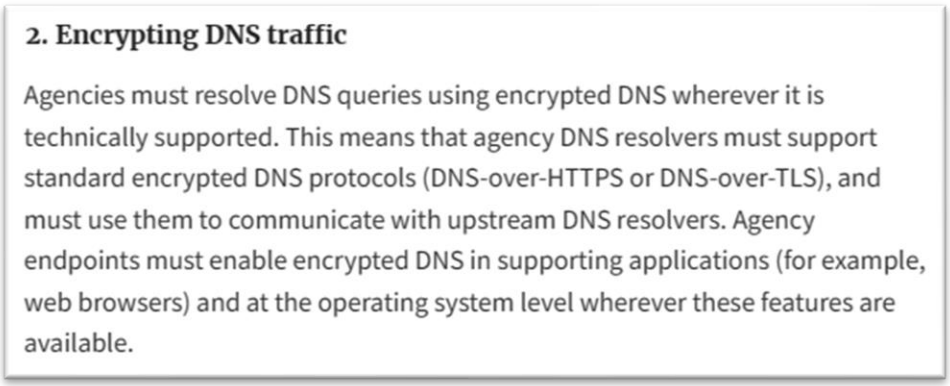
In-depth interpretation of the U.S. Federal Zero Trust Strategy (II): DNS Security

The U.S. federal government released the "Federal Zero Trust Strategy" two years ago, and the author wrote an interpretation article at that time - In-depth Interpretation of the U.S. "Federal Zero Trust Strategy" (I): Website Security, it is recommended that readers read the first interpretation focusing on HTTPS encryption before reading this article, This is the second interpretation: DNS Security.

1. Interpret the requirements for DNS security in the Federal Zero Trust Strategy

Let's take a look at how the Federal Zero Trust Strategy requires federal government agencies to strengthen the security of DNS traffic - Encrypting DNS traffic: DNS services used by federal government agencies must use encrypted DNS protocols (DNS-over-HTTPS or DNS-over-TLS) and must use encrypting protocols to communicate with upstream DNS resolvers, and government agencies must enable encrypted DNS to support various application software (e.g., browsers, custom-developed software), and operating system-level encrypted DNS applications. This task must be completed in fiscal year 2024.



2. Encrypting DNS traffic

Agencies must resolve DNS queries using encrypted DNS wherever it is technically supported. This means that agency DNS resolvers must support standard encrypted DNS protocols (DNS-over-HTTPS or DNS-over-TLS), and must use them to communicate with upstream DNS resolvers. Agency endpoints must enable encrypted DNS in supporting applications (for example, web browsers) and at the operating system level wherever these features are available.

The original text is only 315 words, and the author summarizes the following four key contents:

(1) The DNS service of all federal government agencies must be encrypted, which is clearly applicable and mandatory.

(2) The DoH or DoT standard must be used to encrypt the DNS, which is a clear technical route. Please note: DNSSEC technology is not required.

(3) All kinds of software, including browsers and custom-developed software must support encrypted

DNS, which is to clarify which software must support encrypted DNS.

(4) This task must be completed in FY2024, which is a clear time for completion.

I believe that after reading this requirement, you will definitely feel that it is very simple and clear, clear at a glance. So, why did the U.S. Federal Zero Trust Strategy introduce this mandatory policy? The second part of this article will explain the ins and outs of DNS and encrypted DNS in detail.

2. What is DNS? What is Encrypted DNS?

What is DNS? When the browser uses HTTP or HTTPS to access the website, it must first access an IP address query service to obtain the IP address of the website domain name, so as to obtain the website content from the website normally, and the IP address query service is the DNS service. In other words, we can't do without DNS services every day on the Internet, so DNS security is very important, DNS is the foundation of reliable IT operations, and DNS data must be protected from illegal theft and tampering. However, traditional DNS security generally refers to the attack protection of DNS servers and does not give more consideration to the transmission security of DNS data.

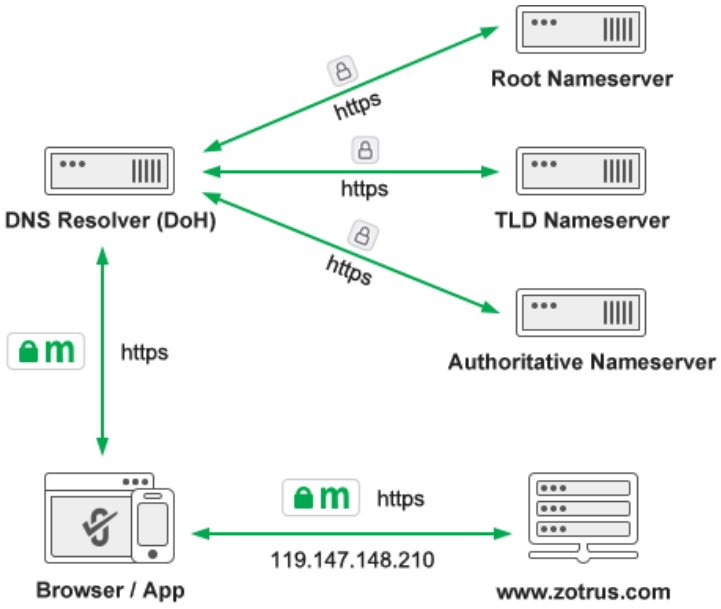
When the DNS system was born in 1983, it was the same plaintext transmission protocol as the HTTP service that was born later, and the DNS packets of the browser querying the DNS service were transmitted on the Internet in clear text, and anyone could view and even tamper with these domain name resolution data (DNS hijacking), which not only affected whether the user could access the correct website, but also very easy to leak the user's Internet access history and leak the user's privacy. It is a pity that the DNS query service used by users on the Internet is still almost 100% transmitted in plaintext 40 years after the birth of DNS service, and the HTTP protocol, which is 6 years later than the DNS protocol, has achieved more than 90% of the world's traffic encryption. So why isn't DNS encryption implemented?

DNS encryption technology was developed as early as 1999 - DNSSEC (Domain Name System Security Extension), but the focus of this technology is to ensure the integrity of DNS responses (to prevent attackers from tampering with the content of the responses) rather than encrypting the transmission of DNS query data. Although DNSSEC uses digital signature technology to ensure the

integrity of DNS data, its disadvantage is that key management is too complex, resulting in the fact that this technology has not been widely used. The shortcomings of DNSSEC technology can be simply understood as the encryption mechanism does not use the mature PKI system but uses a self-signed key system that is difficult to manage to achieve the digital signature of DNS data.

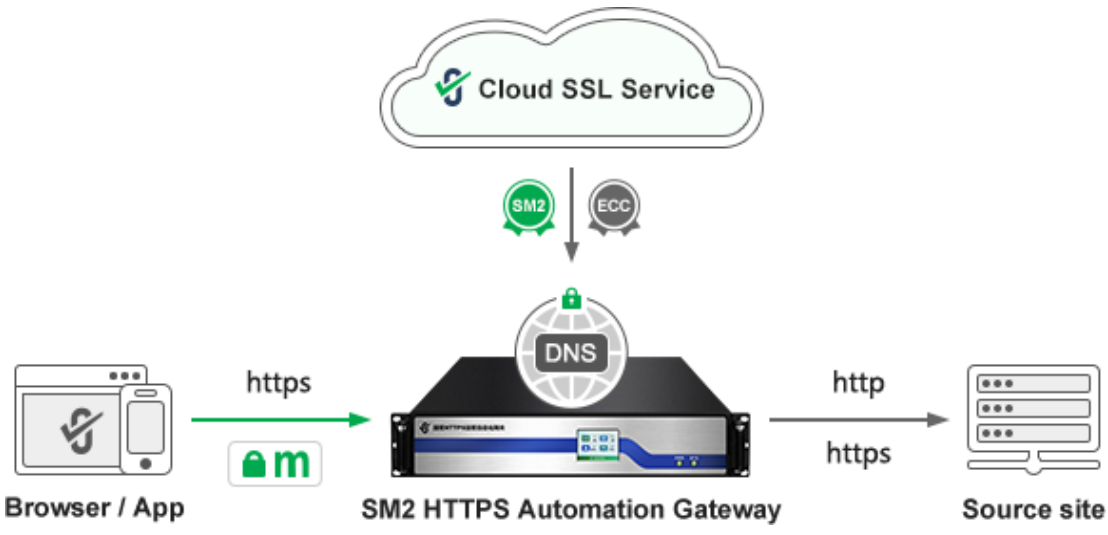
With the popularization and application of HTTPS encryption technology, this technology is naturally used to protect the transmission security of DNS data, because HTTPS is a very mature encrypted transmission technology, which can efficiently solve the problem of plaintext transmission of DNS data. These are the two encrypted DNS technologies recommended by the Federal Zero Trust Strategy: DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) technologies, both of which have become RFC standards, and are SSL certificates based on the mature PKI system to achieve DNS data transmission encryption. The difference between DoH and DoT technologies is that the former is based on a very mature HTTPS encrypted channel to encrypt DNS data, while the latter uses a dedicated port 853 and TLS/SSL encryption via the UDP protocol.

So, which of the two encrypted DNS technologies is better, DoH or DoT? Which technology should users choose to secure their DNS? From a network security perspective, DoT technology enables network administrators to monitor and block DNS queries due to the use of specific ports, which is important for identifying and blocking malicious traffic. DoH queries, on the other hand, are hidden in regular HTTPS traffic, which means that malicious DNS traffic cannot be blocked. However, from a privacy perspective, DoH is arguably the better technology. With DoH, DNS queries are hidden from HTTPS traffic, which weakens the visibility of network administrators but enhances user privacy. The author prefers to use DoH technology, because it uses HTTPS encryption technology, which makes it very easy for browsers to integrate DoH services, and also makes the solutions for automatic certificate management HTTPS encryption support automatic certificate management of encrypted DNS without any change, which is very important, especially after the validity period of SSL certificate is about to be shortened to 90 days, automatic certificate management ensures the continuous and uninterrupted service of encrypted DNS services.

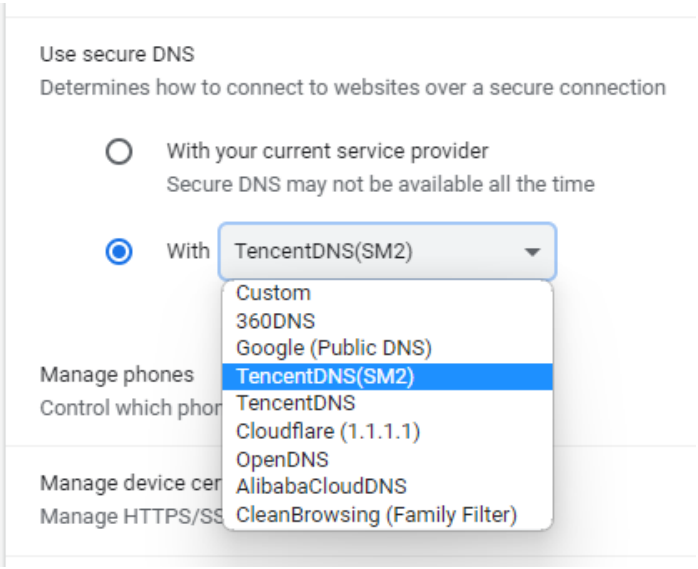


3. ZoTrus DNS Encryption Solutions

ZoTrus Technology provides HTTPS automation solutions, and encrypted DNS is the beginning of HTTPS Internet access, only by first realizing DNS encryption, coupled with HTTPS encryption, can we truly realize the full encryption security of users' Internet access, and truly protect user data security and ensure Internet security. DNS encryption and HTTPS encryption are indispensable, which is why ZoTrus SM2 HTTPS Automation Gateway integrates encrypted DNS services in the recently upgraded version, based on the open-source Bind 9 DNS system, to achieve automatic configuration of dual-algorithm SSL certificates for DoH services, and automatically realize SM2 HTTPS encryption and SM2 DNS encryption (SM2 DoH), providing users with one-stop HTTPS encryption and DoH encrypted DNS services. This is one of ZoTrus DNS encryption solutions.



The second of ZoTrus DNS encryption solution is that ZT Browser supports DoH/DoT encrypted DNS service, users can enable encrypted DNS service in the "Use secure DNS" menu. ZT Browser provides DNS encryption services for users to browse the Internet, which effectively guarantees the privacy and security of users. ZT Browser released an upgraded version today, adding 4 well-known China encrypted DNS services on the basis of the default built-in 4 world-renowned encrypted DNS services in Chromium, it is recommended to choose TencentDNS(SM2), which is the only encrypted DNS service (DoH) that the author has found at present, which uses the SM2 algorithm to achieve the encrypted DNS service. ZT Browser will automatically use the SM2 algorithm to encrypt DNS information to achieve the full Internet security and SM2 protection of SM2 DNS encryption and SM2 HTTPS encryption.



4. Secure Internet access starts with the use of encrypted DNS

From the moment the user enters the domain name of the website in the address bar of the browser, the DNS resolver begins to translate from the domain name to the IP address and returns the IP address to the browser through the HTTPS encrypted channel, and the browser can access the website to obtain the website content. It can be seen from the working principle of this encrypted DNS service that the encrypted DNS service realizes the whole process encryption protection of DNS data query, which is an important technical means to protect the privacy and information security of users on the Internet. To ensure the Internet security of China Internet users, it is necessary to use the SM2 algorithm to encrypt DNS, and the SM2 SSL certificate to realize the SM2 DoH/DoT encrypted DNS service.

The U.S. Federal Zero Trust Strategy requires that the DNS services used by federal government agencies must adopt the encrypted DNS protocol (DoH or DoT), which is zero trust in the traditional plaintext DNS, and only trusts encrypted DNS, which is very worthy of learning and reference by Chinese government agencies. China Cryptography Law and Regulations on the Management of Commercial Cryptography require that all critical information infrastructure must use commercial cryptography to ensure its network security, which requires the use of SM2 DoH or SM2 DoT technology to ensure the DNS security of China's critical information infrastructure system, which is very worthy of all critical information infrastructure operators in China to attach great importance to and popularize the application of SM2 encrypted DNS as soon as possible.

ZT Browser not only supports SM2 HTTPS encryption, but also supports SM2 DNS encryption service, which effectively protect the user's Internet security and privacy protection. The ZoTrus HTTPS Automation Gateway integrates the encrypted DNS service module to realize the automation of encrypted DNS, providing a one-stop DNS encryption and HTTPS encryption automation solution. Welcome to try ZT Browser for free and choose ZoTrus SM2 HTTPS Automatic Gateway.

Richard Wang

Jan. 29, 2024
In Shenzhen, China