efficient iP™
DEFINING SMART DDI

Datasheet

DNS FIREWALL

Protecting and Defending Network Infrastructure Against Malware

DNS is a business-critical network component that ensures the accessibility of almost any connected service. This system is by design an open service to network devices, providing connectivity to any company's public or private IT service. The central and critical role of DNS services has been identified by hackers, and has become a favourite attack vector, especially for malware/APT (91% according to the 2016 Cisco Security Report).

In this current ever-evolving environment where mobile and IoT devices are proliferating, and BYOD is becoming the norm, DNS Firewall from EfficientIP offers a dedicated layer of defense to fill the gap left by traditional security solutions to protect against DNS threats.

DNS Firewall provides advanced DNS query filtering capabilities combined with dynamic threat intelligence feeds that allow for the quick identification of suspicious device activity, preventing malware infection and spread within a network, as well as phishing campaigns and data exfiltration attempts.

Highlights:

- Active blocking of DNS traffic to malicious destinations
- Automated threat intelligence to adapt protection to ever-evolving threat landscape
- Proactive protection against malware
- Phishing prevention
- Data exfiltration risks mitigation
- Infected device identification and location

DNS Response Policy Zones

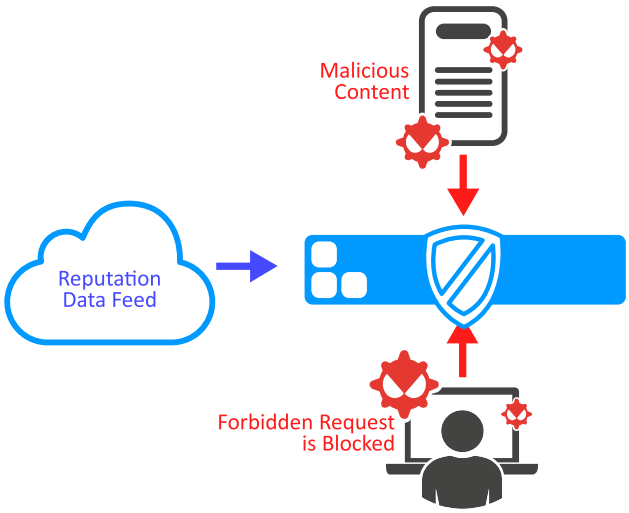
Domain Name Service Response Policy Zones (DNS RPZ) is a mechanism implemented in all modern recursive DNS engines. It allows for dynamic modification of DNS answers obtained from the global Domain Name System, and provides alternate answers to any DNS query. This mechanism is leveraged within DNS Firewall to permit DNS administrators to define the precise filtering and redirecting rules applied on DNS traffic according to:

- A queried domain name
- A queried NameServer (NS)
- An IP address, resulting from a computed DNS query

This allows for the application of different policies based on traffic type:

- Redirection to another CNAME or IP address
- Reply with non-existent domain (NXDOMAIN)
- Reply with no-data (NODATA)
- Force TCP
- Passthru
- Drop

EfficientIP's DNS Firewall solution brings an additional security layer to complement an existing network security solution. The latter offers limited performance when filtering access according to anything other than IP addresses and static flow characteristics, such as protocol and ports. Whilst NG Firewalls offer various functionalities, these are unfortunately limited to ensuring performance, as these devices deal with huge amounts of heterogeneous traffic. On the contrary, DNS Firewall is specialized in preventing IP address resolution process for any known malicious domain, inhibiting any connection to the associated IP addresses.



Threat Intelligence Data Feeds

The best way to protect a network infrastructure and its users against phishing and malware campaigns is to prevent any connection to known malicious services that are used to steal credentials, or deliver the initial infection payload of malware. However, maintaining appropriate filtering rules regarding known malicious domains is difficult because of the dynamic property of the threat. Attackers use several, often randomly generated domains (using DGAs-Domain Generating Algorithms) to control their botnets and leverage the huge amount of poorly secured servers to run their activities. Relying on a dynamically-updated filtering rule repository that can be extended through a customized filtering policy is the most sustainable solution.

SOLIDserver™'s DNS Firewall comes with this kind of dynamic data feed built from various distributed sources. It aggregates reports of suspicious activity from identified IP addresses or domains such as MailSecurity, PhishTank, OITC and PhishLabs. The provided lists offer various filtering combinations based on the following lists' categories:

- Abuse and spam
- Phishing
- Malware
- Cracked websites

Ensure Proactive and Efficient Protection Against Malicious Use of DNS Services

Phishing Prevention

Criminals leverage phishing attacks to lure the unsuspecting into visiting a compromised web service or pushing the user to download malicious software, expressly to steal sensitive information. Relying on threat intelligence services allows SOLIDserver™ DNS Firewall to automatically prevent users from accessing such abused web services, even when they use their own device within the corporate network. This significantly reduces the risk of personal data theft from users, who are misdirected to provide their credentials using fake malicious applications.

Containing Malware Spread and Data Exfiltration

Malicious software is well known to be designed for disrupting system operations, gathering sensitive information, gaining access to private infrastructure, ransoming users, or displaying unwanted advertising. As soon as a system establishes an internet connection it becomes exposed to malware attacks. Considering the current threat landscape and the augmentation of the attacks, preventing the spread across a network has become an urgent priority.

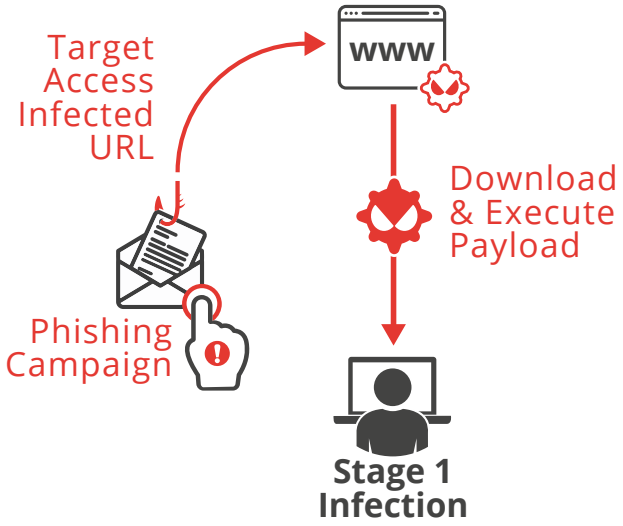
Existing security solutions cover a wide range of possible attack vectors such as:

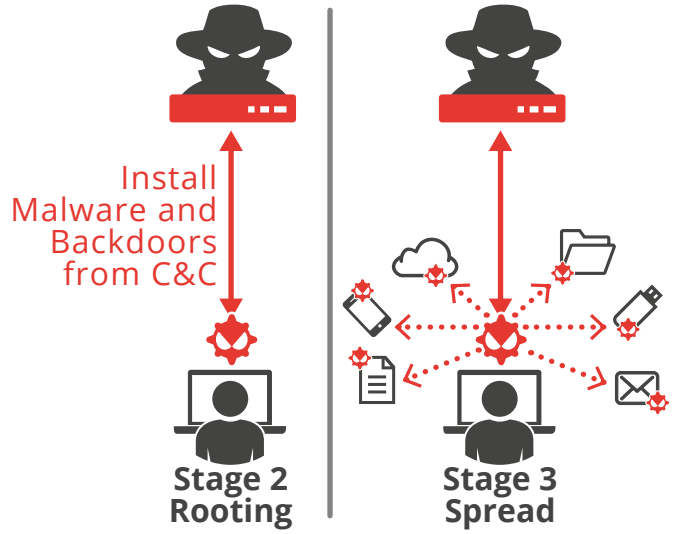
- Email malware attacks, which are generally mitigated using anti-spam filters
- Web page/download malware attacks, which are generally mitigated using web gateway anti-virus
- File sharing malware spread, which are generally mitigated using anti-virus

They lack the ability to identify threats coming from unmanaged network devices and specially-crafted attacks that don't match existing threat patterns. SOLIDserver™ DNS Firewall prevents the initial malware infection of a device by blocking the suspicious queries that would otherwise redirect a user to domains and IP addresses identified as related to malicious activities, independent of the traffic pattern.

It also reduces the offensive capabilities of any malware that would already have infected an existing 'connected but mobile' device such as a laptop, tablet or mobile phone. It does so by blocking the communications with known Command and Control servers in order to avoid malware updates, remote control and most data exfiltration attempts.

Even more advanced protection can be achieved by combining DNS Firewall with DNS Guardian. The latter product leverages real time DNS Traffic Inspection (DTI) and behavioral malicious activity detection, triggering automatic and adaptive countermeasures when necessary.





This mitigates the most advanced DNS tunneling techniques, and proactively protects any recursive DNS engine against any type of DNS attack, securing the accessibility of every application of an information system.

Identify Infected Devices

Containing a threat is not just about blocking the traffic and isolating a contagious agent. It requires quick intervention on the infected device in order to analyze and treat the infection.

Relying on appropriate logging policies, DNS Firewall allows for the quick identification of any IP address originating the detected suspicious queries. Combining this with an IPAM and its associated network discovery tool permits the fast localization of infected devices for immediate remediation.

Advanced Threat Reporting

Combining the SOLIDserver™ logging capabilities with any existing event manager (or SIEM - Security Information and Event Manager) allows for easy exportation of DNS Firewall logs in standard syslog format. This in turn allows for the execution of advanced analytics on the suspicious DNS traffic, and generates appropriate reports using either custom models or any available plugins compatible with the deployed solution (for instance Splunk or Graylog).

DNS Firewall 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.

efficient iP™

REV: B-1708

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