Changes required while using Exchange 2019 as HTTPS Real Server

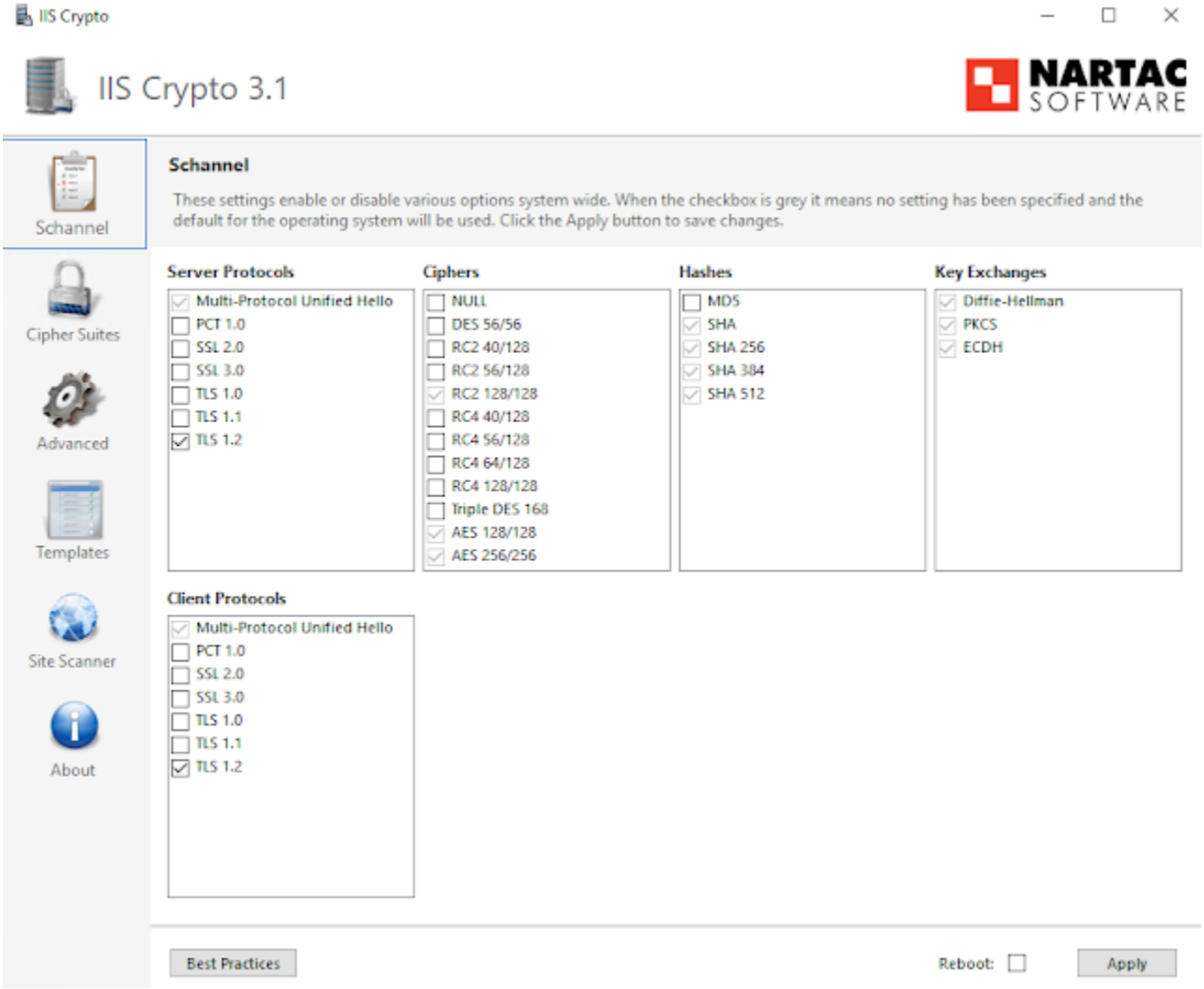
🤔 Problem

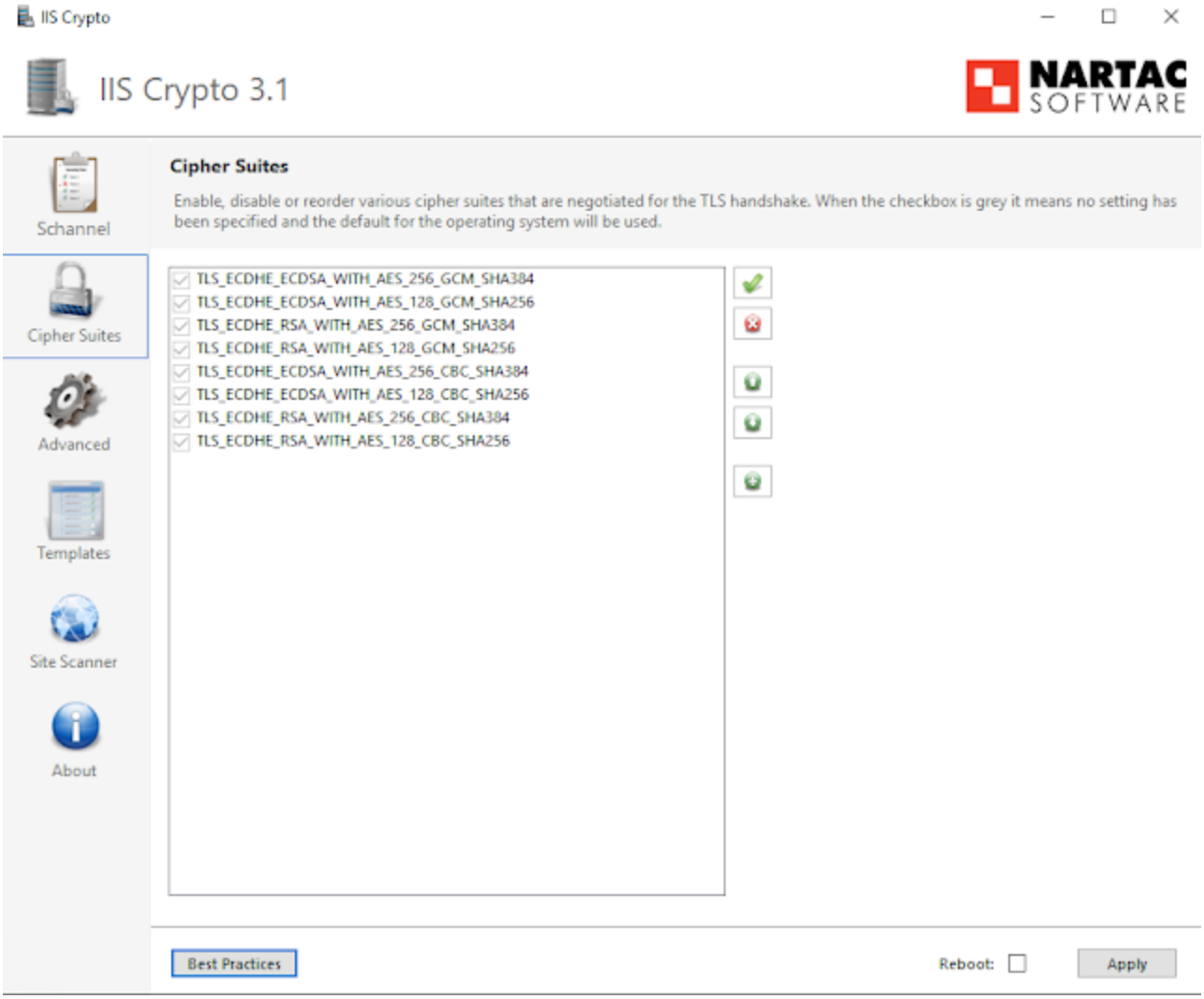
When we mapped Exchange 2019 servers on existing Group and existing SSL Real Host, application was not working.Whereas it was working fine with old Exchange 2013 Servers.

Solution was tested on `ArrayOS Rel.APV.8.6.1.199`

🌱 Solution

Microsoft Exchange 2019 is secured by default and allows only TLS 1.2. Therefore default schannel settings are as follows (using IISCrypto tool from Nartac Software):

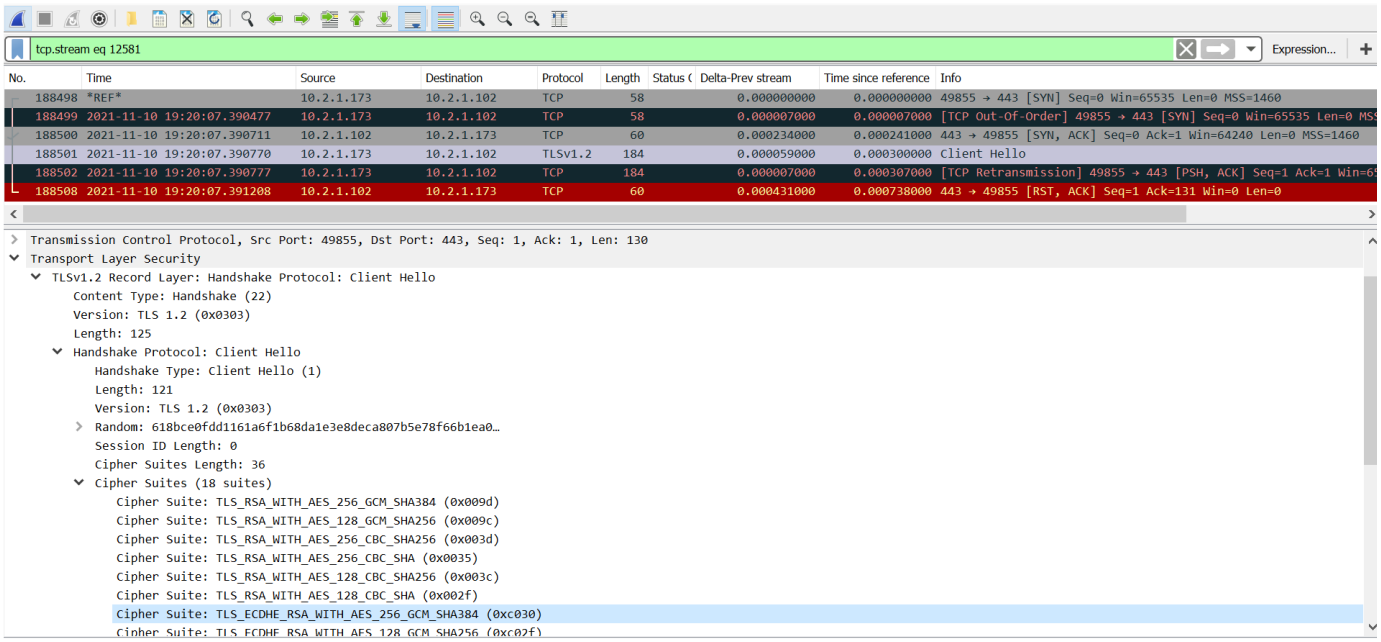




Hence select correct TLS version and appropriate cipher suites.

In Exchange 2019 servers it is observed that because of security update for [IETF RFC5746](#) , insecure renegotiation is disabled by default.

Due to this TLS handshake fails as Server sends TCP reset and closes connection.



This setting is controlled by below registry keys

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL
The following table shows how these DWORD values can be used:

DWORD	Value = zero	Value = nonzero
AllowInsecureRenegoClients	Strict Server	Compatible Server
AllowInsecureRenegoServers	Strict Client	Compatible Client

In order to disable strict server mode we need to set the value of this registry key to 1

Once we make these changes connections to real servers starts working.

"AllowInsecureRenegoClients"=dword:00000001

"AllowInsecureRenegoServers"=dword:00000001

References :

https://www.exchangelog.info/2020/02/netscaler-vs-exchange-2019-time-out.html

https://support.microsoft.com/en-us/topic/ms10-049-vulnerabilities-in-schannel-could-allow-remote-code-execution-d4258037-ad3a-c00c-250f-6c67a408bd7c