Windows-Firewall Ausnahmen für Docusnap konfigurieren

Inhaltsverzeichnis

1. Windows Firewall Konfiguration - 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. Die Beispiele – manuelle Konfiguration wurden für Windows 7, Vista und XP entworfen.

1.1 Übersicht - benötige Firewall Ausnahmen

Es erfolgt nun eine kurze Beschreibung der zu treffenden Ausnahmen. Die Beschränkung der Ausnahmen auf bestimmte IP Bereiche kann nur über die Konfiguration von Gruppenrichtlinienobjekten (GPO) erfolgen.

Datei und Druckfreigabe

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

Hinweis: Diese Einstellung lässt 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.

Hinweis Sicherheit: Es sollte festgelegt werden, für welche IP-Adressen oder Subnetze die eingehenden Meldungen zulässig sind.

Remoteverwaltungsausnahme zulassen

Entspricht im wesentlichen der Windows 7 / Vista Ausnahme Windows-Verwaltungsinstrumentation (WMI) und ermöglicht die Remoteverwaltung des Windowssystems mit Verwaltungsprogrammen, wie z. B. Microsoft Management Console (MMC) und Windows-Verwaltungsinstrumentation (WMI). Windows-Firewall öffnet hierzu TCPPort 135 und 445. Dienste verwenden diese Ports normalerweise für die Kommunikation mithilfe von Remoteprozedur aufrufen (RPC) und DCOM (Distributed Component Object Model).

Darüber hinaus ermöglicht diese Richtlinieneinstellung den Programmen SVCHOST.EXE und LSASS.EXE unerbetene eingehende Meldungen zu empfangen und ermöglicht gehosteten Diensten, zusätzliche dynamisch zugewiesene Ports zu öffnen.

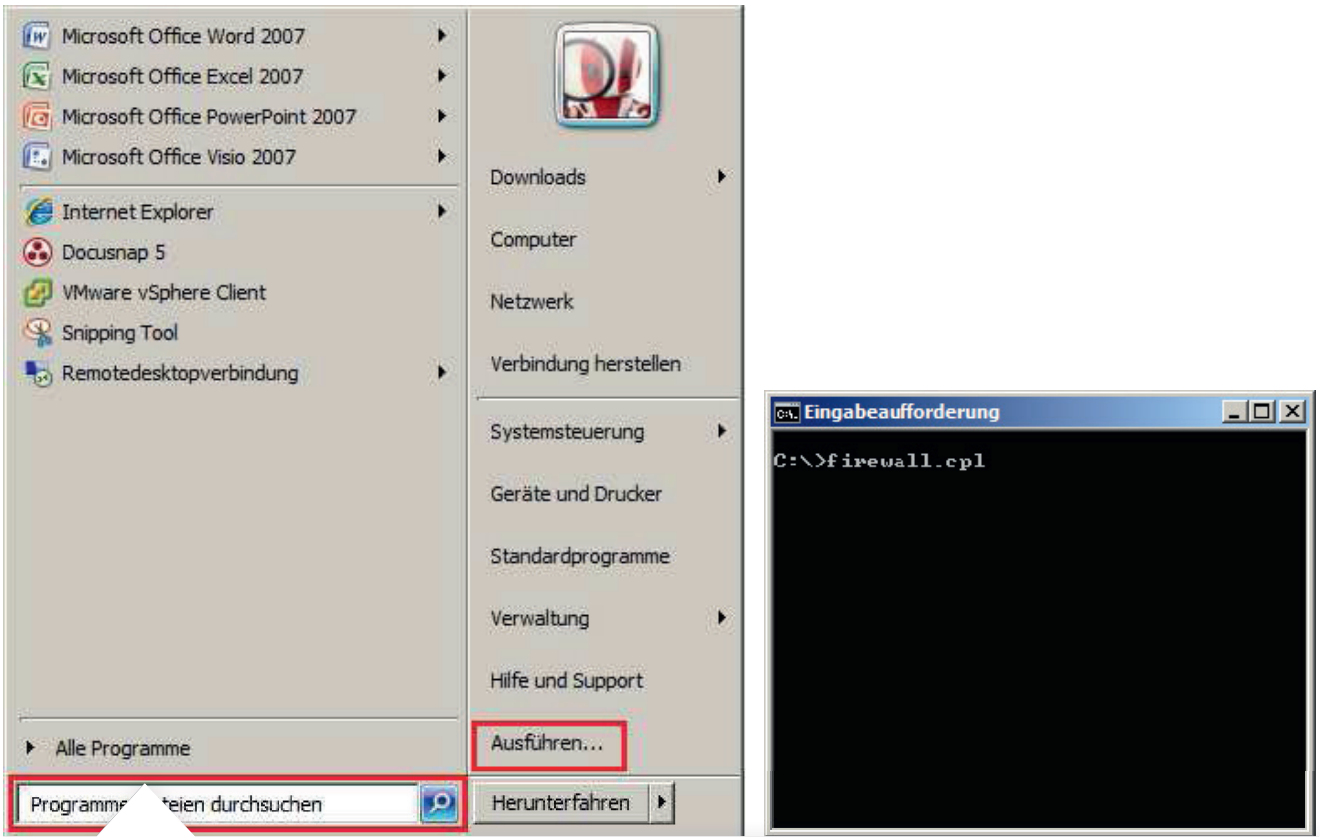
Hinweis Sicherheit: Es sollte festgelegt werden für welche IP-Adressen oder Subnetze diese eingehenden Meldungen zulässig sind.

2. Windows 7

2.1 Windows 7 – Windows Firewall Konfiguration per Befehl starten

Der einfachste Weg die Firewall-Konfiguration zu starten ist per Befehl firewall.cpl

Folgende Varianten für die Befehlseingabe sind möglich:



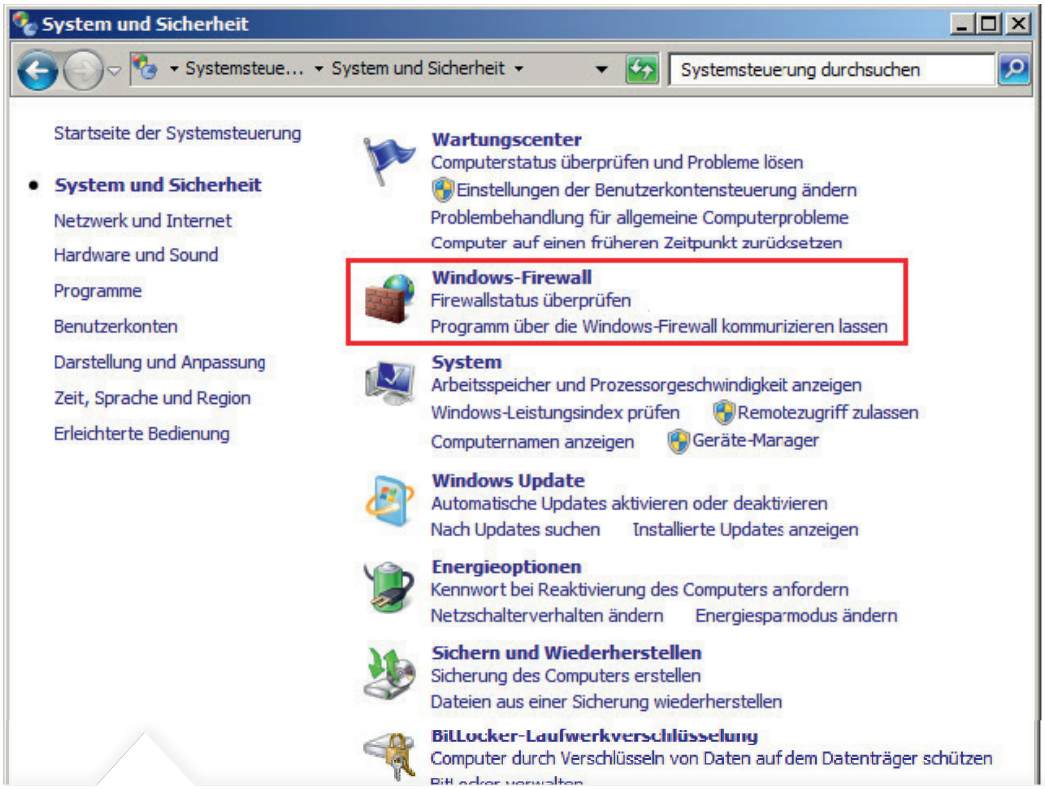
Start > Programme/Dateien durchsuchen Eingabe: firewall.cpl
> Ausführen Eingabe: firewall.cpl

Alternativ kann der Befehl auch in einem Konsolenfenster erfolgen.

2.2 Windows 7 – Windows Firewall Konfiguration interaktiv starten

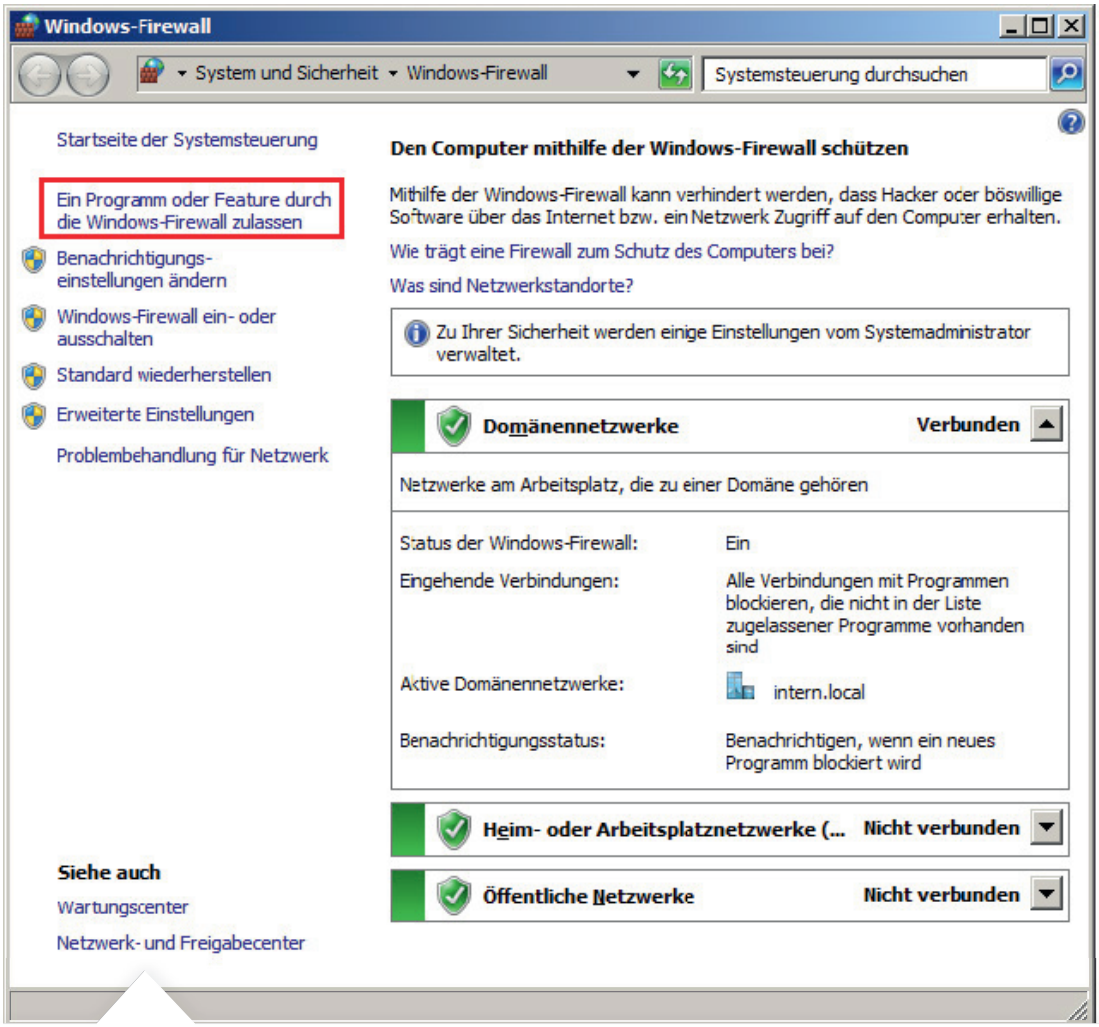
Start > Klicken und Systemsteuerung auswählen

> System und Sicherheit anklicken

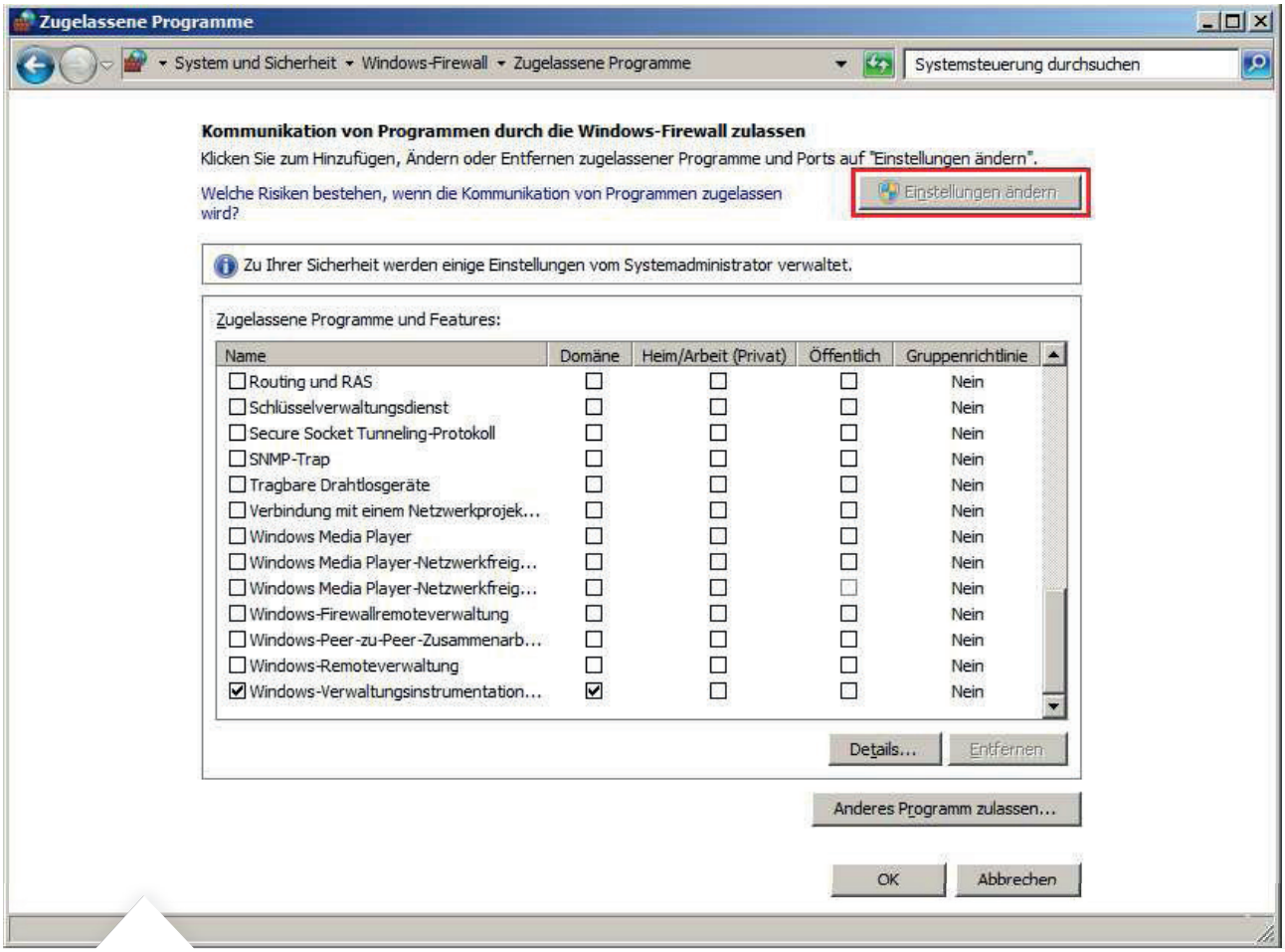


> Auf Windows-Firewall klicken

2.3 Windows 7 – Windows-Firewall Ausnahmen festlegen



> Ein Programm oder Feature durch die Windows-Firewall zulassen anklicken



> Einstellungen ändern schaltet, entsprechende Benutzerrechte vorausgesetzt, die Bearbeitung von Programmen und Features frei. Windows 7 kennt drei unterschiedliche Netzwerktypen (Domäne, Heim/Arbeit, Öffentlich). Die Firewall Ausnahmen werden separat für jeden Typ definiert. Für die verwendeten Netzwerk Typen sind folgenden Ausnahmen per Haken in der Liste Zugelassene Programme und Features zu setzen:

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

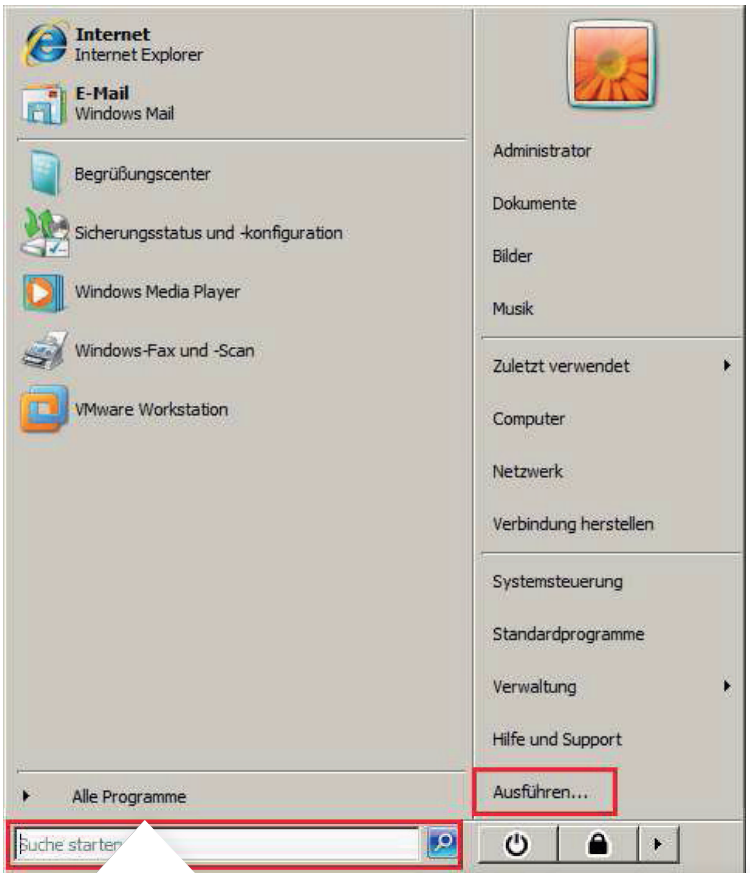
Die neuen Einstellungen nun per Klick auf die OK Schaltfläche übernehmen. Diese Firewall Einstellungen ermöglichen Docusnap den Rechner zu scannen.

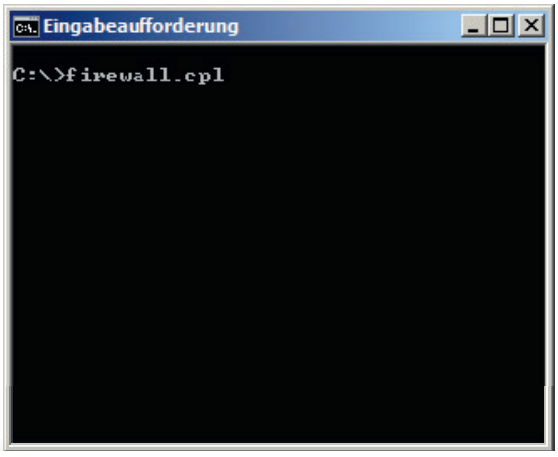
3. Windows Vista

3.1 Windows Vista – Windows Firewall Konfiguration per Befehl starten

Der einfachste Weg die Firewall-Konfiguration zu starten, ist per Befehl firewall.cpl.

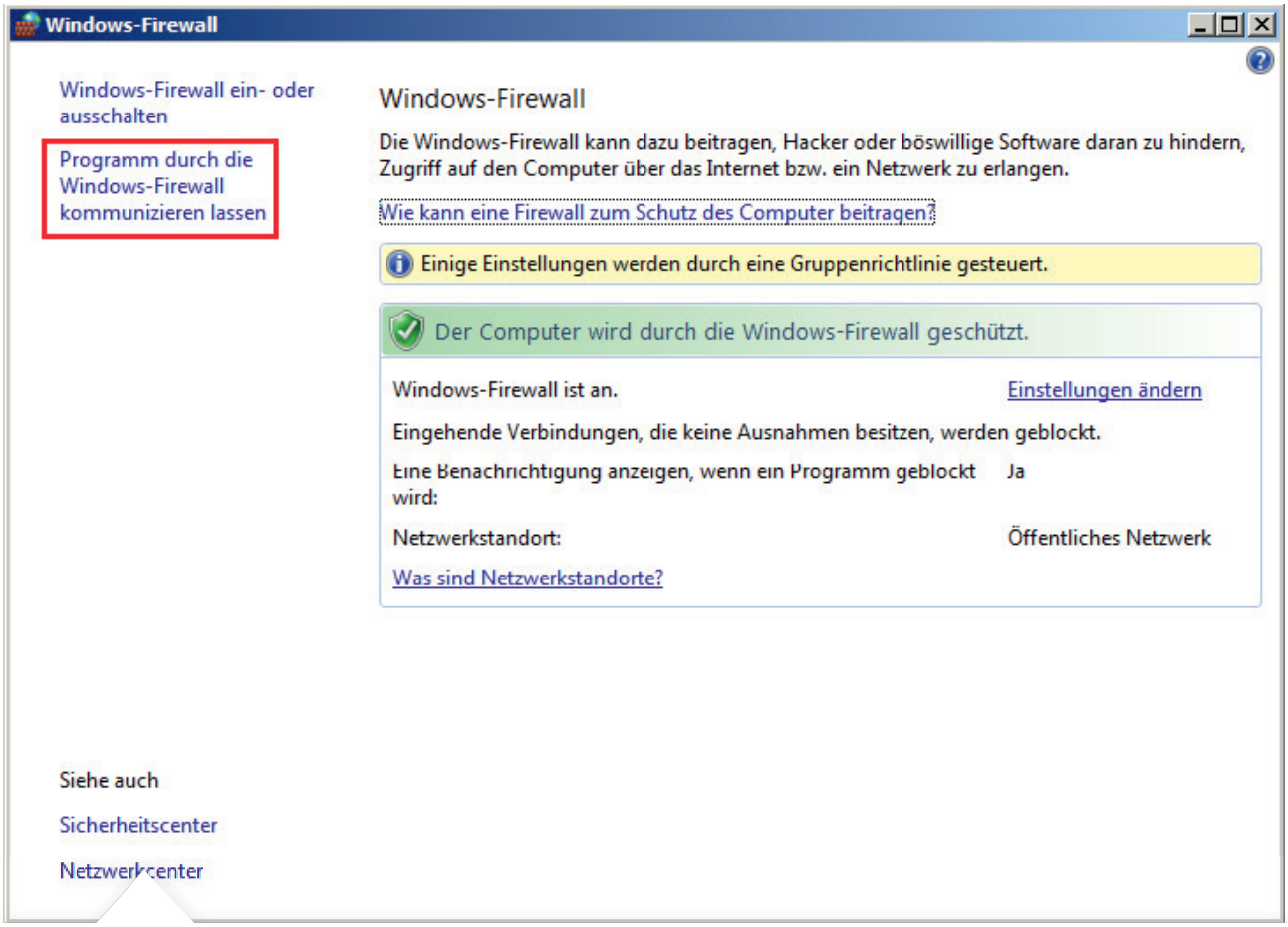
Folgende Varianten für die Befehlseingabe sind möglich:





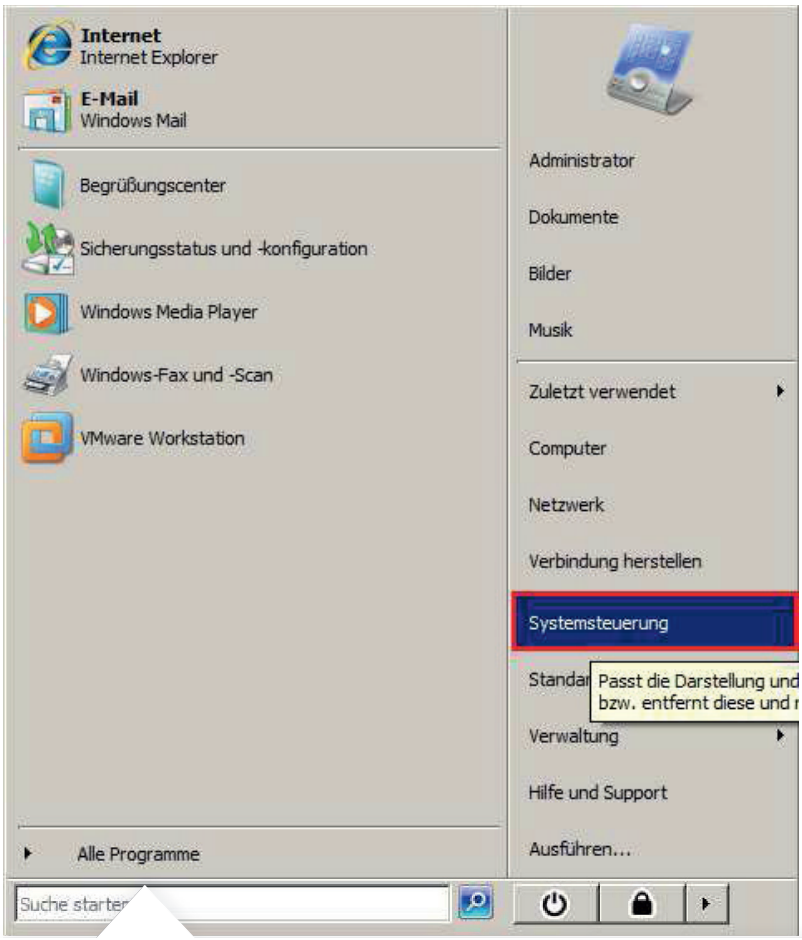
Start > Suche starten Eingabe: firewall.cpl
> Ausführen Eingabe: firewall.cpl

Alternativ kann der Befehl auch in einem Konsolenfenster erfolgen.



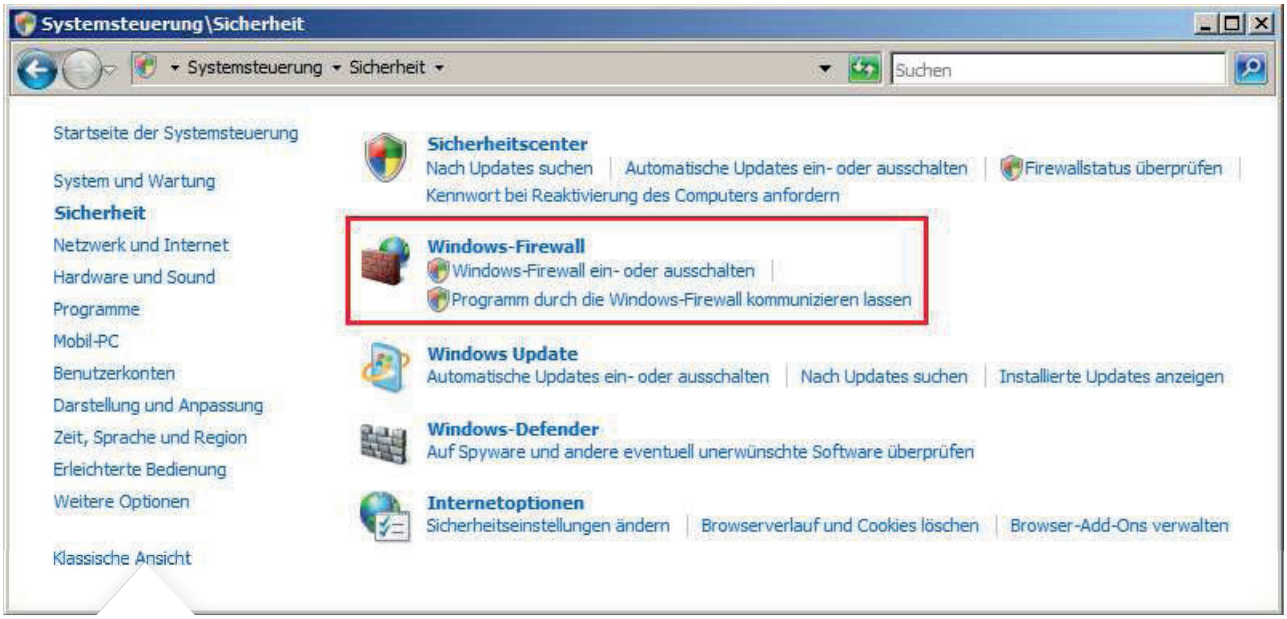
> Mit Klick auf Programm durch die Windows-Firewall kommunizieren lassen gelangt man in die Ausnahmen Konfiguration.

3.2 Windows Vista – Windows Firewall Konfiguration interaktiv starten



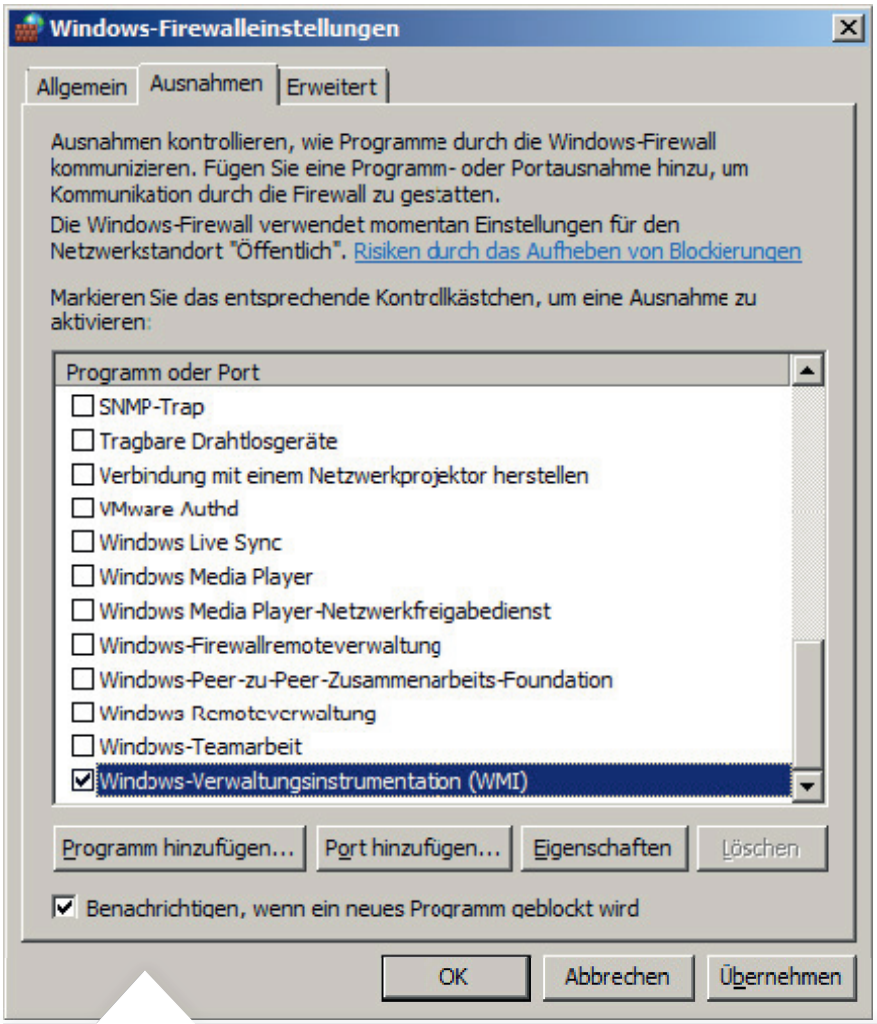
Start > Klicken und Systemsteuerung auswählen

> Programme durch die Windows-Firewall kommunizieren anklicken



> Programm durch die Windows-Firewall kommunizieren lassen anklicken

3.3 Windows Vista – Windows-Firewall Ausnahmen festlegen



> In der Liste Programm oder Port sind folgende Ausnahmen per Haken anzuwählen:

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

Nun die gewählten Einstellungen mit der Schaltfläche Übernehmen und dann OK bestätigen. Diese Firewall Einstellungen ermöglichen Docusnap den Rechner zu scannen.

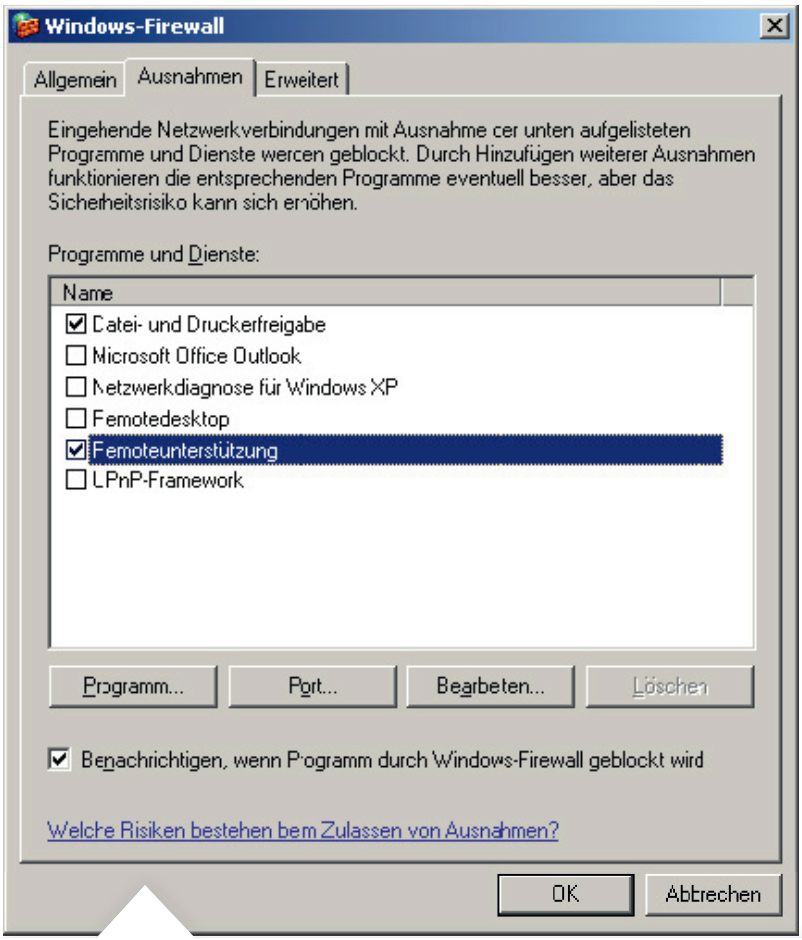
4. Windows XP (ab SP2)

4.1 Windows XP – Windows Firewall Konfiguration starten

Der schnellste Weg um die Firewall-Konfiguration aufzurufen ist per Befehl firewall.cpl

> per Eingabeaufforderung
> über Start > Ausführen

4.2 Windows XP – Windows Firewall Konfiguration interaktiv starten

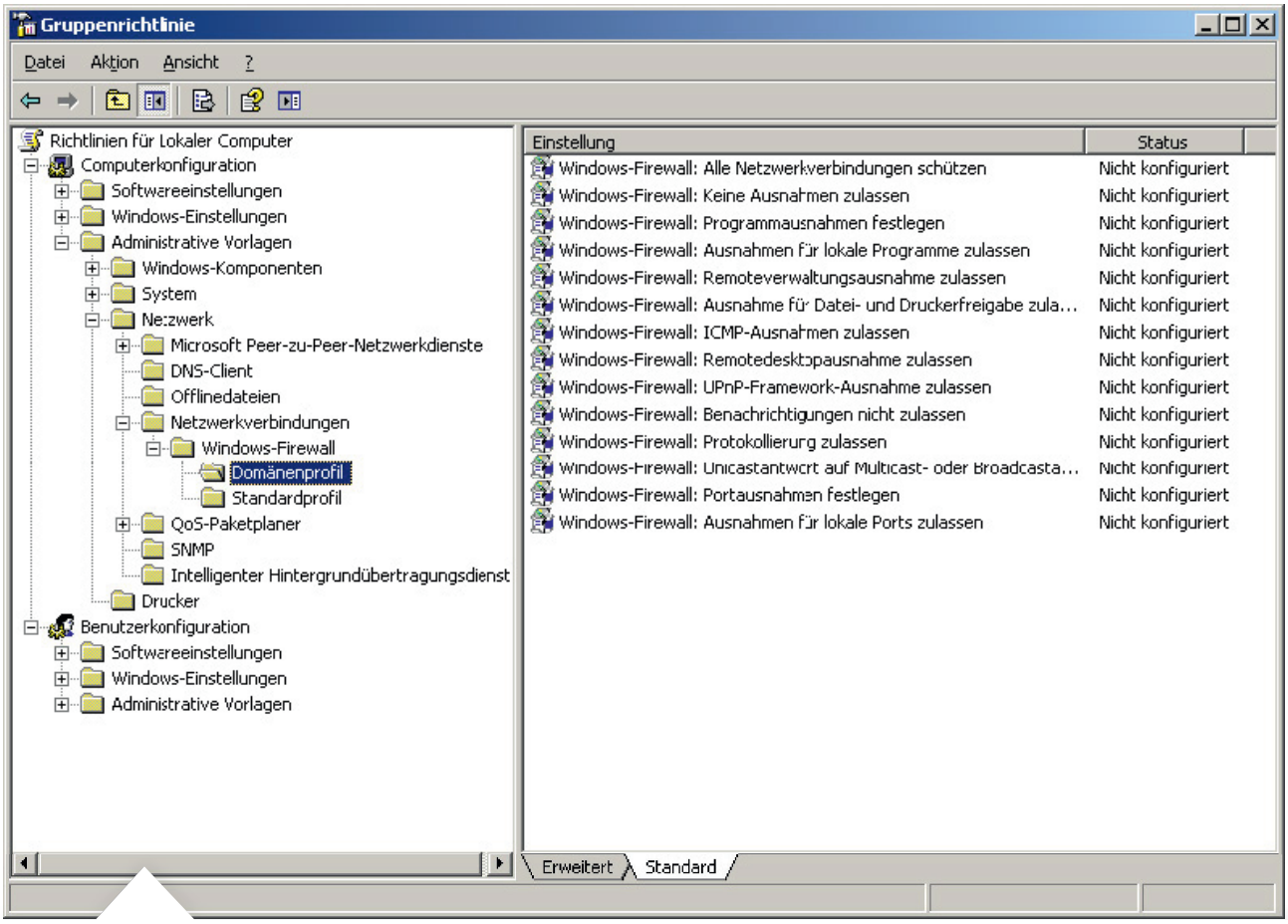


> Auf den Reiter Ausnahmen klicken. In der Liste Programm oder Dienste ist folgende Ausnahme per Haken anzuwählen:

• Datei- und Druckerfreigabe

Mit der Schaltfläche OK bestätigen. Die Windows-Firewall kann nun geschlossen werden.

4.3 Windows XP – per GPO zusätzliche Ausnahme aktivieren – GPO Editor starten

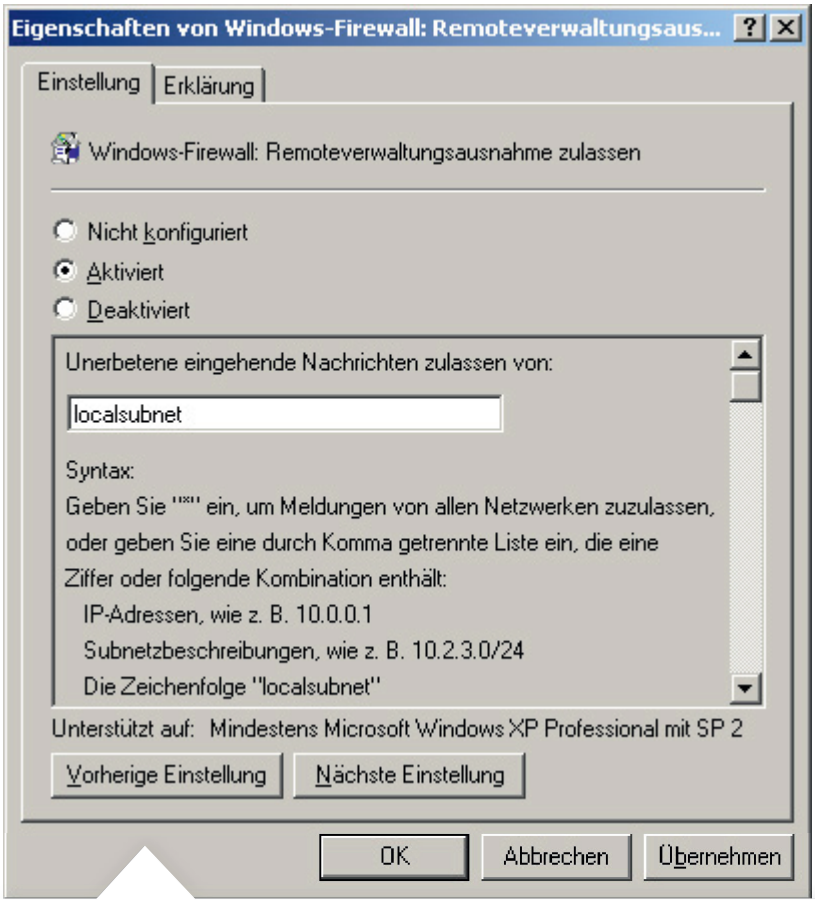


>In Windows XP Firewall Ausnahmen fehlt die in Windows Vista und Windows 7 vorhandene Ausnahme Windows Verwaltungsinstrumentation (WMI)

Diese Ausnahme wird in Windows XP per Gruppenrichtlinien Einstellung aktiviert. Deshalb wird in den lokalen Gruppenrichtlinien Einstellungen die Firewall Ausnahme Remoteverwaltungsausnahme zulassen konfiguriert. Das Programm wird mit gpedit.msc gestartet. (per Eingabeaufforderung oder über Start > Ausführen)

Die zu aktivierende Gruppenrichtlinie befindet sich in: Richtlinien für Lokaler Computer
Computerkonfiguration
Administrative Vorlagen
Netzwerk
Netzwerkverbindungen
Windows – Firewall
Domänenprofil

4.4 Windows XP – per GPO zusätzliche Ausnahme aktivieren



>Die Gruppenrichtlinie Windows Firewall: Remoteverwaltungsausnahme zulassen aktivieren und die Reichweite der Einstellung im Eingabefeld festlegen. Dann Fenster mit Klick auf die OK Schaltfläche schließen.

Unerbetene eingehende Nachrichten zulassen von:

- Ein Stern im Eingabefeld schaltet die Firewall für jeden beliebigen Rechner frei
- Die Ausnahme gilt nur für ein bestimmtes Subnetz
(z.B. volles Class C – Netzwerk 192.168.100.0/24)
- Das lokale Subnetz kann auch über die Zeichenfolge localsubnet freigeschaltet werden
- Die Ausnahme auf einen bestimmten PC beschränkt werden (z.B. 192.168.100.10)

Die Anwendung kann jetzt geschlossen werden. Die Windows-Firewall Ausnahmen für Windows XP sind nun vollständig konfiguriert.

5. Windows Firewall Konfiguration – Active Directory

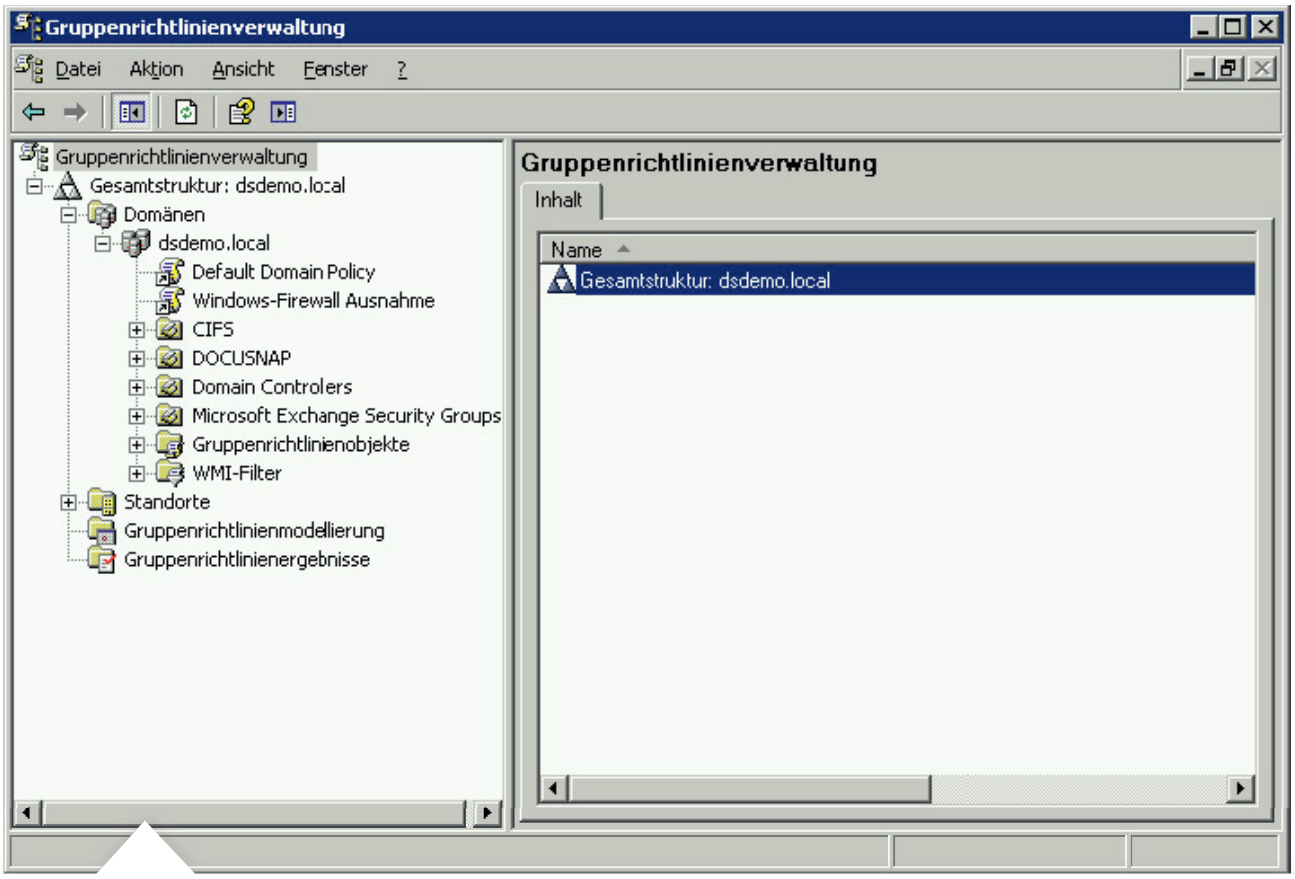
5.1 Grundlagen: Firewall – Gruppenrichtlinien/Verwaltungskonsole (GPMC)

Um die Firewall-Konfiguration für mehrere Rechner durchzuführen, wird empfohlen die benötigten Einstellungen per GPO vorzunehmen. Die Einstellungen sind ab XP SP2 gültig. Es ist nicht nötig für Vista und Windows 7 Rechner gesonderte Windows-Firewall Ausnahmen zu definieren.

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.

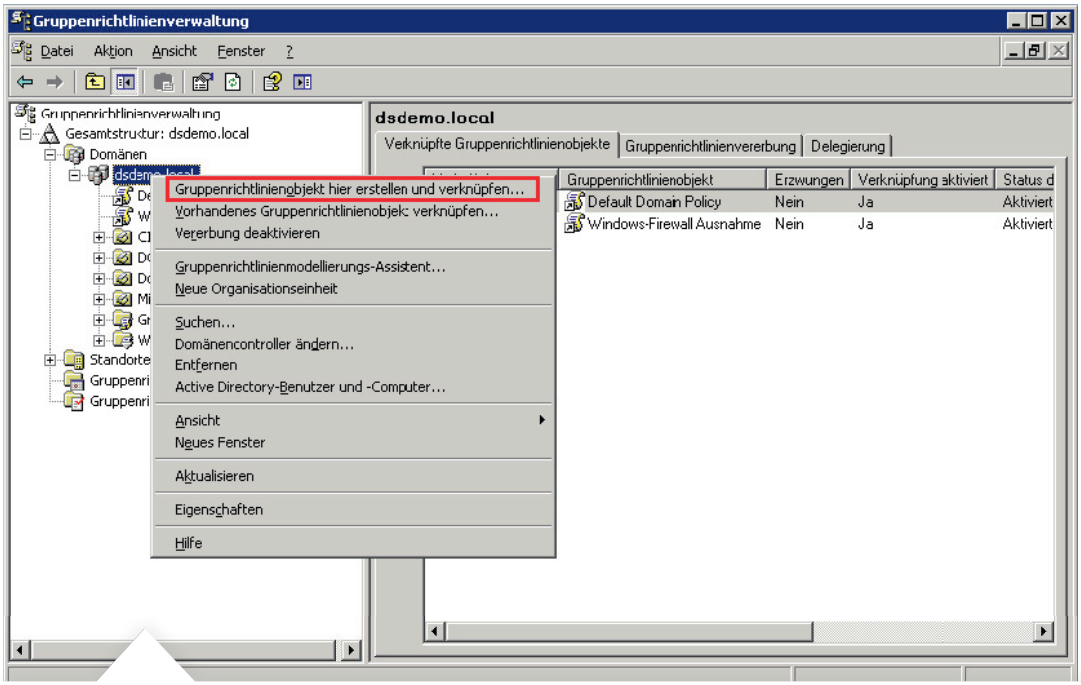
Die Gruppenrichtlinien Verwaltungskonsole kann auf der Microsoft Webseite kostenlos geladen werden. Dieses Tool ändert in diesem Beispiel die Firewall Einstellungen für alle in der Domäne vorhandenen Systeme und sollte nur mit Bedacht verwendet werden.

5.2 AD Windows Firewall Konfiguration – GPMC starten

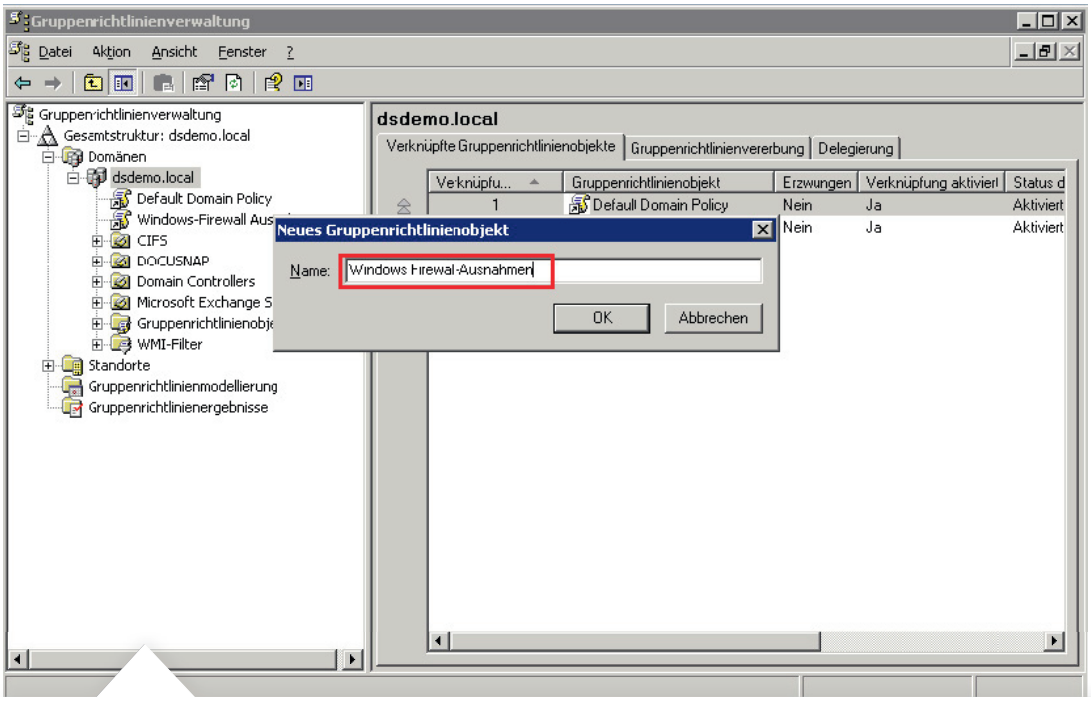


> Der einfachste Weg um die Verwaltungskonsole aufzurufen ist per Befehl gpmc.msc (Eingabeaufforderung oder über Start > Ausführen)

5.3 AD Windows Firewall – Gruppenrichtlinienobjekt für die Domäne erstellen

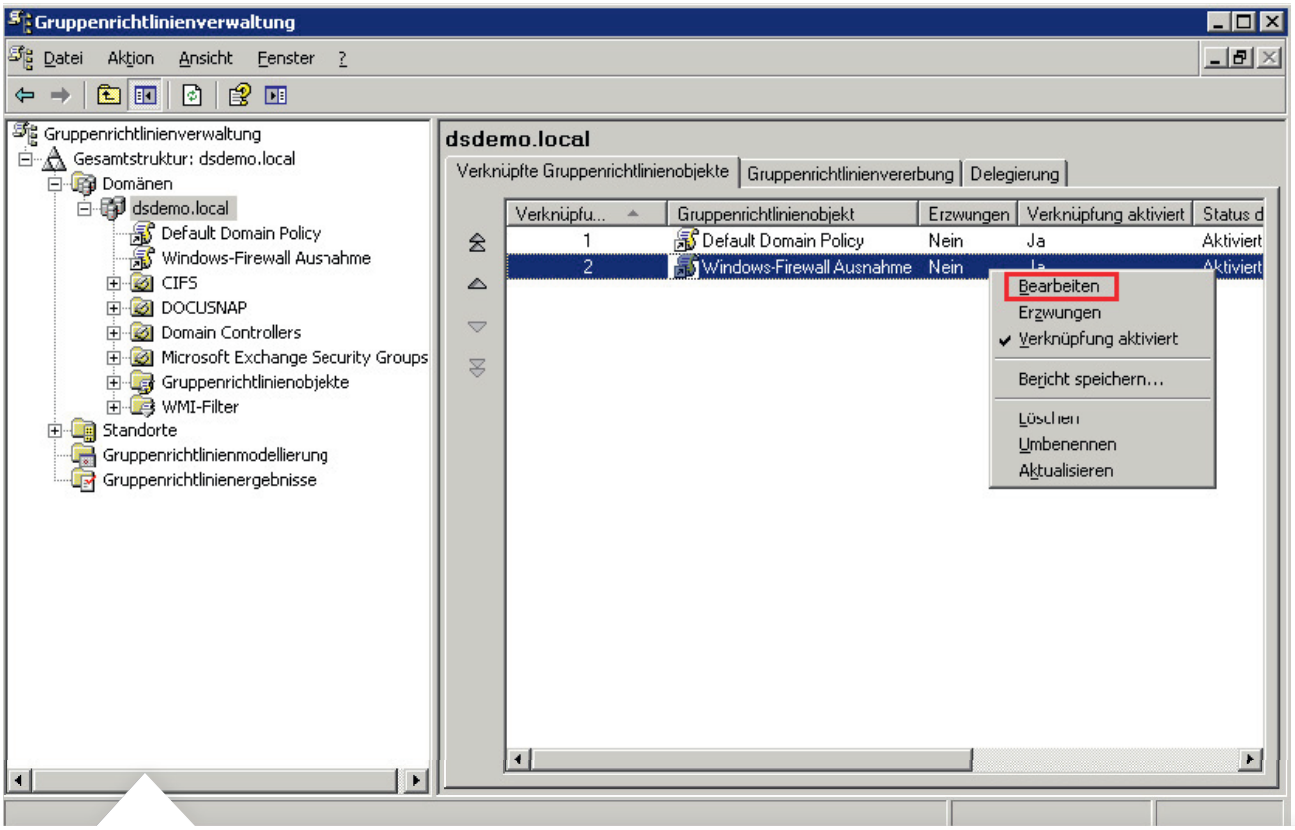


> Per Rechtsklick auf die gewünschte Domäne gelangt man zur Auswahl Gruppenrichtlinenobjekt hier erstellen und verknüpfen...



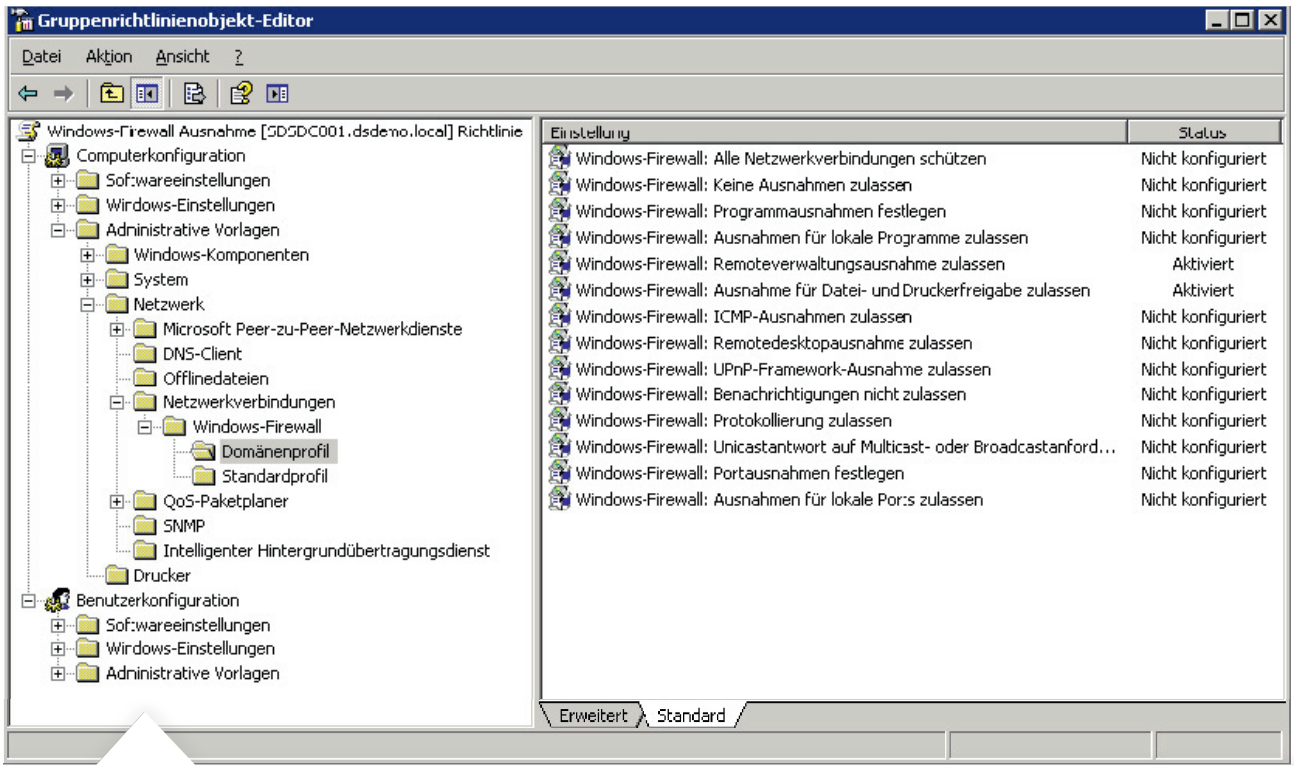
> Einen entsprechenden Namen für das Gruppenrichtlinenobjekt festlegen

5.4 AD Windows Firewall –
Zuvor erstelltes Gruppenrichtlinienobjekt bearbeiten



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

5.4 AD Windows Firewall –
Zuvor erstelltes Gruppenrichtlinienobjekt bearbeiten

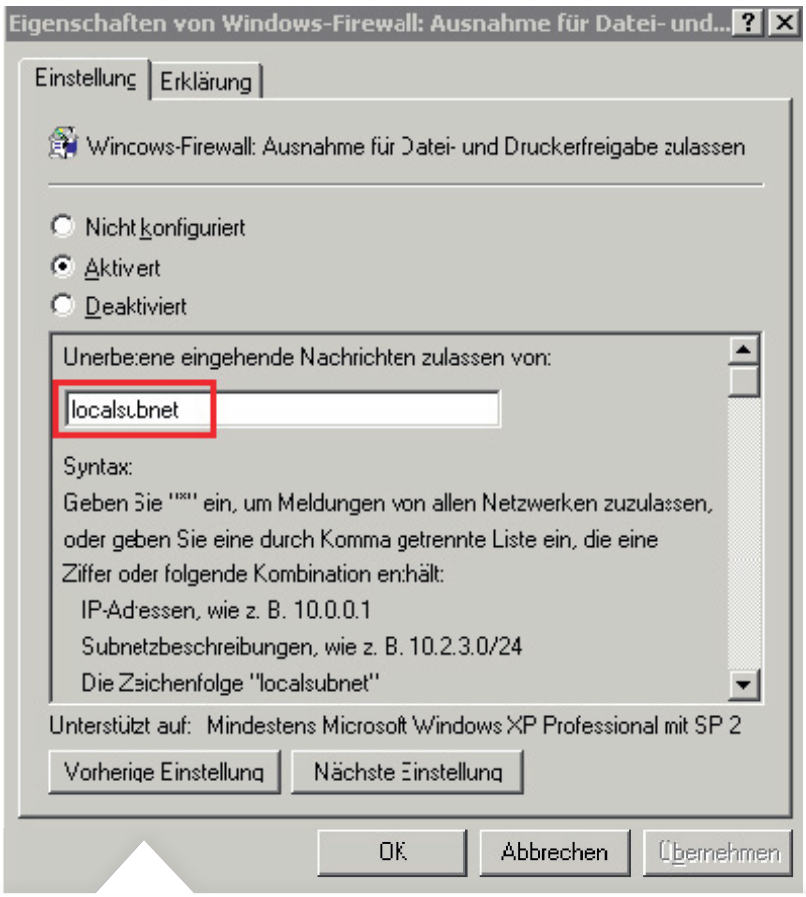


> Nun öffnet sich der Gruppenrichtlinienobjekt-Editor

Die zu aktivierenden Gruppenrichtlinien befinden sich in:

Richtlinien für Lokaler Computer
Computerkonfiguration
Administrative Vorlagen
Netzwerk
Netzwerkverbindungen
Windows – Firewall
Domänenprofil

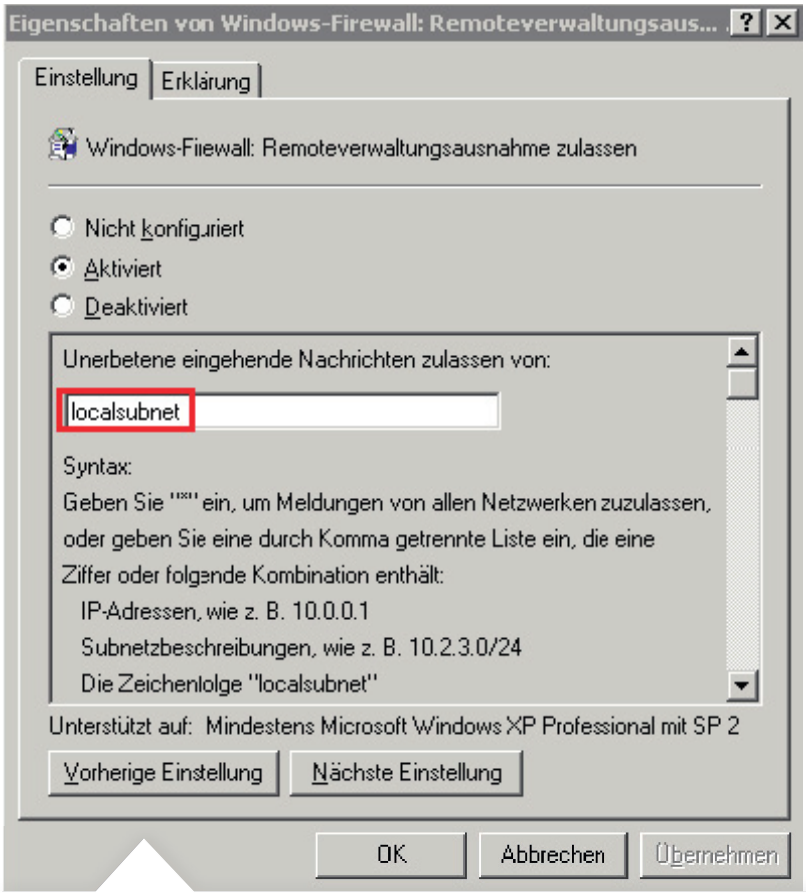
5.5 AD Windows Firewall – Ausnahme für Datei- und Druckerfreigabe aktivieren



> Windows-Firewall: Ausnahme für Datei- und Druckerfreigabe zulassen aktivieren

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

5.6 AD Windows Firewall – Remoteverwaltungsausnahme aktivieren



> Windows-Firewall: Remoteverwaltungsausnahme definieren aktivieren

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