efficient iP™
DEFINING SMART DDI

Datasheet

DNS BLAST

La solution de cache DNS la plus rapide et la plus élaborée au monde

Ces derniers mois ont vu une spectaculaire augmentation des attaques DDoS visant les services DNS, à la fois en termes d'échelle, de fréquence et de sophistication. Pour la troisième année consécutive, le DNS est le composant de la couche applicative le plus ciblé par les malwares qui le détournent via l'élaboration d'attaques massives d'importance jusque là jamais observée.

Les derniers rapports ont démontré l'approche insidieuse retenue par les pirates dans l'élaboration d'attaques DNS furtives visant à exfiltrer de l'information confidentielle ou encore à perturber significativement l'activité économique d'une entreprise. Ces attaques sont aujourd'hui impossibles à détecter à l'aide des systèmes de protection classiques.

Or, la croissance rapide des déploiements d'objets connectés (IoT) non sécurisés, de la mobilité des utilisateurs et du BYOD, amplifie les menaces et impose de re-considérer très sérieusement l'approche de la sécurité DNS, via des technologies d'analyse élaborées, spécifiquement conçues pour assurer la performance et la disponibilité du service. La compréhension de ces risques et le déploiement de nouvelles solutions de sécurité sont indispensables pour renforcer de façon efficace et proactive la continuité de l'activité, la confidentialité des données ainsi que l'expérience utilisateur.

Points Forts :

- Un cache DNS capable d'absorber les attaques DDoS les plus massives
- Un cache DNS capable d'absorber les attaques DDoS les plus massives
- Un service DNS renforcé assurant la continuité de tous les services du système d'information
- Une inspection en profondeur du trafic DNS assurant la détection des comportements suspects
- Filtrage intelligent des requêtes associées à du contenu malveillant
- Une meilleure expérience utilisateur grâce à une très faible latence
- Simplification des infrastructures et réduction des coûts via une technologie de sécurité spécifiquement conçue pour DNS

DNS Blast : la solution de sécurité du cache DNS la plus rapide et la plus élaborée

DNS Blast d'EfficientIP s'appuie sur une technologie révolutionnaire, proposant une approche innovante de la sécurité des fonctions cache et récursives des résolveurs DNS. Les innovations de DNS Blast associent l'appliance de cache la plus rapide du monde et les systèmes de sécurité intégrés les plus élaborés, offrant une protection optimale contre le plus large éventail de menaces.

Des performances exceptionnelles dédiées à ladisponibilité et à la protection optimales des services DNS

La gamme d'appliances de cache DNS Blast est la seule solution du marché capable de répondre jusqu'à 17 millions de requêtes par seconde, et donc d'absorber ainsi les attaques DDoS volumétriques à grande échelle, tout en offrant une robustesse et une évolutivité sans équivalent, ainsi qu'une latence ultra faible. Plus important encore, des fonctionnalités de sécurité sophistiquées sont activées à des vitesses record afin d'assurer l'intégrité et la continuité des services DNS critiques, même en cas d'attaque de grande ampleur.

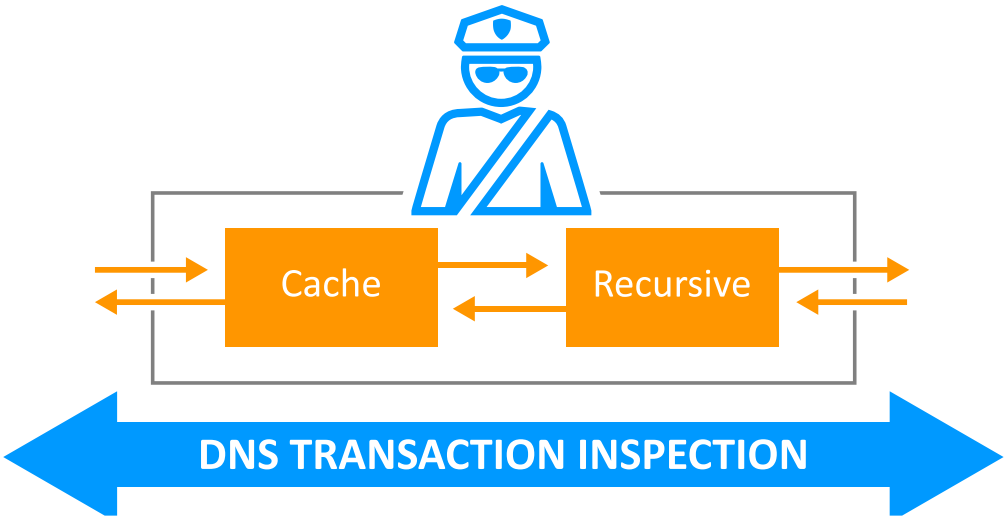
Des technologies de sécurité élaborées pour préserver la continuité de l'activité et la confidentialité des données

DNS Blast est une appliance de cache à la sécurité renforcée, spécifiquement conçue, et intégrant des innovations brevetées, spécifiquement conçue pour protéger les services DNS quel que soit le type d'attaque : vulnérabilités de type zero-day, exfiltration de données, volumétrie ou encore attaques furtives. La solution intègre les fonctionnalités de sécurité élaborées suivantes :

DNS Guardian : La première solution de sécurité DNS permettant une inspection comportementale complète en temps réel des transactions DNS ainsi que des analyses poussées, pour une détection efficace des menaces et des comportements suspects. DNS Guardian dépasse les limitations des systèmes de sécurité qui s'appuyent uniquement sur des systèmes de signatures et n'offrent qu'une visibilité périphérique du trafic. Ses fonctionnalités intelligentes et brevetées assurent une sécurité adaptative unique pour préserver la confidentialité des données et garantir une continuité inégalée des services DNS, même lorsque la source de l'attaque est impossible à identifier (par exemple une attaque distribuée à signal faible).

Hybrid DNS Engine : L'appliance SOLIDserver™ Blast intègre deux moteurs de cache DNS (BIND & Unbound), gérés de façon transparente comme une entité unique. Il fournit des templates SmartArchitecture™, permettant une implémentation respectant l'état de l'art d'une architecture DNS hybride et pilotée de façon centralisée. Une solution unique permettant de facilement définir, déployer et gérer centralement une architecture DNS hybride possédant des serveurs issus de technologies différentes. Hybrid DNS Engine garantit le plus haut niveau de sécurité réduisant immédiatement l'impact potentiel d'une vulnérabilité de type zero-day tout en garantissant et en maintenant le contrôle complet sur les processus de mise à jour.

DNS Firewall : DNS Firewall détecte, bloque ou redirige les requêtes des clients qui souhaitent accéder à des adresses IP et/ou à des domaines connus pour être frauduleux. Le pare-feux empêche les appareils connectés d'être infectés par les malwares en bloquant leurs activités et contribue activement à limiter les risques d'exfiltration de données. Les services de flux de données de connaissance des menaces permettent la mise à jour dynamique des listes (fraude, spam, phishing, malware ou sites web piratés) pour s'adapter à l'évolution permanente des risques.



DNS Guardian Innovative Security Framework

Haute disponibilité des services DNS avec redondance LAN & WAN flexible

L'appliance SOLIDserver™ Blast implémente les mécanismes de résilience les plus modernes de regroupement (clustering) et d'anycast. La flexibilité des méthodes de redondance permet la création d'architectures maillées, garantissant un accès immédiat et transparent au serveur disponible le plus proche, afin de préserver la continuité de l'activité et le plus haut niveau de disponibilité des applications.

Des architectures DNS simplifiées pour réduire les coûts et obtenir un ROI rapide

DNS Blast est une appliance de sécurité spécifiquement conçue pour le DNS qui permet une simplification drastique de l'architecture de ce service par la suppression de dizaines de clusters DNS, de nombreux équilibreurs de charge et de pares-feu inutiles. Le serveur DNS assure ainsi sa propre sécurité, sans recourir à des configurations complexes ou à l'élaboration fastidieuse de règles de filtrage approximatives.

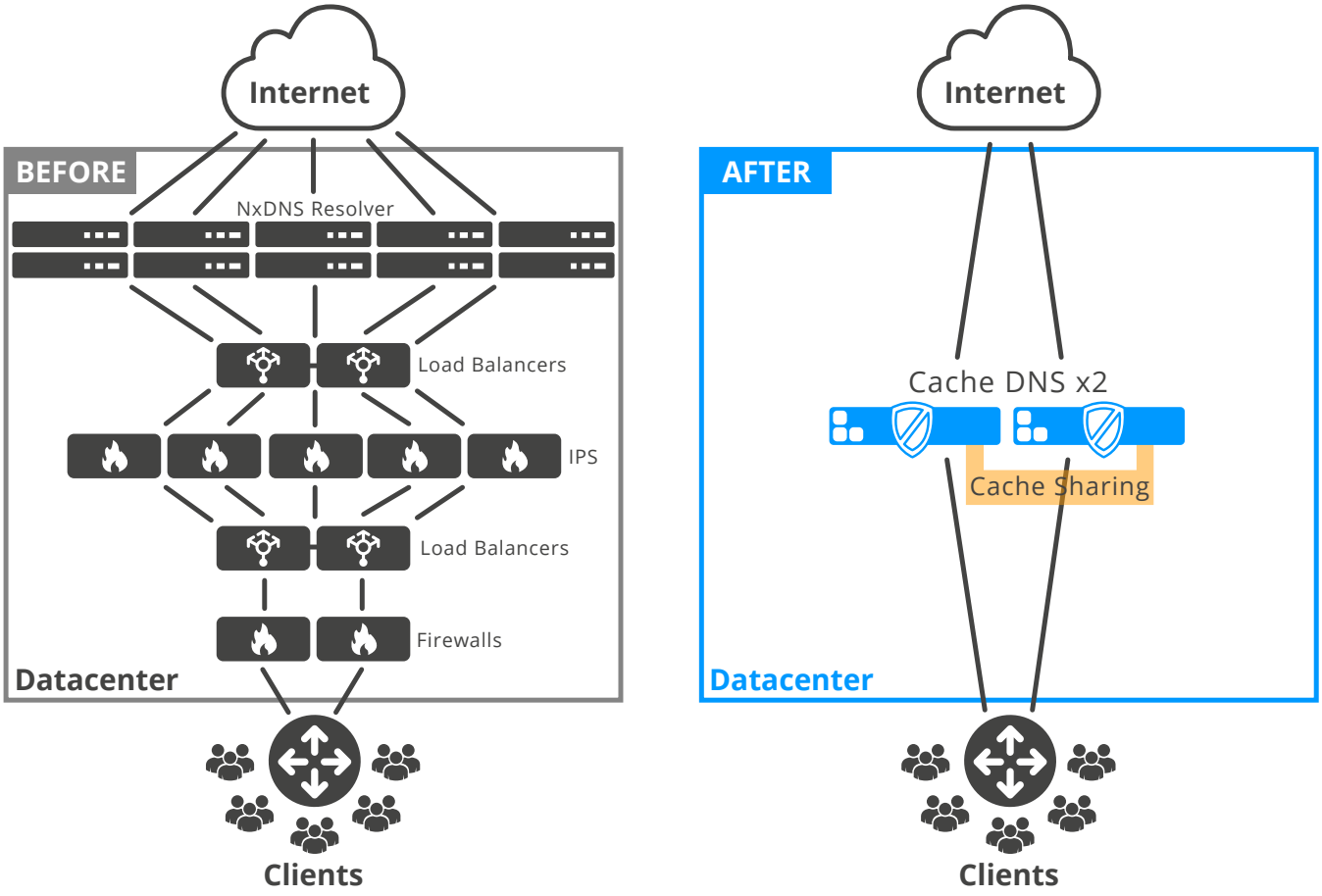
En plus d'être économique, DNS Blast est une solution unique et sophistiquée qui se déploie rapidement et se maintient aisément, avec un déploiement rapide et à la maintenance aisée. En conséquence, les coûts associés à la maintenance du service aux services DNS sont considérablement réduits, la sécurité nettement améliorée et vous bénéficiez d'une évolutivité sans précédent.

Une résilience et une expérience utilisateur renforcées grâce à une architecture DNS décentralisée

DNS Blast, l'appliance haute performance spécifiquement dédiée à la sécurité DNS, permet la conception de nouvelles architectures basées sur le déploiement de serveurs aussi proches que possible des utilisateurs, de la même façon que les CDN avec leurs appliances de contenu.

DNS Anycast renforce la disponibilité des services et optimise l'accès au point de présence le plus proche à l'aide de tout protocole de routage courant (BGP/OSPF/ISIS).

Cette approche distribuée et innovante améliore la robustesse et la résilience globales des services, économise l'utilisation de la bande passante et contribue au confort des utilisateurs grâce à une latence ultra faible.



Simplified DNS Architecture using EfficientIP Appliances

Gestion améliorée du cache

Partage du cache pour réduire la consommation de bande passante

DNS Blast permet le partage du cache DNS entre plusieurs appliances en s'appuyant sur les mécanismes IP multicast. Le partage de ce cache améliore les performances globales (hit rate) des plateformes DNS distribuées, et améliore sensiblement la latence des services DNS. Il réduit également le nombre de requêtes récursives envoyées aux serveurs d'autorité, et donc minimise les risques de corruption d'empoisonnement du cache. Associé au "Rescue Mode" et à l'ensemble des mécanismes de sécurité offerts par le produit DNS Guardian embarqué, il permet le déploiement d'un service DNS cache et récursif, distribué et sécurisé.

Des performances inaltérées du cache après redémarrage

La plupart des caches DNS sont réinitialisés au redémarrage du service, ce qui a pour effet de retarder leur retour en condition opérationnelle, le temps de reconstruire un cache pérenne et nécessitent donc du temps et du trafic pour être à nouveau pleinement efficaces. Lorsque SOLIDserver™ est redémarré, le cache est sauvegardé, de sorte que le serveur est immédiatement opérationnel à son redémarrage. Vos clients bénéficient ainsi du meilleur service possible.

Compatibilité assurée avec l'architecture existante de serveurs DNS

DNS Blast est s'appuie sur une technologie agnostique, et peut être déployé sur n'importe quel moteur DNS existant. Il peut par exemple être intégré au sein d'une architecture Microsoft Active Directory, afin de protéger la disponibilité des services dépendants tels que l'authentification ou et le courrier électronique, ou déployé parallèlement à un cache DNS existant ou une architecture d'autorité basée sur BIND.

Disponibilité de l'appliance en version matérielle ou virtuelle

Afin de s'adapter aux différentes stratégies des réseaux d'entreprises, y compris le cloud privé et la virtualisation, DNS Blast est disponible en tant qu'appliance matérielle ou virtuelle. Leurs caractéristiques sont les suivantes :

Appliance	Performances * Version matérielle	Performances * Version virtuelle **
SOLIDserver™ 4000	3 MQPS	3 MQPS
SOLIDserver™ 5000	10 MQPS	-
SOLIDserver™ 5500	17 MQPS	-

* Les performances indiquées ont été obtenues en environnement de test.
Les performances en production peuvent différer.
MQPS = Million queries per second (millions de requêtes par seconde).

** Configuration de VM requise :
- VCPU = 12
- RAM = 32 Go
- IOPS >= 160 IOPS
- Disque dur >= 128 GB
- Chipset dédié Intel X520 en mode PCI pass-through

efficient iP™

REV: B-1711

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
101C Telok Ayer Street #04-00
SINGAPORE 068574
+65 6678 7752