QlikView

Force SSL 3.0 and TLS 1.0 IIS web server communication

Version:	1
Date:	2011-11-28
Author(s)	Frederik Nünning (FNG)
OS	Microsoft Windows 2008 R2
QV	QlikView 10 SR3

”A best practice is a technique or methodology that, through experience and research, has proven to reliably lead to a desired result.”

Contents

1 Motivation

Security is an important topic when data is accessed from the internet into a local network. Sometimes older security methods have been levered or do not stand the current security policies of large enterprise networks. This small article shows in details how to setup IIS webserver to communicate via SSL 3.0 and/or TLS 1.0 instead of SSL 2.0 which is the default setup in Windows Server 2008. SSL 2.0 has some known issues and it is possible to decrypt the traffic.

2 Change SSL Configuration

All changes to the SSL configuration of a Windows Server have to be made in the registry. So we use the tremendous graphical tool “regedit”. First start “regedit.exe” and navigate to the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

Export the complete “Protocols” key into a reg-file. If anything goes wrong, the old entries can be restored.

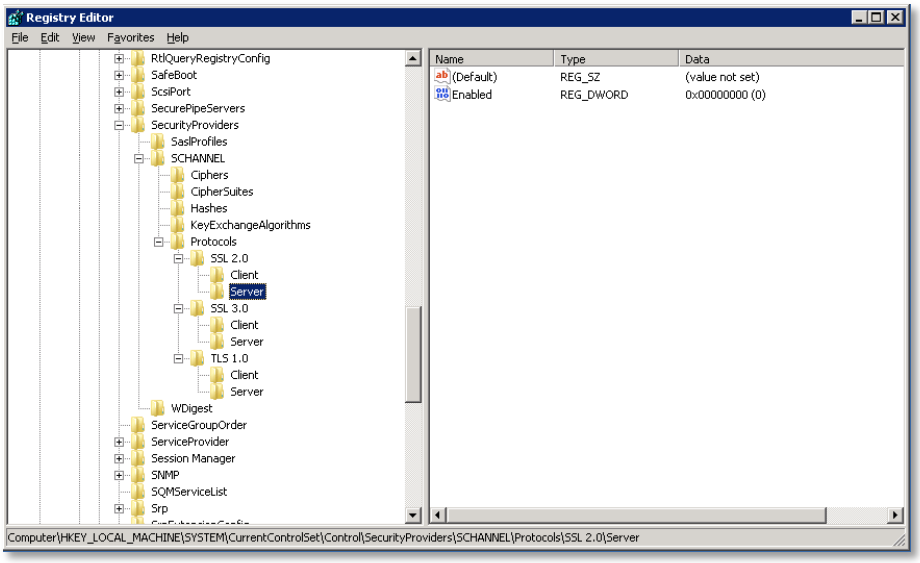
After the default installation of Windows Server you will just find a key called “**SSL 2.0\Client**”. Several other Keys need to be created:

- **SSL 2.0\Server**
- **SSL 3.0\Client**
- **SSL 3.0\Server**
- **TLS 1.0\Client**
- **TLS 1.0\Server**

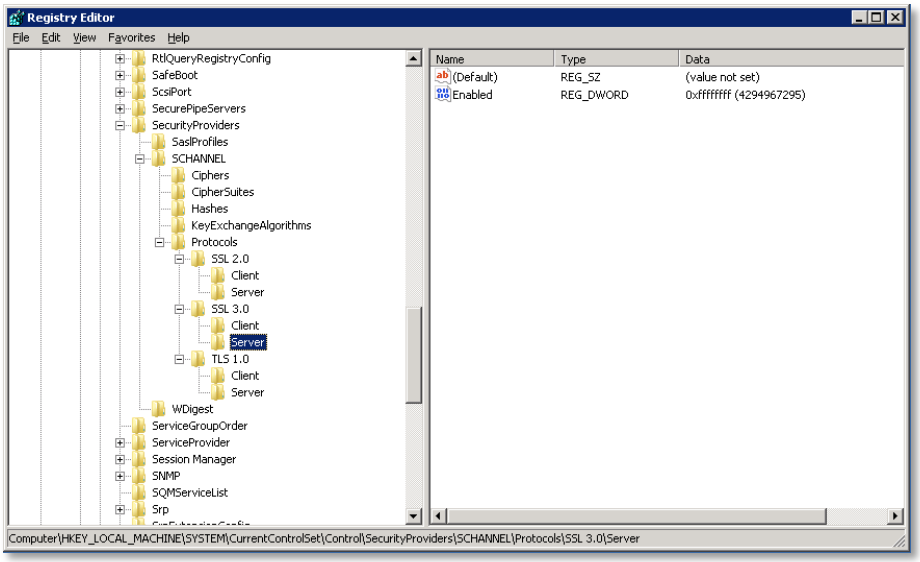
In this example SSL 2.0 is going to be **disabled**, SSL 3.0 and TLS 1.0 **enabled**:

To disable SSL 2.0 a new DWORD entry with the name “**Enabled**” must be created. The value for this entry is “**00000000**”. Enabling SSL 3.0 and TLS 1.0 requires the DWORD entry to be set to “**FFFFFFFF**”.

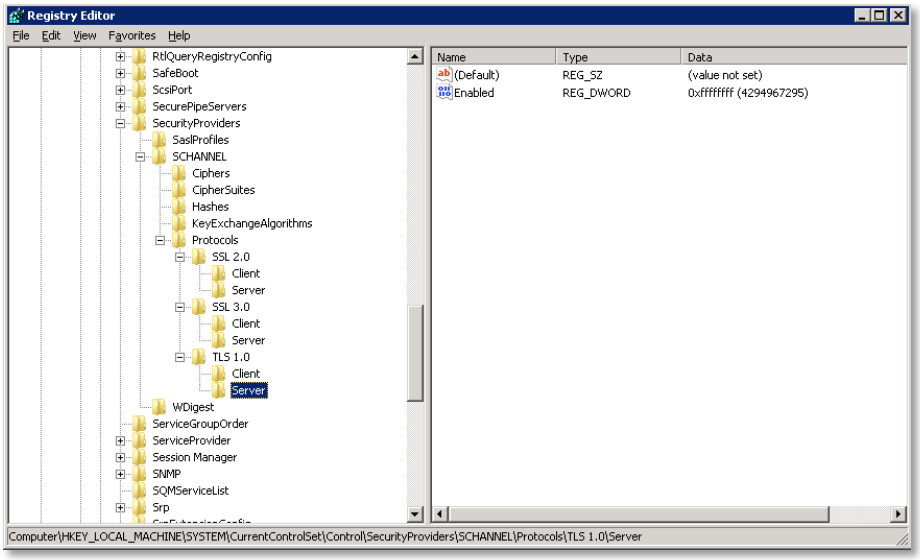
SSL 2.0



SSL 3.0



TLS 1.0



To ensure the client configuration meets the server configuration, the DWORD entries should also be made in the “Client” keys in each SSL/TLS configuration.

Microsoft advises to restart the server after the configuration has been changed!

3 Registration file

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]
"DisabledByDefault"=dword:00000001
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
"Enabled"=dword:ffffffff
```