**Product Summary**

The Infoblox DNS Firewall delivers a new layer for defense-in-depth security strategy to protect business networks from advanced malware and attacks that use DNS to communicate with command-and-control (C&C) sites and botnets in order to spread malware and exfiltrate data. DNS Firewall complements industry-standard layers of security such as next-generation firewalls (NGFWs), intrusion prevention and detection systems (IPSs and IDSs), secure web gateways (SWG), endpoint security, network access control (NAC), and data loss prevention (DLP), which are specialized to solve other problems and do not integrate with DHCP and IP address management capabilities to help pinpoint infected devices (also known as endpoints). Because no single security solution will address all threats, Infoblox leverages partnerships with leading security vendors to share security event and network context data. We are flexible in terms of how we share data with other security technologies: REST API, STIX/TAXII, and custom/third-party protocols such as Cisco pxGrid. Regardless of which method is used, the goal is the same—to help customers enhance their risk mitigation efforts by providing them with actionable network and security context. By integrating with or working alongside many commonly used security technologies—without requiring additional network infrastructure—DNS Firewall serves as an important security layer that helps organizations stay ahead of advanced attacks early in the cyber kill chain, prevents the lateral spread of malware in the network, and enables them to take action on devices that are already infected.

**Infoblox DNS Firewall**

DNS Firewall is the leading DNS-based network security solution that protects against advanced malware and attacks that use DNS to communicate with C&C sites and botnets to spread malware and exfiltrate data. DNS Firewall works by employing DNS Response Policy Zones (RPZs), timely threat intelligence, and optional Infoblox DNS Threat Analytics to prevent data exfiltration. Through collaboration with Infoblox DHCP, IP address management, and Reporting and Analytics solutions, DNS Firewall provides valuable information to help pinpoint infected devices for remediation. Furthermore, it integrates with Infoblox Identity Mapping for capturing the user name tied to an infected device.

Advanced malware uses a multitude of applications and protocols (e.g. HTTP, IRC, FTP, VoIP, RPC, SIP, SSH, Telnet) to make requests to bad domains that are using fast-flux to rapidly change the IP addresses of domains to get around security layers such as NGFW, IPS, IDS, SWG, endpoint security, and DLP solutions. Hence, DNS Firewall adds a layer of defense to remove the DNS protocol as a conduit for APTs and data exfiltration.

Infoblox's specifically designed threat intelligence service compiles and correlates bad domains and IP addresses (as well as geographic blocks for designated countries such as China and the Ukraine) that can be applied globally in RPZ policy, leveraging feed data from multiple public and private resources all over the world. Infoblox delivers a best-of-breed reputational feed that enables the setup of just a single RPZ on a DNS Firewall server, which simplifies reporting and management.

Furthermore, Infoblox is the industry's first and only DNS, DHCP, and IP address management (DDI) vendor to seamlessly integrate DNS Firewall with leading security solutions such as FireEye and Carbon Black and exchange valuable security event information with NAC solutions such as Cisco Identity Services Engine (ISE) to automate security response and quarantine infected endpoints.

Many security strategies today are designed to only be proactive in nature. Uniquely, DNS Firewall is both proactive and reactive. In addition to proactive defense-in-depth strategies, many companies are now building incident-response policies and security layers that will help prevent the proliferation of infections and drastically reduce associated data loss. DNS Firewall can have a major, immediate impact on an organization's incident-response plan by preventing communication from the infection to outbound sources. This can virtually eliminate concerns of an infection's impact on an environment and can assist in pinpointing the infected device for swift quarantine and remediation.
Next-generation Firewalls
NGFWs are multipurpose security appliances that provide application-layer firewall, VPN, NAT, and possibly web filtering and UTM functionality. NGFWs are not DNS-based network security solutions.

Because DNS Firewall is integrated with the Infoblox DNS server, it can easily identify domain names associated with malicious domain registrars and can thereby disrupt device communications to those domain locations. DNS Firewall blocks threats at their source by simply not allowing communications of a device with a malicious destination—instead of relying on another network element such as the firewall to block and then having to worry about topology and scaling of that element.

Essentially, DNS Firewall can be implemented in the form of a dedicated DNS appliance that is part of the highly scalable Infoblox Grid™ distributed database architecture, versus having to deploy a large firewall at the network edge that must effectively handle multiple types of traffic, including DNS, at scale.

Intrusion Prevention and Detection Systems
IPSs and IDSs typically inspect network traffic passing through frontline security devices, such as firewalls, SWGs, and email security gateways, for malicious activity. They detect malicious traffic via several methods—signatures, protocol anomaly detection, behavioral, or heuristics. IPSs and IDSs typically must build a knowledgebase of malicious network traffic and associated malware signatures before they can start blocking such traffic in the network. Building the knowledgebase of malicious network traffic takes time, and given the dynamic nature of malware and the applications and protocols used, outward-bound traffic such as DNS queries to bad domains (with or without small payloads) will likely be resolved, and the victim device will become infected with malware, exposing the network to further infection and possibly data exfiltration.

Specifically with IDSs, which are out-of-band, by the time malicious traffic is blocked, sensitive data may already have been exfiltrated. Also, IPSs and IDSs cannot detect attacks disguised within encrypted communications.

Because malware uses the DNS protocol to resolve the IP address of the domains it is seeking connectivity to, bad networks use rapid fast-flux change to quickly create unique combinations of IP addresses and new domains. This means that many combinations will not be identified as bad by an IPS or IDS solution, and traffic will pass through misclassified.

Furthermore, IPS and IDS solutions do not have integration with DHCP (IP address leasing) or IP address management, so they cannot pinpoint infected devices by MAC address for remediation.

Secure Web Gateways
SWG is a web access gateway that protects web-accessing devices (laptops, BYOD, mobile) from infection and enforce corporate web security policies. Typical SWG solutions filter unwanted software and malware from user-initiated web/Internet traffic and enforce corporate and regulatory policy compliance. SWG products include URL filtering, malicious-code detection and filtering, and application controls for popular web-based applications, such as instant messaging (IM) and Skype.

SWG focuses on web-based application traffic originating from internal devices. Therefore, malware using Internet-based applications such as FTP, VoIP, RPC, SIP, SSH, and Telnet is neither tracked nor reviewed by the SWG and will pass through unfettered. Even though SWGs can be used to proxy DNS requests and cross-check domains against a blacklist, this approach does not account for fast-flux changes. Also, the major SWG vendors create their own blacklists based on information from their customer installed base only, which makes for a myopic view of the threat landscape.

Lastly, SWGs do not have integration with DHCP or IP address management for a granular view of infected devices (by IP or MAC address) and, therefore, do not provide assistance in remediation.
Endpoint Security

Endpoint security solutions protect against malware by running a monitoring agent on every endpoint that connects to the corporate network and enforcing policy on the endpoint to take an admin-defined action (quarantine device, kill process on the device that is responsible for malware, etc.). However, these solutions don't have visibility into devices that may already be infected with malware. In particular, they cannot detect malware that uses DNS to call home to the C&C server. Also, if certain endpoints lack an agent altogether, then it is nearly impossible to detect malware callbacks unless the DNS server itself is able to detect and intercept it. Infoblox complements endpoint security solutions by providing an added layer of defense, a DNS Firewall, that detects advanced malware and attacks that are exploiting DNS, essentially sharing this information or indicator of compromise (IoC) in real-time with endpoint security and endpoint threat detection and response (ETDR) solutions to enhance their ability to quickly respond and contain threats. Also, DNS Firewall provides contextual data on infected devices (e.g. IP address, MAC/DUID, host name, threat severity, and policy state) that can aid with remediation.

Network Access Control

NAC solutions are focused on controlling network access by using policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. Infoblox DNS Firewall detects malware and advanced attacks that are exploiting DNS, and can share this IoC in real-time with NAC, to enhance its ability to quickly take remediation action (e.g. quarantine device, enforce firewall policy to block infected endpoint from connecting to Internet until it has been cleaned up, etc.). Also, DNS Firewall provides contextual data on infected devices (e.g. IP address, MAC/DUID, host name, threat severity, and policy state) that can aid with remediation. Conversely, DNS Firewall can receive user identity and network privilege information from NAC. This contextual data can be appended to associated events in Infoblox to provide the additional context of the user and network-access level, so that analysts can better understand the significance of either a security or IP address management event.

Data Loss Prevention

While data loss prevention (DLP) solutions help protect against data leakage via email, web, ftp, and other vectors, those solutions don't have visibility into DNS-based exfiltration. Infoblox helps prevent DNS-based data exfiltration with DNS Threat Analytics, an add-on for DNS Firewall. Infoblox DNS Threat Analytics complements traditional DLP solutions by closing the gap and preventing DNS from being used a back door for data theft.

Completing Your Network Security by Protecting Your DNS

DNS Firewall can play a critical role in your defense-in-depth security approach. Next-generation firewalls, incident prevention and detection systems, secure web gateways, endpoint security, network access control, and data loss prevention solutions provide important protection, but they don't deliver DNS services and therefore cannot disrupt DNS communication to botnet and C&C domains; they do not offer advanced streaming analytics for detecting data exfiltration; and they have no integration with DHCP or IP address management to leverage for reporting on infected devices for remediation.

Contact us today and find out more about how Infoblox DNS Firewall mitigates malicious communications and data exfiltration attempts and assists in speeding remediation by pinpointing infected devices.