

Changes required while using Exchange 2019 as HTTPS Real Server

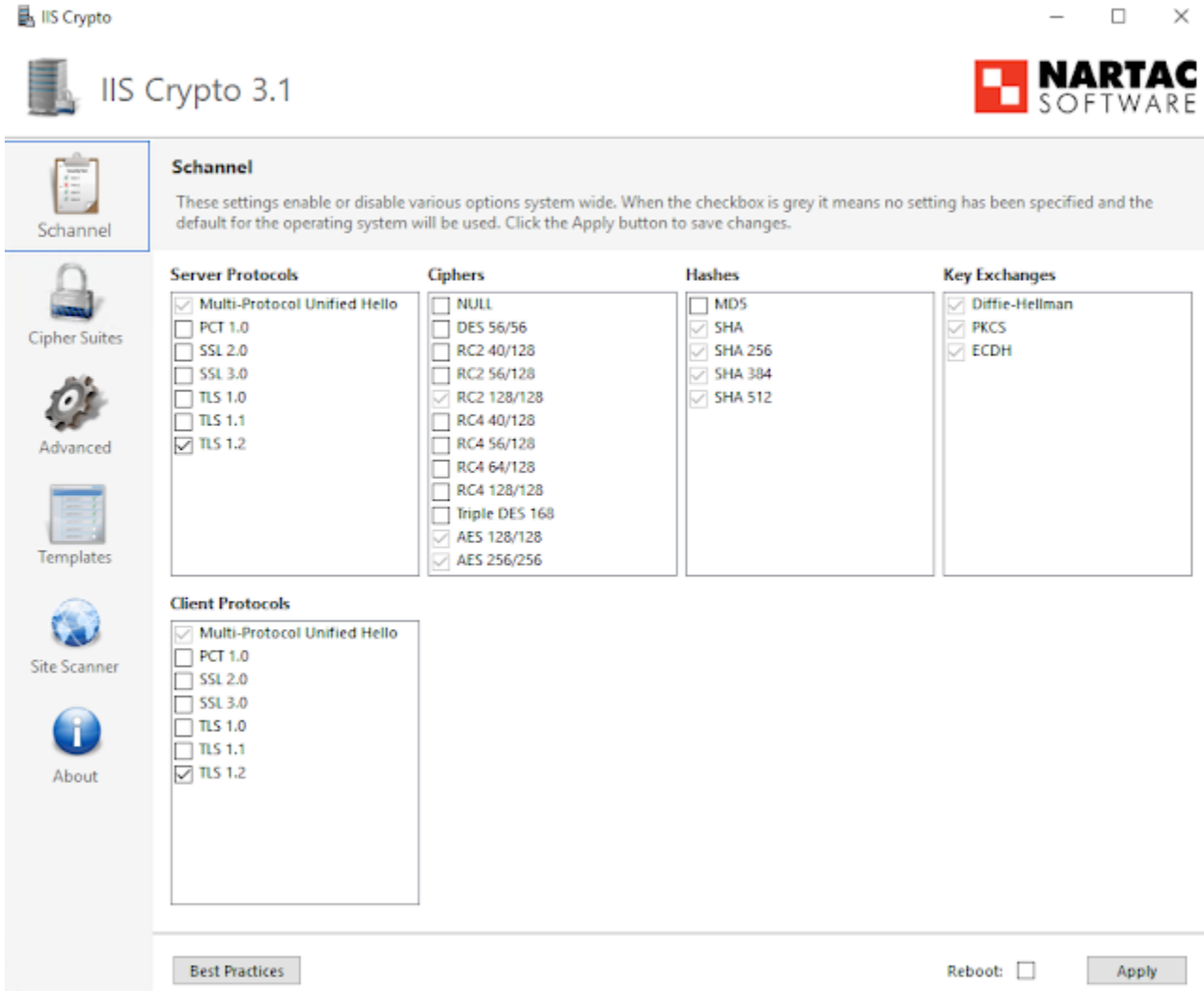
🤔 Problem

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):



The screenshot shows the IIS Crypto 3.1 application window. The title bar reads "IIS Crypto 3.1" and the NARTAC SOFTWARE logo is in the top right corner. The main window is titled "Schnannel" and contains the following settings:

Schnannel
These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used. Click the Apply button to save changes.

Server Protocols	Ciphers	Hashes	Key Exchanges
<input checked="" type="checkbox"/> Multi-Protocol Unified Hello	<input type="checkbox"/> NULL	<input type="checkbox"/> MD5	<input checked="" type="checkbox"/> Diffie-Hellman
<input type="checkbox"/> PCT 1.0	<input type="checkbox"/> DES 56/56	<input checked="" type="checkbox"/> SHA	<input checked="" type="checkbox"/> PKCS
<input type="checkbox"/> SSL 2.0	<input type="checkbox"/> RC2 40/128	<input checked="" type="checkbox"/> SHA 256	<input checked="" type="checkbox"/> ECDH
<input type="checkbox"/> SSL 3.0	<input type="checkbox"/> RC2 56/128	<input checked="" type="checkbox"/> SHA 384	
<input type="checkbox"/> TLS 1.0	<input type="checkbox"/> RC2 128/128	<input checked="" type="checkbox"/> SHA 512	
<input type="checkbox"/> TLS 1.1	<input type="checkbox"/> RC4 40/128		
<input checked="" type="checkbox"/> TLS 1.2	<input type="checkbox"/> RC4 56/128		
	<input type="checkbox"/> RC4 64/128		
	<input type="checkbox"/> RC4 128/128		
	<input type="checkbox"/> Triple DES 168		
	<input checked="" type="checkbox"/> AES 128/128		
	<input checked="" type="checkbox"/> AES 256/256		

Client Protocols

<input checked="" type="checkbox"/> Multi-Protocol Unified Hello
<input type="checkbox"/> PCT 1.0
<input type="checkbox"/> SSL 2.0
<input type="checkbox"/> SSL 3.0
<input type="checkbox"/> TLS 1.0
<input type="checkbox"/> TLS 1.1
<input checked="" type="checkbox"/> TLS 1.2

At the bottom of the window, there is a "Best Practices" button, a "Reboot:" checkbox, and an "Apply" button.

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>