National Cyber Security Centre
Ministry of Security and Justice

DNS Encryption

The new standard for DNS traffic

Factsheet FS-2023-237 | 2.1 | February 2023

Modern, encrypted DNS transport protocols make it difficult to monitor and intercept DNS traffic for detection and mitigation purposes, for example inside corporate networks. On the one hand this poses challenges for system and network administrators.

On the other hand it brings great security benefits to end-users and organizations. DNS encryption is closing the loop in one of the last protocols that was widely unencrypted, solving an important piece in the zero trust puzzle.

NCSC advices organizations to familiarize themselves with encrypted DNS, start planning a transition to encrypted DNS infrastructure and configure endpoints to strictly adhere to explicitly configured DNS resolvers.

Background

The Domain Name System (DNS) is one of the most important internet protocols, as a fundamental part in the initiation of most internet traffic sessions. DNS is the phonebook for the Internet. Humans access information on digital devices through domain names, wich offer translation from human-readable text to technical ip-adresses meant for routing network packets.

The DNS protocol traditionally communicates over UDP port 53. Its original design does not apply any authenticity or integrity checks, and is unencrypted.

A rising trend, especially amongst technology enthusiasts, has been for end-users to manually change their prefered DNS server to a third party, out of bounds of their own internal network and their Internet Serviceprovider network. The first motivation was to get better performance, as some third party DNS providers market their services based on improved lookup times that materially translate in a faster browsing experience. Secondly, and more recently, encryption has been added to the list of benefits for choosing a third party DNS provider.

The benefits of DNS encryption could make a critical difference for end users and their organizations, especially in corporate environments where confidentiality is at stake, or in societies where freedom of expression is limited and monitored by government regimes.

This is why application and operating system developers have started to widely adopt DNS encryption, both in the OS network stack and by implementing DNS override functionality in web browsers. Especially the latter, where a browser chooses a third party encrypted DNS provider, could pose challenges for corporate IT teams trying to monitor and detect malicious activity on their networks.

Target audience

System and Network Administrators, Information Security Officers

Important facts

1. Internet Browser Vendors are implementing automatic DNS switching. If an unencrypted DNS server is assigned to the Operating System, browsers may switch to a third party encrypted DNS server of their choosing.

2. If this automatic switching behaviour is not moderated by network and system administrators there may be adverse effects like connectivity issues, data leakage or unmonitored data exfiltration.

What is going on?

Encrypted DNS transport will become the norm for modern operating systems, webbrowsers and smartphones.

Dutch internet providers are working on solutions to directly provide their small and medium sized business customers with encrypted DNS resolvers. These customers use internet routers that sometimes still use a local unencrypted DNS server for endpoint communication. The lack of DNS encryption seems less urgent, as their local network is seen as a trusted zone. The same could be applied to the connection to the internet – it is unencrypted but the network segments are trusted by the user and the ISP.

Larger organizations normally implement and manage their own DNS resolvers and assign these to their endpoints and servers. These are used to resolve both public DNS records and records that are only published internally, for example to access servers only available on the local network. These type of implementations still are largely unencrypted for the same reasons as consumers and small companies don’t apply encryption on local DNS: their internal network is seen as a trusted segment and usually extra network segmentation and monitoring is in place to properly safeguard this assumption.

The modern architecture used to design and develop modern devices and software, where any part of the infrastructure including a local zone is regarded to be insecure, and extra safeguards are put in place to secure integrity, confidentiality and validity of information.

This new trend in design should be regarded as valuable and NCSC advices software developers and architects to adhere to its philisophy wherever possible. Unencrypted DNS could be susceptable to interference, tampering and eavesdropping, by a malicious actor within network boundaries.

Most importantly, for the short term, NCSC advices network and system administrators to anticipate on different DNS behaviour on endpoints and networks under their control. Every webbrowser vendor may have a slightly different roadmap for implementing DNS, with different policies for administrators to choose from, but their goal will ultimately be encrypted-only DNS. This strategy could be compared to the shift from HTTP to HTTPS, where unencrypted HTTP connections are straight out refused by modern browsers.

Implications of Encrypted DNS

Technical background

Encrypted DNS has been in development for a number of years, with RFC7578 *DNS over TLS* (DoT) dating from May 2016, RFC8484 *DNS over HTTPS* (DoH) from October 2018 and RFC9250 *DNS over dedicated QUIC* (DoH3 or DoQ) most recently, published in May 2022. In essence, all of these variants encapsulate DNS traffic in encryption over TCP, using different transport variants. DoT uses tcp/853, DoH and DoQ both use tcp/443. DNS over HTTPS seems to be the most prevalent standard for now, with an expected shift to Quick when that recent RFC receives a wider adoption.

DNS shifts to the appliction layer

Application developers traditionally used the OS software libraries to perform DNS queries. There would be a call to the operating system, that would handle the query itself and present the application its results. Many applications running on one OS would use a single DNS stub resolver for all of their DNS traffic.

In modern applications, using modern development frameworks, software developers have several options at their disposal to validate what type of DNS server is offered by the OS. They can assess whether or not the application should use it, and whether or not to fail open or safe based on its criteria, set by the developer.

All tech providers involved in operating systems and software development tooling, like Apple, Google and Microsoft, now offer a comprehensive toolkit and guidance on how to use encrypted DNS at the application level, effectively overriding operating system settings.

Encrypted DNS in specific webbrowsers

Mozilla Firefox, Google Chrome and its Chromium derivatives such as Microsoft Edge, all offer similar DNS encryption evaluation. They may select a third party encrypted DNS provider, prevalently Cloudflare or Google, if the Operating System has been provided non-encrypted DNS servers. Browsers may try to upgrade the locally provided DNS connection to an encrypted variant, if that fails it may attempt the third party provider.

Most browsers also take into account any locally installed root certificates, for example specific organizational certificates, and will disable their DNS encryption evaluation altogether. Their evaluation also depends on locality: Firefox, for example, detects if the browser is used in America or in a country on a specific list of repressive regimes. For these regions, the browser will select its third party DNS provider, if no other way of DNS encryption is available. In Europe, however, Firefox will not automatically switch to an encrypted provider but will use any unencrypted DNS server provided by the operating system.

This behavior could change over time and we expect it to mandate encrypted DNS at some point in the future, following a gradual path of log-notification, end user notification and eventually blocking unencrypted DNS. This path may be similar to the phasing out of HTTP and will take several years.

Application layer DNS could prove unpredictable for system and network administrators

The way application layer DNS will be implemented will vary, both in technology type and time of publication. The fact that all common web browsers and operating systems currently support encrypted DNS offers opportunities for administrators to proactively switch to their encrypted DNS infrastructure of choice and thereby anticipate on application changes concerning encrypted DNS.

When application changes with regards to encrypted DNS are not anticipated but just rolled out as part of regular application updates, this could have adverse effects on both end-user experience and loss of control over DNS traffic. DNS leakage could occur when users try to connect to a local server with a DNS name only known locally, also resulting in inability to connect to the service.

DNS encryption in and of itself offers a safer, more consistent adherence to modern security principles and can be implemented today with existing standards, good vendor support and widely available tooling.

Changes in DNS infrastructure are not done overnight and demand extensive preparation as it will affect all network connected IT infrastructure. A proactive, programmatic and broad approach are highly recommended.

As a final consideration, administrators are recommended to evaluate current DNS monitoring solutions. Commonly DNS is monitored by both logparsing the DNS server logs and packetmonitoring DNS network traffic. The latter will stop working when traffic is encrypted. Combined with loose network segmentation and filtering this could pose a risk for unmonitored network egress using malicious DNS traffic.

Measurements

Gain knowledge and insight on the techology behind DNS encryption and the way your core applications such as web browsers evaluate assigned DNS servers.

Keep current, as roadmaps for full DNS encryption in browsers have yet to be crystalized.

Force prefered DNS servers on endpoints and block undesired behavior such as autoswitching to an external third party DNS.

Implement policies for DNS behavior at both the Operating System and the Application Level.

Prepare a program for your IT organization to switch to encrypted DNS.

Evaluate your DNS monitoring capabilities and make sure they meet your detection requirements.

Publication

National Cyber Security Centre (NCSC)
PO BOX 117, 2501 CC The Hague, The Netherlands
Turfmarkt 147, 2511 DP The Hague, The
Netherlands
+31 (0)70 751 5555

More information

www.ncsc.nl
info@ncsc.nl
@ncsc_nl

February 2023