URMAZI

DATASHEET

iSafer
DNS Booster

Services | Security | Visibility

DNS Firewall

DNS Proxy

DNS Server

Multihoming

Threat Intelligence

About Domain Name System

The Domain Name System (DNS) is a fundamental protocol of the internet, used for hierarchical and decentralized naming. Its purpose is to translate human-readable domain names into IP addresses. It consists of a database used to store domain names and their associated IP addresses, much like a directory or phone book for the internet. DNS plays a crucial role in enabling the smooth functioning of services such as corporate websites, chatbots, e-conferencing, online shopping, customer support, telemedicine, e-banking, and more, all of which rely on internet connectivity to provide their services. Due to its importance as a critical information infrastructure for organizations, DNS requires strict protection.

Risks of DNS Threat Attacks

According to the Global Network Security Threat Report, DNS-based attacks are rapidly evolving and becoming highly complex and extensive. Attackers are employing diverse techniques and leveraging various components of DNS to pose threats. For instance, they target both recursive resolvers and authoritative DNS servers, or exploit DNS covert channels to leak data that typically goes undetected in legitimate DNS traffic. The difficulty in self-detection and defense against these attacks has been increasing for businesses. The consequences of an insecure domain system can lead to higher risks of data breaches, service disruptions, substantial financial losses, regulatory non-compliance, and damage to the organization's reputation, all of which are irreversible risks.

©2023 URMAZI Networks Inc. All rights reserved

“iSafer” to Boost DNS Defense Capability

iSafer is a specialized security protection software platform for DNS services, actively intervening in the security check and defense during the service connection query phase at the endpoint. It possesses robust defense mechanisms as tools for organizations to detect, block, and mitigate network threats.

We advocate the concept of "Preventive Security," which is based on intercepting known threats at the very beginning of network service connections. For unknown threats, iSafer automatically learns, records, and observes them, and then combines multiple blocking policies to minimize the impact of the threats. By stopping threats before they even begin, it significantly reduces the risk of service collapse caused by DNS-related risks such as DDoS attacks, hijacking, poisoning, and tunneling. Administrators can use iSafer's DNS trace records to clearly trace and locate potential threats, allowing them to take necessary remedial measures, completing the three-step preventive security process: Detection, Defense, and Remediation. According global DNS security statistics show that the number of malicious domains doubles every year. Therefore, security teams should prioritize domain security as a primary task.

Endpoint Safe, Organization Safe

Enterprises can seamlessly connect and adopt the iSafer DNS Booster solution without changing their existing network environment. The true benefit that iSafer can bring is preventing disasters caused by DNS attacks on online services while significantly improving network efficiency and the flexibility of various business services. It strengthens the organization's security, visibility, and control, allowing network threats to be blocked right from the initial connection phase. Additionally, through the USRA Security Research Academy established by URMAZI, combined with deep learning and artificial intelligence technologies, the ability to identify unknown threats is continuously strengthened, and a global network threat intelligence database is maintained to protect your enterprise from potential attacks.

- **Easy Management**
- **Seamless Adoption**
- **Efficient Protection**
- **Cost Effective**

iSafer Solution Advantages

Advanced DNS Protocol

Support converting and communicating the encrypted protocols of DoH, DoT, and DNSCrypt with the traditional DNS protocol without the need to rebuild or upgrade the existing domain name system. This ensures the privacy of personal information and secure transmission during communication.

Auto Learning

iSafer incorporates a dynamic observation and analysis mechanism, enabling it to self-learn and update based on DNS query requests, relevant response information, and other data. It not only proactively issues warnings for previously unrecorded domain names and response combinations but also automatically adds detected abnormal connections to a whitelist. This facilitates better control and synchronization to enhance the system's protective capabilities.

Malicious Protection

iSafer equipped with a domain feature database containing 58 categories, enabling rapid identification of malicious or inappropriate sources, such as phishing, scams, botnets, or ad tracking threats. It can efficiently handle encrypted website connections without performance bottlenecks, significantly reducing the resolution workload on other network security devices.

LoadBalancing & Multihoming

The advanced DNS Server feature allows you to evenly distribute public service connections across different external routes. Simultaneously, it automatically identifies and responds with the address of the functioning route, ensuring uninterrupted service.

Global Threat Intelligence

Actionable and accurate intelligence is essential for effectively formulating defense measures. iSafer collects massive domain intelligence from around the world, over billions of records, along with hundreds of thousands of daily updates. It not only serves as a cornerstone of organizational security defense but also becomes a crucial piece of evidence for analyzing internal connections within the organization.

Boost Queries & Protection

iSafer supports query logging and data packet caching mechanisms. During the recursive query process, it stores information about responsible name servers at each level of the caching DNS, which accelerates and shortens response times for subsequent identical queries and reduces the frequency of repeated queries. Query rate detection and protection also help alleviate sudden spikes in query requests, ensuring the normal operation of public services.

iSafer Product Feature

Feature & Version	Essential	Advanced	Superior
System Model	SF10 / 20E	SF10 / 20A	SF50S
Query per second (QPS)	10k / 20k[a]	10k / 20k[a]	50k
System Main Services			
DNS Proxy[b] & Request Route	✓	✓	✓
DNS Server Load Balance	✓	✓	✓
DNS Server [b]	N/A	✓	✓
DNS Multihoming[c]	N/A	✓	✓
Black & White List Import by IP or Subnet Based	✓	✓	✓
RRL[d] Control for IP or Subnet or Domain Based	✓	✓	✓
SafeSearch Content Filtering	✓	✓	✓
DNS Sinkhole Protection	N/A	✓	✓
DDoS Dynamic Block Protect			
Set blocking time by query number or query rate	✓	✓	✓
Set blocking time by RCode respond number or ratio	✓	✓	✓
Set blocking time by QType query number or query rate	✓	✓	✓
DDoS Protect Policy			
Set Query Threshold Limitation	✓	✓	✓
Allow, Block, Delay, Translate IP or DomainName	✓	✓	✓
Global Threat Intelligence Service			
Go-start Category Pack(Botnet, Phishing, Scam)	Subscription		
Plus Category Pack(Ransomware, Crypto, URL Shortening, NRD, etc)[e]	Subscription		
Min. system requirements: 4 Cores, 8 GB RAM, 128 GB Storage, VMware ESXi v6.5 or higher.			

[a] Factory default with 10k QPS, it's able to upgrade to 20k by order individual license. [b] Service supports UDP, TCP, DoT, DoH, and DNSCrypt. [c] Product comes with license of 2 domains. If more domains are needed, extra license is required. [d] RRL stands for Response Rate Limit. [e] Total of 58 categories which includes Go-start, no need to pay extra license fee within valid subscription period if number of category increases.
Remark. URMAZI keeps the right for adjusting system features or performance without notice.