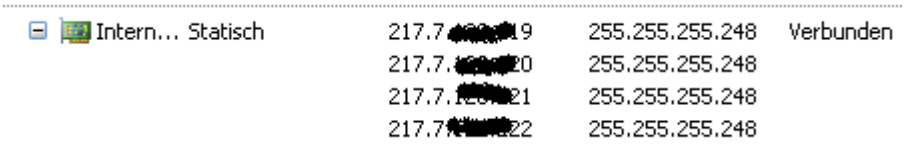
Forefront TMG und multiple ausgehende IP-Adressen

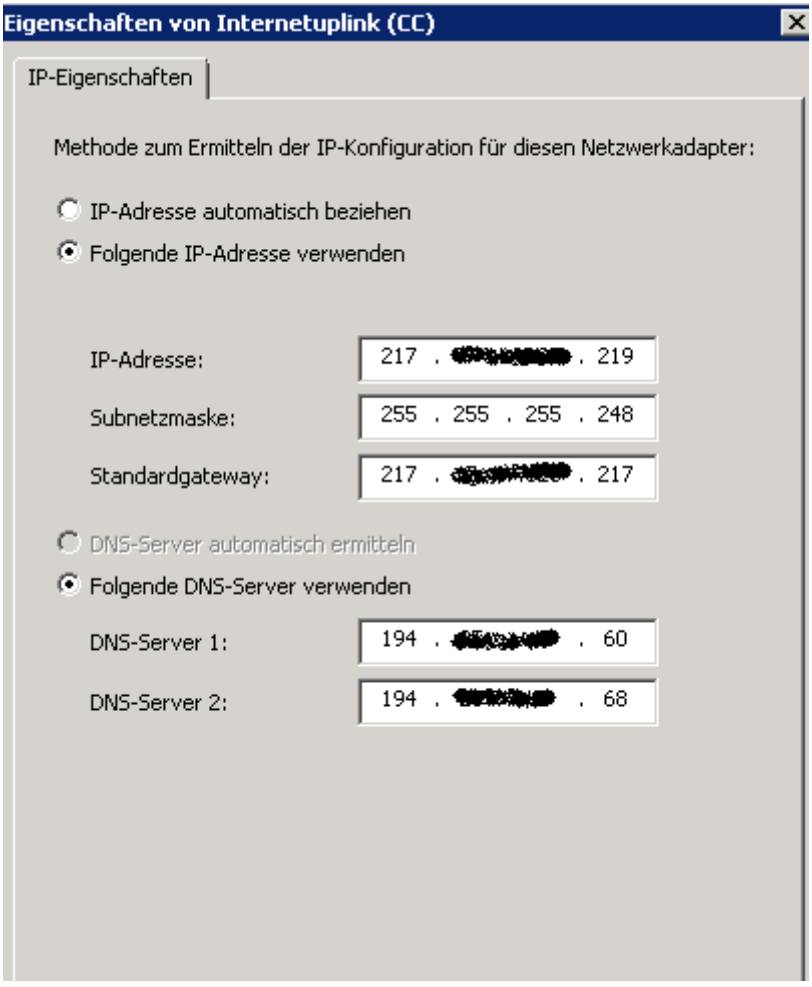
Wenn mehrere IP-Adressen an das externe Netzwerkinterface gebunden sind und auf der vorgeschalteten Firewall nur Verbindungen auf einer bestimmten IP-Adresse angenommen werden, scheint TMG nicht mehr die erste gebundene IP-Adresse am Netzwerkinterface zu verwenden, so dass man in der TMG Konfiguration die ausgehende IP-Adresse angeben muss.

In der TMG Verwaltungskonsole ist die Anzeige der gebundenen IP-Adressen wie folgt:

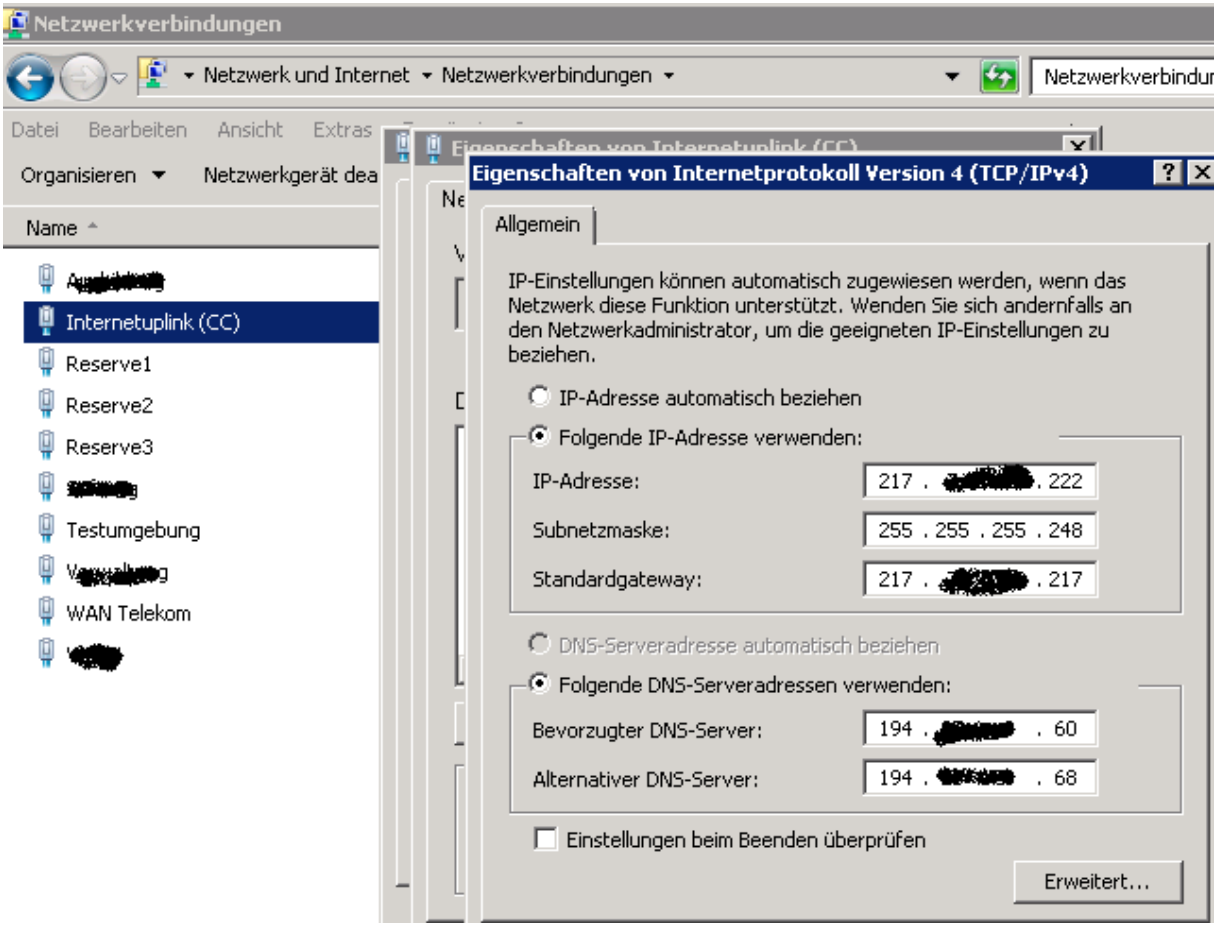


Sieht also aufsteigend aus und ich war bisher der Annahme, dass die Darstellung nur der Uebersichtlichkeit dient.

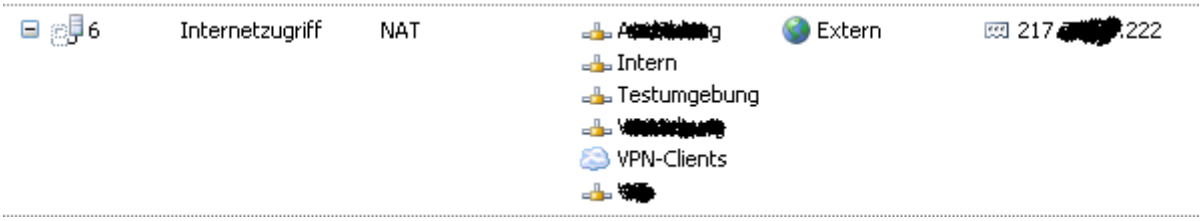
In den Karteneigenschaften in der TMG Verwaltungskonsole sieht es wie folgt aus:



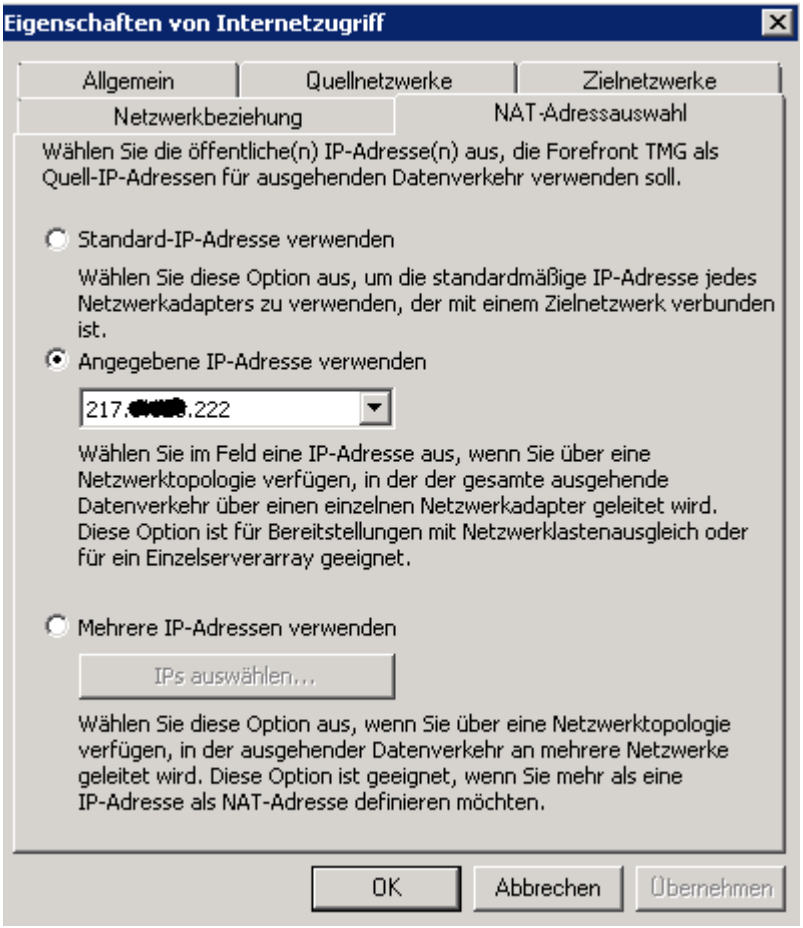
In den Netzwerkkarteneigenschaften in der Windows Umgebung ist die korrekte oeffentliche IP als erstes gebunden:



Jetzt wird fuer ausgehende Verbindungen scheinbar die falsche IP Adresse genommen, so sagt zumindest das TMG Log. Loesung ist es die neue Funktion des ENAT von TMG zu verwenden, bei einem NAT Verhaeltnis die ausgehende IP zu bestimmen.



Eintragen der ausgehenden IP-Adresse:



Danach funktionierte der ausgehende Datenverkehr problemlos, bis auf das Surfen am TMG selbst. Hier gibt es die Abhilfe, am TMG im IE den Proxy auf den TMG zu setzen, aber NIS/E-Mail und Malware Updates ueber die TMG-Konsole lassen sich auch nicht laden, da hier der Proxy scheinbar nicht verwendet wird und das TMG Netzwerkobjekt LOCALHOST kann man nicht in die NAT Netzwerkregel fuer ENAT setzen. Loesung war hier mit Proxycfg den Proxy zu setzen.

Die Frage die sich mir stellt: Wie loest man das Problem wenn als Netzwerkverhaeltnis ROUTE verwendet wird. Funktioniert es da dann wieder wie bei ISA 2006?

Mangels eines vergleichbaren und zugreifbaren Kundensystems konnte ich noch nicht abschliessend evaluieren, ob das Problem kundenspezifisch oder ein Bug/Feature von TMG ist. Im April werde ich eine aehnliche Konstellation bei einem anderen Kunden implementieren und dann auf meinem Blog berichten.