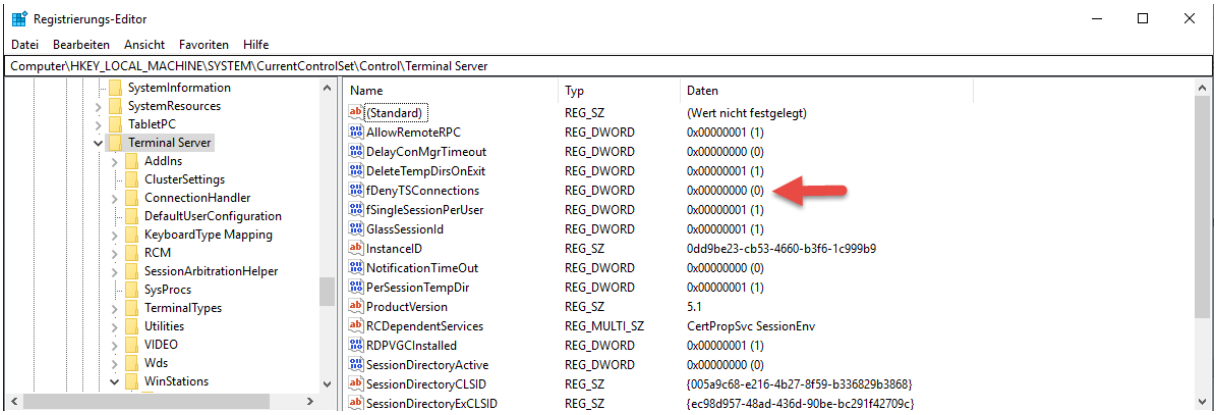
Sicherheitsempfehlung beim Einsatz von RDP

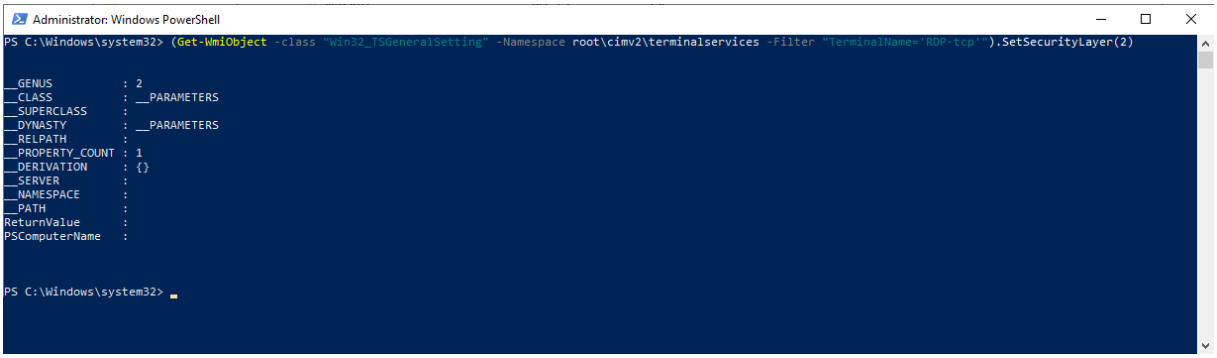
Zuerst aktivieren wir Remote Desktop.

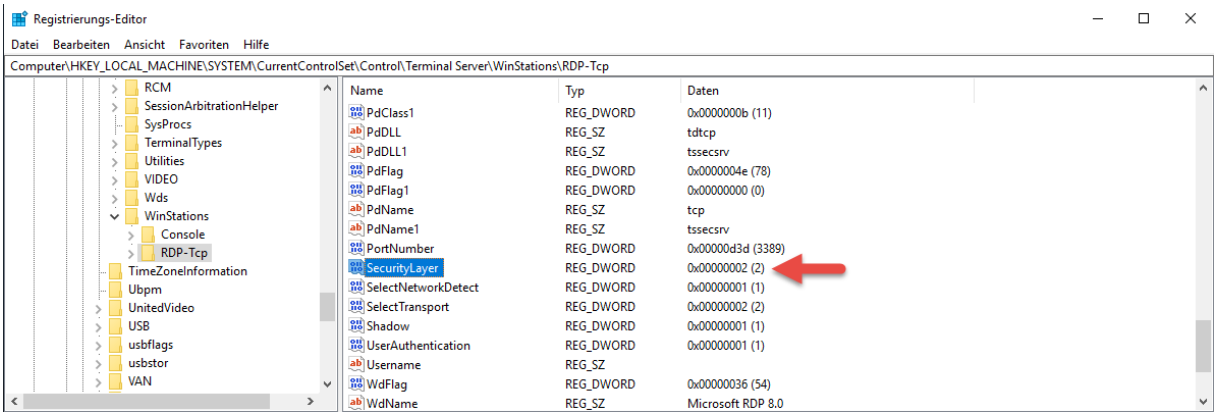
```
Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server" -Name "fDenyTSConnections" –Value 0
```



Dann stellen wir den Security Layer auf TLS ein:

```
(Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp'").SetSecurityLayer(2)
```





Erklärung zu den möglichen Parametern:

SecurityLayer = 0 - Bei einer niedrigen Sicherheitsstufe wird das genutzt was der Client anzubieten hat.

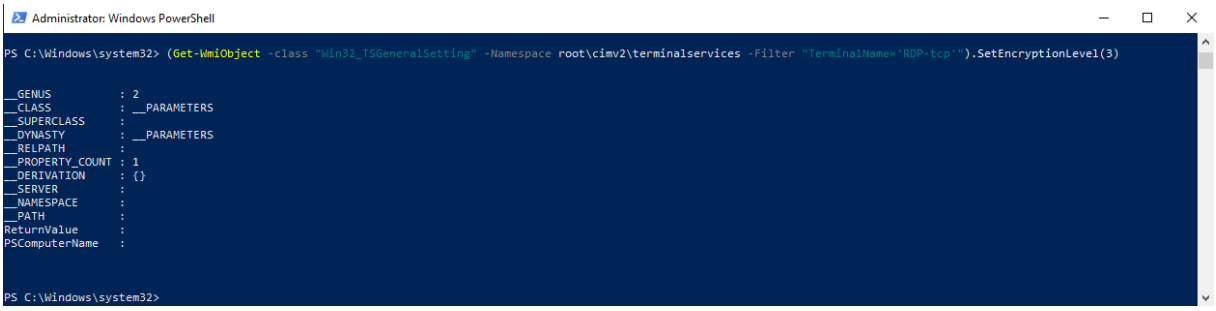
SecurityLayer = 1 - Bei einer mittleren Sicherheitsstufe verhandeln Server und Client die Authentifizierungsmethode aus, bevor eine Remotedesktopverbindung hergestellt wird.

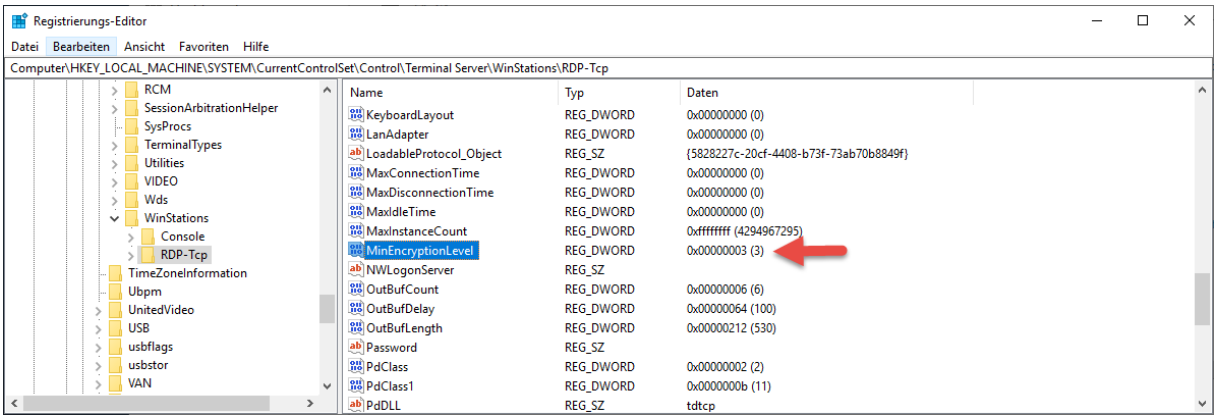
SecurityLayer = 2 - Mit der hohen Sicherheitsstufe wird TLS erzwungen!

Erstellt von Jörn Walter **28.03.2020**

Dann setzen wir den Client Connection Encryption Level auf HIGH-Level. Jetzt wird vorausgesetzt das mindestens 128 Bit eingesetzt wird. Es folgt nun mehr keine Aushandlung der Verschlüsselungsstufe zwischen Client und Server. Kann ein Partner nicht mindestens 128 Bit anbieten, wird der Verbindungsversuch sofort beendet.

(Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp'").SetEncryption**Level**(3)





Erklärung zu den Encryption-Level-Parametern:

Niedrig (1): Alle vom Client an den Server gesendeten Daten sind mindestens mit 56-Bit verschlüsselt. Der Server sendet an den Client aber unverschlüsselt.

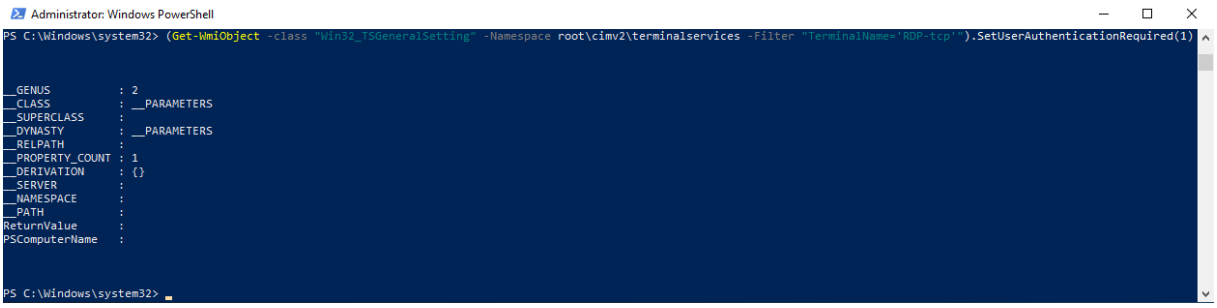
Client-kompatibel (2): Alle zwischen dem Client und dem Server gesendeten Daten sind verschlüsselt, basierend auf der vom Client unterstützten maximalen Schlüsselstärke. Ist nur was für sehr alte Umgebungen! Sollte es heute gar nicht mehr geben.

Hoch (3): Alle zwischen dem Client und dem Server gesendeten Daten sind mindestens 128-Bit verschlüsselt.

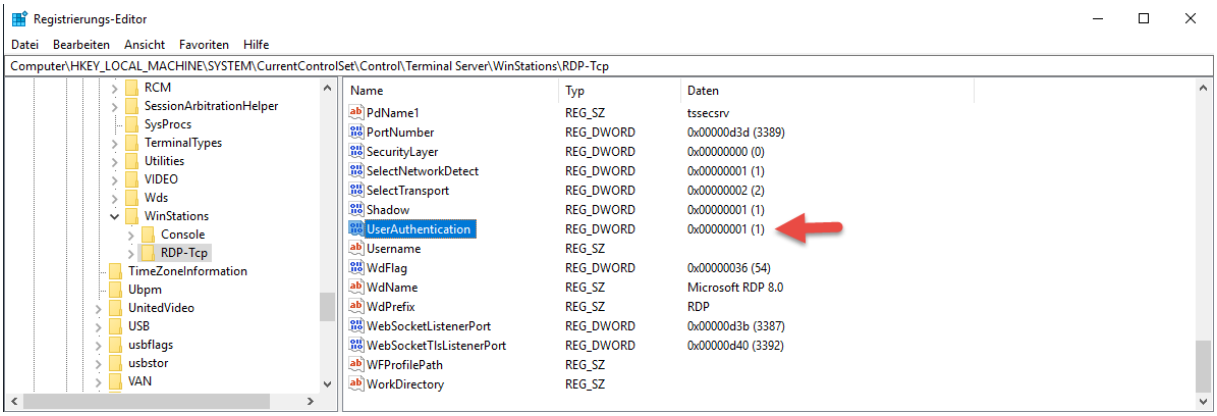
FIPS (4): Alle zwischen Client und Server gesendeten Daten werden mit validierten Verschlüsselungsmethoden gemäß Federal Information Processing Standard 140-1 geschützt. Hierbei handelt es sich um die höchste Sicherheitsstufe. Diese sollte nur eingesetzt werden, wenn alle Partner kompatibel sind.

Dann aktivieren wir die User Authentication (NLA) für Remote Desktop:

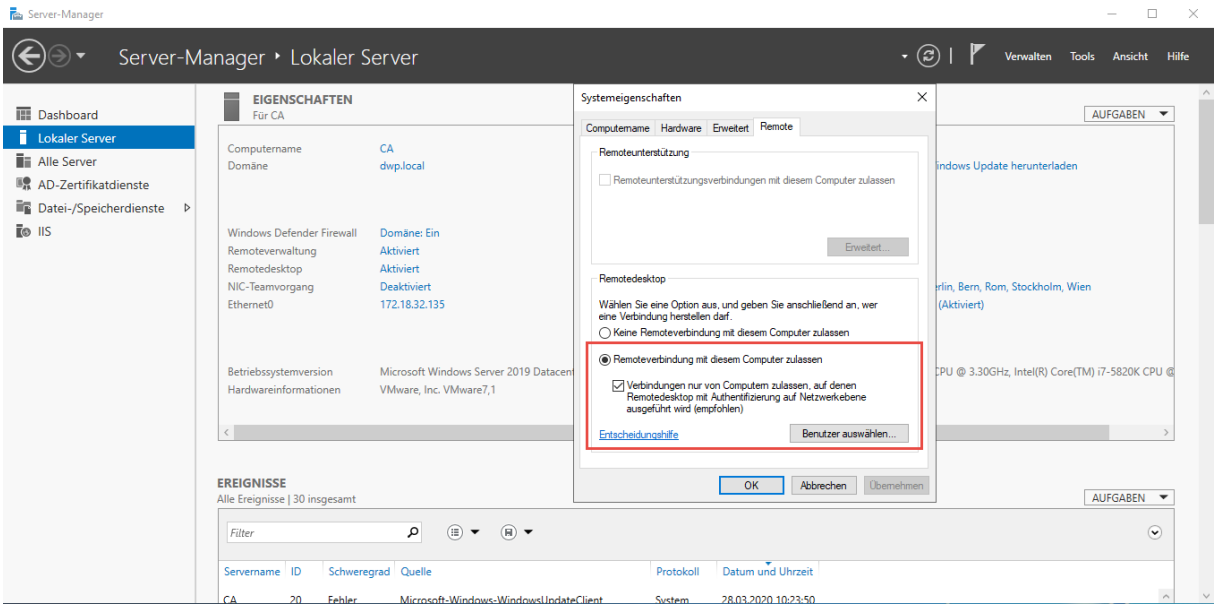
```
(Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp'").SetUserAuthenticationRequired(1)
```



Das bedeutet, das sich der Benutzer auf Netzwerkebene (Kerberos, NTLM) authentifizieren muss.



Das Ergebnis der empfohlenen Einstellungen sieht dann wie folgt aus:



Dann aktivieren wir die Firewall-Gruppenregeln für Remote Desktop:

Englisches OS:

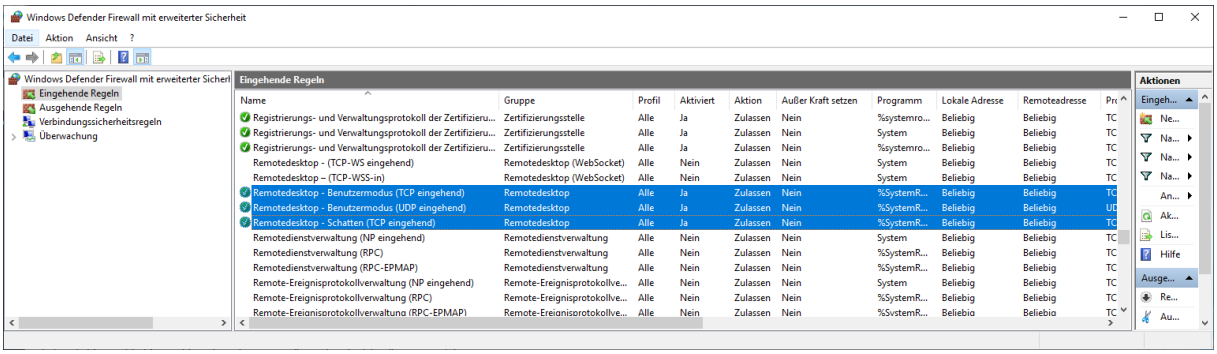
```
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
```

oder

```
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

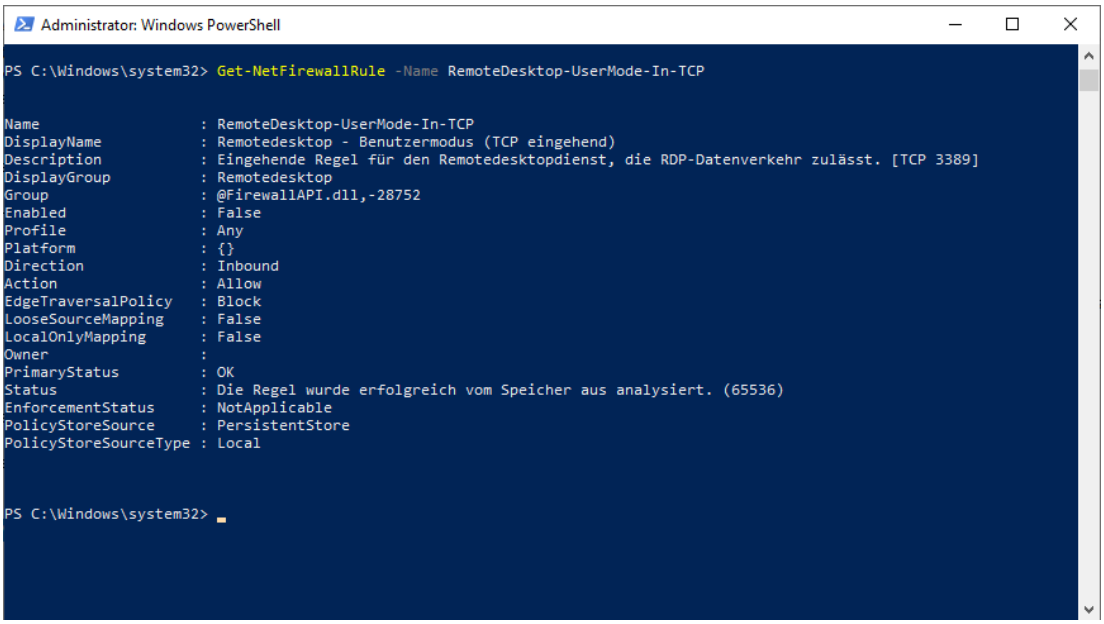
Deutsches-OS:

```
netsh advfirewall firewall set rule group="RemoteDesktop" new enable=yes
```



Firewall-Regeln für RDP gezielt abfragen:

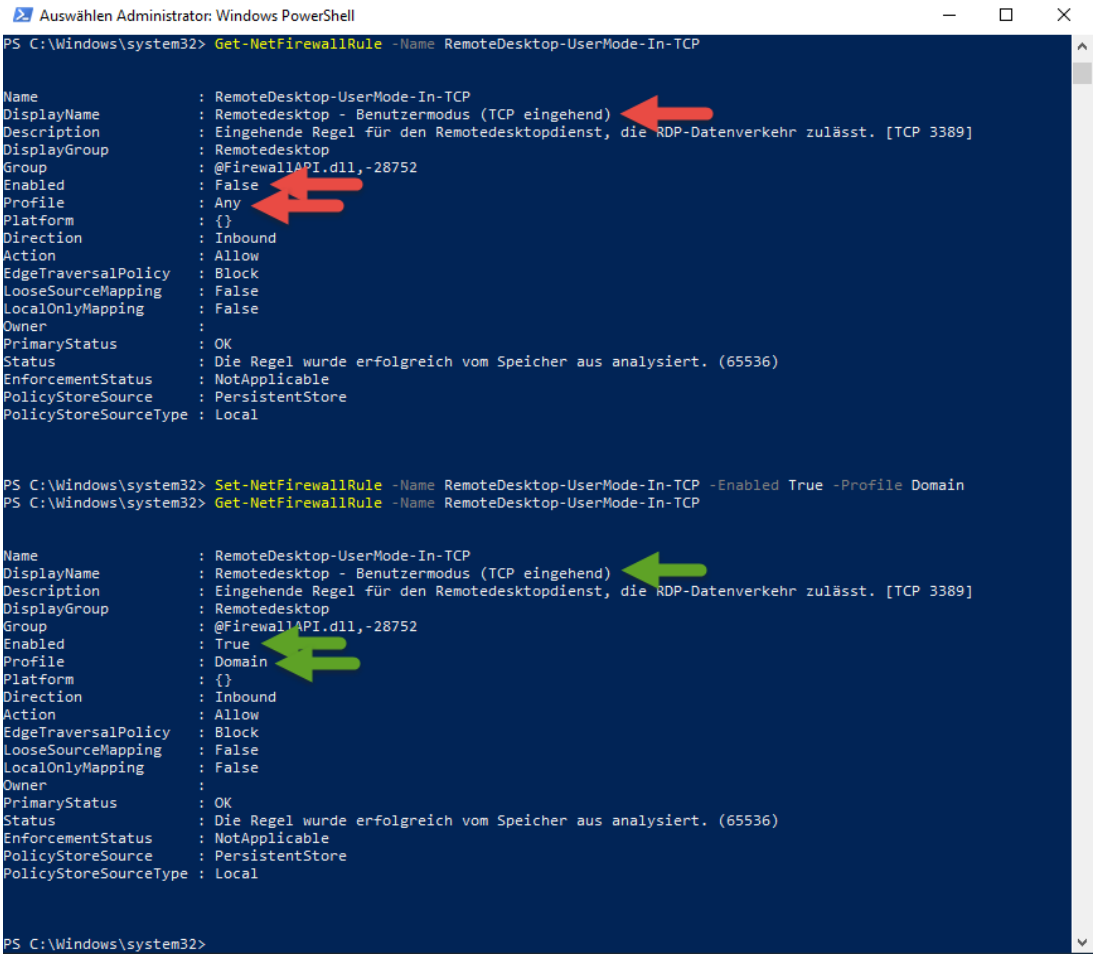
```
Get-NetFirewallRule -Name RemoteDesktop-UserMode-In-TCP
```



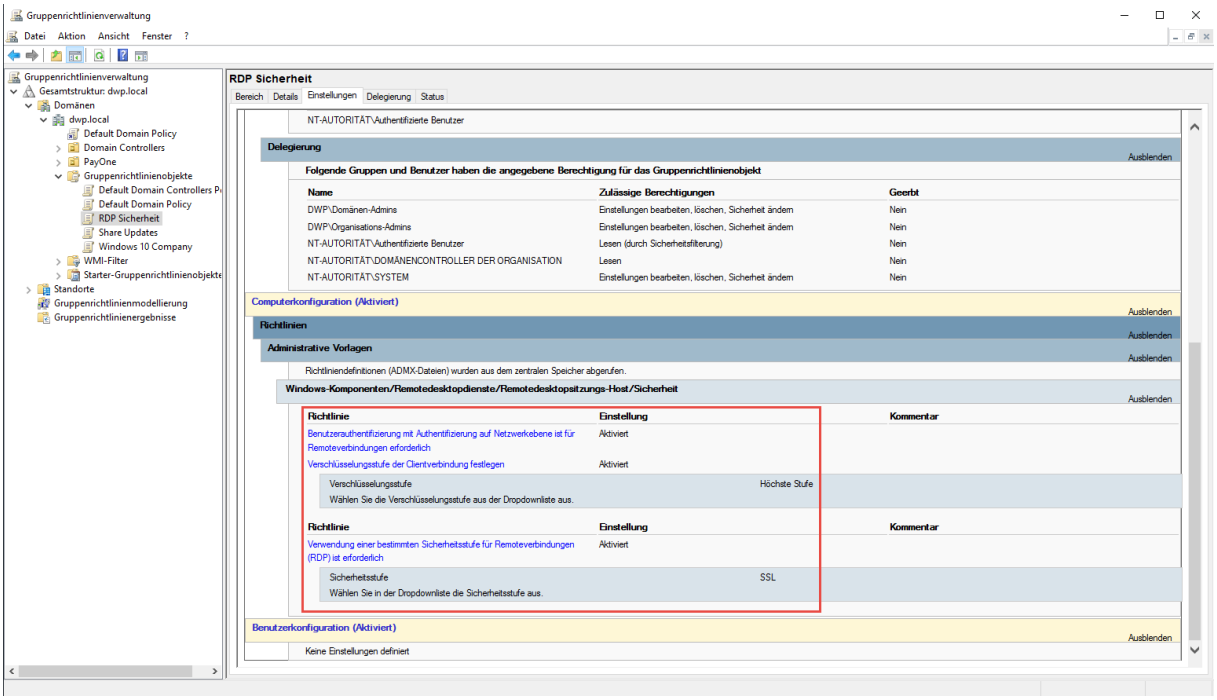
Sicherheitsempfehlung beim Einsatz von RDP

Die Firewall gezielt für die Domäne aktivieren:

Set-NetFirewallRule -Name RemoteDesktop-UserMode-In-TCP -Enabled True -Profile Domain



Die oben gezeigten Einstellungen spiegeln diese Richtlinie wieder.



Optional

RDP per REG-KEY deaktivieren:

```
reg add “HKEY_LOCAL_MACHINE\SYSTEM\CurRentControlSet\Control\Terminal Server” /v fDenyTSConnections /t REG_DWORD /d 1 /f
```

RDP per Powershell deaktivieren:

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-name "fDenyTSConnections" -Value 1
```

Abfrage des NLA-Levels (Network Authentication Level):

```
(Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp'").UserAuthenticationRequired
```

Firewall (RDP Gruppe) wieder deaktivieren:

```
Disable-NetFirewallRule -DisplayGroup "RemoteDesktop"
```