efficient iP™
DEFINING SMART DDI

Product Description

DNS FIREWALL

Protecting and Defending Network Infrastructure Against Malware

DNS servers deliver critical services to your company, such as internet visibility for your customers, partners and employees, access to network applications, and other indispensable services such as email.

DNS servers also represent one of the most vulnerable entry points to enterprise network and are therefore regularly targeted by hackers. DNS-based malware is particularly dangerous as they're used to steal critical company and customer data.

EfficientIP's DNS Firewall is a comprehensive DNS security solution that proactively prevents new at- tacks and protects SOLIDserver™ appliance and Linux - based DNS infrastructure by detecting and blocking malware activity, and identify infected devices.

Ensure Proactive and Efficient Protection Against Malware

The best way to protect your network infrastructure against malware is to eliminate the risk of devices corruption. SOLIDserver™ DNS Firewall prevents connected devices from becoming infected with malware by enabling recursive DNS servers to block queries from clients that want to access domains and/ or IPs known to be malicious.

Define DNS Response Policies

Recursive DNS server response policy (DNS RPZ) is based upon domain data feeds created manually by the IT administration team and /or provided by an external service. SOLIDserver™ DNS Firewall offers a granular approach to RPZ zone management. Instead of blocking an entire domain, exceptions for subdomains are created and then for each individual subdomain response policies are created. For example, a redirection to a corporate warning page could be defined. SOLIDserver™ DNS Firewall offers easy to deploy and reliable malware protection that can be personalized to meet specific and granular requirements.

Contain Malware Spreading and Identify Infected Devices

Based on DNS query analysis, SOLIDserver™ DNS Firewall detects and isolatesclients infected with malware, blocking all communication with external websites and then disrupting malware activity. SOLIDserver™ DNS Firewall identifies the IP of the client responsible for the query which, when combined with NetChange's network discovery, localizes where the IP is connected on the network enabling a quick device cleansing.

Protect Against DNS-Based Malware Across the entire DNS Architecture

SOLIDserver™ DNS Firewall policies can be automatically replicated across the entire DNS architecture, on selected servers, sites or SmartArchitectures assuring overall consistency, decreased cost and improved global security.

DNS Best Practices Application

In addition to protection against malware, there are several DNS principles that must be followed to optimize the security and reliability of DNS servers and DNS architecture. EfficientIP's solution dramatically simplifies the implementation of the following best practices:

Update BIND as often as possible to limit bug problems: EfficientIP releases security patches within 24 hours following the official publication of the update in order to ensure the highest level of security by running the latest version of BIND.These patches are available on EfficientIP's web site and customers are notified via EfficientIP's customer mailing list. SOLIDserver™ is a «one button» update technology, enabling top-tier security for your network and lower administration costs.

Use Forwarders: Forwarders avoid the need for a particular DNS server to do resolution work by pushing the DNS request to another DNS server which handles the request. Forwarders enable the separation of DNS flows within DNS architecture in order to minimize the load on authoritative DNS servers. In addition, authoritative DNS servers can be hidden behind recursive servers to which forwarders transfer DNS requests.

Split authoritative name servers and recursive servers: Authoritative name servers are assigned responsibility for specific domains and are reference points for DNS data validity. As such, it is critical to ensure the integrity of authoritative DNS servers. Splitting authoritative name servers from recursive servers and enabling modifications of authoritative DNS server configurations only directly from other authoritative servers or administrators eliminates all risk of corruption. Authoritative DNS servers are dedicated to only one function with strict policy access for modifications: an authoritative server will NOT cache. In case of DNS recursive server corruption, there will be no impact on the authoritative server.

Restrict recursive queries as much as possible to prevent spoofing: Limiting recursive queries is a fundamental rule when implementing the DNS architecture. This approach limits the risk of malicious requests that may corrupt DNS data or supply DNS architecture information to non-authorized DNS clients.

Use hidden Primary server: Hiding Primary server limits the risk of having the primary server attacked. This point is detailed below (see Stealth DNS architecture below).

ABOUT EFFICIENTIP

EfficientIP solutions address organizations' needs to drive business efficiency through the innovative use of IT. Its unified management framework for DNS-DHCP-IPAM, devices and network configurations enhances security, availability and agility of the IT infrastructure. EfficientIP's solutions have been chosen by hundreds of the most demanding organizations across all industries.
www.efficientip.com

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