Infoblox Protective DNS Elevates Existing NGFW and SASE Platforms

The Value of a Complete Defense-in-Depth Security Solution

PREEMPTIVE SECURITY: A CRITICAL PART OF DEFENSE IN DEPTH

Cyber threats continue to grow year after year and cause significant disruption to businesses. The cost of downtime and recovery is skyrocketing, not to mention the brand damage and fines that come with becoming the victim of a cyberattack.

To effectively protect systems and data, organizations should employ a multi-layered defense-in-depth strategy. Instead of considering options that "check a box" or are "good enough," a defense-in-depth approach promotes the best possible solutions to address key requirements and enhance an organization's security posture.

For example, next-gen firewall(NGFWs) expertly provide application-level traffic inspection, packet filtering and intrusion prevention services at the network perimeter. Secure access service edge (SASE) solutions effectively combine WAN and security services, such as secure web gateways (SWGs) and cloud access security brokers (CASBs) to securely connect users with applications regardless of where the apps reside - on-premises, SaaS, or cloud-hosted.

While NGFW and SASE vendors may offer some basic DNS filtering or security capabilities, deploying best-of-breed preemptive DNS security in a DNS server, is the most effective way to monitor DNS traffic to proactively identify threats and offers the following benefits:

- Identify threat actor infrastructure to block attacks before they are launched
- Block access to malicious sites earlier in the lifecycle of the threat (92 percent, of malware uses DNS control plane)
- Block additional threats, such as DNS tunneling, DNS infiltration, DNS data exfiltration, domain generation algorithm (DGA) and more using behavioral analytics
- Gain brand protection by identifying lookalike domains and leveraging fast takedown services for offending domains
- Decrease the downstream load on NGFWs and SASE platforms. Let these tools do what they are designed to do best.
- Improve endpoint protection, particularly with IoT and OT devices that cannot support endpoint agents and may have communications that don't always go through a web gateway solution
- Extend DNS security to all network traffic. NGFWs and SASE platforms may not see and inspect all DNS queries, such as guest network or IoT traffic
- Protect east-west traffic, specifically malware Command & Control (C2) communications and lateral movement

Infoblox Protective DNS enhances overall security posture by preemptively providing necessary protections beyond what NGFW and SASE solutions offer. By adding Infoblox DNS-layer security, users gain:

- **A Complementary Layer of Defense:** purpose-built Infoblox Protective DNS adds a layer of defense, catching threats that NGFW or SASE may not see. This layered approach increases the likelihood of detecting and mitigating threats early.
- **Enhanced Threat Intelligence:** our robust threat intelligence feeds can be integrated with NGFW and SASE, improving their efficacy and providing consistent protection.
- **Improved Incident Response:** Infoblox DNS-layer security can help security teams quickly identify and respond to incidents by providing detailed DNS traffic logs and asset insights, reducing the time it takes to detect and mitigate threats.

CATCH THREATS THAT NGFW AND SASE SEE TOO LATE

Every network connection starts with a DNS query—nothing runs without it. Because of its critical role in connectivity, attackers also use DNS in various stages of the cyber kill chain for initial infection, C2 and data exfiltration. In fact, 92 percent of malware uses DNS, according to the United States Cybersecurity and Infrastructure Security Agency (CISA) analysis.

Despite the investment in NGFW and SASE cybersecurity solutions, breaches continue. This occurs because most of these tools are malware-centric and reactive; the threat has already entered, infecting "patient zero" before the industry can identify and block it. A complementary solution, like Infoblox Threat Defense™, which is proactive and works with existing defense-in-depth security technologies to improve an organization's overall security posture, solves this problem by shifting protection to the "left of boom."

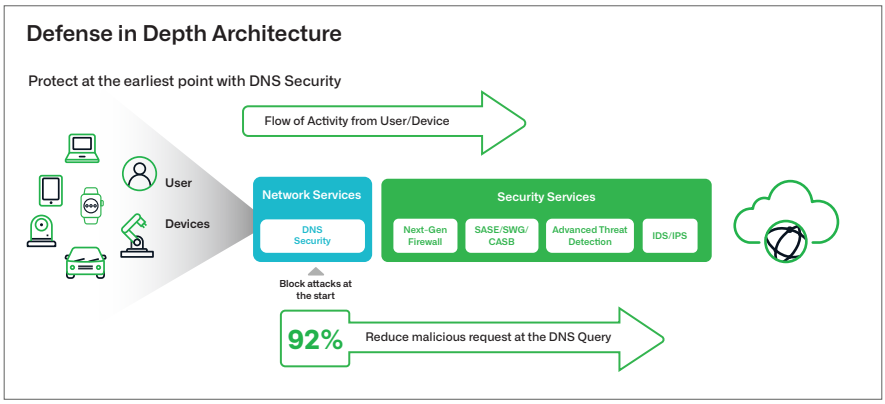

Figure 1: DNS-layer security disrupts the attack cycle at the initial step when a user or device tries to connect to a malicious destination. This is done before other security devices see the malicious activity or can act on it.

- Disrupt the attacker supply chain at the start
- Block **75.4%** of attacks before an incident occurs
- Block **82%** of attacks within 24 hours of the first query
- Protect on an average of **63** days before attacks are launched
- Achieve **0.0002%** false positive rate

With Infoblox Threat Defense, most malicious activity can be blocked at the earliest point in the kill chain before the other security technologies even see it. This cost-effectively provides maximum protection across on-premises, cloud and remote environments, reducing malicious traffic in enterprise networks.

BETTER TOGETHER: INFOBLOX THREAT DEFENSE AND NGFW AND SASE

Infoblox Threat Defense delivers unique and powerful DNS-layer security capabilities that complement NGFW and SASE solutions. By focusing on the DNS layer, it can detect and block threats preemptively, provide detailed visibility into DNS traffic and protect against DNS-specific attacks. Integrating Infoblox Protective DNS with NGFW and SASE enhances overall security, providing a comprehensive and robust defense against a wide range of cyber threats.

Key Capability	Description	Infoblox Threat Defense	NGFW	SASE
Enterprise-Wide Secure Resolver and DNS Query Logging	Uses DNS query data to find and convict domains	●	◑	◑
Full DNS Behavior Monitoring	Monitors all DNS record types for malicious activity	●	●	◔
Lookalike/Doppelganger Domain Detection and Takedown	Mitigates lookalike/doppelganger attack surface	●	○	◑
Zero Day DNS Protection	Identifies new or emerging domains for your organization that could pose a threat	●	◑	◑
Behavior-Based DNS Tunneling Detection	Detects DNS tunnels being used for data exfiltration/infiltration, C2 communications, etc.	●	◑	◑
Proactive Suspicious/High-Risk Domain Protection	Identifies and blocks suspicious domains premptively that are likely to be used in future malicious campaigns	●	◑	◑
Automatic, Native Context Enrichment	Correlates network context without the need for clients or sinkholing (user, device, source IP, location, MAC address, VLAN)	●	◑	◑
Proactive Threat Distribution Systems (TDS) Detection and Disruption	Identifies threat actor TDS infrastructure, not just individual domains, to counter threat actors rotating across numerous domains to evade detection	●	◔	○

Chart 1: Key Infoblox Threat Defense capabilities and how NGFWs and SASE compare.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054