Infoblox

SOLUTION NOTE

Zero Trust and DNS Security

This solution brief will share an overview of the Zero Trust architecture and why it is compelling for modern enterprise and government institutions. We will describe a Zero Trust architecture's components and its core capabilities. We overview the critical role of DNS security as an essential part of modern Zero Trust architecture and highlight how DNS security can provide protection against a multitude of cyberattacker techniques which we further define using the lexicon provided by MITRE ATT&CK.

The Evolution of Zero Trust

Zero Trust states that the concept of a trusted internal network zone and an untrusted external network zone should be eliminated. Zero Trust presents the mantra "Never Trust, Always Verify" so that every device, user, workload, and data trust should be viewed as untrusted until proven otherwise.

At each step in the data flow through networks, the reauthentication, and validation of all parties is essential. Over time, Zero Trust has grown to be a comprehensive cybersecurity strategy which includes a data-centric security model, guiding principles for system design, and overall system management guidance. Zero Trust eliminates the premise that users, devices, and network components should be trusted based on their location within the network.

Drivers for Zero Trust

Cyberattacks continue to see increased activity driven by organized crime and malicious nation states and their proxies. The sophistication of these attacks continue to increase, as does the funding available to fuel this malicious activity. This higher level of risk has seen recent strong endorsements of Zero Trust by the U.S. Government White House directive Moving the U.S. Government Toward Zero Trust Cybersecurity Principles[1], and the National Security Agency document on Embracing a Zero Trust Security Model.[2]

The digital transformation has brought a very rapid move to the cloud, remote office connectivity with SD-WAN, rapid growth in internet of things (IoT) devices, mobile device proliferation, and the widespread use of personal bring your own devices (BYOD). The speed of adoption of the digital transformation and lag in the development and deployment of the cybersecurity strategy to support it has exposed a far larger and rapidly growing attack surface. This is characterized by disparate and disconnected security stacks for on-premise, cloud, and remote workers. This is compounded by the growing shortfall of cybersecurity personnel that have the skills to properly set up and configure these environments.

The COVID-19 pandemic further accelerated the digital transformation and brought higher levels of vulnerability to networks and assets as remote workers required access from home offices and other remote locations using a mix of the BYOD, mobile, and corporate platforms. All of these drivers have positioned Zero Trust as a compelling solution to reduce the risk of asset compromise and data breach.

Zero Trust Core Design Principles

There are several basic design tenets of Zero Trust. These are the hardcore philosophy that you must embrace as you lay out your Zero Trust strategy. The first tenet is that data is the central and critically important element that must be protected. All access to this data must be continually authorized and validated. You must understand the critical flows of your data—you need to know where it might be required in order to validate it later. Micronetworks should be established to protect critical data. These should map to the flow of data and expected user access, and somewhat ruthlessly restrict access. Visibility, monitoring, and extensive logging are essential. You must be able to review this data continuously to determine if there is any malignant activity.

"How can you tell if your DNS is being used as a tunnel to steal your data and intellectual property if you don't have visibility into it? "

Security automation and orchestration tools are a key part of your design—only automation will have the speed of response to meet and defeat a threat in real-time. SOAR is essential to scale your resources over time. Finally, the integration of a centralized point of policy implementation, management, and administration for your security controls and technologies will reduce risk, save time, and improve the effectiveness of your cybersecurity ecosystem.

Zero Trust assumes that threats exist continuously inside and outside of enterprise network boundaries. One of the best ways to address this is to apply the concept of least privileged access to every access decision. Least privileged access allows or denies access to resources based upon organizational policy which, when implemented, utilizes authentication, role privileges, device, location, and user activity. This mix of contextual data allows the lowest risk decision to grant access to be applied and enforced. Zero Trust also brings comprehensive monitoring, logging, and integration with SOAR automation that can help protect important assets.

Zero Trust and DNS Security

Everything on your networks whether on premise, in the cloud, IOT, or mobile will need to use DNS services. DNS has a key role to play in zero trust architecture, as it provides better-centralized visibility and control of all computing resources, including users and servers in a micro-segment, all the way to an individual IP address. Since most traffic, including malicious traffic, goes through DNS resolution first, it is an important source of telemetry providing detailed client information, helping to detect anomalous behavior, and protecting east-west traffic between micro segments. DNS security can also continuously check for, detect, and block Command and Control (C&C) connections and attempts to access websites that host malware. For all of these reasons, DNS security is a core enabler of Zero Trust strategy today.

DNS security restores DNS as an absolute Zero Trust control point where every internet address can be scanned for potentially malicious behavior as identified by integrated threat intelligence. DNS security provides a single point of control to administer and manage all of your environments including cloud, on-premise, WFA, and mobile devices. This provides one DNS security administration point for all of your security stacks, which can easily be integrated with SOAR and other critical cybersecurity ecosystem controls.

DNS security is often a major gap in the build-out of a Zero Trust strategy. Many enterprises have not yet included DNS, DHCP, and IPAM (DDI) controls and data, administration, and management within their cybersecurity strategy. Typically these capabilities have defaulted to a mix of ISPs, on- and off-premises local hardware, and multiple disparate cloud-based capabilities. These disparate and separate DNS capabilities generally have no integration with cybersecurity threat intelligence, web filtering, or other important defensive capabilities. Most of these have no integrated support for the most common cyberthreats, distributed denial of service (DDoS) attacks, nor provide the necessary visibility around DNS.

Organizations must always be in control of, and have complete visibility to, DNS traffic. DNS traffic must be resolved by servers controlled by the organization, not external resolvers over which the IT team has no control.

DoH/DoT Brings New Challenges to DNS Security and Zero Trust

- DNS over TLS (DoT) and DNS over HTTPS (DoH) are two new versions of DNS designed to encrypt the communication between DNS clients and recursive DNS servers. These have solved a longstanding “gap” where DNS queries were transmitted unencrypted.
- If an organization’s DNS servers support DoH/DoT, that’s best practice—all traffic, including DoH/DoT should be routed to those servers. If an organization is routing DoH/DoT traffic to external unauthorized DNS resolvers, bypassing internal DNS servers, then their security team loses visibility and control of the DNS traffic, which will lead to the exposure of many security gaps.
- As a best practice rule, organizations should not allow individual applications and devices to bypass internal DNS infrastructure. Such access to unauthorized external DoH/DoT resolvers should be blocked at firewalls and gateways, forcing DNS resolution to internal resolvers. Looking forward, every organization should plan on implementing internal DNS infrastructure that supports DoT/DoH.

Common Cyberattack Techniques Leverage DNS Services

There are a multitude of ways that cyberattackers can leverage unprotected DNS services. The following MITRE ATT&CK techniques and sub-techniques explicitly define how cyberattackers will target and use DNS services. The Tactic represents the goal the attacker is trying to achieve. The Techniques and Sub-Techniques represent the different ways that cyberattackers can achieve the goals and objectives of the tactic. Mitigation of these techniques require comprehensive DNS security solutions.

MITRE ATT&CK Techniques Which Use DNS

TACTIC - GOAL OF ATTACKER	TECHNIQUES USING DNS	SUB-TECHNIQUE USING DNS
Reconnaissance	T1590 Gather Victim Network Information	.001 Domain Properties
		.002 DNS
		.004 Network Topology
		.005 IP Address
	T1598 Phishing for Information	.003 Spearphishing Link
Resource Development	T1583 Acquire Infrastructure	.001 Domains
		.002 DNS Server
	T1584 Compromise Infrastructure	.001 Domains
		.002 DNS Server
	T1608 Stage Capabilities	.002 Upload Tool
Initial Access	T1189 Drive-by Compromise	
	T1190 Exploit Public-Facing Application	
	T1566 Phishing	.002 Spearphishing Link
Execution	T1204 User Execution	.001 Malicious Link
Credential Access	T1557 Adversary-in-the-Middle	
	T1040 Network Sniffing	
Command and Control	T1071 Application Layer Protocol	.004 DNS
	T1132 Data Encoding	
	T1568 Dynamic Resolution	
	T1573 Encrypted Channel	
	T1008 Fallback Channels	
	T1105 Ingress Tool Transfer	
	T1572 Protocol Tunneling	
	T1090 Proxy	.001 Internal Proxy
		.002 External Proxy
Exfiltration	T1030 Data Transfer Size Limits	
	T1048 Exfiltration Over Alternative Protocol	.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol
		.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
		.003 Exfiltration Over Unencrypted Obfuscated Non-C2 Protocol
	T1041 Exfiltration Over C2 Channel	

BloxOne® Threat Defense

BloxOne Threat Defense secures traditional networks, as well as SD-WAN, IoT, the cloud, and the move to mobile devices. BloxOne Threat Defense brings all of your DNS controls, administration, and management into one hybrid architecture. Everything on your networks whether on premise, in the cloud, IOT, or mobile will need to use DNS services. This gives you one architecturally efficient, centralized point of control and visibility to any traffic that requires resolution of a domain name with DNS services for all of your on-premises and cloud-based resources. Once you assert this control, you have very effectively enabled the defensive build-out of DNS. DNS is now a core part of your Zero Trust strategy.

Conclusions and Recommendations

VISIBILITY & AUTOMATION	PROTECTION EVERYWHERE	REDUCING COST OF THREAT DEFENSE
Identify all devices across the enterprise and **improve productivity of SecOps** through automated data sharing	**DNS as a "signal" for security events** and control point for security enforcement **ACROSS EVERYTHING**	**Offload blocking** of known threats and **preserve processing power** of perimeter security

Organizations must always be in control of their DNS traffic

Foundational core network services such as DNS, DHCP, and IPAM provide deep visibility as incredibly valuable security controls and threat intelligence assets. You can rapidly investigate a threat or anomalous behavior and share valuable data with the rest of your security ecosystem. Using DNS security and leveraging DNS related data within a Zero Trust architecture can bring risk reduction for every cloud and on-premise data center used by your organization.

About Infoblox

Infoblox delivers the next-level network experience with its Secure Cloud-Managed Network Services. As a pioneer in providing the world's most reliable, secure, and automated networks, we are relentless in our pursuit of next-level network simplicity. A recognized industry leader, Infoblox has more than 12,000 customers, including more than 80% of the Fortune 500. To learn more, please visit our website via www.infoblox.com.

1. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
2. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF