efficient iP™

Datasheet

DNS Guardian

Protect Data and Ensure DNS Services Continuity

Highlights:

- Detection, protection and remediation features for DNS cache, recursive and authoritative
- Real-time DNS transaction inspection for advanced DNS analytics
- Behavioral threat detection for accurate decision making
- Granular domain filtering per user for improved application access control
- Adaptive security countermeasures for unequalled service continuity
- Central management of DNS security policies across the entire network
- Advanced DNS statistics for smarter reporting
- Integration with Cisco Umbrella to protect apps, data & users on/off network

DNS service is a mission-critical network component, a fact which has not gone unnoticed to hackers. In recent years, a high pace of attacks targeting DNS servers has been observed (highlighted in EfficientIP's 2020 DNS Threat Survey). The nature of DNS threats is quickly evolving, and attacks have become highly sophisticated based on distributed, multi-vector and multi-stage assault models. Traditional DNS security solutions have proved to be insufficient. Worse still they present high risk of creating false positives. As a result, a new approach to security is required for preventing network outages and potential data theft that could significantly impact a business.

Thanks to innovative technological breakthroughs, DNS Guardian from EfficientIP is the first DNS security solution enabling complete DNS transactions inspection and advanced analytics for real-time behavioral threat detection. Patented smart countermeasures provide unique adaptive security to protect data confidentiality and guarantee unmatched continuity of DNS services, even under the most insidious attacks.

A Hardened Security Framework

DNS Guardian benefits from an architectural innovation that separates the DNS cache from the recursive and authoritative functions to dramatically strengthen and enhance the security of the overall service. When under attack, each function is protected separately regarding its own properties, avoiding side effects and ensuring service availability. DNS Guardian patented countermeasures can be adapted according to each function's specific needs and detected attack, for unequalled protection efficiency.

DNS Transaction Inspection Technology

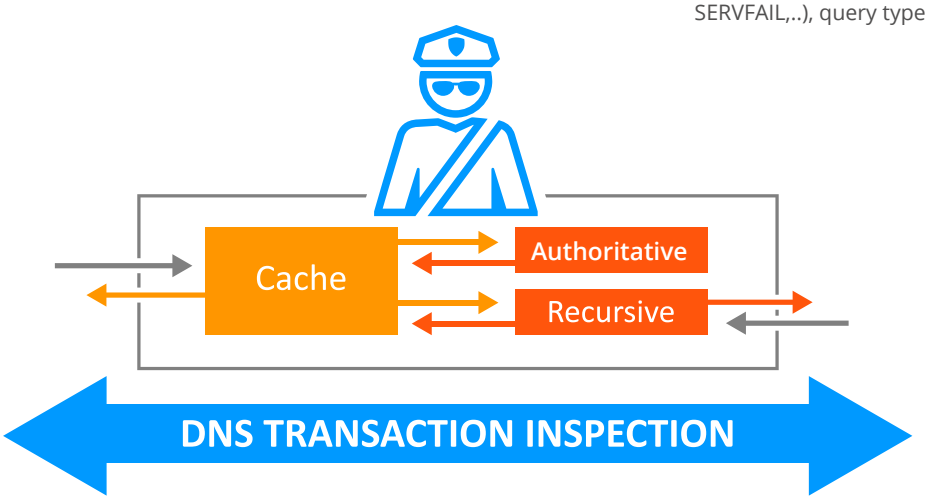
DNS Guardian is the first and unique market solution offering complete DNS Transactions Inspection (DTI), in real-time and without any performance impact. DNS Guardian examines, at the very heart of the protocol, the overall sequences of query exchanges for every single DNS transaction:

- Fragments, Queries and their payload and related answers
- Transaction duration and size

DNS Guardian transaction inspection innovation allows for a complete understanding of the client's context, overcoming limitations of signature-based security systems that only offer limited peripheral traffic visibility. This is key for delivering true DNS analytics and behavioral threat detection capabilities.

Advanced User Identification

DNS Guardian deeply analyzes the client behavior in order to apply appropriate countermeasures when required. Standard client identification is based on the source IP address of the DNS request, but complex topologies require the client to be identifiable from other parameters. DNS Guardian can use the embedded EDNS as identification source rather than the IP address. This allows use cases such as parental control, CG-NAT in telecom networks, and cascading DNS requests from another forwarder.



DNS Guardian Innovative Security Framework

DNS Transparent Proxy

There are situations where DNS requests addressed to specific Internet servers are required to be intercepted in order to provide additional services like filtering, accounting or traffic interception. DNS Guardian can be configured to take into account such traffic, acting as a DNS transparent proxy. Any DNS request arriving at the DNS Guardian will then be analyzed with standard security features and forwarded to the original destination - the answer will be forwarded to the client upon reception. This solution is ideal for global RPZ filtering or deep behavioral client traffic analysis in order to filter or quarantaine malicious IPs.

Central Management of Security Policies

Global Security Policies to be applied on multiple DNS Guardians can be set up from a central GUI. These policies will enforce behavioral threat detection settings and mitigation configuration over the entire network, for unified management of the security mechanisms that leverage and secure DNS components. This capability to simultaneously manipulate a group of servers reduces administration costs and allows fine tuning of thresholds.

Advanced DNS Analytics for Behavioral Threat Detection

In-depth visibility of DNS traffic

DNS Guardian transactional inspection capacity ensures in-depth visibility and accurate understanding of DNS traffic over time. It collects, gathers and stores in real-time the most advanced statistics on a global and per client basis:

- Cache Miss/Hit ratio, malformed requests, fragmentation, recursion time, return code distribution, latency
- DNS bandwidth consumption
- Top list: Clients, requested domains, return code (NX domain, SERVFAIL,..), query type

Multi-factor threat analysis for unequalled attack detection

This unique visibility, coupled with real-time multi-factor traffic analysis (that considers global traffic trends, clients' behaviors and DNS functions performance), ensures unmatched behavioral threat detection based on the most advanced DNS security analytics capacity.

It enhances threat visibility well beyond known attack patterns and quickly outdated blacklist mechanisms, enabling the identification of the most advanced attacks such as DNS tunneling, phantom or sloth domain attacks.

DNS Guardian protects from any of the following attacks:

- Invalid Queries - Analyzing the DNS queries, and dropping those that do not comply with the applicable RFC(s), before they hit the recursive DNS engine

- NXDOMAIN attacks - Analyzing the proportion of nxdomain answers per source IP address. This allows for a more efficient detection and mitigation than any approach based on regular expression pattern matching that pull down a DNS engine's performance

- Random Subdomain / Phantom Domain attacks- Analyzing the proportion of nxdomain and servfail answers per source IP address. This allows for a more efficient detection and mitigation than any approach based on regular expression pattern matching that pull down a DNS engine's performance

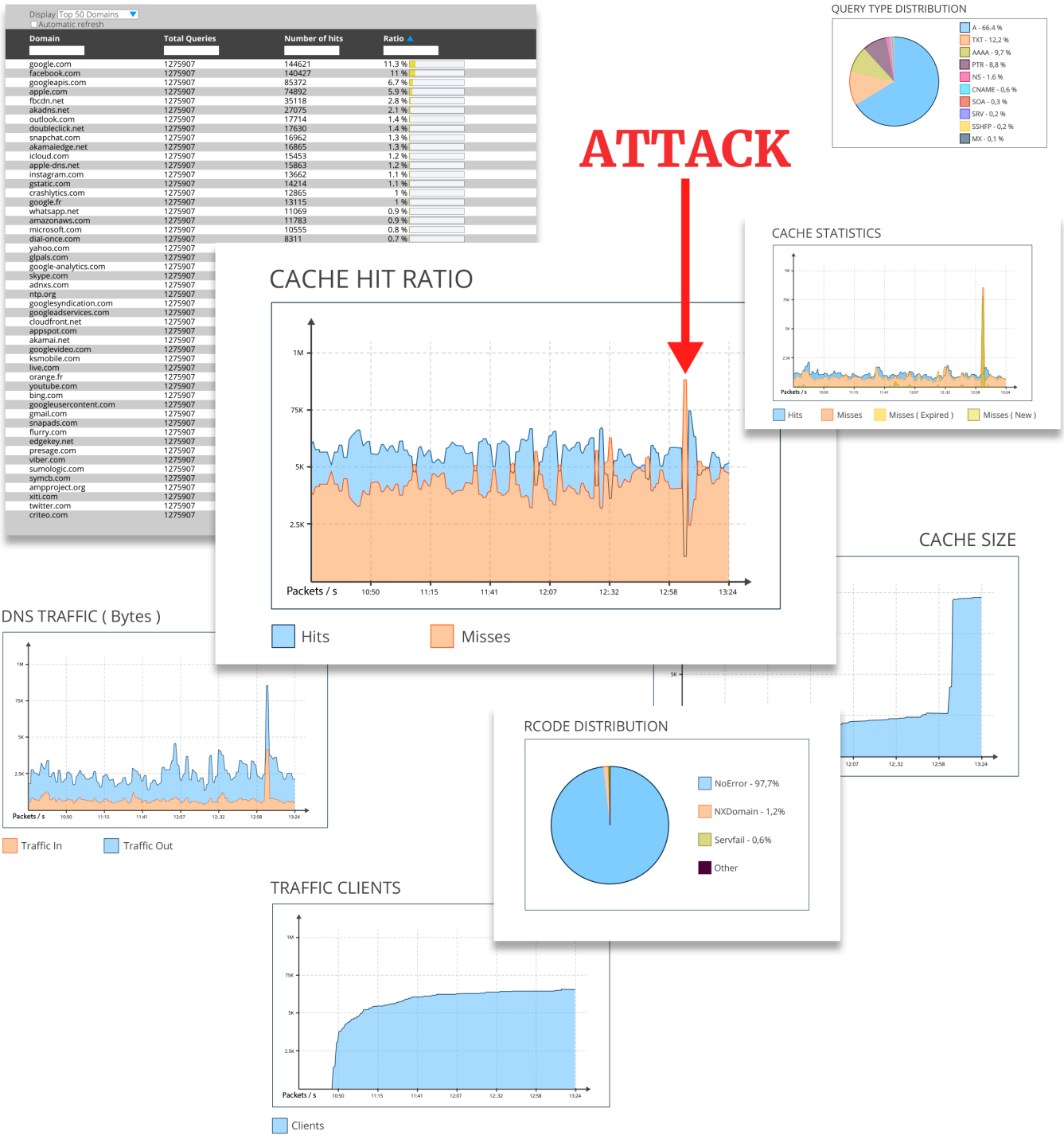
- Sloth Domain attacks - Analyzing the time spent waiting for DNS answers from any domain name server to clients' queries. This allows for the quick identification and isolation of any client generating requests that target any domain name server specially crafted to slow the recursive engine with slow answers

- DNS Tunneling attacks - Analyzing non-cached DNS queries and size. This allows for efficient tunneling detection and prevention, far more so than a pattern-based detection based on a known, potentially outdated reference database

- Cache Poisoning attacks - Implementing support for EDNS DNS cookies and queries source port randomization in combination with a 16-bit cryptographically-secure nonce drastically reduces the probability of successful DNS race attacks. However, only the support of DNSSEC guarantees the validity of any answers provided by signed zones

- Distributed Reflective attacks - Analyzing queries per source IP address rate limiting the query rate (Note: The most effective solution to prevent such an attack is still to avoid source IP spoofing within a network). This allows for the prevention of use of your infrastructure as a reflective vector for any attack

- DNS Flooding - Analyzing the overall DNS traffic performance allows for the isolation of suspicious clients or activation of the Rescue Mode, ensuring DNS cache availability under extreme attack conditions



EfficientIP DNS Guardian Threat Monitoring

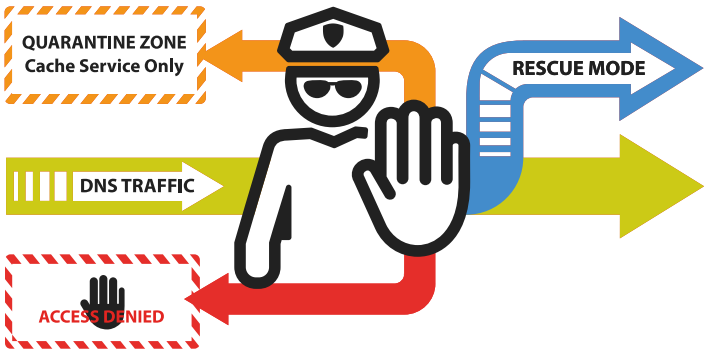
Smart Countermeasures for Adaptive Security

DNS Guardian's advanced analytics provide an unprecedented understanding of DNS threats, offering the opportunity to activate the right countermeasure at the right time according to each specific attack type. EfficientIP's unique adaptive security solution delivers smart countermeasures to protect both DNS services continuity and data confidentiality:

- Block source IPs of the attacks
- Rate Limit DNS traffic per IP source
- Quarantine suspected source IPs of attacks (Patented)
- Activate Rescue Mode: Ensure service continuity even if the attack source is unidentifiable (Patented)

The Quarantine Mode isolates IP addresses with malicious behaviors so that they have unrestricted access to cache data only, while their recursive requests are blocked. This protects the server from the attack and reduces the risk of blocking legitimate clients.

However, under extreme conditions when a source attack is not identifiable (typically in the case of a slow-drip or highly distributed attack), DNS Guardian detects the risk of exhaustion of server capacity and activates the patented Rescue Mode. This exclusive countermeasure ensures that the cached DNS answers remain 100% available to the clients, even if a data validity update is not possible, ensuring 100% accessibility to most critical business applications and services.



DNS Guardian Actions

Upstream DNS Servers Failure

When the global DNS system fails or becomes unreachable because of an internet backbone failure, a recursive DNS engine may not be able to serve a client's recursive DNS queries. As a result, clients end up disconnected from every service, while in fact they may still be accessible, up and running. DNS Guardian intelligence prevents such a situation occurring. When a request is received for a domain present in the cache but expired, DNS Guardian ignores the failure coming from the local recursive engine and responds to the client using the answer stored in the cache with a low TTL value (30 seconds). The benefit is an increased continuity of service during a short external failure, much like Rescue Mode.

Improving Application Access Control

Security is an important topic in DNS traffic handling. The Guardian solution implements DNS firewalling that filters client requests against a list of domains which require to be either denied or authorized depending on the global policy (whitelist or blacklist approach). The firewalling can serve different purposes, from protecting devices and clients against malicious applications to only authorizing selected well known and identified applications for specific devices like IoT, shared devices or industrial equipment.

In addition to the firewalling feature focusing primarily on the application traffic destination, DNS Guardian implements a client oriented approach with the Client Query Filtering (CQF) solution, which helps reduce exposure risk by offering a security barrier controlling app access at the earliest point in flow. With CQF it is possible to apply some more granular filtering lists in the firewall to a group of clients or devices. By mixing lists of clients and lists of domains to authorize or deny, the number of potential use cases is significantly widened. The dynamic nature of the lists used in CQF allows automated scenarios where clients can be added and removed on-the-fly, as well as the domains listed in the DNS firewall. These dynamic updates directly bring improved security to the network. This allows a global security approach within the ecosystem with more control points brought between the client and its application by combining the DNS with other common firewall and IP filtering solutions.

User Experience Improvement

Unequalled cache performance

DNS Guardian implements a DNS cache system that significantly enhances the cache lookup performance. Combined with SOLIDServer™ Blast Appliances, Guardian is capable of reaching up to 17 million queries per second.

Multicast cache sharing

DNS Guardian cache sharing enhances the performance of the overall DNS platform, reducing the amount of recursive queries sent to authoritative servers and reducing the DNS service latency. It relies on an IP multicast mechanism for optimized network usage. Combined with the Rescue Mode and the overall security mechanisms offered by Guardian, this allows for the deployment of highly secure and distributed collaborative recursive DNS platforms, strengthening the overall infrastructure security.

Persistent cache (Restart & Restore)

DNS Guardian allows for the backup of the cache. Existing cache data can therefore be used at restart, allowing for immediate DNS performance recovery. It eliminates the need for the DNS engine to perform recursive queries until its cache is rebuilt, which can lead to excessive load and dramatically impact service performance.

Local DNS traffic ciphering

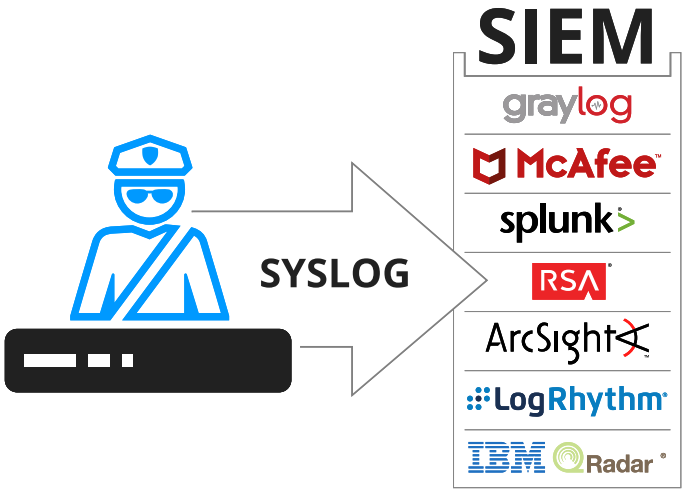
DNS Guardian allows user traffic protection through ciphering by enabling DoT (DNS over TLS). This access method comes in addition to the standard DNS over UDP and DNS over TCP which carry the traffic unciphered. When using DNS over TLS, the traffic is ciphered and access can be protected through digital certificates, which prevents eavesdropping on client DNS requests and therefore their traffic intent. 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.

High Performance Logging Centralization

The DNS is a fundamental network service and valuable data source to be used by network defenders. DNS monitoring has to be part of the security strategy and is key to keeping track of DNS activity for forensic purposes. This could allow for the detection and understanding of suspicious activity such as malware spread, phishing campaigns or any attack that may have compromised an information system in the past without being noticed.

DNS Guardian offers a unique high-performance logging system which doesn't impact the DNS software performance. Asynchronous logging ensures ongoing detailed visibility of transaction history even under volumetric attacks, overcoming the limitation of traditional DNS services. It sustains standard syslog format to comply with existing log management systems. Typical implementations can leverage third party appliances such as Splunk, Graylog, ELK, or any SIEM to collect and analyze this enormous amount of archived data to build advanced traffic analysis reports.

DNS Guardian is part of EfficientIP's unique 360° Security solution designed to protect public and private DNS infrastructures from both internal and external DNS threats, regardless of the attack type.



High Performance Logging Technology

efficient iP™

REV: C-201019

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
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752