DNS Firewall vs. Do-It-Yourself

Infoblox
CONTROL YOUR NETWORK

Executive Summary: DNS Firewall enables businesses to quickly implement a new layer of security in a defense-in-depth strategy protecting largely unprotected DNS-based Internet infrastructure. A separate 'Do-It-Yourself' DNS Firewall solution could be implemented by an experienced IT staff but would take considerable time expertise and resources, deliver less protection and would not enable IT to quickly remediate infected devices.

Infoblox DNS Firewall

DNS Firewall, an application that is integrated with the Infoblox DNS Server, provides a strong new layer of security by actively disrupting malware communication to domains and IP addresses of botnet Command & Control (C&C) servers. Utilizing Infoblox DNS, DNS Firewall, DHCP, and IP Address Management along with Infoblox Reporting Server, IT has continual access to reports showing those devices generating DNS queries to malicious botnets and C&C servers by IP and MAC address for remediation. DNS Firewall is kept up to date on malicious domains 24 x 7 with a malware data feed service that includes blocking of IP addresses on a geographic basis to protect businesses against the rapidly changing security threat. Infoblox backs DNS Firewall with field support, 24 x 7 technical support and extensive documentation.

Do-It-Yourself DNS Firewall

Some IT staffs will try to replicate DNS Firewall services with a separate do-it-yourself (DIY) solution based on BIND and a third-party threat feed service and hardware (physically or virtually resourced). While this can be done, there are costs, risks and reduced functionality with a do-it-yourself approach. A DIY DNS Firewall implementation takes a significant amount of expertise and time to do the following processes. An IT group with an extensive background in Linux and networking could spend weeks working through setup, configuration, testing and documentation and still not produce a platform that meets reliability or performance requirements.

DIY - Increased Hard and Soft Costs

In any DIY project there are added costs and complexity that are often overlooked or underestimated. For a DIY DNS Firewall, the activity list for getting such a project started is listed below.

Hard Costs	Soft Costs
1. Hardware – CPU/memory/storage/rack space costing 2. VMware License(s) a. HA resource planning & allocation 3. IP address and network ports 4. Increased power consumption and cooling costs	1. Setup/Configuration@ a. Linux OS installation/configuration b. BIND installation/configuration c. DNS Firewall installation/configuration d. Reputational feed configuration e. DNS Firewall reporting (correlate DNS requests to IP address) 2. Testing a. BIND b. DNS Firewall c. DNS Firewall reporting 3. Documentation a. Linux OS configuration b. BIND configuration c. DNS Firewall configuration d. Reputational feed configuration e. DNS Firewall reporting 4. On-going maintenance (patching) 5. Self-support

@ - Dependent on having right personnel who can do setup/configuration, testing, on-going maintenance, and self-support.

DNS Firewall vs. Do-It-Yourself

Infoblox
CONTROL YOUR NETWORK

Below is a quick table that calculates the time differences between implementing Infoblox DNS Firewall and building a DIY DNS Firewall using BIND. To calculate the time in business days, simply divide the total hours by eight (8). To tally soft costs of DIY, simply multiply the average of the low and high numbers in the totals by the hourly cost of IT staff members (fully loaded).

	Availability of CPU / IP address (physical / virtual)	Software Installation & configuration	Reputational Feed Setup	Reporting Setup on 1 RPZ/Feed	Documentation (write/verify)	Totals (does not include maintenance)
DNS Firewall	0 Hour#	1 hour*	0.5 hour	0.5 hour	1 hour	3 hours
DIY DNS Firewall	24 – 36 hours	48 – 72* hours	2 hours	40 – 60 hours•	24 - 36 hours	138 – 206 hours

 # - DNS Firewall resides within DNS Server. About a 15% impact on DNS server CPU resources.

** - Assuming no mistakes made. Errors and incorrect choices will increase installation/configuration time by 2x-3x.*

▪ - High-availability planning and configuration included.

• - Data from DNS Firewall server would need to be captured, separated (good queries from queries to bad domains) and compiled. If second or third feed service is required, then data collection/reporting processes must be created for each additional feed service. Any changes (e.g. reporting tools, network infrastructure, and DNS upgrades) could potentially disrupt configurations which would require troubleshooting, correction, testing, and documentation changes.

Please note that for the DIY DNS Firewall, time consumption for ongoing maintenance and self-support are not included. These activities can easily add six to eight hours per month (average) for an experienced Linux administrator.

Also, given that DIY DNS Firewall (based on BIND) is stand-alone solution and not integrated with IP address management or DHCP, any reporting created for the DIY DNS Firewall application would be able to show a number of queries for certain domains and actions taken but that would be it. It would not be able to provide the IP address of the device initiating the DNS query. This means that IT staff will have to use other applications to try to correlate which device is infected and making the bad DNS queries. When Infoblox DNS Firewall is integrated with a Trinzic Reporting Server, IT knows exactly which device has a lease by IP address or MAC address and which to go to for remediation. One can invest an hour or less locating the device and starting remediation with Infoblox DNS Firewall, or spend between eight and 12 hours digging through logs to locate the infected device with a DIY DNS Firewall.

Infoblox DNS Firewall Malware Data Feed – Keeping up with a changing worldwide threat landscape

For any DNS Firewall to deliver protection (e.g., blocking DNS queries to botnets and C&C servers), it must be continually updated with fresh threat information on bad/malicious domains located throughout the world.

Infoblox designed its malware data feed service to compile and correlate 'bad' domains and IPs (as well as blocking by geography - e.g., China, Moldova) on a global basis from 35-plus public and private resources all over the world. By combining data from a multitude of sources, Infoblox delivers a 'best of breed' reputational feed that enables the setup of just a single response policy zone (RPZ) on a DNS firewall server, which simplifies reporting and management.

In a DIY scenario, a single feed from any vendor is at best going to provide limited coverage of existing botnets and C&C servers that the Infoblox feed addresses and won't support geographic blocking. If it is determined that another feed is required to meet malware or geographic blocking requirements, additional feeds require corresponding RPZs to be configured as the BIND RPZ technology does not have the capability to combine feeds from disparate sources into a single RPZ. This creates creeping complexity in setup/configuration, management, and reporting, which increases costs and operational risk.

DNS Firewall vs. Do-It-Yourself

Infoblox
CONTROL YOUR NETWORK

A strong link in the Infrastructure chain

Security attacks perpetrated on or using DNS and other central IT services can be easily executed if the hardware and software of the solutions are not security hardened. The international industry standard for the securing of IT infrastructure is Common Criteria, which confirms the development, manufacturing and shipment of hardened hardware and software to strict standards. Many common network devices (e.g., firewalls, routers and switches) have been certified for Common Criteria at some level.

Infoblox recently completed a two-year process for Common Criteria (Level 2) certification for its DNS, DHCP, and IPAM (DDI) applications and hardware platforms. Infoblox worked extensively with a compliance verification agency to make changes and develop processes to adhere to strict Common Criteria standards. Going forward, Infoblox DDI and other products will meet Common Criteria standards to ensure a strong link in the infrastructure chain and to help our customers reduce risk. The Infoblox Common Criteria certification can be found at: *http://www.niap-ccevs.org/st/vid10465/*

Implementing DIY DNS Firewall hardware and software is possible but daunting. For a DIY DNS Firewall to be in production in a hardened form, two steps would have to be taken. First, the hardware platform would have to minimize access points (e.g. disable USB ports). Second, the Linux OS would have to be stripped down without compromising reliability or affecting certain applications. Each time the DIY DNS Firewall server is patched, IT personnel will need to review and confirm the hardened configuration has not been breached and if it has, perform remediation. Meeting any Common Criteria standards (level 1 or 2) for DIY-created infrastructure is impossible and may be a point of contention with external auditors or upper-level management in the event of a security breach.

Summary

A hardened and reliable DNS Firewall is a logical choice for removing the DNS protocol as a communication path for malware as well as preventing malware from using other protocols if that communication is mediated by DNS. Infoblox DNS Firewall delivers superior functionality, reduced costs, risk and complexity over a DIY DNS Firewall based on BIND and a third-party feed. Infoblox DNS Firewall will start disrupting malware communication and block exfiltration of your data within a few hours and enables IT to quickly remediate infected devices with identification of IP and MAC addresses. Infoblox DNS Firewall brings the added benefit of being part of a Common Criteria Level 2-certified solution that helps IT meet corporate, industry, or regulatory compliance. A DIY DNS Firewall would at best block a reasonable percentage of malware-based DNS queries but would not assist IT in remediation of infected devices. Additionally, the overhead of creating and maintaining a DIY DNS Firewall would require significant resources which may not be available or could be better spent on new projects or initiatives.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com