SOLUTION NOTE

Protect Against the Widest Range of DNS Attacks and Raise Network Reliability to the Next Level

SUMMARY

With Infoblox Advanced DNS Protection (ADP), you can defend your network against the widest range of external and internal DNS-based threats, such as volumetric attacks, NXDOMAIN, exploits and DNS hijacking. Unlike approaches that rely on infrastructure overprovisioning or simple response-rate limiting, Infoblox ADP intelligently detects and mitigates DNS attacks while responding only to legitimate queries. Moreover, it is the only solution fully integrated with DDI that can automatically protect the DNS server against new and evolving threats without the need to deploy security patches. Our solution is purpose built to protect against DNS-based attacks from within targeted DNS servers. With it, your network is always up and running for core network services, enabling you to achieve a new level of reliability.

Continuously Block New and Evolving DNS Attacks While Responding to Legitimate Requests

DNS servers are mission-critical infrastructure, and they must continue to respond to queries even when they are under attack. If your external DNS server goes down, your entire network is shut off from the Internet. According to leading security reports, DNS is the number one targeted service for application-layer attacks and the number one protocol used in reflection/amplification attacks. Neustar estimates the cost resulting from a distributed denial of service (DDoS) attack carried out through DNS to be upward of $100,000 an hour, not including customer defection and damage to brands.

Attackers look for the weakest links in your network, and the DNS protocol is easy to exploit. As a result, attacks are on the rise that bring down DNS servers and consume network bandwidth—or interfere with or shut down critical IT applications such as email, websites, VoIP, and software as a service (SaaS). Another common threat is DNS hijacking, which compromises the integrity of DNS.

Infoblox delivers the widest range of protection on the market for guarding your mission-critical DNS services from attack, ensuring the five nines availability your organization depends on.

The DNS Threat Landscape

Here are some of the most common and serious DNS threats confronting your organization:

DNS reflection/DDos attacks use third-party DNS servers (open resolvers) to propagate a DoS or DDoS attack.

DNS amplification attacks employ specially crafted queries to create amplified responses to flood their victims with traffic.

TCP, UDP and ICMP floods deny service on layer 3, bringing a network or service down by flooding it with large volumes of traffic.

DNS-based exploits take advantage of vulnerabilities in DNS software as data exfiltration through known tunnels.

Protocol anomalies cause servers to crash by sending malformed packets and queries.

Reconnaissance probes attempt to get information on the network environment before launching a large DDoS or other type of attack.

DNS hijackings override a domain's registration information, usually at the domain's registrar, to point to a rogue DNS server.

NXDOMAIN attacks send queries to a DNS server to resolve false domain names, flooding the server's cache with NXDOMAIN results and slowing response time for legitimate requests.

Many IT organizations today use load-balancers, IPS and firewall devices, generic DDoS protection solutions and cloud-based solutions to try to counter DNS-based attacks. But all of these approaches are limited in what they can protect. Most of them are external solutions that are "bolted on" rather than built from the ground up to secure DNS against attacks. None of them compares to the effectiveness of a purpose-built, DNS-specific defense solution. That solution is Infoblox ADP.

The Power of Infoblox Advanced DNS Protection

Infoblox Advanced DNS Protection solution components include:

- **Infoblox Advanced Appliances**
  These purpose-built tools have dedicated processing power for the Advanced DNS Protection Service. These are DNS appliances only; they do not include DHCP and IPAM.
- **Infoblox Trinzic Hardware and Virtual Appliances**
  These components consist of existing Trinzic TE-1410/1420/2210/2220 appliances as well as newer Trinzic TE-815/825/1415/1425/2215/2225/4015/4025 appliances with ADP software subscription add-on. Virtual appliances are supported on VMWare and KVM.
- **Infoblox Advanced DNS Protection Service**
  The software, in conjunction with Infoblox Threat Adapt technology, protects against existing and new threats to the DNS server.

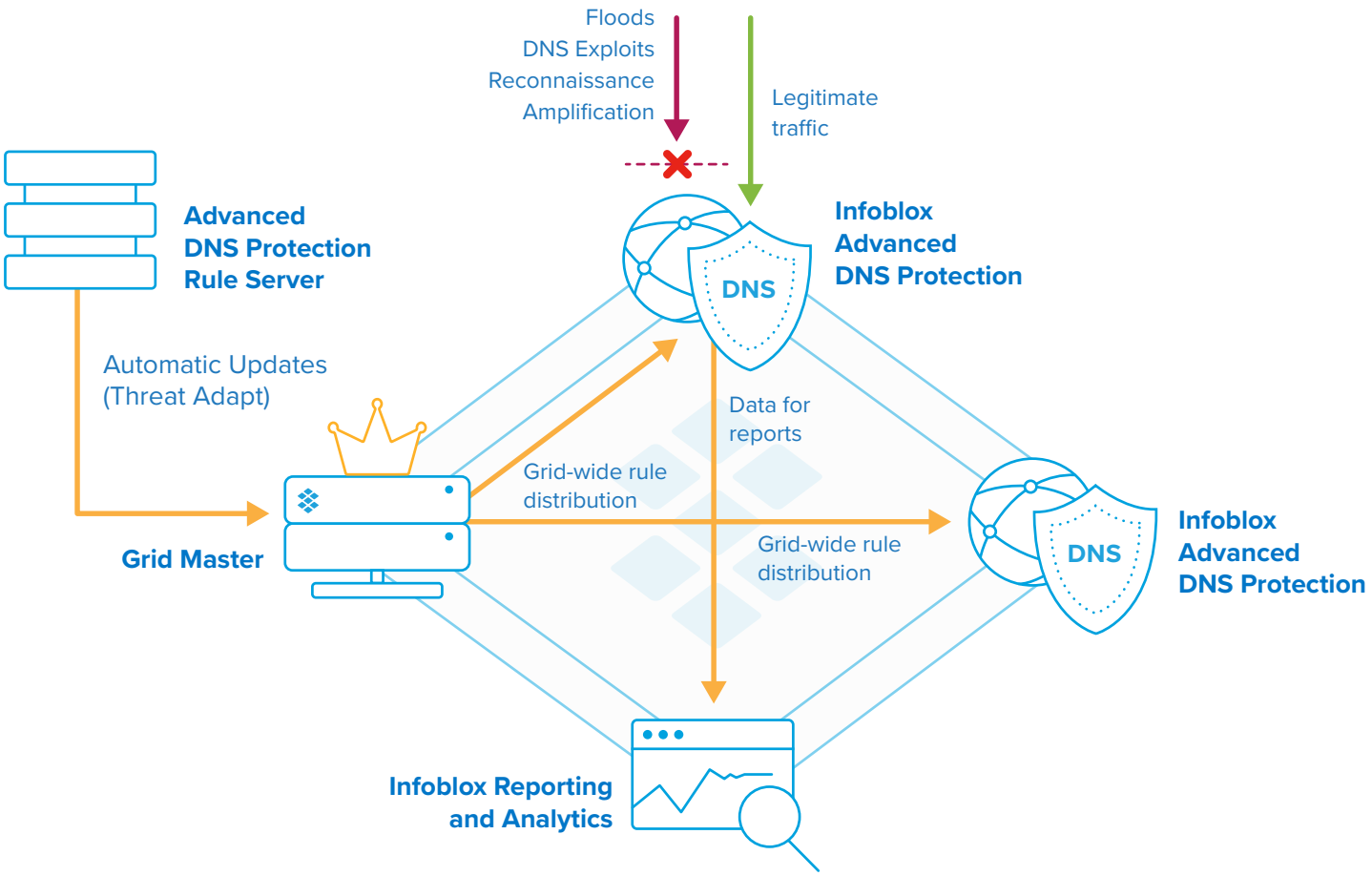

Figure 1: Infoblox Advanced DNS Protection provides a unique defense against DNS-based attacks.

Reduce DNS Service Disruption

Infoblox Advanced DNS Protection continuously monitors, detects, and stops all types of DNS attacks—including volumetric attacks and non-volumetric attacks such as exploits and DNS hijacking—while responding to legitimate queries. It also maintains DNS integrity, which DNS hijacking attacks can compromise. Infoblox provides a solid foundation with five nines availability for next level reliability.

Adapt to Evolving Threats

Infoblox ADP uses Infoblox Threat Adapt technology to automatically update protection against new and evolving threats as they emerge. Threat Adapt applies independent analysis and research to evolving attack techniques, including what our threat specialists have seen in customer networks, to update protection. It automatically adapts protection to reflect DNS configuration changes.

Use Data for Threat Remediation

With Infoblox, your organization can easily view prior or current DNS attacks and improve operational efficiency through our rapid threat remediation. Infoblox Advanced DNS Protection also provides a single view of attack points across the network and attack sources, supplying the intelligence necessary for threat management. It is already integrated with our DNS solution.

Gain Flexible Deployment Options

With Infoblox, you have the option of deploying as a subscription add-on to virtual and physical Trinzic appliances, or as specialized advanced appliances.

Note: You can also deploy Advanced DNS Protection in a trial or proof-of-concept mode, either in line in monitor mode to detect and monitor attacks without blocking them or in out-of-band mode using port mirroring to detect attacks.

Conclusion

Security built in is better than security bolted on. The best place to defend against DNS-based attacks is from within the DNS servers that hackers and cybercriminals target. And the only solution built to do so is Infoblox Advanced DNS Protection.

Contact us today to find out more about the widest range of protection available for your external and internal DNS servers.

Infoblox
NEXT LEVEL NETWORKING

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com