INFRASTRUCTURE PROTECTION
SOLUTION DESIGN

Infoblox Solutions

1. Infoblox can differentiate between "good" DNS traffic and malicious DNS traffic such as (D)Dos. This enables Infoblox to maintain performance in answering legitimate queries whilst actively rate limiting or dropping the malicious traffic. Availability can be enhanced with support for both HA and Anycast DNS.

   The solution can be extended into the cloud with support for AWS and Azure. In addition, 3rd party cloud-based secondary services can also be utilized to further enhance the capacity where appropriate.

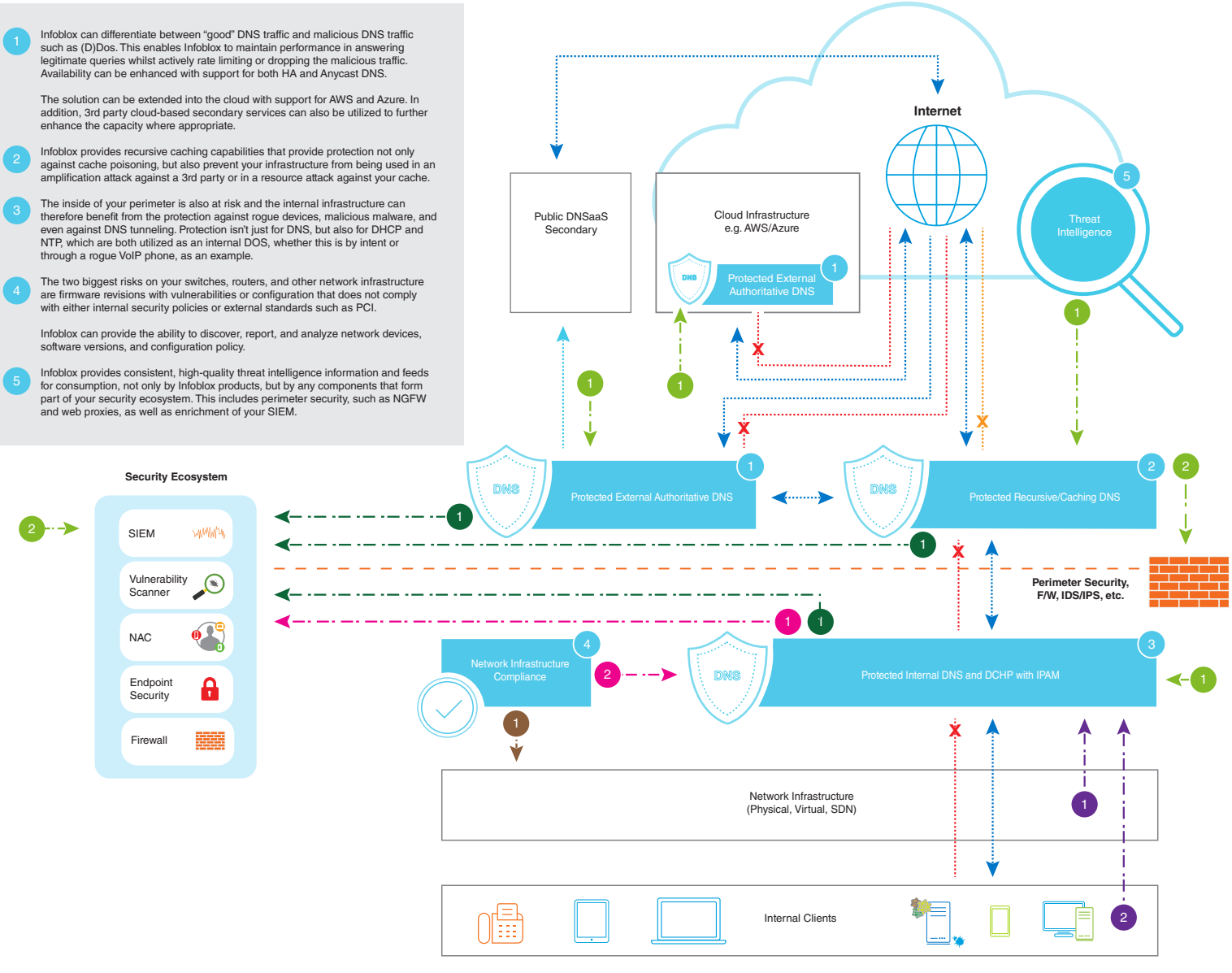
2. Infoblox provides recursive caching capabilities that provide protection not only against cache poisoning, but also prevent your infrastructure from being used in an amplification attack against a 3rd party or in a resource attack against your cache.

3. The inside of your perimeter is also at risk and the internal infrastructure can therefore benefit from the protection against rogue devices, malicious malware, and even against DNS tunneling. Protection isn't just for DNS, but also for DHCP and NTP, which are both utilized as an internal DOS, whether this is by intent or through a rogue VoIP phone, as an example.

4. The two biggest risks on your switches, routers, and other network infrastructure are firmware revisions with vulnerabilities or configuration that does not comply with either internal security policies or external standards such as PCI.

   Infoblox can provide the ability to discover, report, and analyze network devices, software versions, and configuration policy.

5. Infoblox provides consistent, high-quality threat intelligence information and feeds for consumption, not only by Infoblox products, but by any components that form part of your security ecosystem. This includes perimeter security, such as NGFW and web proxies, as well as enrichment of your SIEM.



Key

- Good DNS Traffic
- Bad Traffic
- Cache Poisoning
- Zone Transfer

Communication Flow

Threat Intelligence

1. DNS-related threat intelligence and rulesets
2. Threat data feeds for use across the security ecosystem, including SIEM, NGFW, proxies, etc.

Actionable Intelligence

1. Security events with context such as syslog messages and outbound API notifications

Data Enrichment

1. IP information in the security ecosystem can be enriched from the authoritative IPAM to provide data such as switch port and user information
2. Discovered network, location, and attached endpoint information used to enrich IPAM data

Network Discovery

1. Infoblox can discover the network infrastructure devices and associated interfaces
2. Endpoints attached to the network can be discovered, including their location on the network to enrich IPAM data

Network Infrastructure Compliance

1. Ensure the compliancy of firmware, device supportability, and network configuration

3111 Coronado Drive, Santa Clara, California 95054, USA | 1.866.463.6256 (Toll-free, U.S. and Canada) | sales@infoblox.com | www.infoblox.com |