Docusnap X - Windows Firewall Ausnahmen

Windows Firewall Ausnahmen für Docusnap konfigurieren

TITEL	Docusnap X - Windows Firewall Ausnahmen
AUTOR	Docusnap Consulting
DATUM	18.12.2018
VERSION	1.2 | gültig ab 26.09.2018

INHALTSVERZEICHNIS

1. Einleitung

Docusnap inventarisiert Windows Systeme mit Hilfe der Standardschnittstelle Windows Management Instrumentation (WMI). Ist auf einem Windows System die Windows-Firewall aktiviert, wird hierdurch unter Umständen das Auslesen verhindert. Dieses Dokument beschreibt die notwendigen Anpassungen von Firewall-Einstellungen bei Windows Systemen.

Im Kapitel WINDOWS FIREWALL KONFIGURATION – ACTIVE DIRECTORY wird beschrieben wie die erforderlichen Windows-Firewall Ausnahmen über Gruppenrichtlinien mit Hilfe des Active Directory organisationsweit konfiguriert werden können. Dies ist die von uns empfohlene Methode.

Im Kapitel WINDOWS 10 - WINDOWS FIREWALL KONFIGURATION (LOKAL) wird am Beispiel von Windows 10 beschrieben wie *lokale* Gruppenrichtlinien zu konfigurieren sind. Die Anpassung der *lokalen* Gruppenrichtlinien ist nur in Arbeitsgruppen oder zu Testzwecken sinnvoll.

2. Grundlagen

Damit der Scan von Windowssystemen mit aktivierter Firewall mit Docusnap gelingt sind zwei Firewall Ausnahmen zu überprüfen bzw. zu konfigurieren. Diese Einstellungen können per Gruppenrichtlinien erzeugt und verwaltet werden. Für einen schnellen Test wird die manuelle Konfiguration der Windows-Firewall ebenfalls vorgestellt.

2.1 Benötigte Firewall Ausnahmen

Es erfolgt nun eine kurze Beschreibung der zu treffenden Ausnahmen.

Datei- und Druckerfreigabe

Ermöglicht die Datei- und Druckerfreigabe. Die Windows Firewall öffnet hierzu UDP-Port 137 und 138 sowie TCP-Port 139 und 445. Durch Aktivieren dieser Richtlinieneinstellung öffnet die Windows Firewall diese Ports, sodass das Windows System Druckaufträge und Zugriffsanforderungen für freigegebene Dateien empfangen kann.

Hinweis: Diese Einstellung lässt die Windows Firewall eingehende ICMP-Echoanforderungen (eine vom Dienstprogramm Ping gesendete Meldung) zu und zwar auch dann, wenn die Richtlinieneinstellung „Windows-Firewall: ICMP-Ausnahmen zulassen" sie blockieren würde.

Remoteverwaltungsausnahme zulassen

Entspricht im Wesentlichen der Windows Firewall Ausnahme Windows-Verwaltungsinstrumentation (WMI) und ermöglicht die Remoteverwaltung des Windowssystems mit Verwaltungsprogrammen, wie z. B. Microsoft Management Console (MMC) und Windows-Verwaltungsinstrumentation (WMI). Die Windows Firewall öffnet hierzu TCP-Port 135 und 445. Dienste verwenden diese Ports normalerweise für die Kommunikation mithilfe von Remoteprozeduraufrufen (RPC) und DCOM (Distributed Component Object Model).

Sicherheitshinweis

Es wird empfohlen, die Einstellung per Gruppenrichtlinie zu verteilen, damit erlaubte IP-Adressen oder Subnetze für diese Ausnahmen gesetzt werden können.

3. Windows Firewall Konfiguration – Active Directory

3.1 Verwaltungskonsole (GPMC)

Um die Firewall Konfiguration für mehrere Rechner durchzuführen, wird empfohlen, die benötigten Einstellungen per Gruppenrichtlinie vorzunehmen.

Das folgende Beispiel zeigt wie mit dem Microsoft Tool Gruppenrichtlinien-Verwaltungskonsole (GPMC) eine domänenweite Einstellung vorgenommen wird. GPO Einstellungen können lokal (L), standortweit (S), domänenweit (D) und auf der Organisationsebene (OU) vorgenommen werden. Dabei überschreiben nachfolgende Einstellungen zuvor festgelegte Werte. Die Reihenfolge lautet L, S, D, OU.

Sofern die Gruppenrichtlinien-Verwaltungskonsole nicht bereits installiert ist, kann diese kostenlos bei Microsoft heruntergeladen werden. Im folgenden Beispiel werden hiermit die Firewall Einstellungen für alle in der Domäne vorhandenen Systeme geändert. Ein vorheriger Test in einer Testumgebung oder der Einsatz der Einstellungen nur auf eine spezielle Test- Organisationsebene *(OU)* im Active Directory wird dringend empfohlen.

Die Remoteserver-Verwaltungstools, welche die GPMC enthalten, können für die Windows Client-Betriebssysteme bei Microsoft heruntergeladen werden:

Bei Windows Server-Betriebssystemen (ab 2008) ist die GPMC bereits enthalten, muss aber gegebenenfalls über den Server-Manager nachinstalliert werden.

3.2 GPMC starten

Starten Sie den Windows-Ausführen-Dialog (Windows-Taste+R) und geben *gpmc.msc* ein.

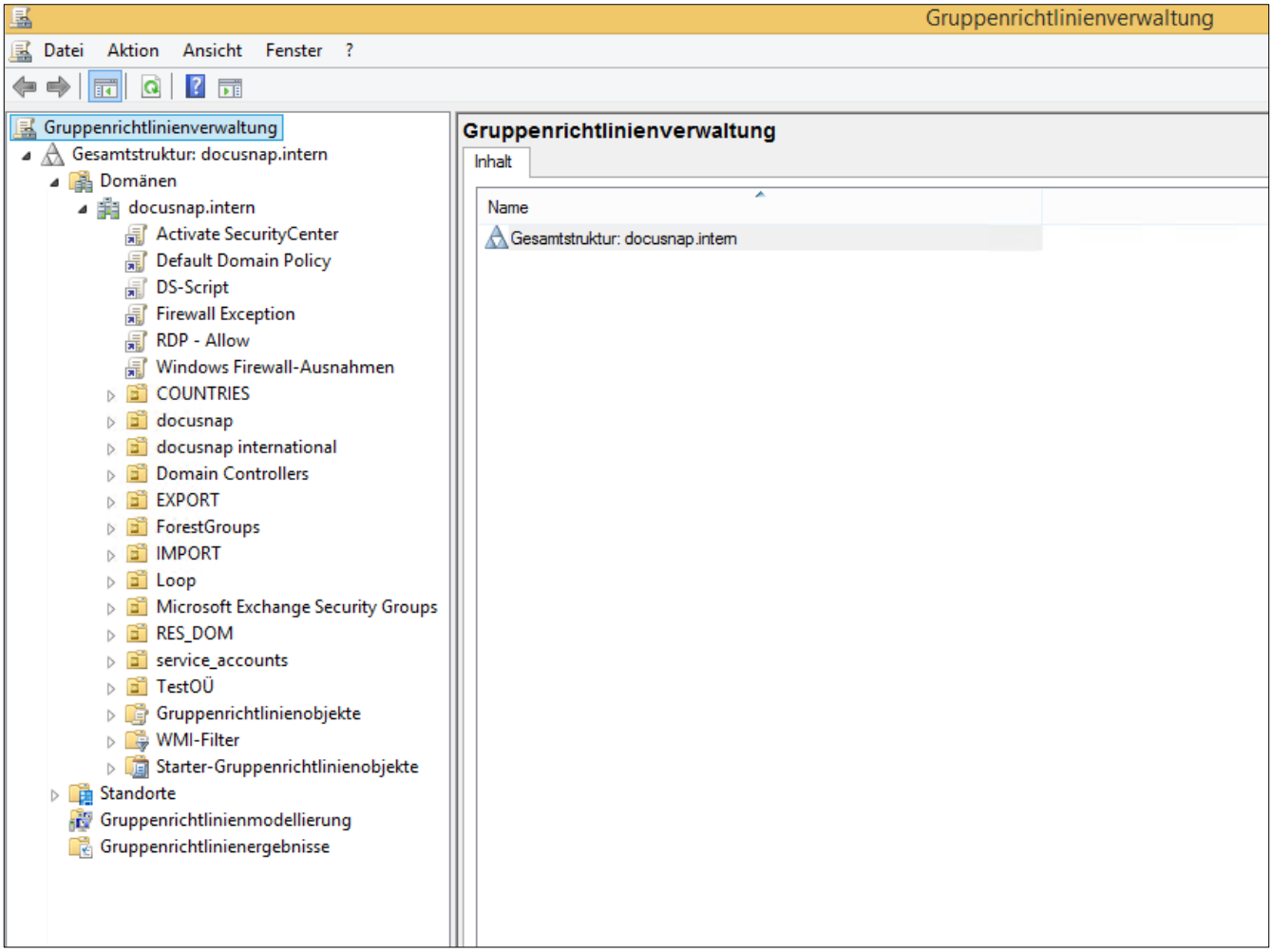

Abbildung 1 - Gruppenrichtlinienverwaltung

3.3 Gruppenrichtlinienobjekt erstellen

Per Rechtsklick auf die gewünschte *Domäne* oder eine *OU* gelangt man zur Auswahl *Gruppenrichtlinienobjekt hier erstellen und verknüpfen*.

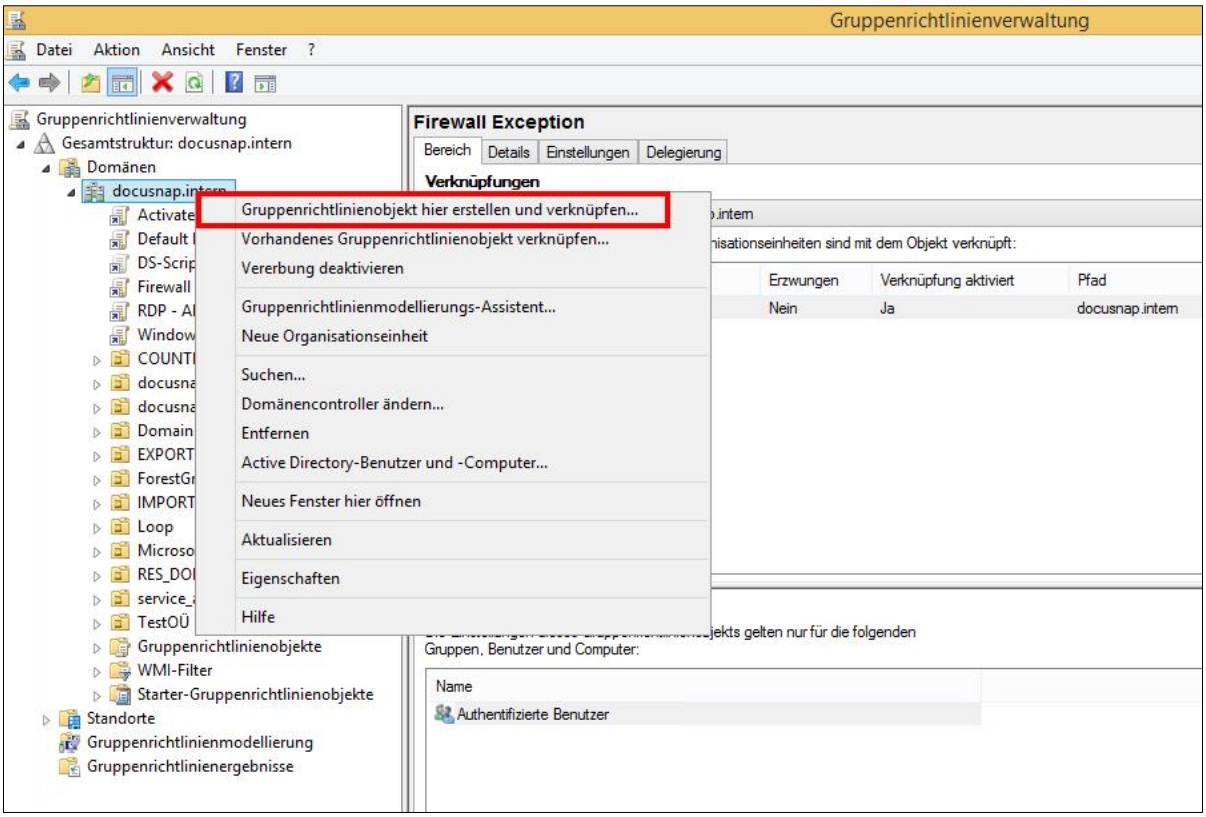

Abbildung 2 - Gruppenrichtlinienobjekt hier erstellen und verknüpfen

Einen „sprechenden" Namen für das Gruppenrichtlinienobjekt festlegen.

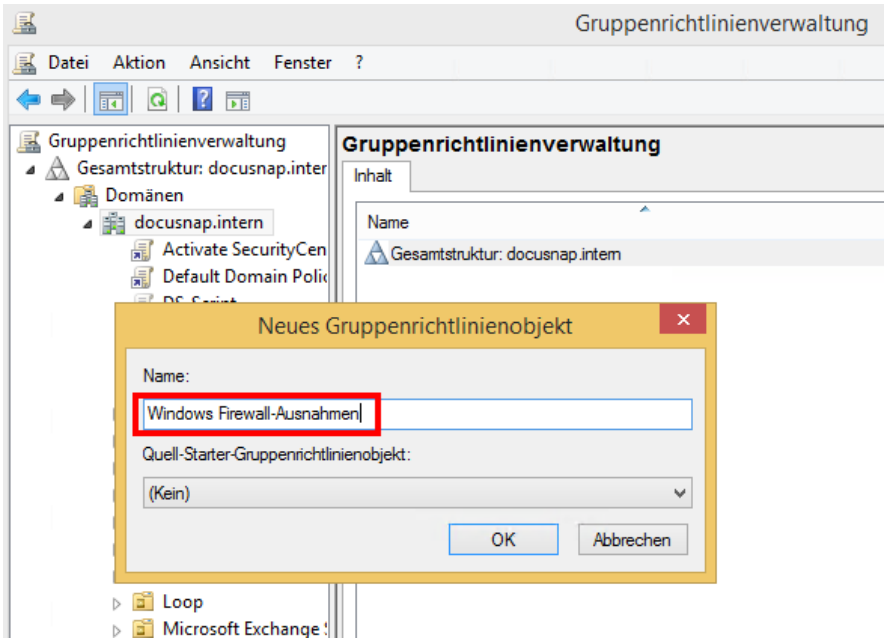

Abbildung 3 - Neues Gruppenrichtlinienobjekt

3.4 Gruppenrichtlinienobjekt bearbeiten

Mit einem Rechtsklick das zuvor erstellte Gruppenrichtlinienobjekt anwählen und die Option *Bearbeiten* auswählen.

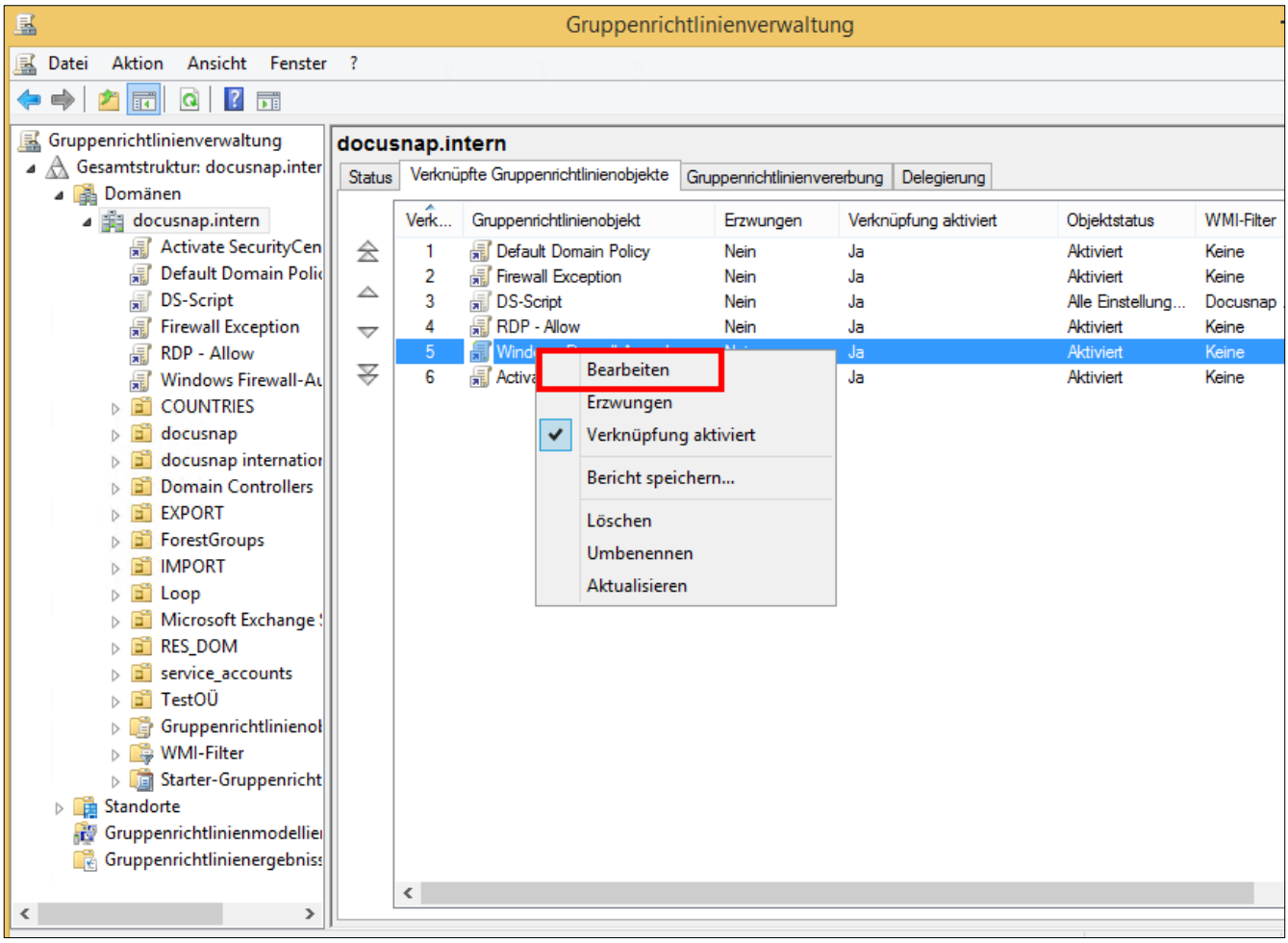

Abbildung 4 - Gruppenrichtlinienobjekt bearbeiten

Der Gruppenrichtlinienobjekt-Editor öffnet sich:

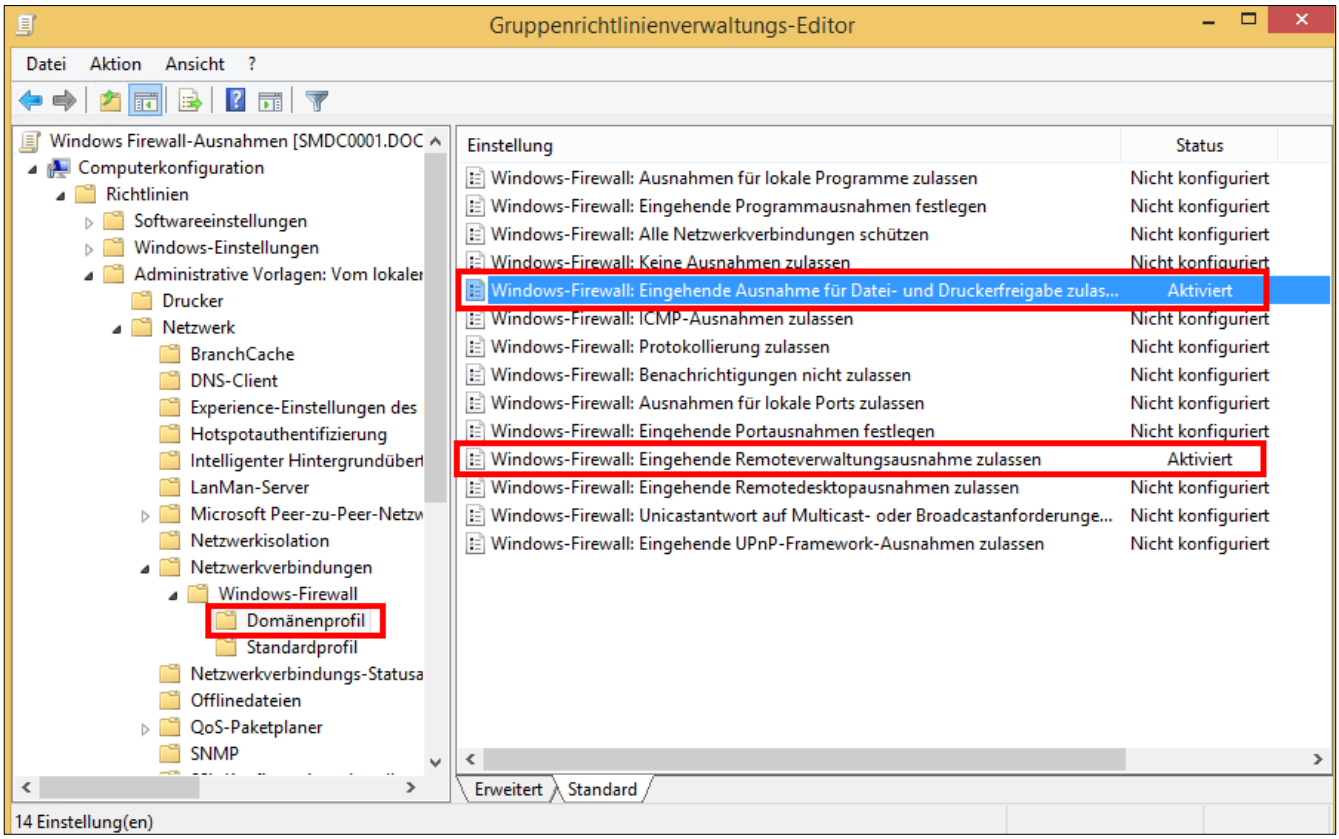

Abbildung 5 - Gruppenrichtlinienobjekt-Editor

Die zu konfigurierenden Gruppenrichtlinien befinden sich unter:

- Computerkonfiguration
  - Richtlinien
    - Administrative Vorlagen
      - Netzwerk
        - Netzwerkverbindungen
          - Windows-Firewall
            - Domänenprofil

3.5 Ausnahme für Datei- und Druckerfreigabe aktivieren

In diesem Beispiel wird die Firewall Ausnahme mit Beschränkung auf das lokale Subnetz aktiviert.

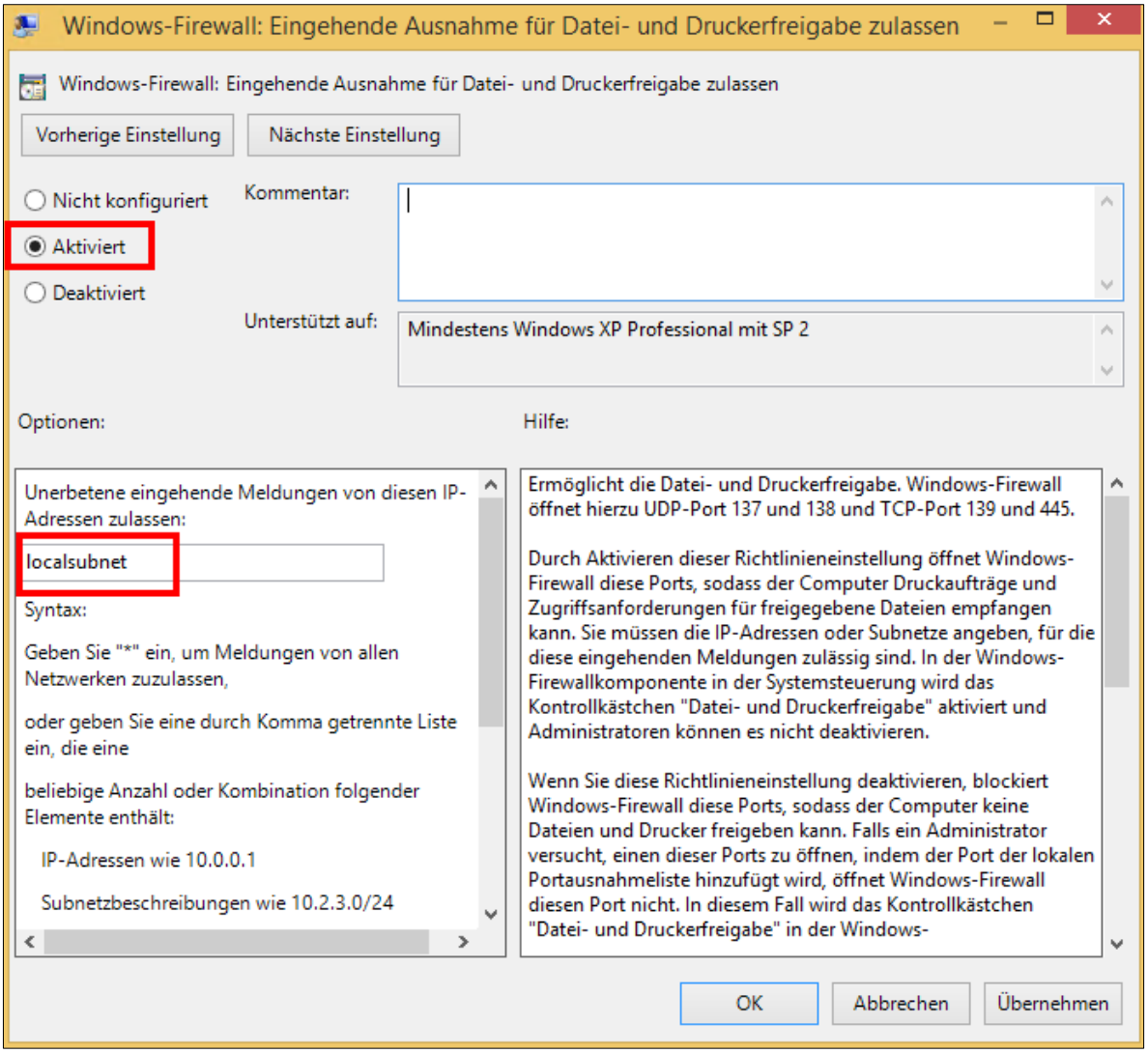

Abbildung 6 - Ausnahme für Datei- und Druckerfreigaben aktivieren und Bereich einschränken

3.6 Remoteverwaltungsausnahme aktivieren

Für dieses Beispiel wird die Firewall Ausnahme mit Beschränkung auf das lokale Subnetz gesetzt.

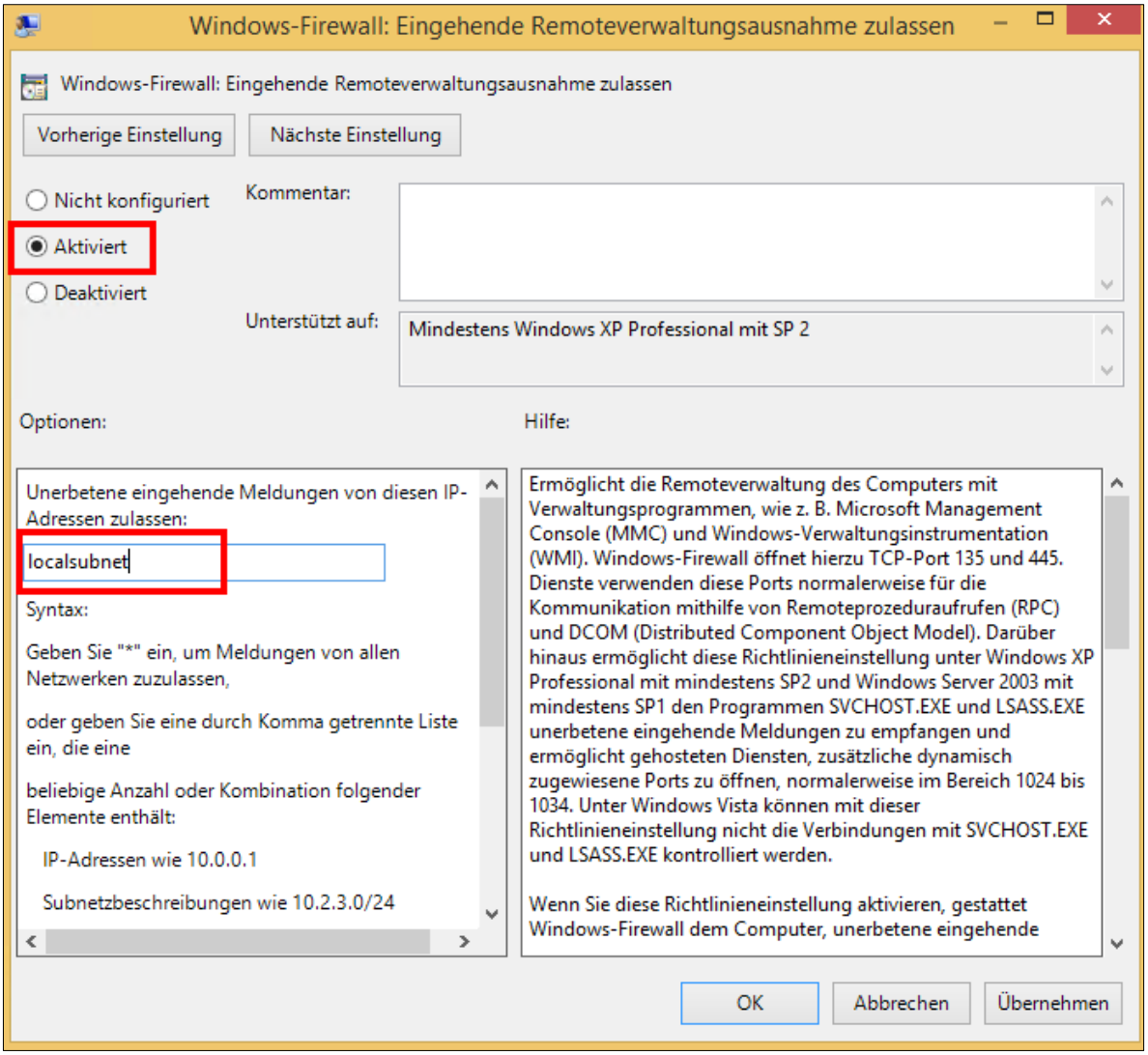

Abbildung 7 - Remoteverwaltungsausnahme aktivieren und Bereich einschränken

3.7 Gruppenrichtlinienobjekt bearbeiten – weitere Möglichkeiten

Mit einem Rechtsklick das zuvor erstellte Gruppenrichtlinienobjekt anwählen und die Option *Bearbeiten* auswählen.

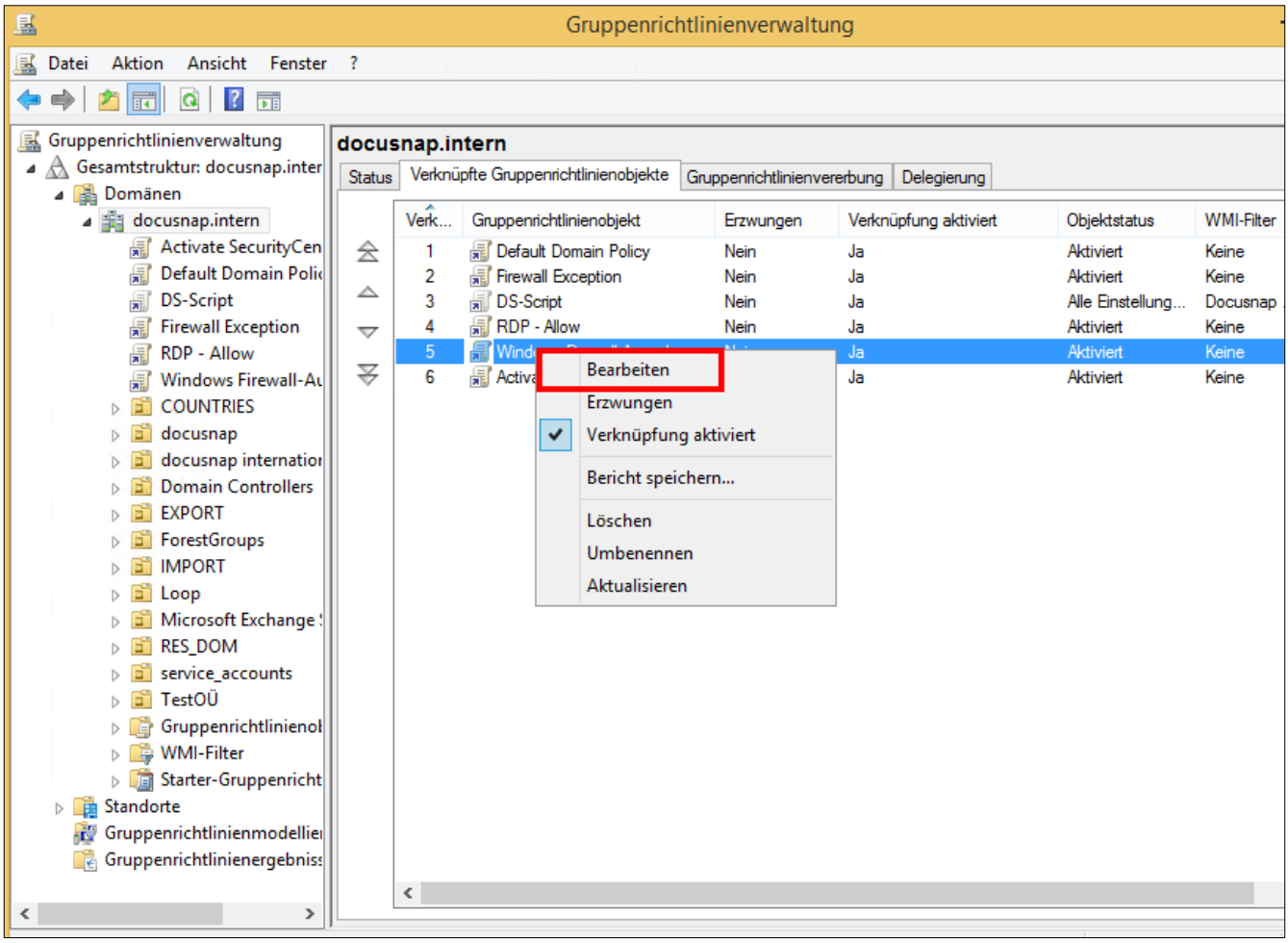

Abbildung 8 - Gruppenrichtlinienobjekt bearbeiten

Der Gruppenrichtlinienobjekt-Editor wird geöffnet:

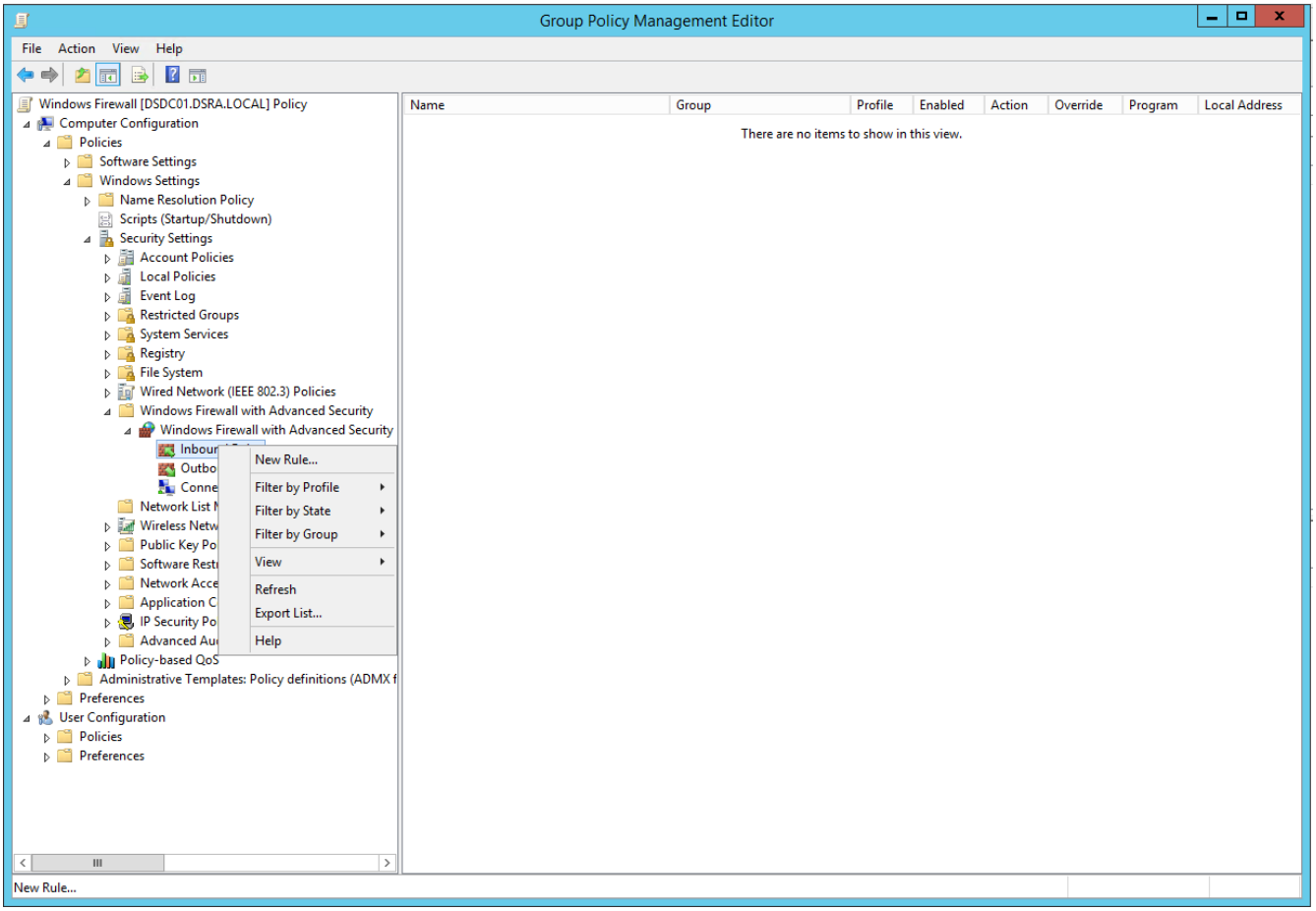

Abbildung 9 - Gruppenrichtlinienobjekt-Editor

Die zu konfigurierenden Firewall Einstellungen befinden sich unter:

- Computerkonfiguration
  - Richtlinien
    - Windows Einstellungen
      - Sicherheitseinstellungen
        - Windows Firewall mit erweiterter Sicherheit
          - Windows Firewall mit erweiterter Sicherheit
            - Eingehende Regeln
              - Neue Regel

3.7.1 Datei- und Druckerfreigabe aktivieren - Ping

Nach der Auswahl „Neue Regel“ wird der Firewall Assistent gestartet. Wählen Sie hier den vordefinierten Regelsatz:

- „Datei- und Druckerfreigabe“

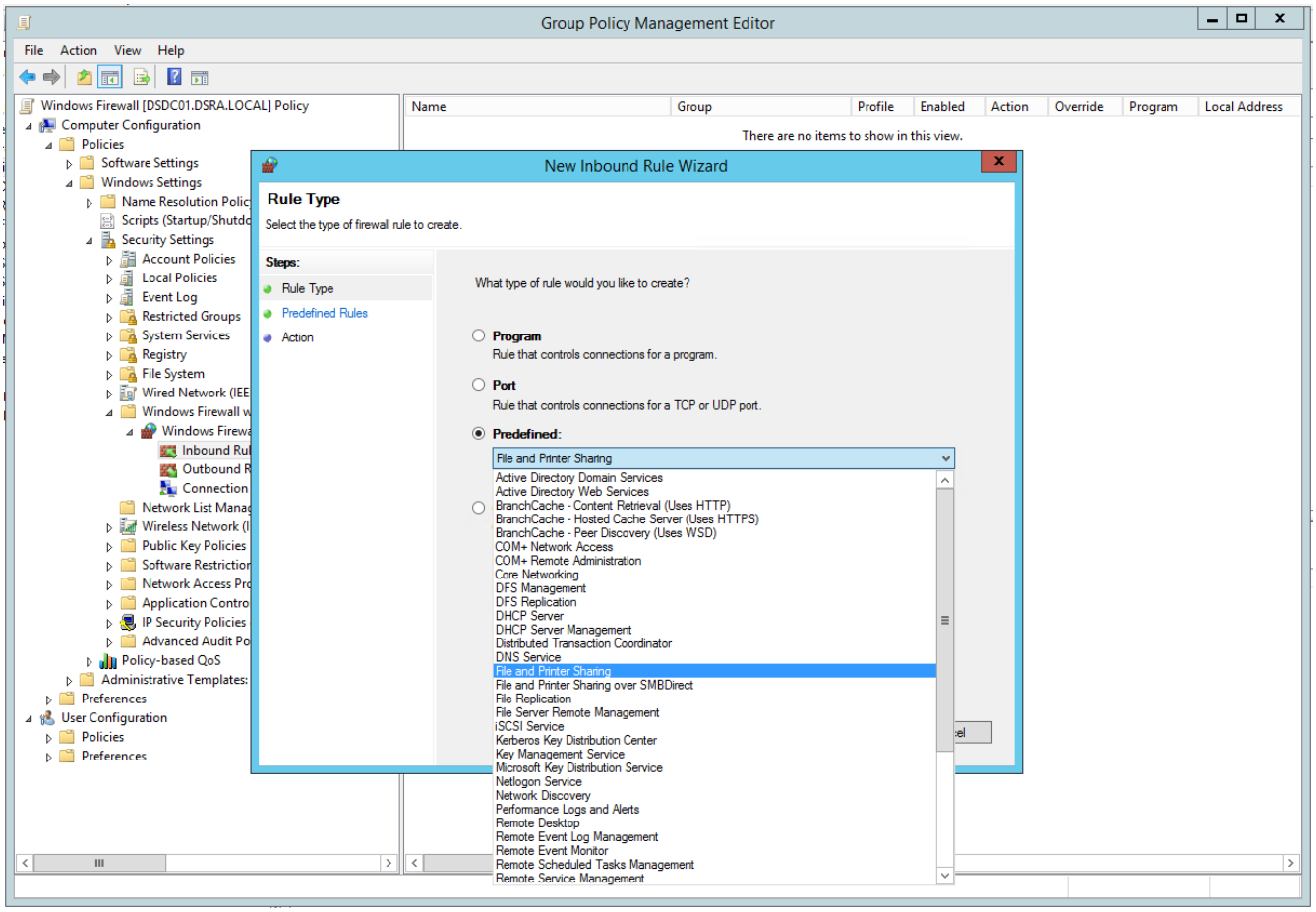

Abbildung 10 - Auswahl des vordefinierten Regelsatz Datei- und Druckerfreigabe

Im nächsten Schritt wird ausgewählt, welche Aktionen im Bereich der Datei- und Druckerfreigabe aktiviert werden sollen. Hier werden folgende Regeln aktiviert:

- Datei- und Druckerfreigabe (ICMP Echoanforderung - ICMPv6-In) und
- Datei- und Druckerfreigabe (ICMP Echoanforderung - ICMPv4-In)

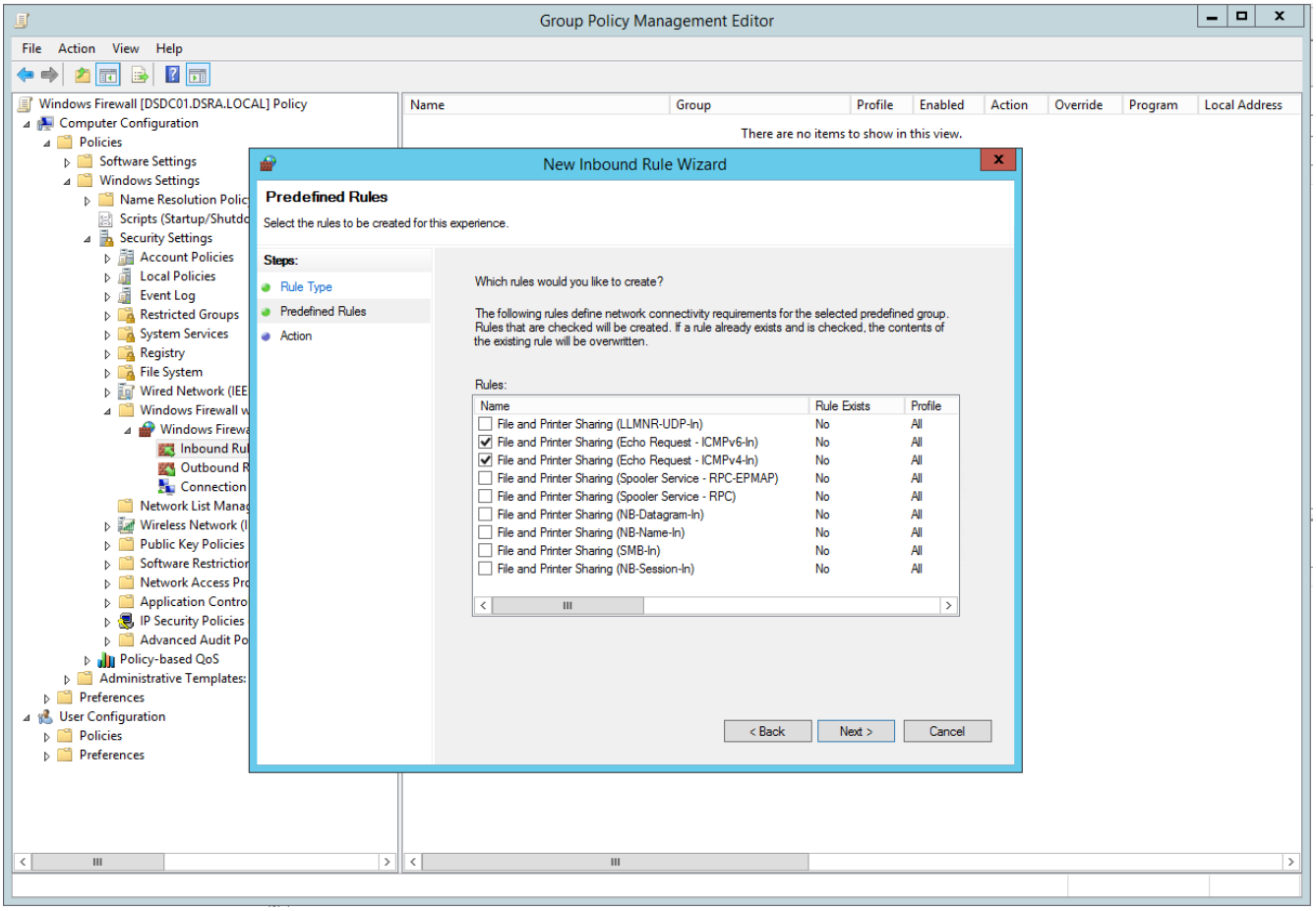

Abbildung 11 - Aktivierung der Regel zur Freigabe von ICMP-Echoanforderungen

Der nächste Schritt besteht darin die Option „Verbindung zulassen“ auszuwählen, welche im Standard bereits aktiviert ist.

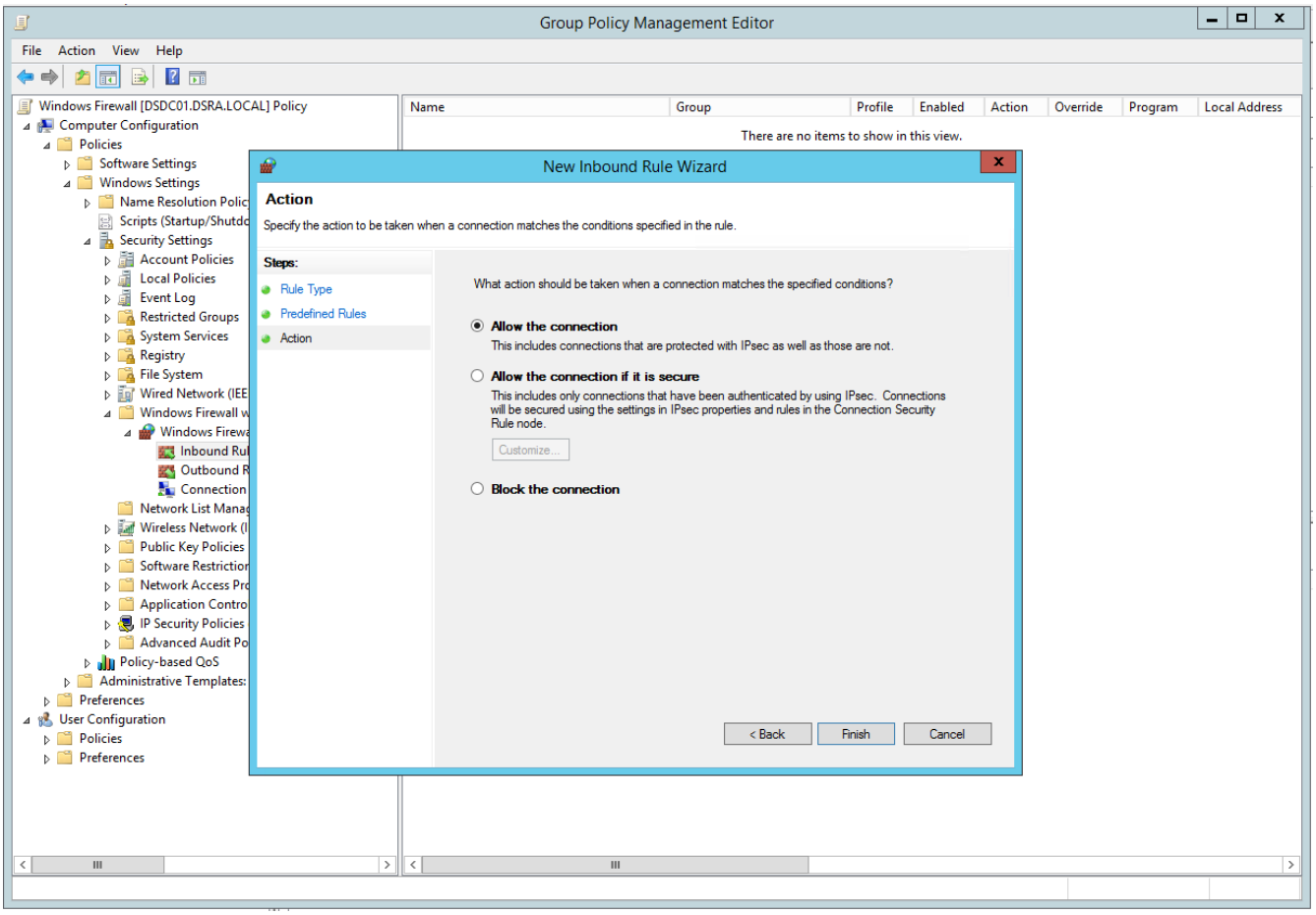

Abbildung 12 - Abschluss der Regelaktivierung - Verbindung zulassen

3.7.2 Windows Verwaltungsinstrumentation (WMI) aktivieren

Neben der Aktivierung der Datei- und Druckerfreigabe - speziell der Ping-Befehl, wird auch die Freischaltung für eingehende WMI-Abfragen benötigt. Hierfür starten Sie wieder den Firewall Assistenten und wählen folgenden vordefinierten Regelsatz aus:

- „Vordefiniert" - „Windows Verwaltungsinstrumentation (WMI)"

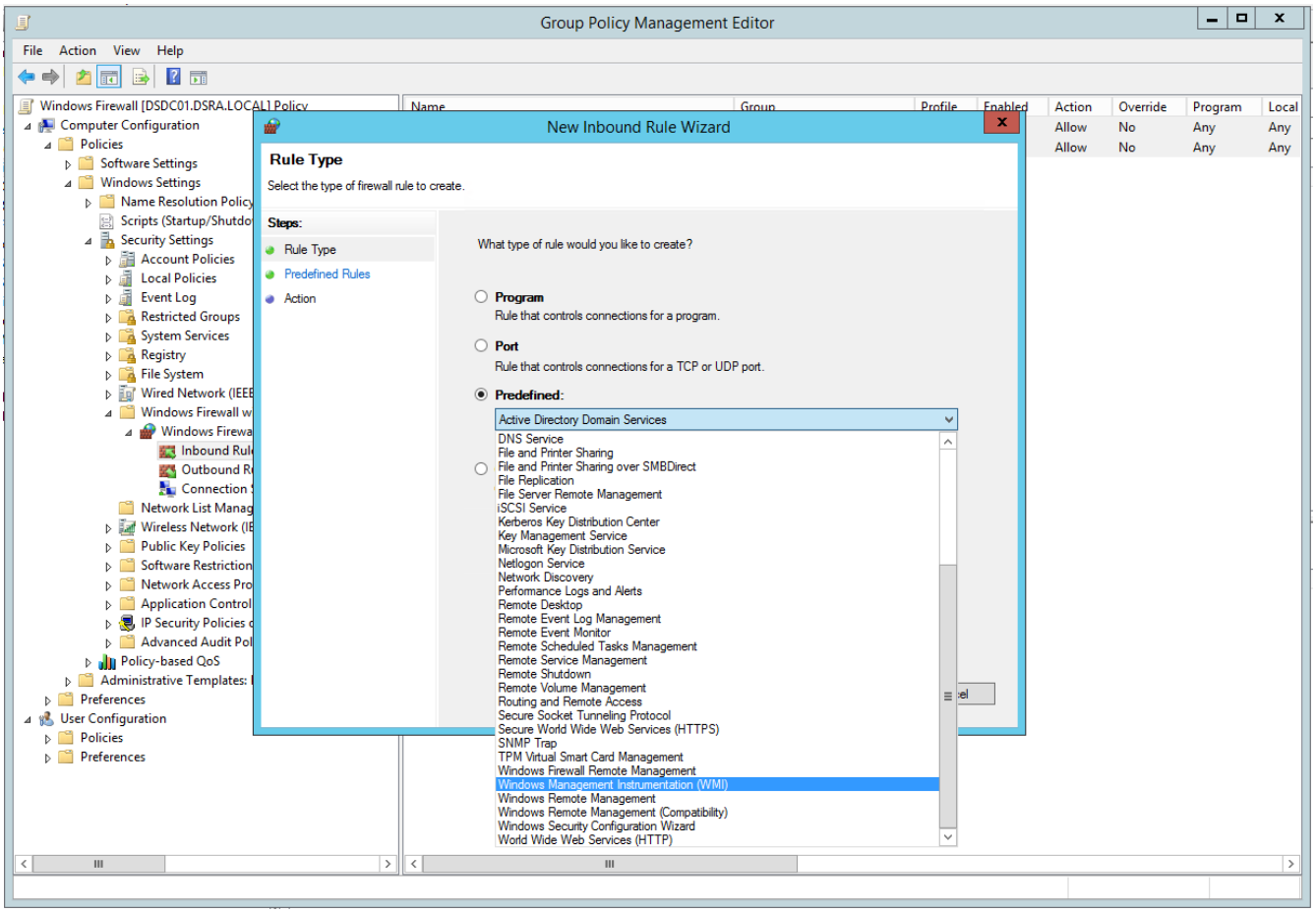

Abbildung 13 - Auswahl des vordefinierten Regelsatz Windows Verwaltungsinstrumentation

Im nächsten Schritt aktivieren Sie die Regel

- Windows Verwaltungsinstrumentation (WMI-In)

Die weiteren Regeln werden nicht benötigt. Die übrigen Schritte zur Aktivierung der Regel sind analog der vorherigen Regel durchzuführen:

- Verbindung zulassen

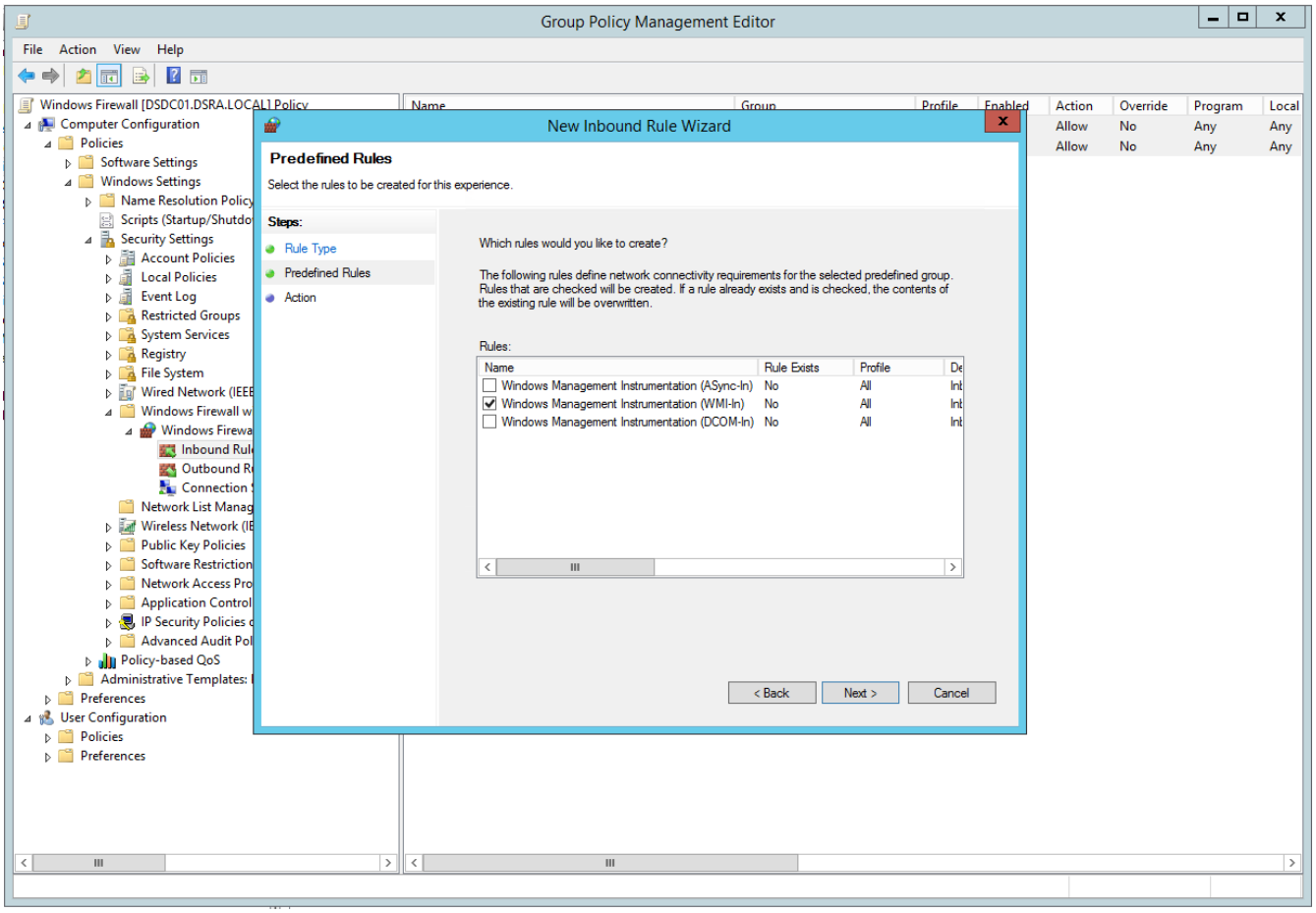

Abbildung 14 - Aktivierung der Regel zur Freigabe eingehenden WMI Abfragen

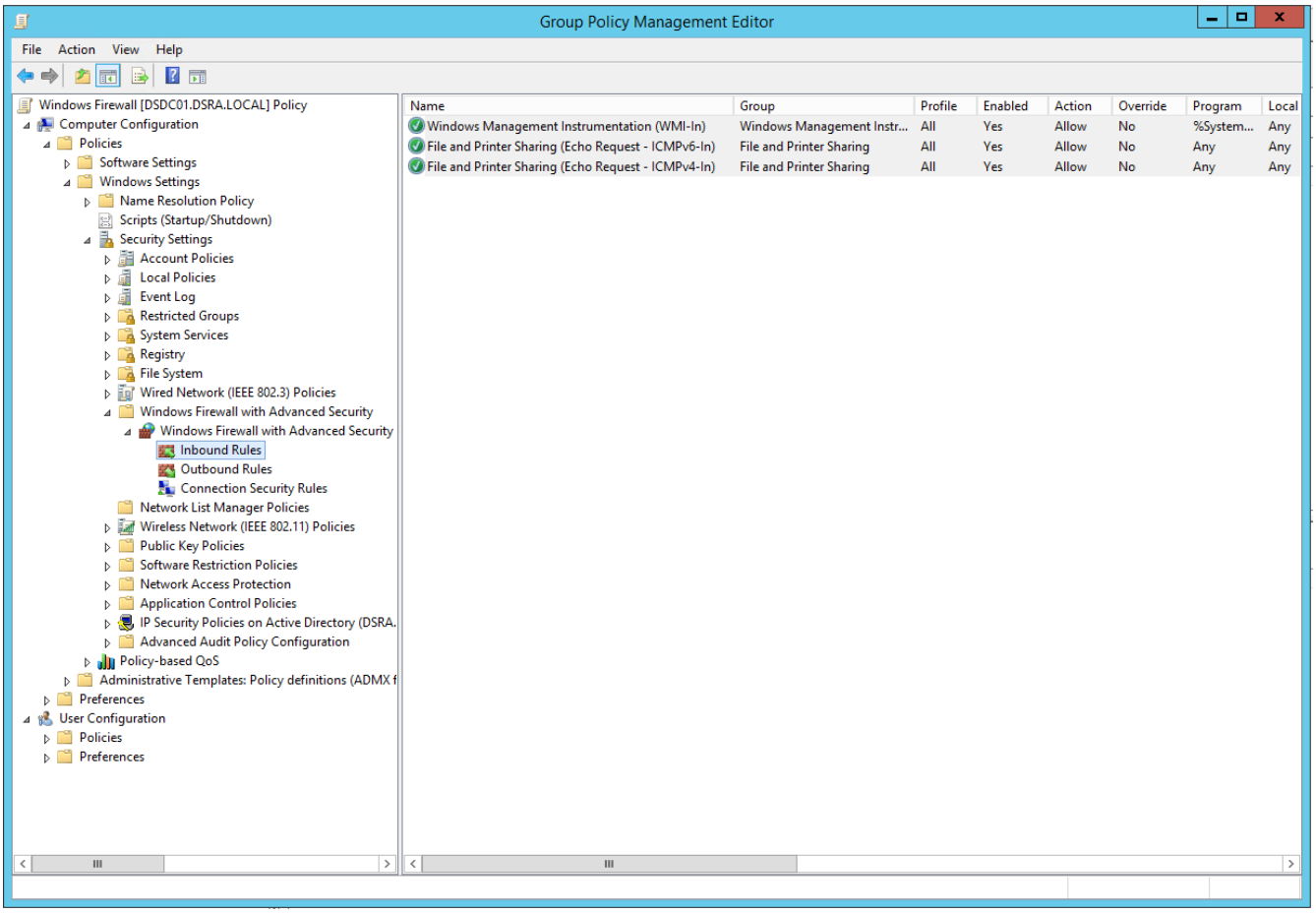

Abbildung 15 - Abschluss der Firewall Konfiguration

4. Windows 10 – Windows Firewall Konfiguration (lokal)

Die Firewall Konfiguration kann direkt über den Befehl *firewall.cpl* aufgerufen werden.

- *Suchen* – Eingabe: *firewall.cpl*

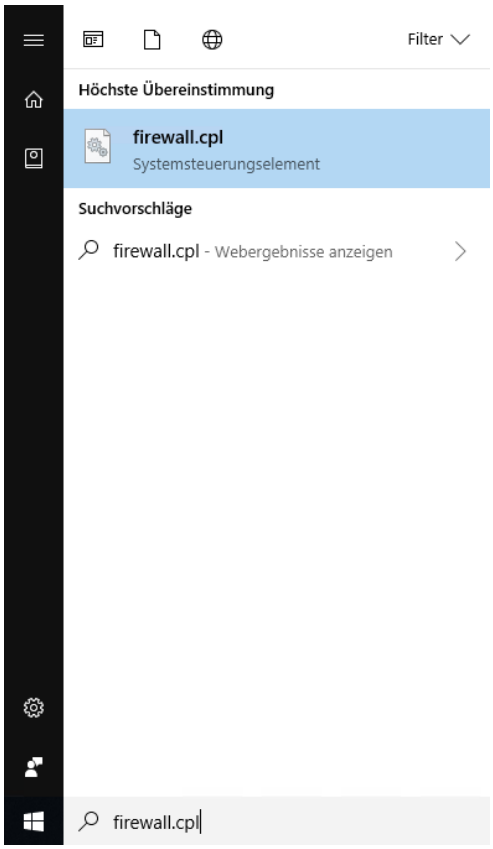

Abbildung 16 - Windows 10 - Suche - Eingabe firewall.cpl

Alternativ kann der Befehl auch in einem Konsolenfenster ausgeführt werden:

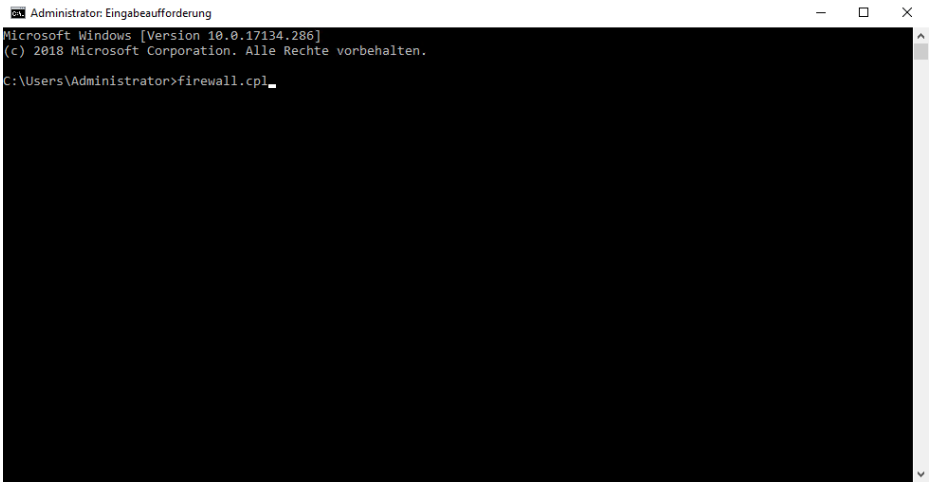

Abbildung 17 - Windows 10 - Eingabeaufforderung firewall.cpl

4.1 Ausnahme festlegen

Eine App oder ein Feature durch die Windows-Firewall zulassen anklicken.

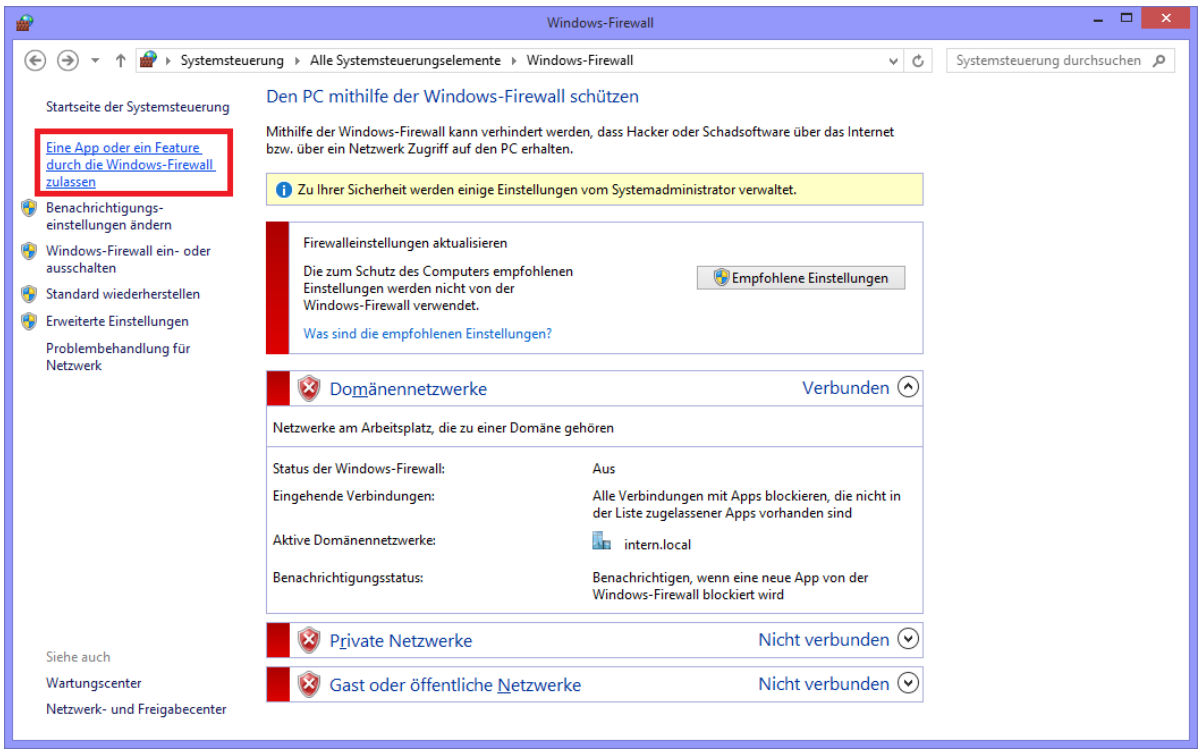

Abbildung 18 - Windows 10 - Windows-Firewall - App oder Feature zulassen

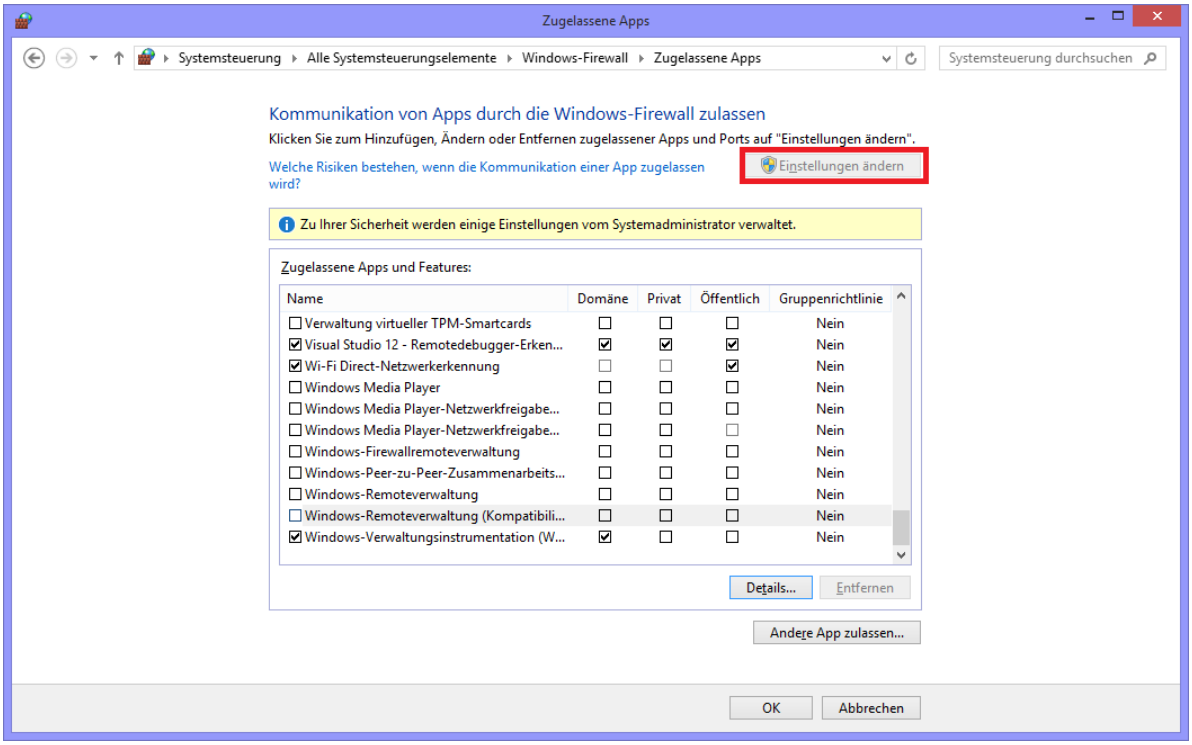

Abbildung 19 - Windows 10 – Windows-Firewall Zugelassene Apps und Features

Einstellungen ändern schaltet, entsprechende Benutzerrechte vorausgesetzt, die Bearbeitung von Programmen und Features frei. Windows 10 kennt drei unterschiedliche Netzwerktypen (Domäne, Privat und Öffentlich). Die Firewall Ausnahmen werden separat für jeden Typ definiert. Für die verwendeten Netzwerktypen sind folgende Ausnahmen per Haken in der Liste *Zugelassene Apps und Features* zu setzen:

- Datei- und Druckerfreigabe
- Windows-Verwaltungsinstrumentation (WMI)

Die neuen Einstellungen werden über die Schaltfläche *OK* übernommen. Diese Firewall Einstellungen ermöglichen Docusnap den Rechner zu scannen.

ABBILDUNGSVERZEICHNIS

VERSIONSHISTORIE

Datum	Beschreibung
03.01.2017	Erstellung des How-Tos
24.10.2018	Screenshots und Inhalt auf Windows 10 aktualisiert