SALES CONVERSATION GUIDE

DNS Security

TOP INITIATIVES

- Facilitate business productivity and scalability while reducing costs
- Reduce risk and increase protections against advanced cyber threats
- Ensure data centers are running at optimum efficiency with minimum friction
- Maximize availability and uptime of key business resources
- Comply with standards and regulations for web and data security

WHO TO TARGET

All segments | All verticals
Upsell to Zscaler accounts & net new

Primary
CISO, CIO, Network Operations Manager

Secondary
- Firewall/Network Administrator
- Security Analysts

Practioner
- Firewall/Network Administrator

BASIC TERMS

DNS– The "Domain Name System" is commonly regarded as the phone book of the internet. Since 1985, it's been the backbone of how the internet works. Web browsers interact through IP addresses, whereas humans interact using domain names. DNS translates between the two so that web browsers can access internet resources.

HTTP, HTTPS, FTP, DNS, RTSP, PPTP– Web and non-web protocols used to send and receive information, all of which can be secured and inspected by the Zscaler Cloud Firewall and DNS Security.

DNS Tunneling– A type of attack in which threat actors use DNS requests as a way to communicate with command-and-control servers or exfiltrate data. By its nature, DNS must accept fairly broad queries — as a domain name can be pretty much anything. Malware authors exploit this DNS request / response system to send and receive commands from the adversary on the compromised system, deliver further malware payloads in multistage attacks, or even exfiltrate stolen data 255 characters at a time. It is difficult to detect malicious DNS tunnels because the network traffic generated by DNS tunnels very much resembles normal-looking DNS traffic. It's become even more difficult with the widespread adoption of DNS-over-HTTPs (DoH) traffic, which encrypts traffic to protect its privacy, but also reduces IT visibility. If organizations aren't inspecting SSL/TLS traffic, attackers can use this channel to hide their malicious activity.

DNS over HTTPS (DoH)– Encrypted DNS traffic intended to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks. While DoH does have these security benefits, it can also make it harder to analyze and monitor traffic for cybersecurity purposes. Threat actors can abuse DoH to mask connections to command-and-control servers or to exfiltrate data unnoticed.

DNS spoofing– DNS spoofing—frequently executed using Man-in-the-Middle (MitM) techniques—involves altering the DNS entries on a DNS server or entering false information into the DNS cache, resulting in the targeted user traffic getting redirected to an attacker-controlled fraudulent site which may resemble its original site. This can be used for phishing or to trick users into installing malicious software like worms or viruses. The risk level is fairly high if an attacker manages to compromise the DNS server and manipulate the DNS entries.

Protective DNS (PDNS)– PDNS resolvers are special resolvers that add inspection and other security controls, powered by government threat intel. Both UK and US government agencies have recent mandates to exclusively use PDNS resolvers to protect sensitive information. Zscaler can translate plaintext DNS into DoH and forward to these PDNS resolvers to enable our customers to comply with these regulations.

PAIN POINTS

- Applications and workloads are no longer solely in company-controlled data centers. Instead, they are increasingly deployed natively in private and public clouds and as SaaS applications.
- Work-from-anywhere (WFA) users connect to corporate networks while on the move, making the internet the new corporate network.
- Backhauling traffic from mobile and cloud services through regional data centers and centralized security stacks before breaking out to the internet results in delayed DNS resolution and poor user experience.
- Widespread adoption of DNS over HTTPS (DoH) and the lack of monitoring and control enables adversaries to perform command and control (C2) communication undetected.
- More than 70% of modern attacks involve DNS at some point in the attack chain.
- IDC found that 87% of enterprises were hit by a DNS attack over the course of a year.
- DNS was not designed for security and is subject to misconfigurations and vulnerabilities across the various infrastructure involved.
- Most security controls—including traditional firewalls—do not monitor DNS traffic.

THINGS TO TALK ABOUT: DNS SECURITY

Differentiator

Zscaler's DNS Security stands above other DNS Security providers by proxying DNS in the cloud-native Zscaler Zero Trust Exchange, delivering services at over 150 edge locations, close to every user no matter where they are around the world. Zscaler is the only security vendor that combines optimal DNS resolution closest to the user, with best-of-breed DNS filtering, security, horizontally scalable DoH inspection, and data exfiltration protection. We protect all users, devices, and applications, on all ports and protocols, with superior security, availability, and performance:

Complete AI-powered inspection to find hidden attacks.

Unlimited inspection of inline traffic and utilization of machine learning and native SSL decryption prevents stealthy threats and terminates malicious connections.

Full coverage across ports and protocols.

Quickly identify and intercept evasive and encrypted cyberthreats using non-standard ports.

Secure DNS without compromised performance.

Localized resolutions sustain superior performance while your users and endpoints stay safe from malicious sites and DNS tunneling.

Translation to DoH

Zscaler can translate plaintext DNS into DoH to send traffic to PDNS resolvers and other DoH resolvers, enabling better security, privacy, and compliance than other DNS services.

Cloud-delivered protection with global edge presence.

Zscaler Firewall provides unmatched security and user experience, as it is fully integrated with Zscaler Internet Access™ and part of the Zscaler Zero Trust Exchange™.

Best-in-class availability.

Ensure users maintain reliable, high-speed access with automatic failover options and configurable error handling.

Exceptional user experience.

Requests are resolved at the edge and content is delivered by the optimal CDN and in the local language and currency for a fast, seamless user experience.

Complete visibility over all DNS traffic.

Investigate all DNS transactions with confidence through context-rich data and forensically complete logs.

Protections powered by Zscaler customers everywhere.

Threat intelligence and ML algorithms are informed by the world's largest inline security cloud and updated in real time.

ZSCALER SOLUTION

Zscaler is the only security vendor that combines optimal DNS resolution closest to the user, best-of-breed DNS filtering, security, horizontally scalable DNS-over-HTTPS (DoH) inspection, and data exfiltration protection. Zscaler has released several new features that further enhance our leading security, performance, and availability, including:

- **DNS Gateway**
  - Optimizes availability to third-party resolvers by redirecting requests to secondary resolvers if the primary resolver fails.
  - Protective DNS that improves DNS-over-HTTPS (DoH) encryption, translating unencrypted DNS traffic into encrypted DNS, protecting and enforcing all DoH traffic regardless of destination, and improving security in alignment with forthcoming standards from CISA.
- **Improved DNS tunnel protection** to prevent data exfiltration through DNS
- **Regionalization with ECS** that optimizes the user experience by providing the best localized resolution based on the country, ensuring users experience webpages with their local language, content, and currency, configurable and subject to privacy requirements.
- **DNS security enhancements,** including enhanced DGA detection to block any command and control malware activities.
- **Enhanced error handling** and reporting including a QBR report.

With DNS Security, you can define rules that control DNS requests and responses. DNS traffic often goes unmonitored and does not go through traditional firewalls. Because of this, DNS traffic can be abused through techniques such as tunneling. DNS Security allows you to detect and prevent DNS tunneling from occurring, and enables you to:

- Monitor and apply policies to all DNS requests and responses, irrespective of the protocol and the encryption used. This includes UDP, TCP, and DNS over HTTPS (DoH).
- Define granular DNS filtering rules using a number of DNS conditions, such as users, groups, or departments, client locations, categorization of domains and IP addresses, DNS record types, the location of resolved IPs, etc.
- Enforce condition-based actions on DNS traffic, such as allowing or blocking traffic, redirecting requests to specific DNS servers, redirecting users by overwriting DNS responses, etc.
- Detect and prevent DNS-based attacks and data exfiltration through DNS tunnels.
- Enhance your security posture by using Zscaler Trusted DNS Resolver for domain resolution.

IMPLICATION METRICS TO TRACK

- Likelihood (%) of risk of a data breach over the next 12 months
- Average data breach cost ($4.35M)
- Number of data loss incidents
- Security resources time and cost to manage alerts and security complexity
- Cost of compliance issues and fines
- Cost of remediation in a production environment
- Number of hours lost in productivity levels
- Number of days in project delays
- Number of breaches as a result of misconfigurations and vulnerabilities

REFERENCE

DNS Security Zsource →

FMD Engagement: **Mark Brozek**

Exec Engagement: **Anusha Vaidyanathan**

Product Management: **Anusha Vaidyanathan, Stefan Sebastian**

Product Marketing: **Mark Brozek**

Slack: **#ask-cfw**

DISCOVERY AND TRAP SETTING QUESTIONS

New Customers/New to Platform

- Have you been impacted by a DNS attack in the past two years?
- What do you currently do for DNS filtering?
- What do you use for DNS resolution?
- Do you have visibility into DNS-over-HTTPS (DoH) traffic?
- Are you able to inspect and protect all web- and non-web traffic?
- How are you protecting and optimizing web and application performance for remote users?
- [Fed clients in US and UK] What are you doing to comply with new protective DNS (PDNS) guidelines?
- Are you a federal/public sector organization that has to comply with the CISA's P-DNS mandate or NCSC's P-DNS initiative?
- Are you concerned about ransomware proliferation and is layered threat defense at the earliest possible layer in the kill chain important?
- Are increasing deployments of encrypted DNS (DoH) a security blindspot in your organization?
- Is secure low-latency DNS resolution with failover and high-availability important for the best user experience for your global remote and hybrid workforce?
- Is consolidated DNS filtering and security important for your authenticated & guest wifi users, devices, servers and workloads?
- Do you need optimal geo-local DNS resolution (ECS) for your global workforce accessing enterprise/Internet applications?

Competitive Displacement

- Are you using a standalone DNS security product like Infoblox, Cisco Umbrella and would like to consolidate this in your Zscaler security platform?
- Are you evaluating SSE platforms like Prisma Access and Netskope IA?