What is SNI? How TLS server name indication works

SNI, or Server Name Indication, is an addition to the TLS encryption protocol that enables a client device to specify the domain name it is trying to reach in the first step of the TLS handshake, preventing common name mismatch errors.

What is SNI (Server Name Indication)?

SNI is somewhat like mailing a package to an apartment building instead of to a house. When mailing something to someone's house, the street address alone is enough to get the package to the right person. But when a package goes to an apartment building, it needs the apartment number in addition to the street address; otherwise, the package might not go to the right person or might not delivered at all.

Many web servers are more like apartment buildings than houses: They host several domain names, and so the IP address alone is not enough to indicate which domain a user is trying to reach. This can result in the server showing the wrong SSL certificate, which prevents or terminates an HTTPS connection – just like a package can't be delivered to an address if the correct person doesn't sign for it.

When multiple websites are hosted on one server and share a single IP address, and each website has its own SSL certificate, the server may not know which SSL certificate to show when a client device tries to securely connect to one of the websites. This is because the SSL/TLS handshake occurs before the client device indicates over HTTP which website it's connecting to.

Server Name Indication (SNI) is designed to solve this problem. SNI is an extension for the TLS protocol (formerly known as the SSL protocol), which is used in HTTPS. It's included in the TLS/SSL handshake process in order to ensure that client devices are able to see the correct SSL certificate for the website they are trying to reach. The extension makes it possible to specify the hostname, or domain name, of the website during the TLS handshake, instead of when the HTTP connection opens after the handshake.

More simply put, SNI makes it possible for a user device to open a secure connection with https://www.example.com even if that website is hosted in the same place (same IP address) as https://www.something.com, https://www.another-website.com, and https://www.example.io.

SNI prevents what's known as a "common name mismatch error": when a client (user) device reaches the right IP address for a website, but the name on the SSL certificate doesn't match the name of the website. Often this kind of error results in a "Your connection is not private" error message in the user's browser.

SNI was added as an extension to TLS/SSL in 2003; it was not originally a part of the protocol. Almost all browsers, operating systems, and web servers support it, with the exception of some of the very oldest browsers and operating systems that are still in use.

What is a server name?

Although SNI stands for Server Name Indication, what SNI actually "indicates" is a website's hostname, or domain name, which can be separate from the name of the web server that is actually hosting the domain. In fact, it is common for multiple domains to be hosted on one server – in which case they are called virtual hostnames.

A server name is simply the name of a computer. For web servers this name is typically not visible to end users unless the server hosts only one domain and the server name is equivalent to the domain name.

What does the TLS SNI extension do?

Often a web server is responsible for multiple hostnames – or domain names (which are the human-readable names of websites). Each hostname will have its own SSL certificate if the websites use HTTPS.

The problem is, all these hostnames on one server are at the same IP address. This isn't a problem over HTTP, because as soon as a TCP connection is opened the client will indicate which website they're trying to reach in an HTTP request.

But in HTTPS, a TLS handshake takes place first, before the HTTP conversation can begin (HTTPS still uses HTTP – it just encrypts the HTTP messages). Without SNI, then, there is no way for the client to indicate to the server which hostname they're talking to. As a result, the server may produce the SSL certificate for the wrong hostname. If the name on the SSL certificate does not match the name the

client is trying to reach, the client browser returns an error and usually terminates the connection.

SNI adds the domain name to the TLS handshake process, so that the TLS process reaches the right domain name and receives the correct SSL certificate, enablir the rest of the TLS handshake to proceed as normal.

Specifically, SNI includes the hostname in the Client Hello message, or the very first step of a TLS handshake.

What is a hostname? What is a virtual hostname?

A hostname is the name of a device that connects to a network. In the context of the Internet, a domain name, or the name of a website, is a type of hostname. Both are separate from the IP address associated with the domain name.

A virtual hostname is a hostname that doesn't have its own IP address and is hosted on a server along with other hostnames. It is "virtual" in that it doesn't have a dedicated physical server, just as virtual reality exists only digitally, not in the physical world.

What is encrypted SNI (ESNI)?

Encrypted SNI (ESNI) adds on to the SNI extension by encrypting the SNI part of the Client Hello. This prevents anyone snooping between the client and server from being able to see which certificate the client is requesting, further protecting and securing the client. Cloudflare and Mozilla Firefox launched support for ESNI in 2018.

What happens if a user's browser does not support SNI?

In this rare case, the user will likely be unable to reach certain websites, and th user's browser will return an error message like "Your connection is not private."

The vast majority of browsers and operating systems support SNI. Only very old versions of Internet Explorer, old versions of the BlackBerry operating system, and other outdated software versions do not support SNI.

To learn more about the TLS/SSL protocol, SSL certificates, and how HTTPS works, see What is an SSL certificate?

RELATED CONTENT

What is SSL?

SSL Handshake

SSL Certificate Types

Public Key Cryptography

What is a Session Key?

Sales

Enterprise Sales

Become a Partner

Contact Sales:

+1 (888) 99 FLARE

About SSL/TLS

About HTTPS

About Encryption

SSL Glossary

Learning Center Navigation