Firewall – Restricted Settings

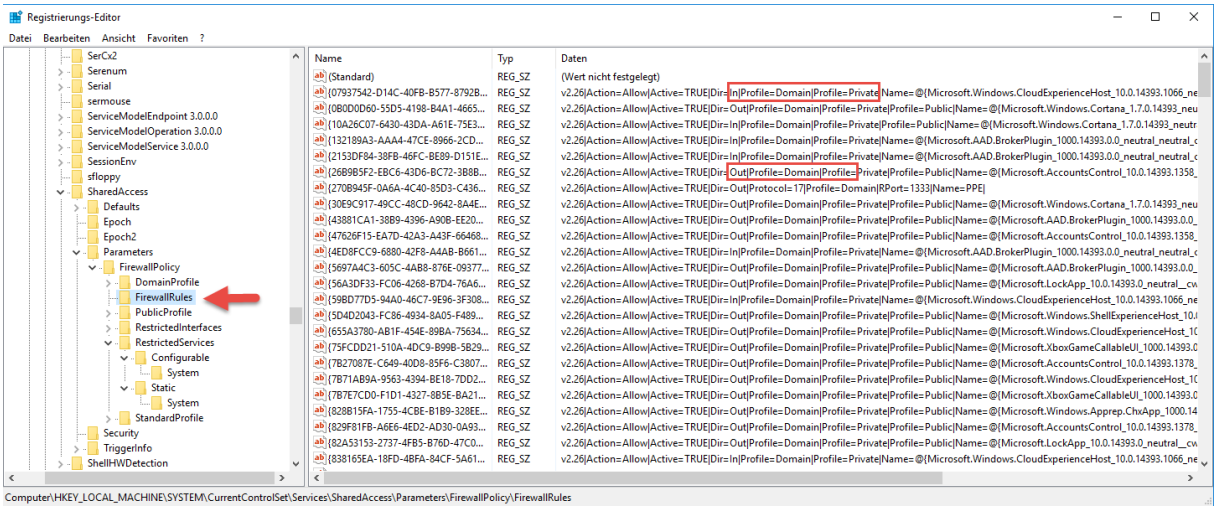
Die Windows Firewall wird in der Regel zur übersichtlichen Konfiguration und Einsicht über die GUI administriert. Mit der Einführung von Windows Server 2008 hat Microsoft das Windows Service **Hardening** (WSH) eingeführt. Betroffen davon ist auch die Windows Firewall.

Das bedeutet, dass es Windows Firewall Regeln gibt, die über die GUI nicht angezeigt bzw. ausgewertet werden können, aber immer angewendet werden, auch dann wenn die Windows Firewall abgeschaltet wird. Das gilt für eingehende sowie ausgehende Verbindungen.

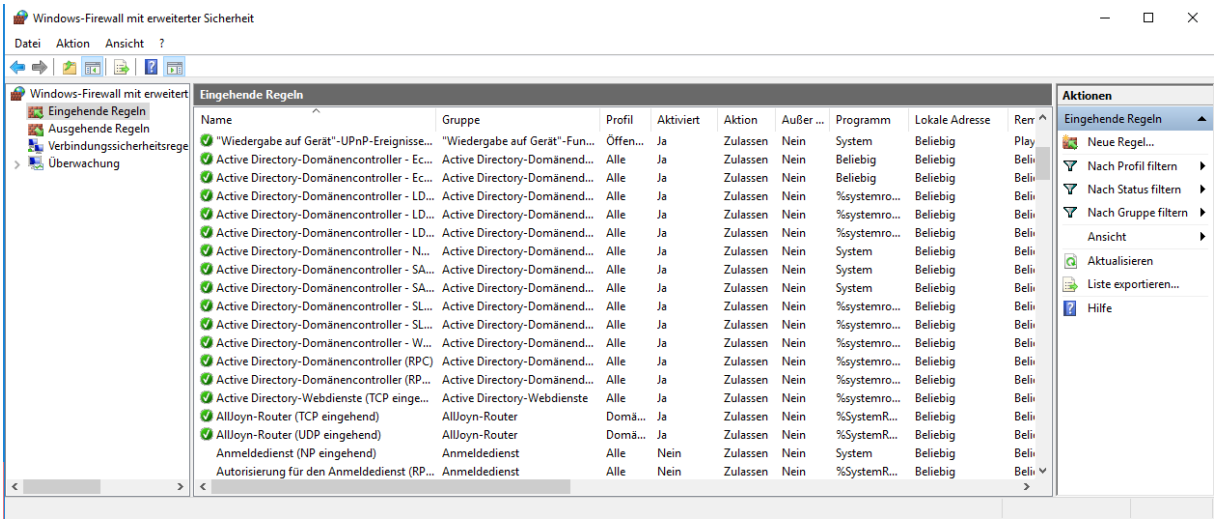
Diese Regeln lassen sich entweder über die Registry anpassen oder über die Schnittstelle namens **NetFwServiceRestriction**.

Schauen wir uns zu allererst die Registry an. In diesem Zweig finden wie alle lokalen Firewall Regeln:

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules



Diese spiegeln sich mit der GUI wieder:

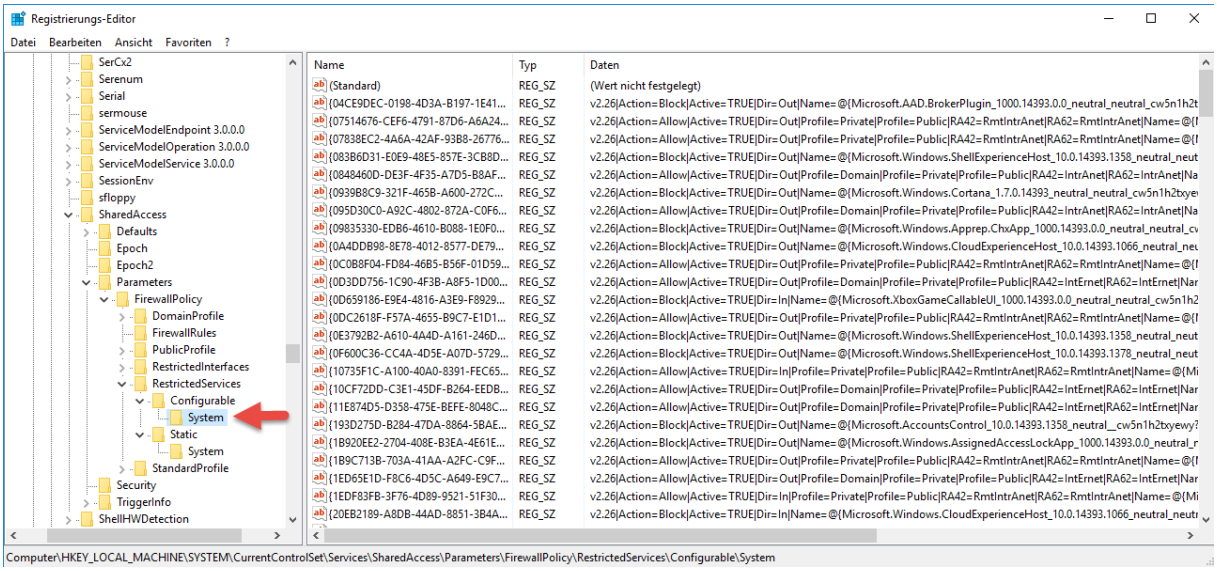


Firewall – Restricted Settings

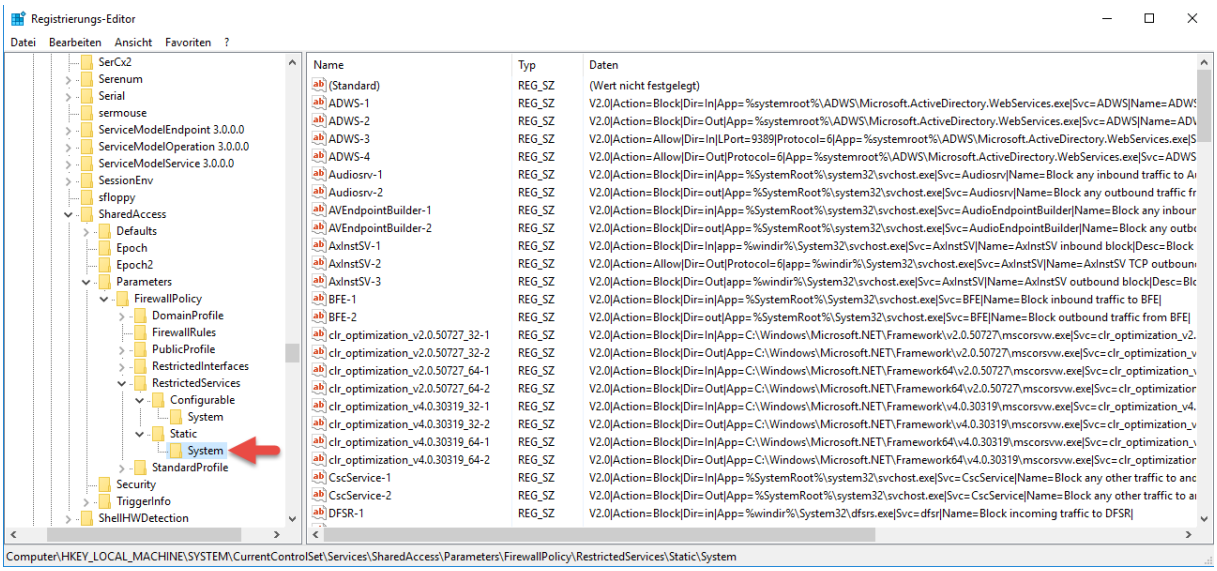
Kommen wir nun zu den Restricted Firewall Regeln:

Diese Regeln werden wir über die GUI nicht einsehen können.

Restricted > Configurable



Restricted > Static



Mit Hilfe der Powershell ist es möglich die Restricted Firewall Regeln auslesen, zu verändern oder zu erstellen.

Firewall – Restricted Settings

Wie bereits oben erwähnt ist das mittels der Schnittstelle **NetFwServiceRestriction** möglich.

Der ActiveStore ist der Speicher also die Summe aller Regeln die auf dieser Maschine eingestellt sind; GPOs, lokale Regeln etc.

 # Alle Regeln aus dem Active Store abfragen
Get-NetFirewallRule -PolicyStore ActiveStore

 # Individuelle Regel aus dem Active Store abfragen
Get-NetFirewallRule -Name "{505ED865-63AB-4B7B-B32E-4795B04BD182}" -PolicyStore ActiveStore

 # Individuelle Regel aus dem Active Store nach Displayname abfragen
Get-NetFirewallRule -DisplayName "Überwachung für virtuelle Computer (DCOM eingehend)" -PolicyStore ActiveStore

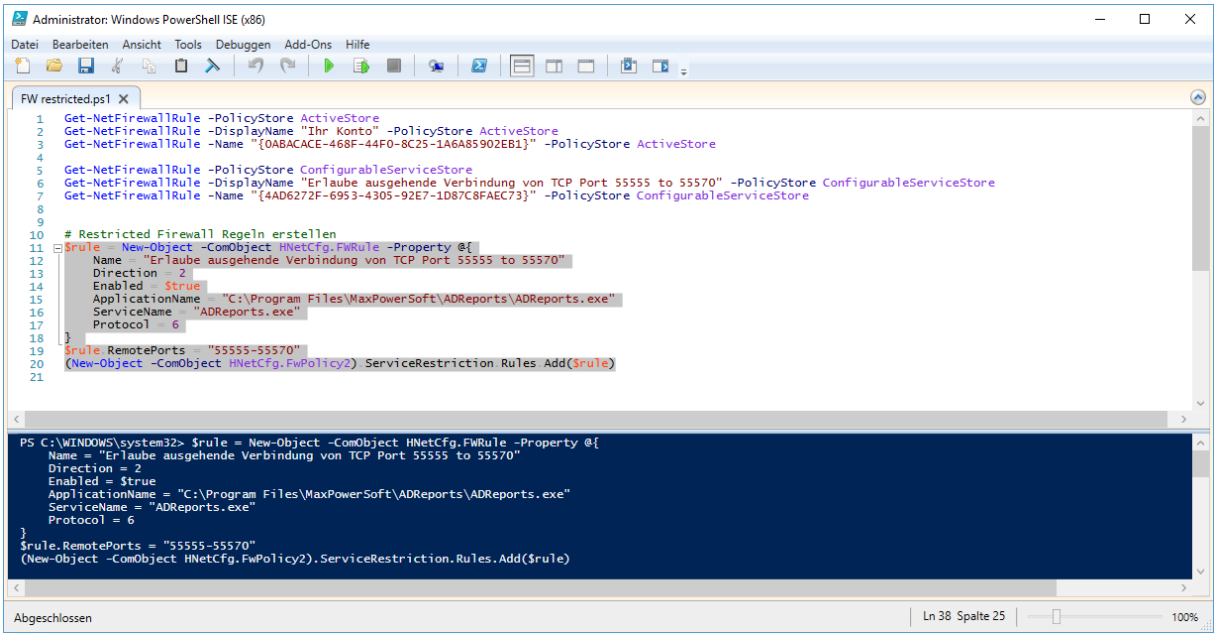
 # Alle Regeln aus dem Service Store abfragen
Get-NetFirewallRule -PolicyStore ConfigurableServiceStore

 # Individuell Regel aus dem Service Store abfragen
Get-NetFirewallRule -Name "{4AD6272F-6953-4305-92E7-1D87C8FAEC73}" -PolicyStore ConfigurableServiceStore

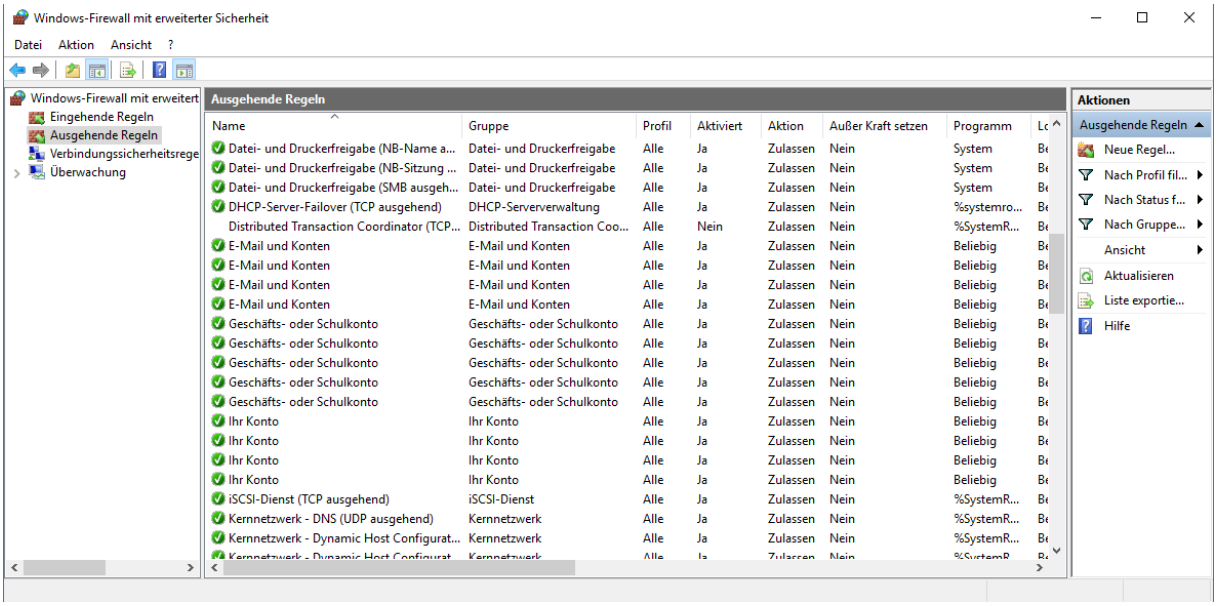
 # Individuelle Regel aus dem Service Store nach Displayname abfragen
Get-NetFirewallRule -DisplayName "MSN Wetter" -PolicyStore ConfigurableServiceStore

Firewall – Restricted Settings

```
# Restricted Firewall Regeln erstellen
$rule = New-Object -ComObject HNetCfg.FWRule -Property @{
    Name = "Erlaube ausgehende Verbindung von TCP Port 55555 to 55570"
    Direction = 2
    Enabled = $true
    ApplicationName = "C:\Program Files\MaxPowerSoft\ADReports\ADReports.exe"
    ServiceName = "ADReports.ps1"
    Protocol = 6
}
$rule.RemotePorts = "55555-55570"
(New-Object -ComObject HNetCfg.FwPolicy2).ServiceRestriction.Rules.Add($rule)
```

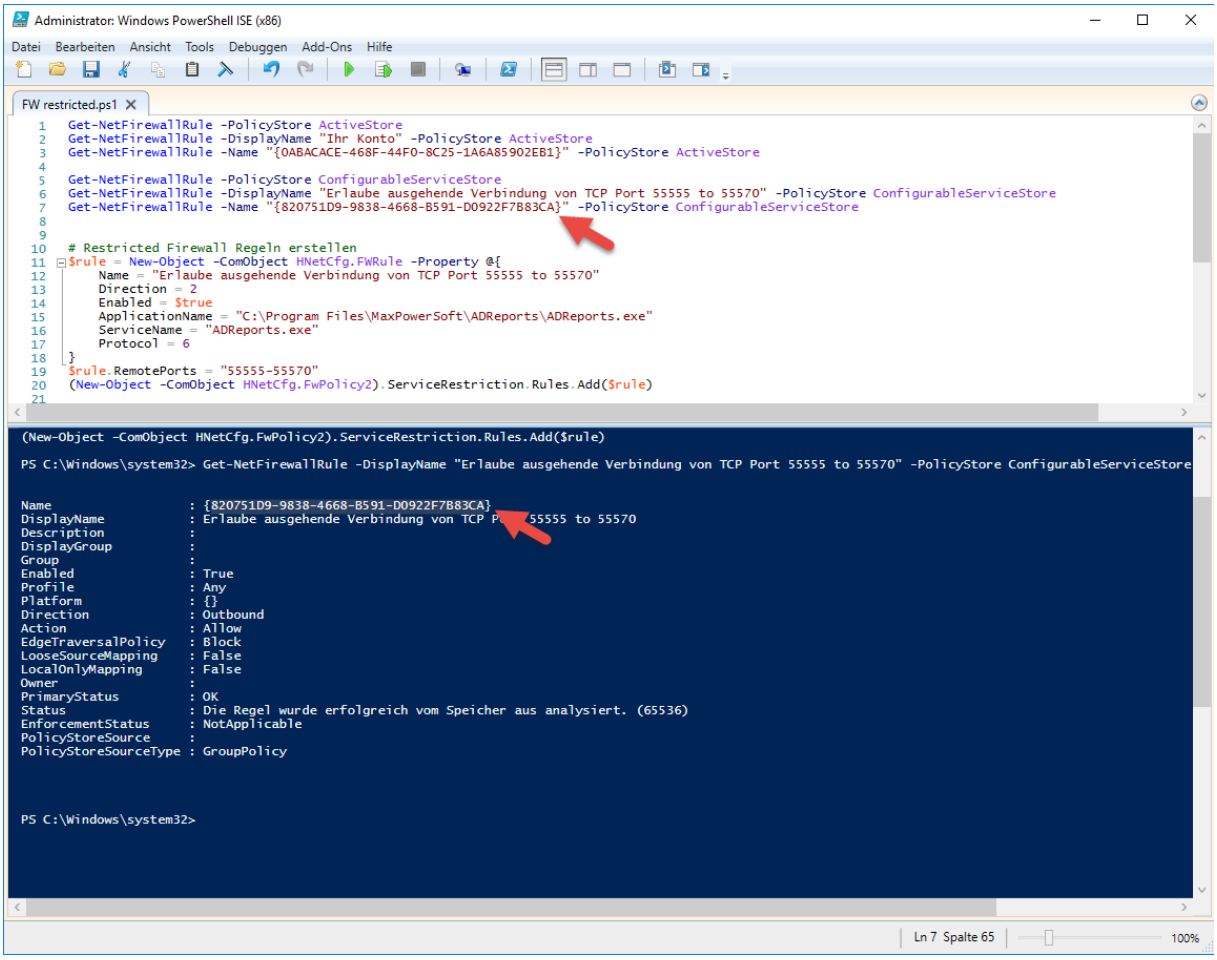


Firewall und Service neustarten! Diese geheime Regel finden wir über die GUI nicht wieder. Ist aber aktiv und das auch bei ausgeschalteter Firewall!

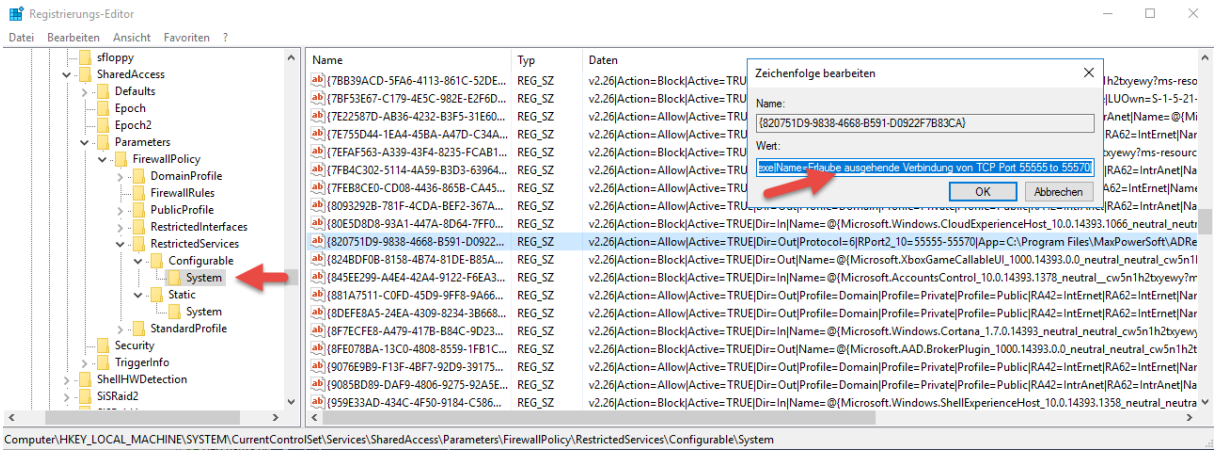


Firewall – Restricted Settings

Das Ganze prüfen wir jetzt in dem wir uns die Regel anzeigen lassen. Ich suche erst nach dem Displaynamen, kopiere mit die ID und starte die Suche nach der ID erneut.



Mithilfe der ID durchsuche ich jetzt die Registry: Voila!



Firewall – Restricted Settings

Nächstes Beispiel:

SNMP spricht nach Default Vorgaben von Microsoft UDP Port 161 und 162.

Möchten wir aber das SNMP ein- und ausgehend über TCP Port 3216 spricht dann gehen wir wie folgt vor.

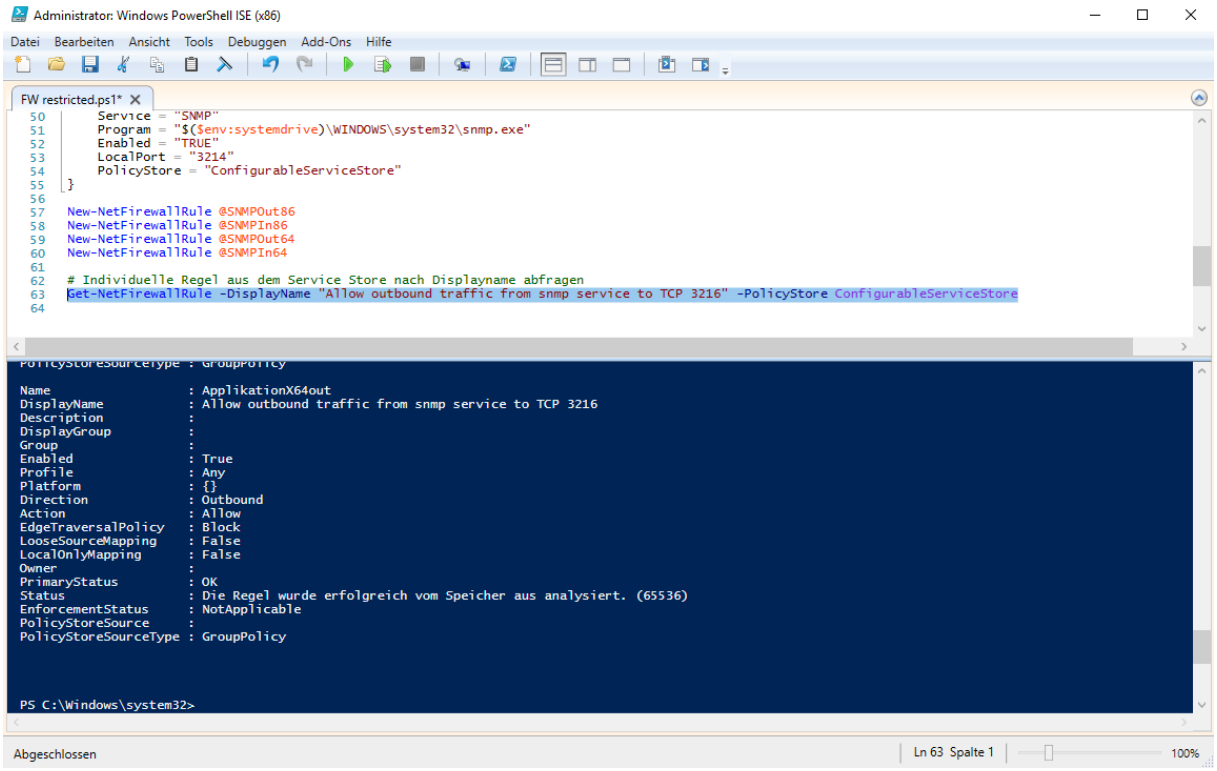
```
$SNMPIN = @{

Name = "ApplikationX64Out"
DisplayName = "Allow outbound traffic from snmp service to TCP 3216"
Direction = "Outbound"
InterfaceType = "Any"
Action =  "Allow"
Protocol =  "TCP"
Service = "SNMP"
Program = "$($env:systemdrive)\WINDOWS\SysWOW64\snmp.exe"
Enabled = "TRUE"
RemotePort = "3216"
PolicyStore = "ConfigurableServiceStore"
}

New-NetFirewallRule @SNMPIN

$SNMPOut = @{

Name = "ApplikationX64In"
DisplayName = "Allow outbound traffic from snmp service to TCP 3216"
Direction = "Outbound"
InterfaceType = "Any"
Action =  "Allow"
Protocol =  "TCP"
Service = "SNMP"
Program = "$($env:systemdrive)\WINDOWS\SysWOW64\snmp.exe"
Enabled = "TRUE"
RemotePort = "3216"
PolicyStore = "ConfigurableServiceStore"
}

New-NetFirewallRule @SNMPOut
```

Erstellen die Regeln in dem wir das Skript ausführen.

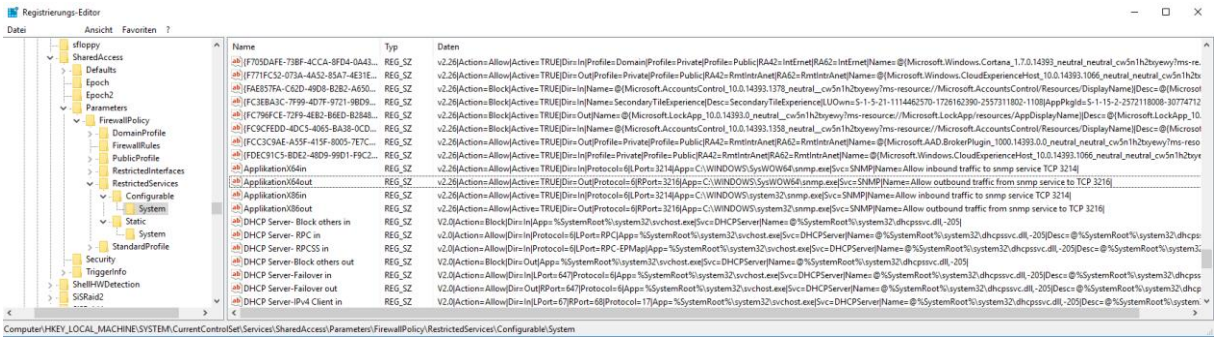
Firewall – Restricted Settings

Fragen die Regeln ab:

Get-NetFirewallRule -DisplayName "Allow outbound traffic from snmp service to TCP 3216" -PolicyStore ConfigurableServiceStore



Auch in der Registry wurden die Regeln sauber unter RestrictedServices angelegt und sind über die GUI nicht einzusehen.



Firewall – Restricted Settings

Get-NetFirewallProfile
Get-NetFirewallProfile -Profile Private
Get-NetFirewallProfile -Profile Domain

Get-NetFirewallRule | Measure
Get-NetFirewallRule -Enabled True | Measure

Get-NetFirewallRule | where {$_.Direction -eq "Inbound" -and (($_.Profile -contains "Any") -or ($_.Profile -contains "

Get-NetFirewallRule -Name "ICMPv4" | Set-NetFirewallRule -Action BlockPublic"))}

Set-NetFirewallProfile -Enabled false
Set-NetFirewallProfile -Enabled true
Set-NetFirewallProfile -Profile Private -Enable True

New-NetFirewallRule -DisplayName "ICMPv4" -Direction Inbound -Action Allow -Protocol icmpv4 -Enabled True

New-NetFirewallRule -Program "C:\Program Files\IDM\idm.exe" -Action Block -Profile Domain, Private -DisplayName "Block IDM"-Description "Block Internet Download Manager" -Direction Outbound

Remove-NetFirewallRule –DisplayName "ICMPv4

Set-NetFirewallProfile -Name Public -DisabledInterfaceAliases "NICNAME"

Optional:

Copy-NetFirewallRule
Disable-NetFirewallRule
Enable-NetFirewallRule
Get-NetFirewallAddressFilter
Get-NetFirewallApplicationFilter
Get-NetFirewallInterfaceFilter
Get-NetFirewallInterfaceTypeFilter
Get-NetFirewallPortFilter
Get-NetFirewallProfile
Get-NetFirewallRule
Get-NetFirewallSecurityFilter
Get-NetFirewallServiceFilter
Get-NetFirewallSetting
New-NetFirewallRule
Remove-NetFirewallRule
Rename-NetFirewallRule
Set-NetFirewallAddressFilter
Set-NetFirewallApplicationFilter
Set-NetFirewallInterfaceFilter
Set-NetFirewallInterfaceTypeFilter
Set-NetFirewallRule
Set-NetFirewallSecurityFilter
Set-NetFirewallServiceFilter
Set-NetFirewallSetting
Show-NetFirewallRule