

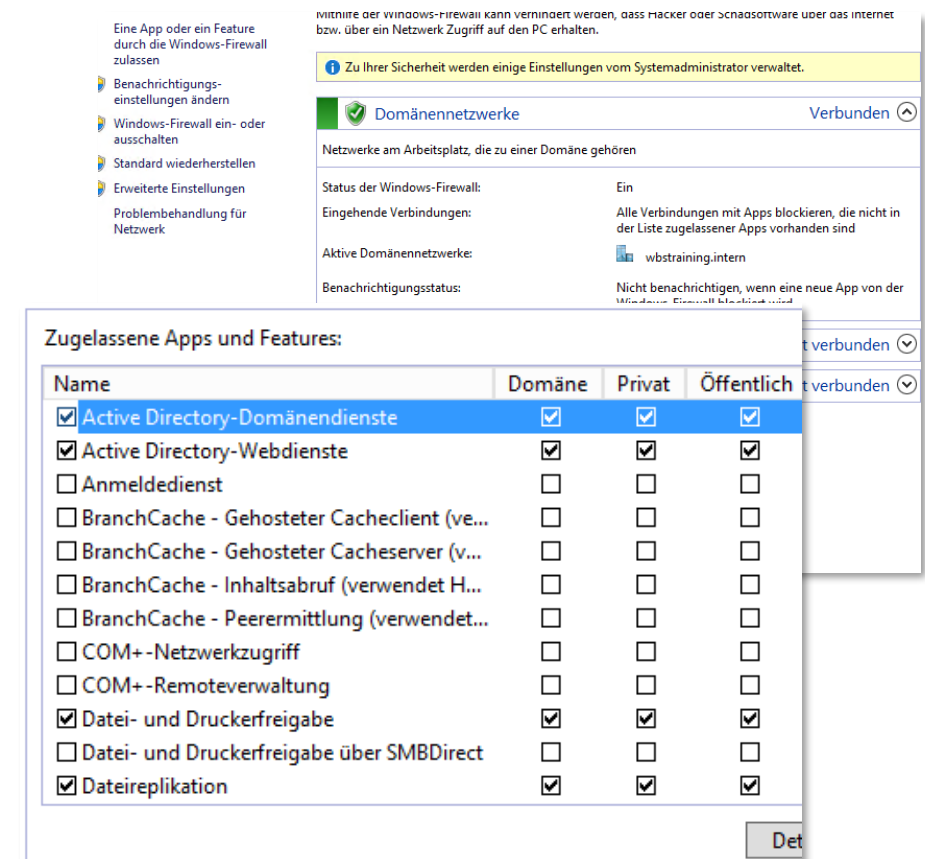
# Windows Server – Windows Firewall

# Agenda

- Windows Firewall
- Konfigurieren der Windows-Firewall mit erweiterter Sicherheit

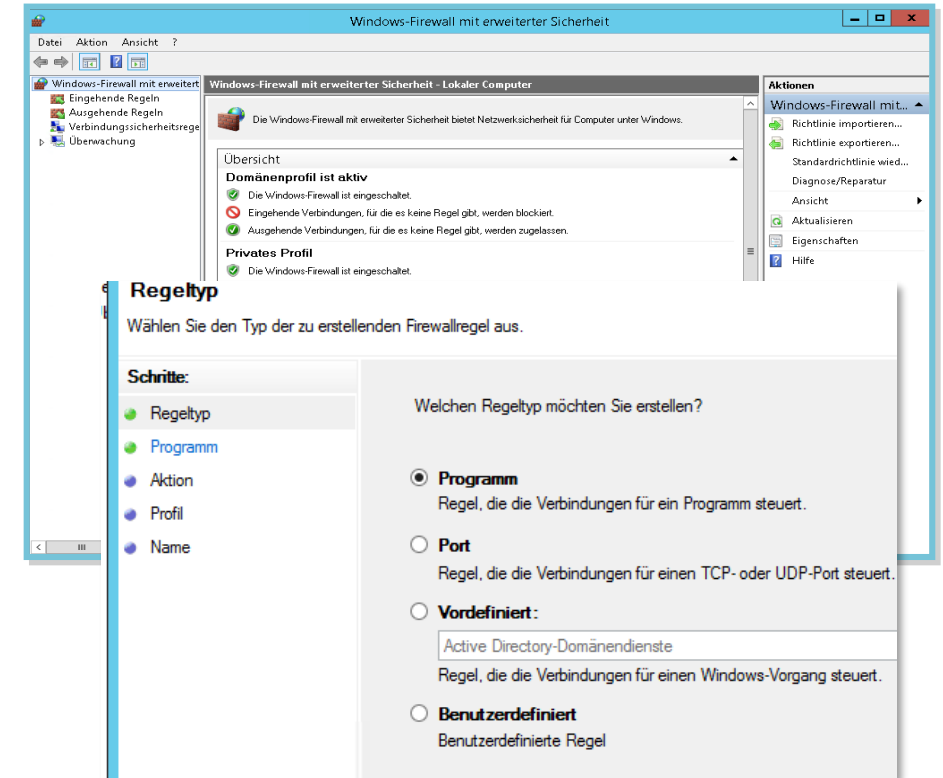
# Windows-Firewall

- Windows-Firewall ist eine statusbehaftete, hostbasierte Firewall, die Netzwerkdatenverkehr je nach Konfiguration zulässt oder blockiert
- nur der gesamte eingehende Datenverkehr wird blockiert
- es können nur Apps oder Features zugelassen werden



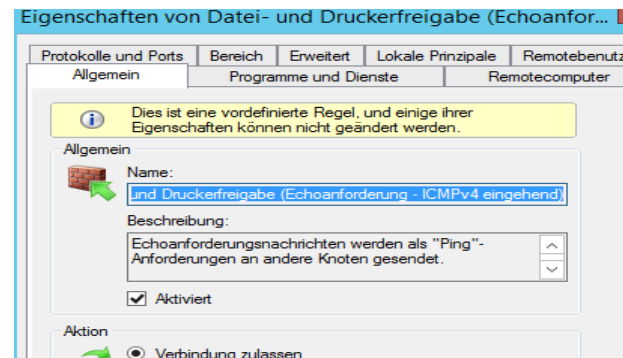
# Windows-Firewall mit erweiterter Sicherheit

- Windows-Firewall mit erweiterter Sicherheit steuert mit Regeln den eingehenden und ausgehenden Datenverkehr
- nur eingehender Datenverkehr wird blockiert
- Regeln erlauben Ausnahmen auf Basis von Programmen, Ports oder vordefinierten Regeln



# Windows-Firewall mit erweiterter Sicherheit

- Windows-Firewall bietet folgende Vorteile
  - Unterstützt Filterung sowohl für eingehenden als auch ausgehenden Datenverkehr
  - Integriert Firewallfilterung und IPsec-Schutzeinstellungen
  - Ermöglicht es Ihnen, Regeln zu konfigurieren, um den Netzwerkdatenverkehr zu steuern
  - Stellt aufenthaltsortspezifische Netzwerkprofile bereit
  - Ermöglicht es Ihnen, Richtlinien zu importieren oder zu exportieren



# Firewallprofile

- Firewallprofile sind ein Satz von Konfigurationseinstellungen, die für einen bestimmten Netzwerktyp gelten
- Es gibt folgende Firewall- Profile
  - Domäne
  - Öffentlich
  - Privat
- Windows Server 2012 bietet die Fähigkeit, mehrere aktive Firewallprofile zu haben

**Domänenprofil ist aktiv**

- ✓ Die Windows-Firewall ist eingeschaltet.
- ✗ Eingehende Verbindungen, für die es keine Regel gibt, werden blockiert.
- ✓ Ausgehende Verbindungen, für die es keine Regel gibt, werden zugelassen.

**Privates Profil**

- ✓ Die Windows-Firewall ist eingeschaltet.
- ✗ Eingehende Verbindungen, für die es keine Regel gibt, werden blockiert.
- ✓ Ausgehende Verbindungen, für die es keine Regel gibt, werden zugelassen.

**Öffentliches Profil**

- ✓ Die Windows-Firewall ist eingeschaltet.
- ✗ Eingehende Verbindungen, für die es keine Regel gibt, werden blockiert.
- ✓ Ausgehende Verbindungen, für die es keine Regel gibt, werden zugelassen.

[Freigabeoptionen für unterschiedliche Netzwerkprofile ändern](#)

Für jedes von Ihnen verwendete Netzwerk wird unter Windows ein separates Netzwerkprofil erstellt. Für jedes Profil können Sie bestimmte Optionen auswählen.

Privat \_\_\_\_\_

Gast oder Öffentlich \_\_\_\_\_

Domäne (aktuelles Profil) \_\_\_\_\_

Netzwerkerkennung \_\_\_\_\_

Wenn die Netzwerkerkennung eingeschaltet ist, kann dieser Computer andere Netzwerke und -geräte sehen, und er ist selbst sichtbar für andere Netzwerkcomputer.

☐ Netzwerkerkennung einschalten

☒ Netzwerkerkennung ausschalten

Datei- und Druckerfreigabe \_\_\_\_\_

Wenn die Freigabe von Dateien und Druckern aktiviert ist, können Netzwerkbenutzer und Drucker zugreifen, die Sie von diesem Computer freigeben.

☒ Datei- und Druckerfreigabe aktivieren

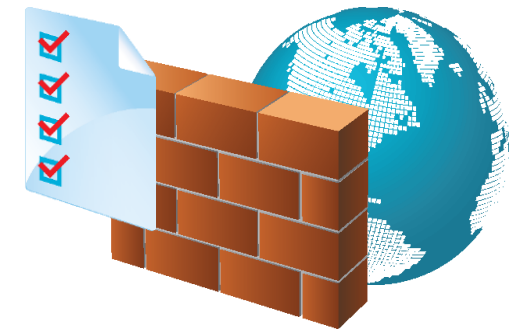
☐ Datei- und Druckerfreigabe deaktivieren

Alle Netzwerke \_\_\_\_\_

# Bereitstellen von Firewallregeln

- Windows-Firewallregeln können auf folgende Arten bereitgestellt werden
  - *Manuell.* Beim Testen oder der Problembehandlung oder für einzelne Computer
  - *Mit Hilfe von Gruppenrichtlinien.* Die bevorzugte Methode. Erstellen und testen Sie die Regeln, und stellen Sie sie anschließend auf einer großen Anzahl von Computern bereit
  - Durch *Exportieren und Importieren.* Verwendet Windows-Firewall mit erweiterter Sicherheit.
  - Beim Importieren von Regeln, werden **alle** aktuellen Regeln ersetzt

Testen Sie Firewallregeln immer in einer isolierten Umgebung, die keine Produktionsumgebung ist, bevor Sie sie in der Produktionsumgebung bereitstellen





**VIELEN DANK  
FÜR IHRE  
AUFMERKSAMKEIT!**