SmartArchitecture templates, a unique solution to easily design, deploy and centrally manage hybrid DNS architectures mixing servers running different technologies. Hybrid DNS Engine ensures the highest level of security to instantaneously mitigate zero-day vulnerabilities and maintain full control of upgrade processes.

DNS Firewall: it detects, stops, or redirects queries from clients that want to access domains and/or IPs known to be malicious. It prevents connected devices from becoming infected with malware, blocks their activity, and actively contributes to mitigating data exfiltration risks. Threat intelligence data feed services ensure the dynamic update of these lists (abuse, spam, phishing, malware, or cracked websites) to adapt to an ever-evolving threat landscape.

DNS Client Query Filtering (CQF): complementing DNS Firewall, this DNS Guardian feature enables the application of different filters for different groups of clients. By grouping clients based on their IP address or more complex information from the DNS frames, like the content of EDNS extensions, organizations and telcos can apply granular application access control very close to the client before hitting the transit networks and the security filtering solutions. DNS CQF also enables advanced use cases like IoT allowlisting or parental control.

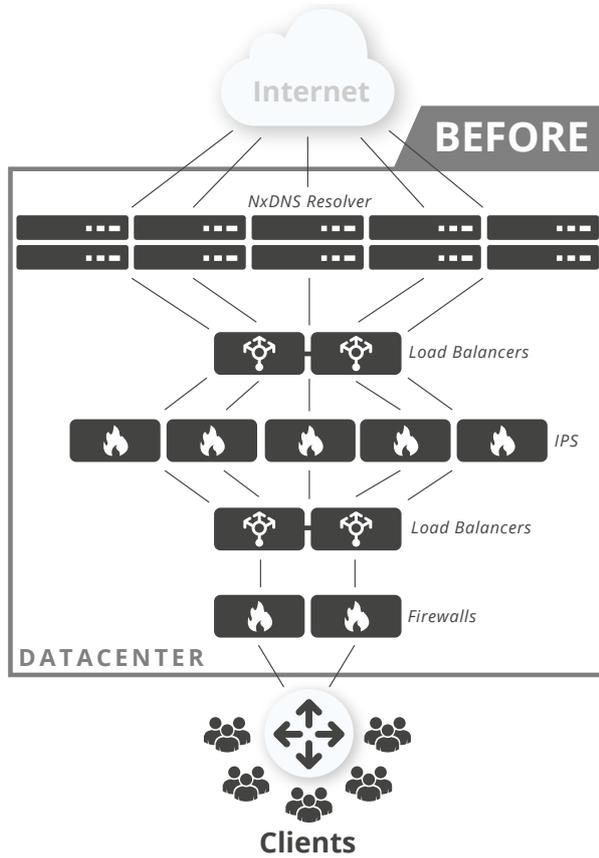
High Availability of DNS Services with Flexible LAN & WAN Redundancy

SOLIDserver Blast implements state-of-the-art clustering and anycast resilience mechanisms. The flexibility of the redundancy methods enables the creation of mesh architectures, ensuring immediate and transparent access to the nearest available server to maintain business continuity and the highest level of user experience.

Simplified DNS Architectures to Decrease TCO and Obtain Quick Return On Investment (ROI)

DNS Blast is a purpose-built DNS security solution that allows for the drastic simplification of a DNS infrastructure by eliminating dozens of DNS clusters, numerous load balancers, and useless firewalls. The DNS server ensures its own protection with performance and security focused on a single point, without the need for complex configurations or the irritating setup of approximate filtering rules.

DNS Blast's unique advanced security solution is quick to roll out and maintain, as well as being very economical. As a result, the TCO of DNS services is drastically decreased, security markedly improved and unrivaled actionable scalability guaranteed.

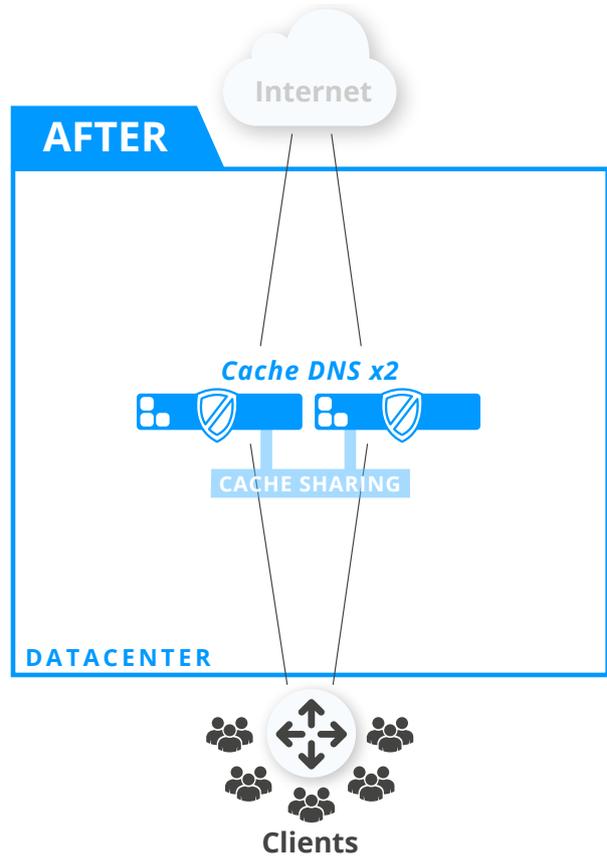


Improved Resilience and User Experience with Decentralized DNS Architecture

DNS Blast's purpose-built high-performance DNS security software appliance enables new architecture designs by deploying servers as close as possible to users through distributed DNS infrastructure, just like CDNs do with their content appliances.

DNS Anycast strengthens the service availability and optimizes access to the closest point of presence using any common routing protocol (BGP/OSPF/ISIS).

This distributed and disruptive approach improves the overall service robustness and resilience, saves the backbone's bandwidth usage, and helps to improve user experience due to ultra-low latency.



Simplified DNS Architecture using EfficientIP Appliances

Enhanced Cache Management

Cache Sharing to Reduce Bandwidth Consumption

DNS Blast offers support for DNS cache sharing relying on IP multicast mechanisms. Sharing the cache enhances the overall performance (hit rate) of the distributed DNS platforms, reducing the DNS service latency. It also decreases the number of recursive queries sent to authoritative servers on the network, minimizing the risks of cache poisoning. Combined with the Rescue Mode and the overall security mechanisms offered by the embedded DNS Guardian product, this allows for the deployment of a distributed, secured cache and recursive DNS service.

Persistent Cache to Restart with Full Performance

Classic cache functions are flushed after a restart and need time to be filled by the incoming traffic to again offer good performance. When SOLIDserver is restarted, the cache is saved, so that the server is immediately prepared for 100% performance delivery. This offers the best possible service to your customers.

Compatible with Existing Architecture of DNS Servers

DNS Blast is an agnostic technology that can be deployed in overlay of any existing DNS engine. For instance, it can easily be integrated within a Microsoft Active Directory architecture, in order to protect the availability of dependent services such as authentication and email, or deployed in line with an existing DNS cache or authoritative architecture based on BIND.

Support of multi-protocol access

DNS Blast is able to be positioned within enterprises and network providers, facing corporate employees as well as Internet end-users. In specific cases, it can be useful to cipher the local DNS traffic between the client and the resolver, which is why DNS Blast supports DNS traffic over UDP (vanilla feature), DNS traffic over TCP, and DNS traffic over TLS (also known as DoT). When using TLS, the traffic is ciphered and access can be protected through digital certificates, to prevent eavesdropping on client DNS requests. In addition to DoT, the DNS over HTTPS (DoH) tunneling protocol is also accepted in order to provide the client with browser security using a de-facto standard.

Softwares Appliances Available for Hardware Platforms or Virtual Machine

In order to support all types of corporate network strategies, including private cloud and virtualization, DNS Blast is available as a Software Appliance targeting various hardware platforms and virtual machines according to the following tables:

Hardware Platforms			
Software Appliance	EfficientIP SOLIDserver medium HW platform	EfficientIP SOLIDserver large HW platform	Performance *
BLAST 4070	Supported	Supported	3M QPS
BLAST 5070	-	Supported	10M QPS
BLAST 5570	-	Supported	17M QPS

Virtual Machine		
Software Appliance	Virtual Machine specification	Performance *
BLAST 4070	VCPU = 12 RAM = 32 GB IOPS >= 160 IOPS Hard Drive >= 128 GB Dedicated Intel X710 10GE or E820 Chipset in PCI Passthrough mode	3M QPS
BLAST 5070	-	-
BLAST 5570	-	-

* Listed performance numbers were reached in a test environment. Performance numbers in production may be different.
M QPS = Million Queries per Second.



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.
Copyright © 2023 EfficientIP, SAS. All rights reserved. EfficientIP and SOLIDserver logo are trademarks or registered trademarks of EfficientIP SAS. All registered trademarks are property of their respective owners. EfficientIP assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document.

REV: C-230223