



## 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**

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
{07937542-D14C-40FB-B577-8792B...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=In Profile=Domain Profile=Private Name=@(Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_ne...
{080D0D60-55D5-4198-84A1-4665...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.Windows.Cortana_1.7.0.14393_neu...
{10A26C07-6430-430A-A61E-75E3...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=In Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.Windows.Cortana_1.7.0.14393_neutr...
{132189A3-AAA4-47CE-8966-2CD...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=In Profile=Domain Profile=Private Name=@(Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_c...
{2153DF84-38FB-46FC-BE89-D151E...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=In Profile=Domain Profile=Private Name=@(Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_c...
{268985F2-EB06-43D6-8C72-388B...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.AccountsControl_10.0.14393.1358...
{2708945F-0A6A-4C40-85D3-C436...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Protocol=17 Profile=Domain Port=1333 Name=PPE)
{30E9C917-49CC-48C0-9642-8A4E...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.Windows.Cortana_1.7.0.14393_neu...
{43881CA1-3889-4396-A908-EE20...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.AAD.BrokerPlugin_1000.14393.0.0...
{47626F15-EA7D-4243-A43F-66468...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.AccountsControl_10.0.14393.1358...
{4ED8FC9-6880-42F8-AA4B-B661...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=In Profile=Domain Profile=Private Name=@(Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_c...
{5697A4C3-605C-4A88-876E-09377...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.AAD.BrokerPlugin_1000.14393.0.0...
{56A3DF33-FC06-4268-87DA-76A6...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Name=@(Microsoft.Windows.CloudExperienceHost_10.0.14393.0_neutral_cw...
{598D77D5-94A0-46C7-9E96-3F308...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=In Profile=Domain Profile=Private Name=@(Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_ne...
{5D4D2043-FC86-4934-8A05-F489...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.Windows.ShellExperienceHost_10...
{655A3780-AB1F-454E-898A-75634...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.Windows.CloudExperienceHost_10...
{75FCDD21-510A-4DC9-B998-5B29...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.XboxGameCallableUI_1000.14393.0...
{7827087E-C649-40D8-85F6-C3807...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.AccountsControl_10.0.14393.1378...
{7871A89A-9563-4394-BE18-7DD2...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.Windows.ShellExperienceHost_10...
{787E7C0D-F1D1-4327-885E-BA21...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.XboxGameCallableUI_1000.14393.0...
{828815FA-1755-4C8E-B189-328EE...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.Windows.Apprep.ChvApp_1000.14...
{829F81FB-A6E6-4ED2-AD30-0A93...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.AccountsControl_10.0.14393.1378...
{82A53153-2737-4FB5-B76D-47C0...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=Out Profile=Domain Profile=Private Profile=Public Name=@(Microsoft.LockApp_10.0.14393.0_neutral_cw...
{838165EA-18FD-48FA-84CF-5A61...}	REG_SZ	v2.26(Action=Allow(Active=TRUE)Dir=In Profile=Domain Profile=Private Name=@(Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_ne...

Diese spiegeln sich mit der GUI wieder:

Name	Gruppe	Profil	Aktiviert	Aktion	Außer ...	Programm	Lokale Adresse	Rem...
Wiedergabe auf Gerät'-UPnP-Ereignisse...	Wiedergabe auf Gerät'-Fun...	Öffent...	Ja	Zulassen	Nein	System	Beliebig	Play
Active Directory-Domänencontroller - Ec...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	Beliebig	Beliebig	Belie...
Active Directory-Domänencontroller - Ec...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	Beliebig	Beliebig	Belie...
Active Directory-Domänencontroller - LD...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Belie...
Active Directory-Domänencontroller - LD...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Belie...
Active Directory-Domänencontroller - LD...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Belie...
Active Directory-Domänencontroller - N...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	System	Beliebig	Belie...
Active Directory-Domänencontroller - SA...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	System	Beliebig	Belie...
Active Directory-Domänencontroller - SA...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	System	Beliebig	Belie...
Active Directory-Domänencontroller - SL...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Belie...
Active Directory-Domänencontroller - SL...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Belie...
Active Directory-Domänencontroller - W...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Belie...
Active Directory-Domänencontroller (RPC)	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Belie...
Active Directory-Domänencontroller (RP...	Active Directory-Domänend...	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Belie...
Active Directory-Webdienste (TCP einge...	Active Directory-Webdienste	Alle	Ja	Zulassen	Nein	%systemro...	Beliebig	Belie...
AllJoyn-Router (TCP eingehend)	AllJoyn-Router	Domä...	Ja	Zulassen	Nein	%SystemR...	Beliebig	Belie...
AllJoyn-Router (UDP eingehend)	AllJoyn-Router	Domä...	Ja	Zulassen	Nein	%SystemR...	Beliebig	Belie...
Anmeldedienst (NP eingehend)	Anmeldedienst	Alle	Nein	Zulassen	Nein	System	Beliebig	Belie...
Autorisierung für den Anmeldedienst (RP...	Anmeldedienst	Alle	Nein	Zulassen	Nein	%SystemR...	Beliebig	Belie...



## Firewall – Restricted Settings

### Kommen wir nun zu den Restricted Firewall Regeln:

Diese Regeln werden wir über die GUI nicht einsehen können.

Restricted > Configurable

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
{04CE9DEC-0198-4D3A-B197-1E41...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Name=@{Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_cw5n1h2t...
{07514676-CFE6-4791-87D6-A6A24...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Profile=Private Profile=Public RA42=RmtInAnet RA62=RmtInAnet Name=@{I...
{08386C2-4A6A-42AF-93B8-26776...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Profile=Private Profile=Public RA42=RmtInAnet RA62=RmtInAnet Name=@{I...
{08386D31-E0E9-48E5-857E-3CB8D...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Name=@{Microsoft.Windows.ShellExperienceHost_10.0.14393.1358_neutral_neu...
{0848460D-DE3F-4F35-A7D5-8BAF...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Profile=Domain Profile=Private Profile=Public RA42=IntraAnet RA62=IntraAnet Na...
{09398C9-321F-4658-A600-272C...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Name=@{Microsoft.Windows.Cortana_1.7.0.14393_neutral_neutral_cw5n1h2tbye...
{095D30C0-A92C-4802-872A-C0F6...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Profile=Domain Profile=Private Profile=Public RA42=IntraAnet RA62=IntraAnet Na...
{09835330-EDB6-4610-B088-1E0F0...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Name=@{Microsoft.Windows.Apprep.ChxApp_1000.14393.0.0_neutral_neutral_cv...
{0A4DD898-8E78-4012-8577-DE79...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Name=@{Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_nes...
{0C088F04-FD84-46B5-B56F-01D59...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Profile=Private Profile=Public RA42=RmtInAnet RA62=RmtInAnet Name=@{I...
{0D3DD756-1C90-4F3B-A8F5-1D00...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Profile=Domain Profile=Private Profile=Public RA42=IntErnet RA62=IntErnet Na...
{0D659186-E9E4-4816-A3E9-F8929...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=In Name=@{Microsoft.XboxGameCallableU_1000.14393.0.0_neutral_neutral_cw5n1h2...
{0DC2618F-F57A-4655-B9C7-E1D1...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Profile=Private Profile=Public RA42=RmtInAnet RA62=RmtInAnet Name=@{I...
{0E379282-A610-4A4D-A161-246D...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Name=@{Microsoft.Windows.ShellExperienceHost_10.0.14393.1358_neutral_neu...
{0F600C36-C44A-4D5E-A07D-5729...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Name=@{Microsoft.Windows.ShellExperienceHost_10.0.14393.1378_neutral_neu...
{10735F1C-A100-40A0-8391-FEC65...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=In Profile=Private Profile=Public RA42=RmtInAnet RA62=RmtInAnet Name=@{Mi...
{10CF72DD-C3E1-45DF-B264-EEDB...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Profile=Domain Profile=Private Profile=Public RA42=IntErnet RA62=IntErnet Na...
{11E874D5-D358-475E-BEFE-8048C...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Profile=Domain Profile=Private Profile=Public RA42=IntErnet RA62=IntErnet Na...
{193D275D-B284-47DA-8864-58AE...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Name=@{Microsoft.AccountsControl_10.0.14393.1358_neutral_cw5n1h2tbyesw...}
{1B920E2-2704-408E-B3EA-4E61E...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Name=@{Microsoft.Windows.AssignedAccessLockApp_1000.14393.0.0_neutral_r...
{1B9C7138-703A-41AA-A2FC-C9F...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=Out Profile=Private Profile=Public RA42=RmtInAnet RA62=RmtInAnet Name=@{I...
{1ED65E1D-F8C6-4D5C-A649-E9C7...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=Out Profile=Domain Profile=Private Profile=Public RA42=IntErnet RA62=IntErnet Na...
{1EDF83FB-3F76-4D89-9521-51F30...}	REG_SZ	v2.26(Action=Allow Active=TRUE Dir=In Profile=Private Profile=Public RA42=RmtInAnet RA62=RmtInAnet Name=@{Mi...
{20E82189-A8DB-44AD-8851-384A...}	REG_SZ	v2.26(Action=Block Active=TRUE Dir=In Name=@{Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neu...

Restricted > Static

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
ADWS-1	REG_SZ	V2.0(Action=Block Dir=In App=%systemroot%\ADWS\Microsoft.ActiveDirectory.WebServices.exe Svc=ADWS Name=ADWS ...
ADWS-2	REG_SZ	V2.0(Action=Block Dir=Out App=%systemroot%\ADWS\Microsoft.ActiveDirectory.WebServices.exe Svc=ADWS Name=ADWS ...
ADWS-3	REG_SZ	V2.0(Action=Allow Dir=In Port=9389 Protocol=6 App=%systemroot%\ADWS\Microsoft.ActiveDirectory.WebServices.exe Svc=ADWS ...
ADWS-4	REG_SZ	V2.0(Action=Allow Dir=Out Protocol=6 App=%systemroot%\ADWS\Microsoft.ActiveDirectory.WebServices.exe Svc=ADWS ...
Audiosrv-1	REG_SZ	V2.0(Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=Audiosrv Name=Block any inbound traffic to Ai...
Audiosrv-2	REG_SZ	V2.0(Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=Audiosrv Name=Block any outbound traffic fr...
AVEndpointBuilder-1	REG_SZ	V2.0(Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=AudioEndpointBuilder Name=Block any inbou...
AVEndpointBuilder-2	REG_SZ	V2.0(Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=AudioEndpointBuilder Name=Block any outbu...
AxInstSV-1	REG_SZ	V2.0(Action=Block Dir=In App=%windir%\System32\svchost.exe Svc=AxInstSV Name=AxInstSV inbound block Desc=Block...
AxInstSV-2	REG_SZ	V2.0(Action=Allow Dir=Out Protocol=6 App=%windir%\System32\svchost.exe Svc=AxInstSV Name=AxInstSV TCP outboun...
AxInstSV-3	REG_SZ	V2.0(Action=Block Dir=Out App=%windir%\System32\svchost.exe Svc=AxInstSV Name=AxInstSV outbound block Desc=Blk...
BFE-1	REG_SZ	V2.0(Action=Block Dir=In App=%SystemRoot%\System32\svchost.exe Svc=BFE Name=Block inbound traffic to BFE ...
BFE-2	REG_SZ	V2.0(Action=Block Dir=Out App=%SystemRoot%\System32\svchost.exe Svc=BFE Name=Block outbound traffic from BFE ...
clr_optimization_v2.0.50727_32-1	REG_SZ	V2.0(Action=Block Dir=In App=C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.exe Svc=clr_optimization_v2...
clr_optimization_v2.0.50727_32-2	REG_SZ	V2.0(Action=Block Dir=Out App=C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.exe Svc=clr_optimization_v...
clr_optimization_v2.0.50727_64-1	REG_SZ	V2.0(Action=Block Dir=In App=C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.exe Svc=clr_optimization_v...
clr_optimization_v2.0.50727_64-2	REG_SZ	V2.0(Action=Block Dir=Out App=C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorlib.exe Svc=clr_optimizatio...
clr_optimization_v4.0.30319_32-1	REG_SZ	V2.0(Action=Block Dir=In App=C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.exe Svc=clr_optimization_v...
clr_optimization_v4.0.30319_32-2	REG_SZ	V2.0(Action=Block Dir=Out App=C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.exe Svc=clr_optimization_v...
clr_optimization_v4.0.30319_64-1	REG_SZ	V2.0(Action=Block Dir=In App=C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.exe Svc=clr_optimization_v...
clr_optimization_v4.0.30319_64-2	REG_SZ	V2.0(Action=Block Dir=Out App=C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.exe Svc=clr_optimizatio...
CscService-1	REG_SZ	V2.0(Action=Block Dir=In App=%SystemRoot%\system32\svchost.exe Svc=CscService Name=Block any other traffic to anc...
CscService-2	REG_SZ	V2.0(Action=Block Dir=Out App=%SystemRoot%\system32\svchost.exe Svc=CscService Name=Block any other traffic to a...
DFSR-1	REG_SZ	V2.0(Action=Block Dir=In App=%windir%\System32\dfsrs.exe Svc=dfsrs Name=Block incoming traffic to DFSR ...

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.exe"  
    Protocol = 6  
}  
$rule.RemotePorts = "55555-55570"  
(New-Object -ComObject HNetCfg.FwPolicy2).ServiceRestriction.Rules.Add($rule)
```

```
Administrator: Windows PowerShell ISE (x86)  
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe  
FW restricted.ps1 X  
1 Get-NetFirewallRule -PolicyStore ActiveStore  
2 Get-NetFirewallRule -DisplayName "Ihr Konto" -PolicyStore ActiveStore  
3 Get-NetFirewallRule -Name "{0ABACACE-468F-44F0-8C25-1A6A85902EB1}" -PolicyStore ActiveStore  
4  
5 Get-NetFirewallRule -PolicyStore ConfigurableServiceStore  
6 Get-NetFirewallRule -DisplayName "Erlaube ausgehende Verbindung von TCP Port 55555 to 55570" -PolicyStore ConfigurableServiceStore  
7 Get-NetFirewallRule -Name "{4AD6272F-6953-4305-92E7-1D87C8FAEC73}" -PolicyStore ConfigurableServiceStore  
8  
9  
10 # Restricted Firewall Regeln erstellen  
11 $rule = New-Object -ComObject HNetCfg.FWRule -Property @{  
12     Name = "Erlaube ausgehende Verbindung von TCP Port 55555 to 55570"  
13     Direction = 2  
14     Enabled = $true  
15     ApplicationName = "C:\Program Files\MaxPowerSoft\ADReports\ADReports.exe"  
16     ServiceName = "ADReports.exe"  
17     Protocol = 6  
18 }  
19 $rule.RemotePorts = "55555-55570"  
20 (New-Object -ComObject HNetCfg.FwPolicy2).ServiceRestriction.Rules.Add($rule)  
21  
PS C:\WINDOWS\system32> $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.exe"  
    Protocol = 6  
}  
$rule.RemotePorts = "55555-55570"  
(New-Object -ComObject HNetCfg.FwPolicy2).ServiceRestriction.Rules.Add($rule)  
Abgeschlossen  
Ln 38 Spalte 25 100%
```

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

Name	Gruppe	Profil	Aktiviert	Aktion	Außer Kraft setzen	Programm	Lc
✓ Datei- und Druckerfreigabe (NB-Name a...	Datei- und Druckerfreigabe	Alle	Ja	Zulassen	Nein	System	Br
✓ Datei- und Druckerfreigabe (NB-Sitzung ...	Datei- und Druckerfreigabe	Alle	Ja	Zulassen	Nein	System	Br
✓ Datei- und Druckerfreigabe (SMB ausgeh...	Datei- und Druckerfreigabe	Alle	Ja	Zulassen	Nein	System	Br
✓ DHCP-Server-Failover (TCP ausgehend)	DHCP-Serververwaltung	Alle	Ja	Zulassen	Nein	%systemro...	Br
Distributed Transaction Coordinator (TCP...	Distributed Transaction Coo...	Alle	Nein	Zulassen	Nein	%SystemR...	Br
✓ E-Mail und Konten	E-Mail und Konten	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ E-Mail und Konten	E-Mail und Konten	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ E-Mail und Konten	E-Mail und Konten	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ E-Mail und Konten	E-Mail und Konten	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Geschäfts- oder Schulkonto	Geschäfts- oder Schulkonto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Geschäfts- oder Schulkonto	Geschäfts- oder Schulkonto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Geschäfts- oder Schulkonto	Geschäfts- oder Schulkonto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Geschäfts- oder Schulkonto	Geschäfts- oder Schulkonto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Geschäfts- oder Schulkonto	Geschäfts- oder Schulkonto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Ihr Konto	Ihr Konto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Ihr Konto	Ihr Konto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Ihr Konto	Ihr Konto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Ihr Konto	Ihr Konto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ Ihr Konto	Ihr Konto	Alle	Ja	Zulassen	Nein	Beliebig	Br
✓ iSCSI-Dienst (TCP ausgehend)	iSCSI-Dienst	Alle	Ja	Zulassen	Nein	%SystemR...	Br
✓ Kernnetzwerk - DNS (UDP ausgehend)	Kernnetzwerk	Alle	Ja	Zulassen	Nein	%SystemR...	Br
✓ Kernnetzwerk - Dynamic Host Configurat...	Kernnetzwerk	Alle	Ja	Zulassen	Nein	%SystemR...	Br
✓ Kernnetzwerk - Dynamic Host Configurat...	Kernnetzwerk	Alle	Ja	Zulassen	Nein	%SystemR...	Br



## 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.

```
Administrator: Windows PowerShell ISE (x86)
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

FW restricted.ps1 X
1 Get-NetFirewallRule -PolicyStore ActiveStore
2 Get-NetFirewallRule -DisplayName "Ihr Konto" -PolicyStore ActiveStore
3 Get-NetFirewallRule -Name "{08BACACE-468F-44F0-8C25-1A6A85902EB1}" -PolicyStore ActiveStore
4
5 Get-NetFirewallRule -PolicyStore ConfigurableServiceStore
6 Get-NetFirewallRule -DisplayName "Erlaube ausgehende Verbindung von TCP Port 55555 to 55570" -PolicyStore ConfigurableServiceStore
7 Get-NetFirewallRule -Name "{820751D9-9838-4668-B591-D0922F7B83CA}" -PolicyStore ConfigurableServiceStore
8
9
10 # Restricted Firewall Regeln erstellen
11 $rule = New-Object -ComObject HNetCfg.FwRule -Property @{
12     Name = "Erlaube ausgehende Verbindung von TCP Port 55555 to 55570"
13     Direction = 2
14     Enabled = $true
15     ApplicationName = "C:\Program Files\MaxPowerSoft\ADReports\ADReports.exe"
16     ServiceName = "ADReports.exe"
17     Protocol = 6
18 }
19 $rule.RemotePorts = "55555-55570"
20 (New-Object -ComObject HNetCfg.FwPolicy2).ServiceRestriction.Rules.Add($rule)
21

(New-Object -ComObject HNetCfg.FwPolicy2).ServiceRestriction.Rules.Add($rule)
PS C:\Windows\system32> Get-NetFirewallRule -DisplayName "Erlaube ausgehende Verbindung von TCP Port 55555 to 55570" -PolicyStore ConfigurableServiceStore

Name                : {820751D9-9838-4668-B591-D0922F7B83CA}
DisplayName          : Erlaube ausgehende Verbindung von TCP Port 55555 to 55570
Description          :
DisplayGroup        :
Group                :
Enabled              : True
Profile              : Any
Platform            : {}
Direction           : Outbound
Action               : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping  : False
LocalOnlyMapping    : False
Owner               :
PrimaryStatus       : OK
Status              : Die Regel wurde erfolgreich vom Speicher aus analysiert. (65536)
EnforcementStatus   : NotApplicable
PolicyStoreSource   :
PolicyStoreSourceType : GroupPolicy

PS C:\Windows\system32>
```

Mithilfe der ID durchsuche ich jetzt die Registry: Voila!

Registrierungs-Editor

Name Typ Daten

Name	Typ	Daten
{78B39ACD-5FA6-4113-861C-52DE...}	REG_SZ	v2.26>Action=Block Active=TRU...
{78F53E67-C179-4E5C-982E-E2F6D...}	REG_SZ	v2.26>Action=Block Active=TRU...
{7E22587D-AB36-4232-B3F5-31E60...}	REG_SZ	v2.26>Action=Allow Active=TRU...
{7E755D44-1EA4-45BA-A47D-C34A...}	REG_SZ	v2.26>Action=Allow Active=TRU...
{7EFAF563-A339-43F4-8235-FCAB1...}	REG_SZ	v2.26>Action=Block Active=TRU...
{7FB4C302-5114-4A59-B3D3-63964...}	REG_SZ	v2.26>Action=Allow Active=TRU...
{7FE8CE0E-CD08-4436-865B-CA45...}	REG_SZ	v2.26>Action=Allow Active=TRU...
{8093292B-781F-4CDA-BEF2-367A...}	REG_SZ	v2.26>Action=Allow Active=TRU...
{80E5D8D8-93A1-447A-8D64-7FF0...}	REG_SZ	v2.26>Action=Block Active=TRU Dir=In Name=@(Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2tbyewy7ms-reso...
{820751D9-9838-4668-B591-D0922...}	REG_SZ	v2.26>Action=Allow Active=TRU Dir=Out Protocol=6 Port2_10=55555-55570 App=C:\Program Files\MaxPowerSoft\ADRe...
{824BD0F8-8158-4874-81DE-8B5A...}	REG_SZ	v2.26>Action=Block Active=TRU Dir=Out Name=@(Microsoft.XboxGameCallableUL_1000.14393.0.0_neutral_neutral_cw5n1h2tbyewy7ms-reso...
{845EE299-A4E4-42A4-9122-F6EA3...}	REG_SZ	v2.26>Action=Block Active=TRU Dir=In Name=@(Microsoft.AccountsControl_10.0.14393.1378_neutral_neutral_cw5n1h2tbyewy7m...
{881A7511-C0FD-45D9-9FF8-9A66...}	REG_SZ	v2.26>Action=Allow Active=TRU Dir=Out Profile=Domain Profiles=Private Profile=Public RA42=IntErnet RA62=IntErnet Nar...
{8DFE8A5-24EA-4309-8234-3B668...}	REG_SZ	v2.26>Action=Allow Active=TRU Dir=Out Profile=Domain Profiles=Private Profile=Public RA42=IntErnet RA62=IntErnet Nar...
{8F7ECF8A-A479-4178-B84C-9D23...}	REG_SZ	v2.26>Action=Block Active=TRU Dir=In Name=@(Microsoft.Windows.Cortana_1.7.0.14393_neutral_neutral_cw5n1h2tbyewy7m...
{8FE078BA-13CD-4808-8559-1FB1C...}	REG_SZ	v2.26>Action=Block Active=TRU Dir=Out Name=@(Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_cw5n1h2t...
{9076E9B9-F13F-4BF7-92D9-39175...}	REG_SZ	v2.26>Action=Allow Active=TRU Dir=Out Profile=Domain Profiles=Private Profile=Public RA42=IntErnet RA62=IntErnet Nar...
{9085BD99-DAF9-4806-9275-92A5E...}	REG_SZ	v2.26>Action=Allow Active=TRU Dir=Out Profile=Domain Profiles=Private Profile=Public RA42=IntErnet RA62=IntErnet Nar...
{959E33AD-434C-4F50-9184-C586...}	REG_SZ	v2.26>Action=Block Active=TRU Dir=In Name=@(Microsoft.Windows.ShellExperienceHost_10.0.14393.1358_neutral_neutra...

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\Configurable\System



## 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
```

```
Administrator: Windows PowerShell ISE (x86)
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

FW restricted.ps1* X
50 Service = "SNMP"
51 Program = "${env:systemdrive}\WINDOWS\system32\snmp.exe"
52 Enabled = "TRUE"
53 LocalPort = "3214"
54 PolicyStore = "ConfigurableServiceStore"
55 }
56
57 New-NetFirewallRule @SNMPOut86
58 New-NetFirewallRule @SNMPin86
59 New-NetFirewallRule @SNMPOut64
60 New-NetFirewallRule @SNMPin64
61
62 # Individuelle Regel aus dem Service Store nach DisplayName abfragen
63 Get-NetFirewallRule -DisplayName "Allow outbound traffic from snmp service to TCP 3216" -PolicyStore ConfigurableServiceStore
64

PolicyStoreSource : GroupPolicy
Name : ApplikationX64out
DisplayName : Allow outbound traffic from snmp service to TCP 3216
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Outbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : Die Regel wurde erfolgreich vom Speicher aus analysiert. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource :
PolicyStoreSourceType : GroupPolicy

PS C:\Windows\system32>

Abgeschlossen | Ln 63 Spalte 1 | 100%
```

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

Name	Typ	Daten
{F705DAFE-73BF-4CCA-8FD4-0A43...}	REG_SZ	v2.28\Actions\Allow\Active\TRUE\Dir\In\Profiles\Domain\Profiles\Private\Profiles\Public\RA42\Internet\RA62\Internet\Names@Microsoft.Windows.Cortana_1.7.0.14393_neutral_neutral_cw5n1h2zweywi/ms-reso...
{F771FC52-073A-4A5D-85A7-4E31E...}	REG_SZ	v2.28\Actions\Allow\Active\TRUE\Dir\Out\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
{FAE857FA-C62D-49D8-B282-A650...}	REG_SZ	v2.28\Actions\Block\Active\TRUE\Dir\In\Names@Microsoft.AccountsControl_10.0.14393.1378_neutral_cw5n1h2zweywi/ms-reso...
{FC3E8A3C-7F99-4D7F-9721-98D9...}	REG_SZ	v2.28\Actions\Block\Active\TRUE\Dir\In\Names@SecondaryTileExperience\UOWms-5-1-5-21-114462570-1726162390-2557311800-1108\AppKlgIdS-1-15-2-2572118008-30774712...
{FC798FCE-72F9-4E8D-866D-B298...}	REG_SZ	v2.28\Actions\Block\Active\TRUE\Dir\Out\Names@Microsoft.LockApp_10.0.14393.0_neutral_cw5n1h2zweywi/ms-reso...
{FC9C9FDD-40C5-4065-8A38-0CD...}	REG_SZ	v2.28\Actions\Block\Active\TRUE\Dir\In\Names@Microsoft.AccountsControl_10.0.14393.1358_neutral_cw5n1h2zweywi/ms-reso...
{FDC3C9AE-855F-415F-8005-7E7C...}	REG_SZ	v2.28\Actions\Allow\Active\TRUE\Dir\Out\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_cw5n1h2zweywi/ms-reso...
{FDC3C9AE-855F-415F-8005-7E7C...}	REG_SZ	v2.28\Actions\Allow\Active\TRUE\Dir\In\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
ApplikationX64in	REG_SZ	v2.28\Actions\Allow\Active\TRUE\Dir\In\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
ApplikationX64out	REG_SZ	v2.28\Actions\Allow\Active\TRUE\Dir\Out\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
ApplikationX64in	REG_SZ	v2.28\Actions\Allow\Active\TRUE\Dir\In\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
ApplikationX64out	REG_SZ	v2.28\Actions\Allow\Active\TRUE\Dir\Out\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
DHCP Server-Block others in	REG_SZ	v2.0\Actions\Block\Dir\In\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
DHCP Server-Block others out	REG_SZ	v2.0\Actions\Block\Dir\Out\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
DHCP Server-Fallover in	REG_SZ	v2.0\Actions\Allow\Dir\In\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
DHCP Server-Fallover out	REG_SZ	v2.0\Actions\Allow\Dir\Out\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
DHCP Server-IPv4 Client in	REG_SZ	v2.0\Actions\Allow\Dir\In\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...
DHCP Server-IPv4 Client out	REG_SZ	v2.0\Actions\Allow\Dir\Out\Profiles\Private\Profiles\Public\RA42\RmtInet\RA62\RmtInet\Names@Microsoft.Windows.CloudExperienceHost_10.0.14393.1066_neutral_neutral_cw5n1h2zweywi/ms-reso...



## 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
```