Forefront TMG FTP / FTPS / SFTP

Forefront TMG bringt wie sein Vorgaenger ISA Server 200x einen FTP-Filter mit, mit dessen Hilfe FTP-Verbindungen sicher etabliert werden koennen. Der FTP-Filter ist u. a. auch fuer die Aushandlung der FTP Data und FTP Control Channel Kommunikation zustaendig. Problematisch wird die Kommunikation, wenn zum Beispiel FTPS verwendet werden soll

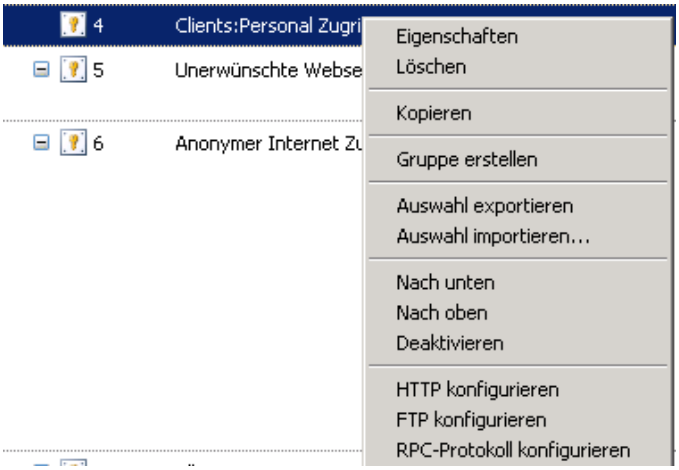
Grundlagen zum FTP Protokoll und der Komplexitaet die Kommunikation ueber eine Firewall zu ermoeglichen:
http://en.wikipedia.org/wiki/File_Transfer_Protocol

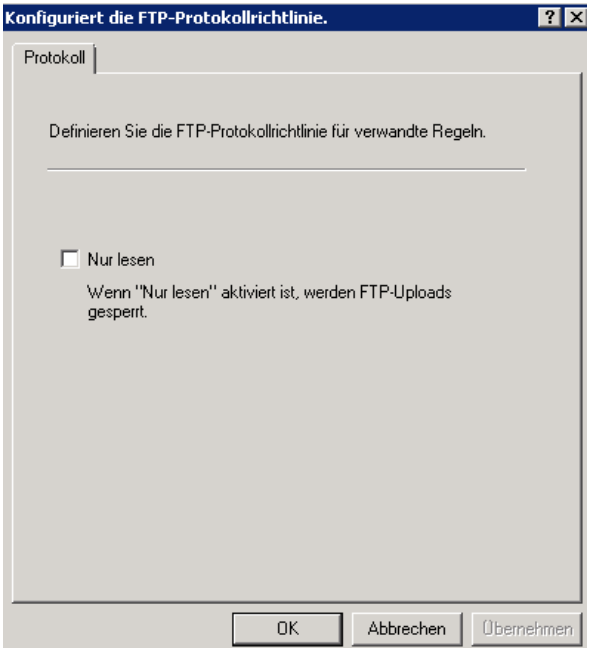
Forefront TMG und FTP:
http://www.isaserver.org/tutorials/Microsoft-Forefront-TMG-FTP-and-FTP-Server-publishing.html

Wichtig: Man muss immer genau auf die FTP Begrifflichkeiten achten:
FTPS ist etwas anderes als SFTP, und auch bei FTPS gibt es verschiedene Begrifflichkeiten, welche u. a. hier erlaeutert werden:
http://en.wikipedia.org/wiki/File_Transfer_Protocol

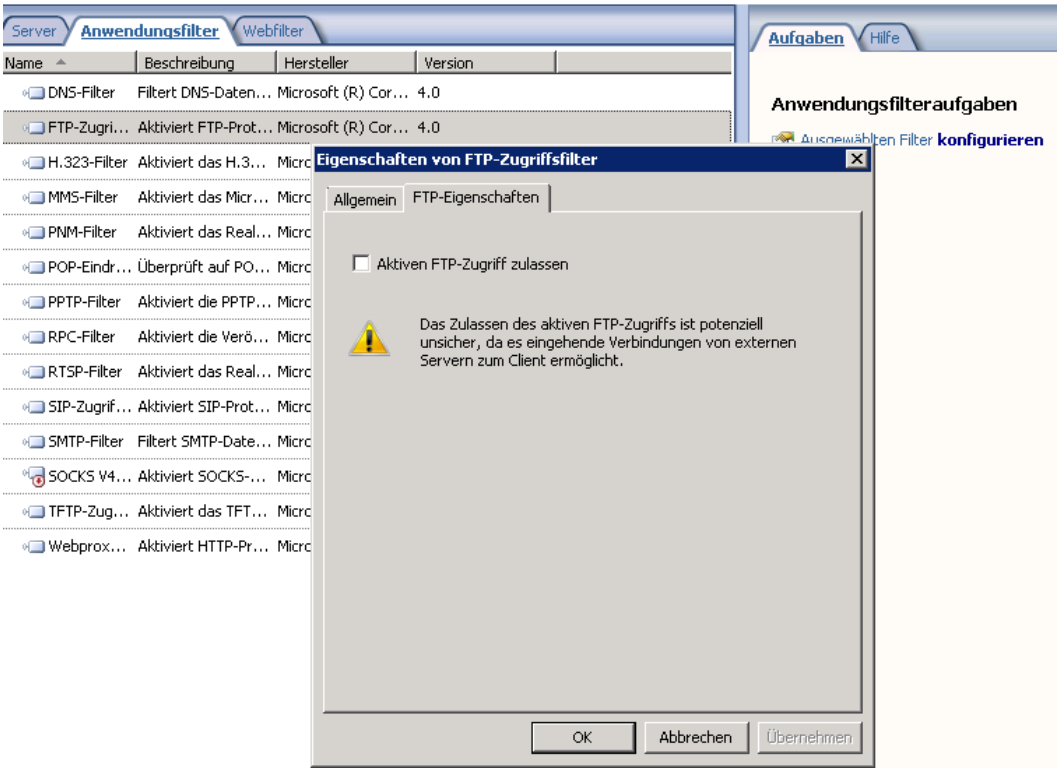
Besonderheiten bei Forefront TMG (ISA):

Standardmaessig laesst TMG nur den FTP Download zu:





Die naechste Huerde ist, dass beginnend mit Forefront TMG aus Sicherheitsgruenden standardmaessig kein Active FTP mehr zulaessig ist:



Forefront TMG mit nur einer Netzwerkkarte (Single NIC Mode) hat auch die Einschraenkung, dass FTP im „nur Lesen“ Modus funktioniert:
http://technet.microsoft.com/en-us/library/cc302586.aspx

Hat man diese Huerden umschifft, beginnt es problematisch zu werden, wenn ein interner Client eine FTPS Verbindung mit einem FTP Server im Internet etablieren soll, weil der FTP-Filter von Forefront TMG nicht in der Lage ist, FTPS Verbindungen dynamisch in der State Table der Packet Filtering Engine zu halten.
Bei einem FTP Client sieht der Verbindungsversuch per FTPS dann so aus:

Entweder bleibt die Verbindung beim TLS negotiate haengen oder …

```
Status:     Verbinde mit 193.159.239.203:21...
Status:     Verbindung hergestellt, warte auf Willkommensnachricht...
Antwort:    220 (vsFTPd 2.3.2)
Befehl:     AUTH TLS
Antwort:    234 Proceed with negotiation.
Status:     Initialisiere TLS...
```

beim LIST Befehl.

Im Internet gibt es dann diverse Anleitungen, wie man sich eigene Protokolldefinitionen bauen kann, welche die High Ports erlauben, bzw. FTP Protokolle ohne FTP Filter erstellen, aber nicht imemr funktioniert das mit jedem FTP Server, was in der Dynamic des FTP-Protokolls und deren Verbindungen begruendet ist.

Eine Loesung ist es, eine Firewallregel zu erstellen, welche den gesamten Datenverkehr mit Ausnahme des standardmaessigen FTP-Protokolls erlaubt, denn an dem Standard FTP-Protokoll ist der FTP-Filter von Forefront TMG gebunden, welcher nicht in der Lage ist, FTPS Verbindungen zu steuern. Um die moeglichen Gefahren einer „Allow All“ Rule zu minimieren, sollte man in der Firewallregel festlegen, von welchem Client zu welchem FTP Server eine Verbindung hergestellt werden kann.