DNS sobre TLS x DNS sobre HTTPS | DNS seguro

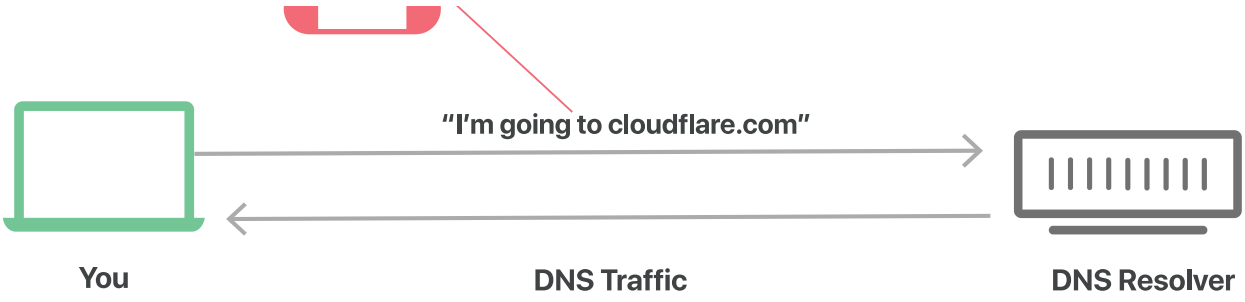
As consultas ao DNS são enviadas em texto simples, o que significa que qualquer pessoa pode lê-las. DNS sobre HTTPS e DNS sobre TLS criptografam as consultas e respostas DNS para manter a navegação dos usuários segura e privada. Entretanto, ambas as abordagens têm seus prós e contras.

Copiar o link do artigo

Por que o DNS precisa de camadas adicionais de segurança?

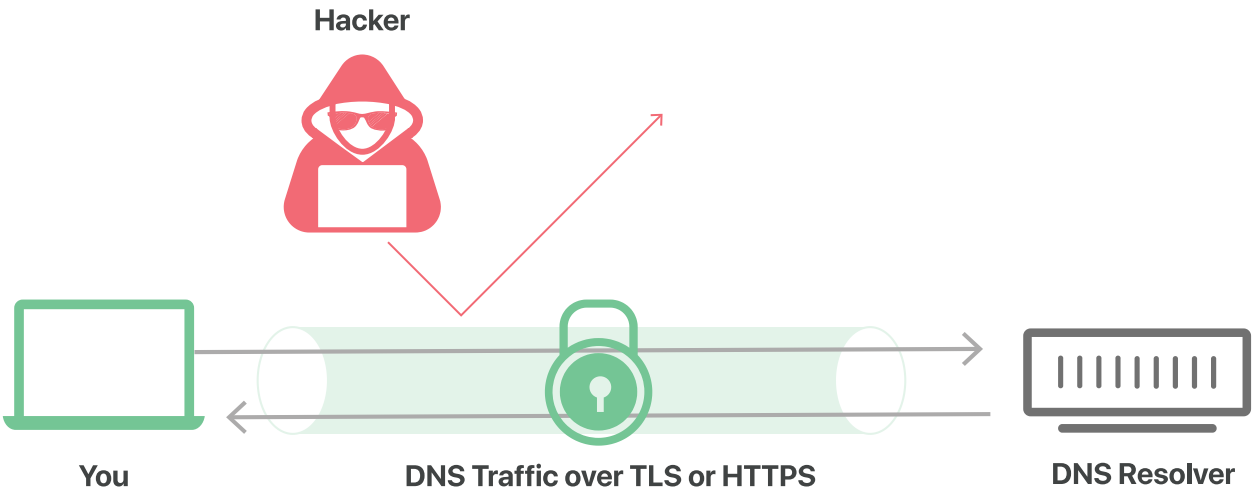
O DNS é a lista telefônica da internet; os resolvedores de DNS traduzem os nomes de domínio legíveis por seres humanos em endereços de IP legíveis por máquinas. Por padrão, as consultas e as respostas de DNS são enviadas em texto simples (via UDP), o que significa que elas podem ser lidas por redes, provedores ou por qualquer pessoa capaz de monitorar transmissões. Mesmo que um site utilize o HTTPS, a consulta DNS necessária para navegar para esse site fica exposta.

Essa falta de privacidade tem um enorme impacto na segurança e, em alguns casos, nos direitos humanos; se as consultas DNS não são privadas, então se torna mais fácil para os governos censurar a internet e para os invasores espionarem o comportamento on-line dos usuários.



Pense em uma consulta DNS normal, não criptografada, como se fosse um cartão postal enviado pelo correio: qualquer um que manuseie a correspondência pode, sem querer, dar uma olhada no texto escrito no verso desse cartão, portanto, não é prudente enviar um cartão postal que contenha informações confidenciais ou privadas.

DNS sobre TLS e DNS sobre HTTPS são dois padrões desenvolvidos para criptografar o tráfego de DNS em texto simples a fim de evitar que partes maliciosas, anunciantes, provedores e outros sejam capazes de interpretar os dados. Usando a mesma analogia, esses padrões visam colocar um envelope em torno de todos os cartões postais que passam pelo correio, para que qualquer um possa enviar um cartão postal sem se preocupar que alguém veja seu conteúdo.



O que é DNS sobre TLS?

DNS sobre TLS, ou DoT, é um padrão para criptografia de consultas DNS a fim de mantê-las seguras e privadas. O DoT usa o mesmo protocolo de segurança, o TLS, que os sites HTTPS usam para criptografar e autenticar as comunicações. (O TLS também é conhecido como "SSL.") DoT adiciona a criptografia TLS no topo do protocolo de datagramas do usuário (UDP), que é usado para consultas de DNS. Além disso, garante que as solicitações e respostas de DNS não sejam adulteradas ou forjadas por meio de ataques on-path.

O que é DNS sobre HTTPS?

O DNS sobre HTTPS, ou DoH, é uma alternativa ao DoT. Com o DoH, as consultas e respostas DNS são criptografadas, mas são enviadas por meio dos protocolos HTTP ou HTTP/2 em vez de serem enviados diretamente sobre o UDP. Da mesma forma que o DoT, o DoH garante que os invasores não possam forjar ou alterar o tráfego DNS. O tráfego DoH se parece com o tráfego de outros HTTPS (por exemplo, interações normais dos usuários com sites e apps da web) da perspectiva de um administrador de rede.

Em fevereiro de 2020, o navegador Mozilla Firefox começou a permitir o DoH para usuários dos EUA por padrão. As consultas DNS do navegador Firefox são criptografadas pelo DoH e vão para o Cloudflare ou para o NextDNS. Vários outros navegadores também são compatíveis com o DoH, embora ele não esteja ativado por padrão.

Mas o HTTPS não usa TLS para criptografia também? Qual a diferença entre o DNS sobre TLS e o DNS sobre HTTPS?

Cada padrão foi desenvolvido separadamente e tem sua própria documentação RFC*, mas a diferença mais importante entre o DoT e o DoH é a porta que eles utilizam. O DoT usa apenas a porta 853, enquanto o DoH usa a porta 443, que é a porta que todo o outro tráfego HTTPS também usa.

Como o DoT tem uma porta dedicada, qualquer pessoa com visibilidade de rede pode ver o tráfego de DoT indo e vindo, mesmo que as próprias solicitações e respostas sejam criptografadas. Por outro lado, com o DoH, as consultas e respostas DNS são camufladas dentro de outro tráfego HTTPS, uma vez que todo o tráfego passa pela mesma porta.

**RFC significa "Pedido de Comentários" e um RFC é uma tentativa coletiva, feita por desenvolvedores, especialistas em rede e líderes de ideias inovadoras, de padronizar uma tecnologia da internet ou um protocolo .*

O que é uma porta?

Na rede, uma porta é um lugar virtual de uma máquina que se encontra aberto para conexões de outras máquinas. Cada computador em rede tem um número padrão de portas, e cada porta é reservada para determinados tipos de comunicação.

Pense nos ancoradouros para navios em um porto: cada ancoradouro de embarque é numerado e diferentes tipos de navios devem ir para ancoradouros de embarque específicos para descarregar carga ou passageiros. A rede funciona da mesma forma: determinados tipos de comunicação devem ir para determinadas portas da rede. A diferença é que as portas da rede são virtuais: são locais para conexões digitais e não para conexões físicas.

O que é melhor, DoT ou DoH?

Isto ainda está sendo debatido. Do ponto de vista da segurança de rede, o DoT é indiscutivelmente melhor, pois dá aos administradores de rede a capacidade de monitorar e bloquear consultas DNS, o que é importante para identificar e interromper o tráfego malicioso. As consultas DoH, entretanto, estão escondidas no tráfego HTTPS regular, significando que elas não podem ser facilmente bloqueadas sem que todo o outro tráfego HTTPS também seja bloqueado.

Entretanto, do ponto de vista da privacidade, DoH é indiscutivelmente preferível. Com o DoH, as consultas DNS são ocultadas dentro do maior fluxo de tráfego HTTPS, o que dá menos visibilidade aos administradores de rede, mas mais privacidade aos usuários.

1.1.1.1, o resolvedor de DNS gratuito da Cloudflare, é compatível tanto com o DoT quanto com o DoH.

Qual é a diferença entre DNS sobre TLS/HTTPS e DNSSEC?

DNSSEC é um conjunto de extensões de segurança para verificação da identidade de servidores raiz do DNS e de nameservers confiáveis nas comunicações com resolvedores de DNS. Ele foi desenvolvido para evitar o ataque de envenenamento de cache DNS, entre outros. Ele não criptografa as comunicações. O DNS sobre TLS ou HTTPS, por outro lado, criptografa as consultas DNS. 1.1.1.1.1 também é compatível com o DNSSEC.

Para saber mais sobre 1.1.1.1, veja O que é 1.1.1.1?

CONTEÚDO RELACIONADO

DNS

Segurança de DNS

Envenenamento de cache de DNS

Tipos de servidor de DNS

DNS dinâmico