Análise das versões do TLS para o .NET (VERSÃO PÚBLICA)

Sumário

1.TLS

TLS é o acrônimo de *Transport Layer Security* (Segurança em Camada de Transporte), um protocolo publicado em 1999 na RFC 2246. O objetivo principal do protocolo TLS é fornecer privacidade e integridade de dados entre dois aplicativos em comunicação. O protocolo é composto por duas camadas: o protocolo de registro TLS e o protocolo de handshake TLS. No nível mais baixo, sobreposto a algum protocolo de transporte confiável (por exemplo, TCP[TCP]), está o protocolo de registro TLS. A Figura 1 mostra como o TLS é implementado na camada de Sessão do modelo Open systems interconnection (OSI)[1].

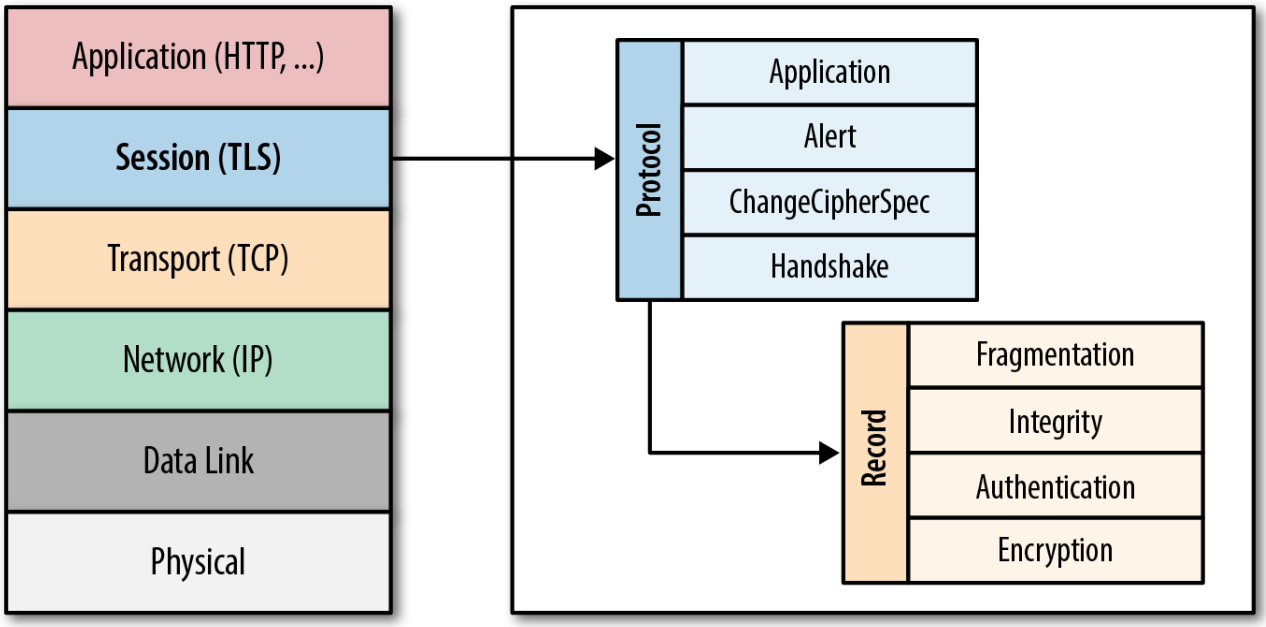

Figura 1: Arquitetura do protocolo Transport Layer Security (TLS)

1.1. Versões do TLS

O protocolo tem mais de uma versão, e assim, mais de uma implementação disponível em diversas linguagens de programação. O uso da versão mais recente é recomendável porque ela implementa o estado da arte da segurança em comunicação.

Tabela 1: Versões do TLS

Versão	RFC	Definida em
1.0	2246	1999
1.1	4346	2006
1.2	5246	2008
1.3	8446	2018

1 A especificação OSI está disponível em: https://www.iso.org/ics/35.100/x/

Há uma implementação de TLS em código livre e aberto, o OpenSSL. No lugar de implementar diretamente o TLS, as linguagens de programação podem usar o OpenSSL. A versão estável mais recente do OpenSSL é a série 3.2 com suporte até 23/11/2025. Também está disponível a série 3.1 com suporte até 14/03/2025, e a série 3.0 que é uma versão de suporte de longo prazo (LTS) com suporte até 07/09/2026. Todas as versões mais antigas versões (incluindo 1.1.1, 1.1.0, 1.0.2, 1.0.0 e 0.9.8) agora estão sem suporte e não devem ser usadas. Os usuários dessas versões mais antigas são incentivados a atualizar para 3.2 ou 3.0 o mais rápido possível. O sítio do OpenSSL contém a lista de vulnerabilidades da implementação e quais são as versões que as corrigem. A Tabela 2 mostra em quais versões de OpenSSL foi adicionado suporte às versões de TLS.

Tabela 2: Versões do OpenSSL e suporte a TLS

OpenSSL	Lançamento	Adicionou suporte a TLS
0.9.0	Não houve	1.0
0.9.1	Não houve	1.1
1.0.1	14/03/2012	1.2
3.0	07/09/2021	1.3

SSL é o acrônimo de *Secure Sockets Layer*, um protocolo publicado na versão 2.0 por uma equipe da Netscape liderada pelo criptógrafo egípcio Taher Elgamal, em 1995. O protocolo TLS foi lançado em 1999 como sucessor do SSL 3.0. O TLS é o sucessor direto do SSL, e todas as versões do SSL agora estão obsoletas. No entanto, é comum encontrar o termo *SSL* descrevendo uma conexão TLS. Na maioria dos casos, os termos *SSL* e *SSL/TLS* referem-se ao protocolo TLS e aos certificados TLS. Assim, o OpenSSL deveria se chamar OpenTLS, pois já nasceu após a obsolescência do SSL.

1.2. Versões do .NET

A versão estável mais recente do .NET é a 8.0, com suporte ativo até 10/11/2026. Essa é a versão recomendada por ter um período de suporte longo. A recomendação geral para o .NET é usar as versões pares, que tem suporte longo (*Long Term Support*). As versões ímpares são recomendadas apenas para prospecção de novas funcionalidades a serem incorporadas nas futuras versões de suporte longo. É vital que a versão de .NET em produção esteja pelo menos na fase de suporte *Maintenance*, em que ainda há atualizações para corrigir vulnerabilidades. Recomenda-se, entretanto, a atualização para a versão com suporte longo para evitar possíveis explorações de vulnerabilidades pela demora na migração de versões.

Todas as versões com suporte ativo até maio de 2024 suportam TLS 1.3. Na Tabela 3 mostramos essas versões.

Tabela 3: Versões do .NET e versões de TLS suportados

.NET	Suporte Ativo	Tipo de Suporte	TLS suportado
8.0	10/11/2026	Long Term (3 anos)	1.3
7.0	14/05/2024	Standard Term (18 meses)	1.3
6.0	12/11/2024	Long Term	1.3

Para garantir que os aplicativos .NET Framework permaneçam seguros, a versão TLS não deve ser codificada permanentemente. Os aplicativos .NET Framework devem usar a versão TLS compatível com o sistema operacional (SO). Por padrão, o .NET Framework 4.7 e versões posteriores são configurados para usar o TLS 1.2 e permitir conexões usando o TLS 1.1 ou o TLS 1.0. O TLS 1.3 é suportado desde a versão 4.8 do .NET Framework. Observe, entretanto, que as versões de .NET anteriores à 6.0 não têm mais suporte.

A recomendação para a construção de aplicações .NET é não especificar a versão do TLS, mas configurar o código para permitir que o sistema operacional decida a versão do TLS. É recomendável executar uma auditoria de código completa para verificar se você não está especificando uma versão TLS ou SSL em sua aplicação .NET.

2.Análise

Conforme relatamos no capítulo anterior, todas as versões de .NET com suporte ativo até maio de 2024 suportam TLS 1.3. A recomendação é que todas as aplicações .NET em produção no Serpro utilizem preferencialmente a versão estável com suporte ativo mais longo (a 8.0). O uso de versões de .NET sem suporte de segurança é um risco para a empresa e para seus clientes.
Considerando que o suporte da versão 6.0 de .NET termina em novembro de 2024, devem ser tomadas providências para migrar as aplicações para a versão 8.0 até o final de 2024.

A existência de versões de .NET anteriores à 6.0 é uma situação temerosa, com gravidade inversamente proporcional ao número da versão. Se existem aplicações em produção nessa situação, elas devem ser migradas com máxima urgência. Caso não seja possível uma migração direta para a versão 8.0 por causa do acúmulo de incompatibilidades, a migração pode ser planejada para ser feita mais de uma etapa (por exemplo, migrando para a versão 6 e depois para a versão 7).

3.Conclusão

Para um uso funcional e seguro de TLS com .NET, é recomendável o uso mínimo da versão 6.0, considerando que o suporte ativo será encerrado em alguns meses.
A recomendação para versões de .NET inferiores a 6.0 é apenas uma: migração imediata para a versão ativa mais recente possível.

Este documento foi finalizado em 8 de março de 2024.