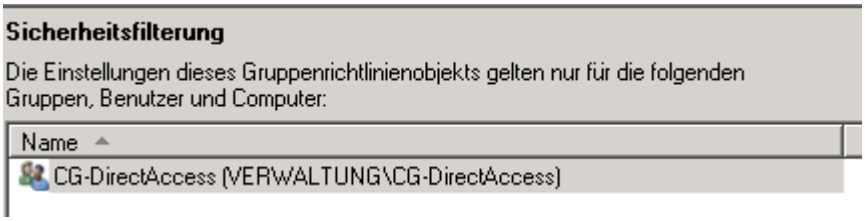
Forefront UAG DirectAccess - Remote Control aktivieren

Immer haeufiger wird Forefront UAG mit DirectAccess eingerichtet und meine Kunden wuenschen sich natuerlich auch eine Remote Control-Moeglichkeit dieser Clients. Das Standardkonzept von DA sieht aber keine klassische Remote Control vor, lediglich der Infrastruktur Server Zugriff im ersten IPSEC Infrastrukturtunnel ist geregelt.

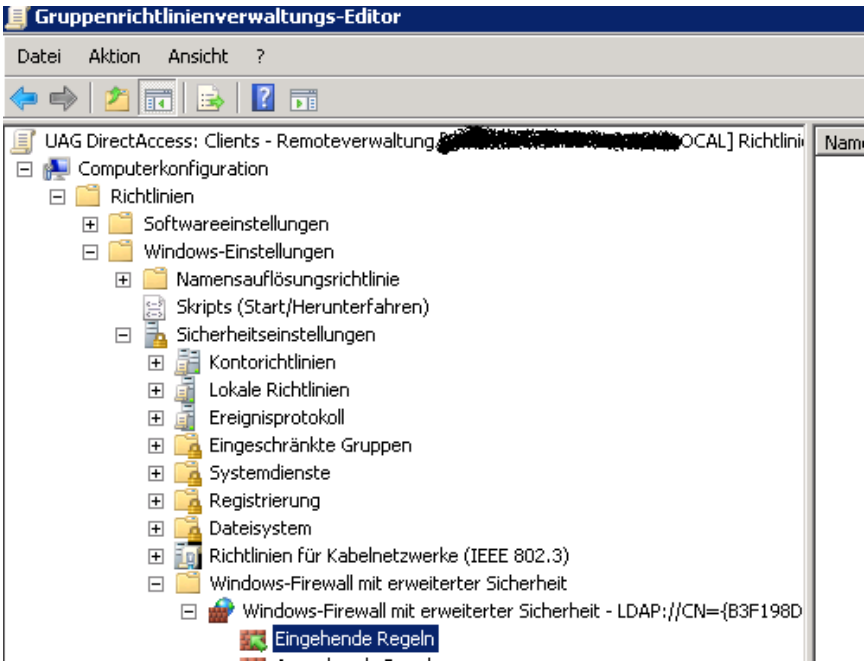
Erstellung einer neuen Gruppenrichtlinie fuer die DA-Clients

Achtung: Die bestehende Gruppenrichtlinie, erstellt von Forefront UAG sollte nicht verwendet werden, da diese ggfs. bei einer neuen Policy-Erstellung in der Forefront UAG-Verwaltungskonsole ueberschrieben wird.

Sicherheitsfilterung auf die gleiche Computergruppe wie fuer die DA-Clients in Forefront UAG

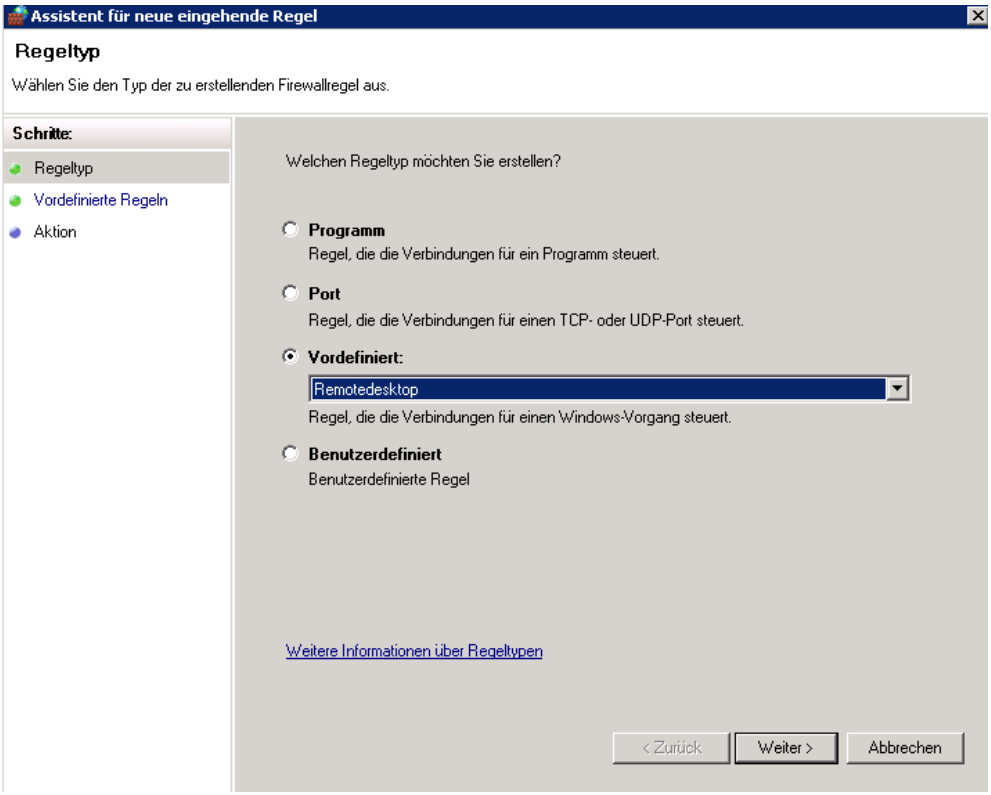


Editieren der Group Policy

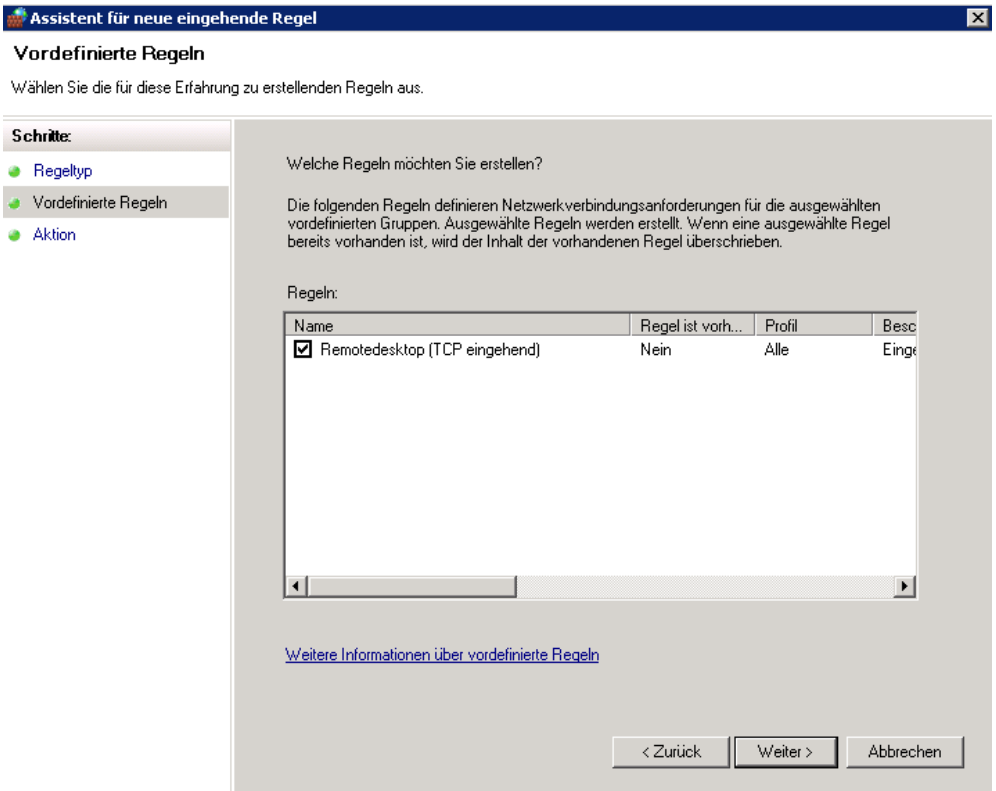


Erstellen einer neuen eingehenden Firewallregel

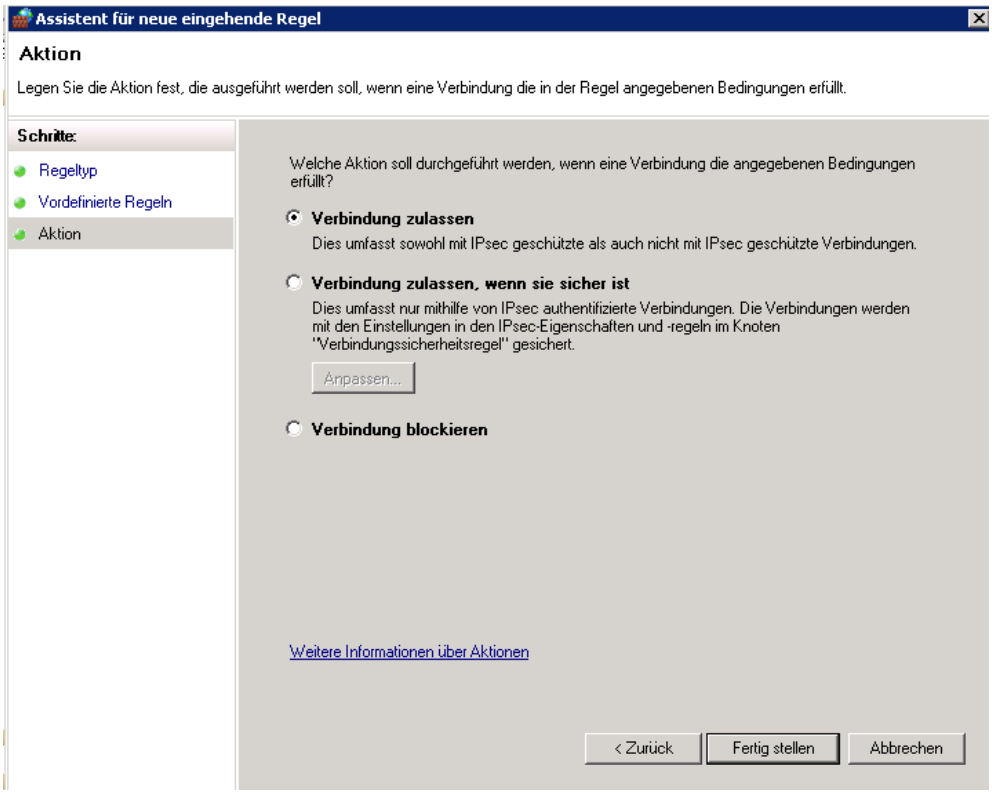
Typ ist in diesem Beispiel Remotedesktop. Es koennen aber beliebige Kombinationen verwendet werden.



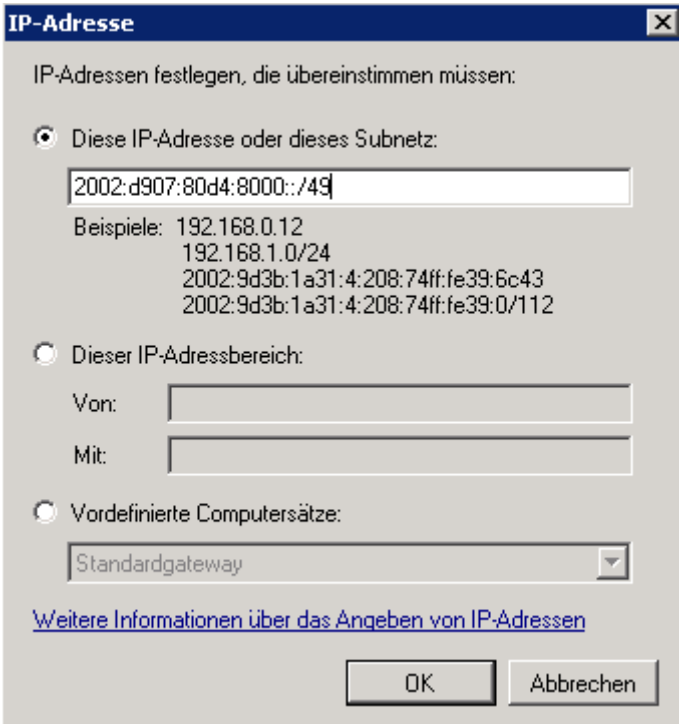
RDP



Verbindung zulassen

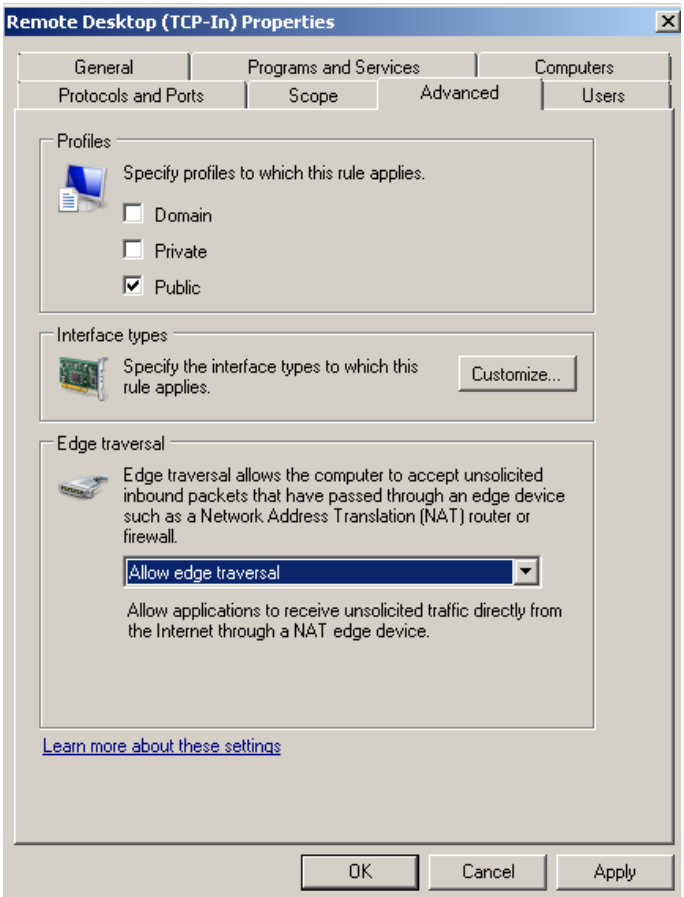


IPv6-IP Adressbereich aus dem Corporate LAN nehmen. Dazu entweder in der DNS Forward Lookupzone nachsehen oder in der erstellten UAG DirectAccess Client GPO, welcher IPv6-Adressbereich verwendet wird. Der IPv6 Adressbereich kann aus den GPO Einstellungen der Verbindungsanforderungsrichtlinien entnommen werden. Der Zugriff sollte auf Verwaltungsnetze oder Verwaltungsrechner beschraenkt werden.



Wichtig:

Auf der Registerkarte Erweitert bei der Edgeausnahme – *Edgeausnahme zulassen* auswaehlen



So sieht die Firewallrichtlinie am DA-Client aus.

Tipp: Da der DA-Client ja schon einen IPSEC-Infrastrukturtunnel etabliert hat, bekommt der DA-Client auch bei ausschliesslicher Internet Verbindung aktualisierte Gruppenrichtlinienobjekte zugewiesen, so dass ein Switchen zwischen LAN und WAN nicht notwendig ist.