Infoblox DNS Firewall

Infoblox
CONTROL YOUR NETWORK

Product Summary

With the Infoblox DNS Firewall, companies can now comprehensively protect against DNS-based malware:

- **Proactive:** Stops clients from becoming infected by going to a malware website and identifies infected clients for cleanup.
- **Timely:** Leverages comprehensive, accurate, and current malware data to detect and resolve malware weeks to months faster than in-house efforts.
- **Tunable:** Allows definition of hierarchical policies – DNS, Malware, and others – that maximize the usefulness of the Malware reputational data feed in the customer's unique environment.

Proactive Protection Against DNS-based Malware

DNS-based Malware – Too Dangerous To Ignore

Statistics from McAfee show that over 7 million new malware threats were detected each quarter in 2012. A 2012 Verizon study indicated that 69% of the successful corporate breaches leveraged malware. Further, 92% of data breaches were discovered by an external party rather than the impacted organization.

Of the various types of malware, DNS-based malware is perhaps the most dangerous. It is often directed to steal customer and /or sensitive corporate information over an extended period of time. As more and more end users bring their own devices (such as smart phones and tablets) to work, malware is able to sidestep outward-facing corporate protective measures such as firewalls. Further, as communications are made using the DNS protocol, existing IP-based malware protection technologies are circumvented.

Proactive and Disruptive at the Same Time

Infoblox is leveraging our market leading DNS technologies into industry's first true DNS Security solution. The Infoblox DNS Firewall protects against DNS-based Malware by proactively preventing clients from becoming infected and by disrupting infected clients' ability to communicate with the Botnet master controller.

How the Solution Works

As shown in Figure 1, the solution works as follows:

1. When the Infoblox experts detect a new malware, the Infoblox Malware Data Feed immediately sends the fix to our customers.
2. Either directly or by leveraging the Infoblox GridTM, the updated data is sent to all Infoblox recursive DNS servers in near real time.
3. If an end user clicks on a malicious link or attempts to go to a known malware website, the attempt will be blocked at the DNS level.
4. The session will be redirected to a landing page / walled garden site defined by the company administrator.
5. For clients that are infected already, very typically user-owned devices, the infected client will attempt to use DNS commands to communicate with the botnet master controller. The Infoblox DNS Firewall will disallow these communications, effectively crippling the Botnet.
6. All activities are written to industry-standard Syslog format so that the IT team can either investigate the source of the malware links or cleanse the infected client. Data is also fed to the Infoblox Trinzic Reporting for analysis and reporting.

Infoblox DNS Firewall

Benefits

- Minimizes Your Business (including Legal) Exposure: The Infoblox DNS Firewall is a premium approach to combatting Malware that provides the maximum protection for your business, your partners, and your customers.
- Minimizes Resources Spent on Malware Defense and Remediation: The solution stops threats in their tracks before they ramp and ensures that all infected clients are identified for cleansing, even user-owned smart phone and tablet devices.
- Builds Malware defense into your IT systems and processes: After setup, no manual intervention is needed for 24x7 protection. Logs and Reporting provide a full audit trail as well as lists of infected clients suitable for inclusion into IT task queues.

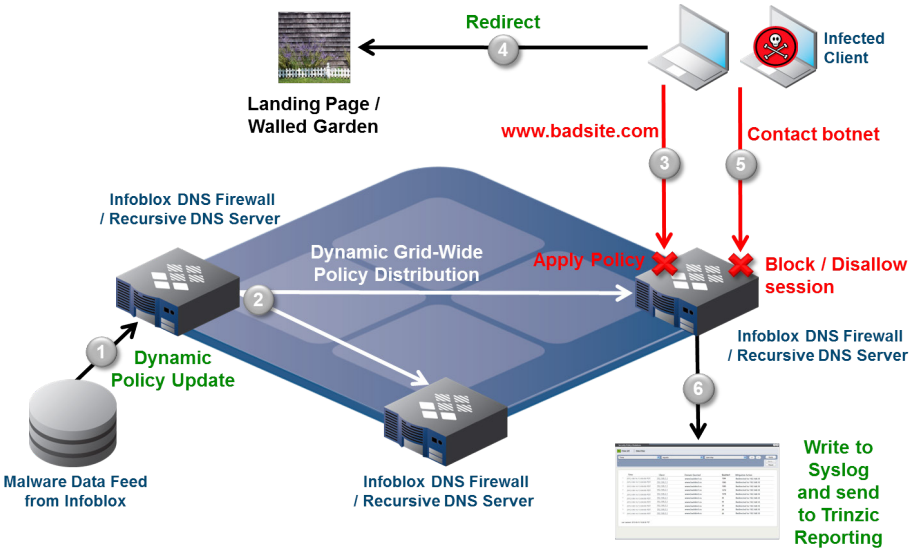

Figure 1: The Infoblox DNS Firewall provides comprehensive protection against DNS-based malware

Why the Solution is Unique

The Infoblox DNS Firewall provides differentiating capabilities to Security and Networking organizations in terms of being Proactive, Timely, and Tunable.

Proactive

The Infoblox DNS Firewall stops clients from becoming infected by going to a malware website or clicking on a malicious link. Further, 'hijacked' DNS Command and Control requests are not executed to prevent the botnet from operating. Lastly, all malware activities are logged and reported to pinpoint infected clients and attacks.

Timely

The Infoblox DNS Firewall leverages comprehensive, accurate, and current malware data to detect and resolve malware weeks to months faster than in-house efforts. The robust data provided by Infoblox is comprehensive in terms of including all known attacks and very accurate in terms of a very low false positive rate. Automated distribution maximizes response timeliness from Infoblox throughout your Grid in near real-time.

Tunable

The solution is tunable to ensure that all threats can be countered in the customer's unique environment. The solution allows the definition of hierarchical DNS, NXDOMAIN Redirection, and Malware policies that maximize flexibility. You also have full control over which policies are enforced by each recursive DNS server. The Infoblox Malware Data Feed includes several options that enable the precise matching of data, including geography, to the threats encountered. In addition, the Infoblox Data Feed can also be combined with multiple internal and external reputational data feeds.

Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.

US Headquarters: +1.408.986.4000 info@infoblox.com EMEA Headquarters: +32.3.259.04.30 info-emea@infoblox.com www.infoblox.com