Anleitung zur Konfiguration von Anti-Virus

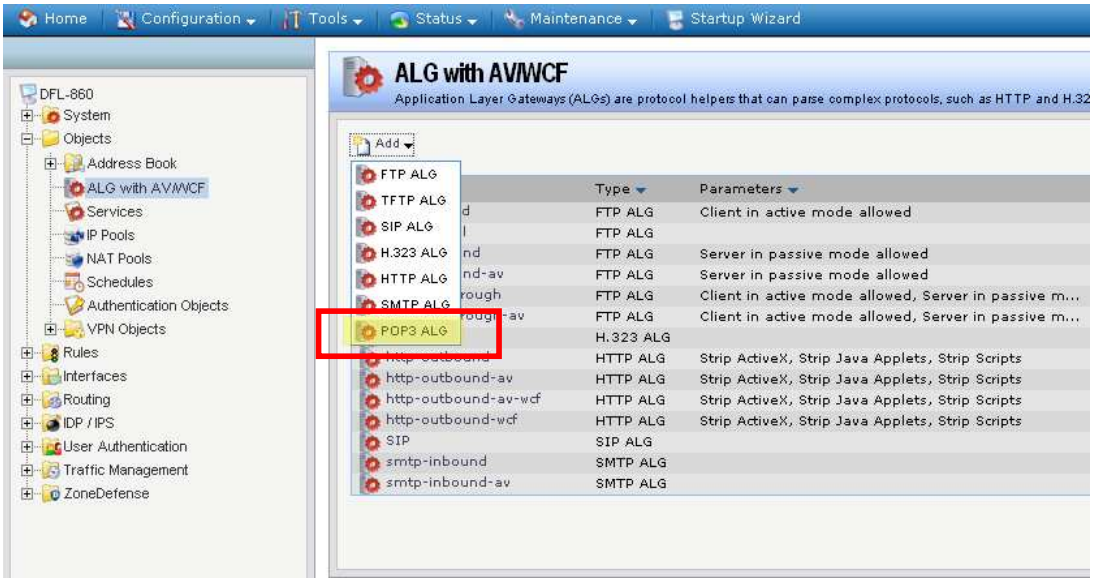
(am Beispiel von POP3)

Konfigurationsschritte:

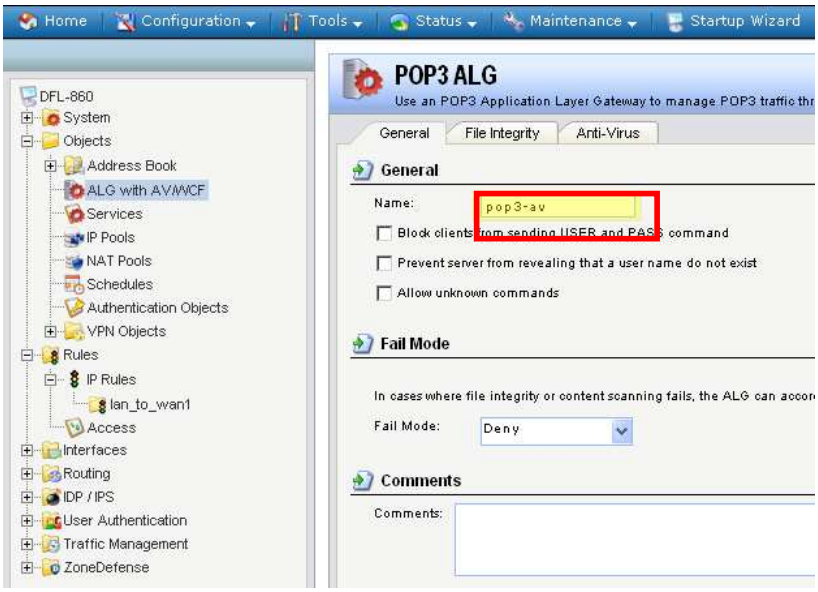
- Anlegen eines ALG Objekts
- Anlegen eines Service Objekts
- Einrichten von IP-Rules für den entsprechenden Traffic (hier: POP3)

1. Anlegen eines ALG Objekts:

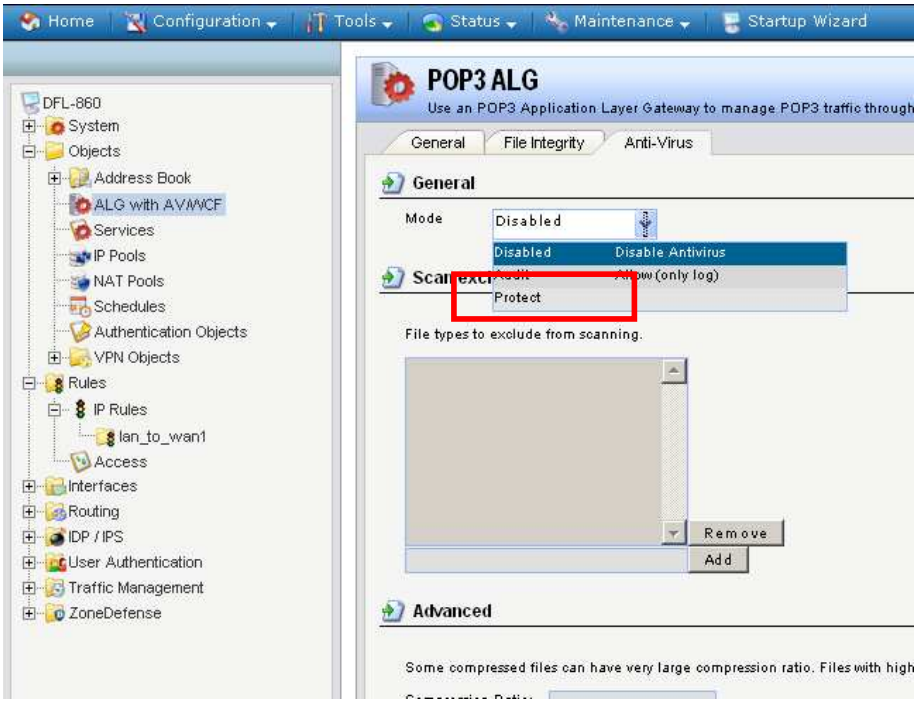
Öffnen Sie den Menüpunkt:
Objects -> ALG with AV/WCF
Fügen Sie hier über „Add“ ein entsprechende ALG Objekt (hier: eine POP3 ALG) hinzu.



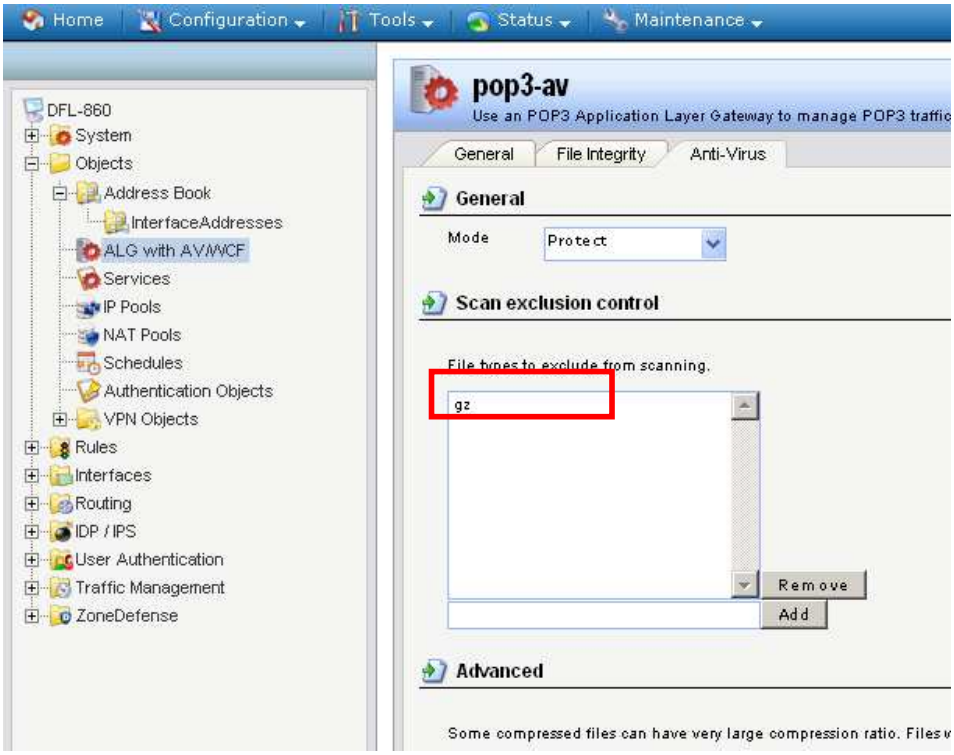
Konfigurieren Sie nun die POP3 ALG:
Vergeben Sie der ALG einen Namen:



Und wechseln Sie anschließend auf den Reiter Antivirus.
Wählen Sie bei Mode „Protect“ aus um Antivir zu aktivieren.



Unter „Scan exclusion control“ können Sie Dateien hinzufügen die nicht von der Antivirus Engine gescannt werden sollen. Hier z.B. *.gz, somit werden Dateien mit der Endung *.gz nicht gescannt.

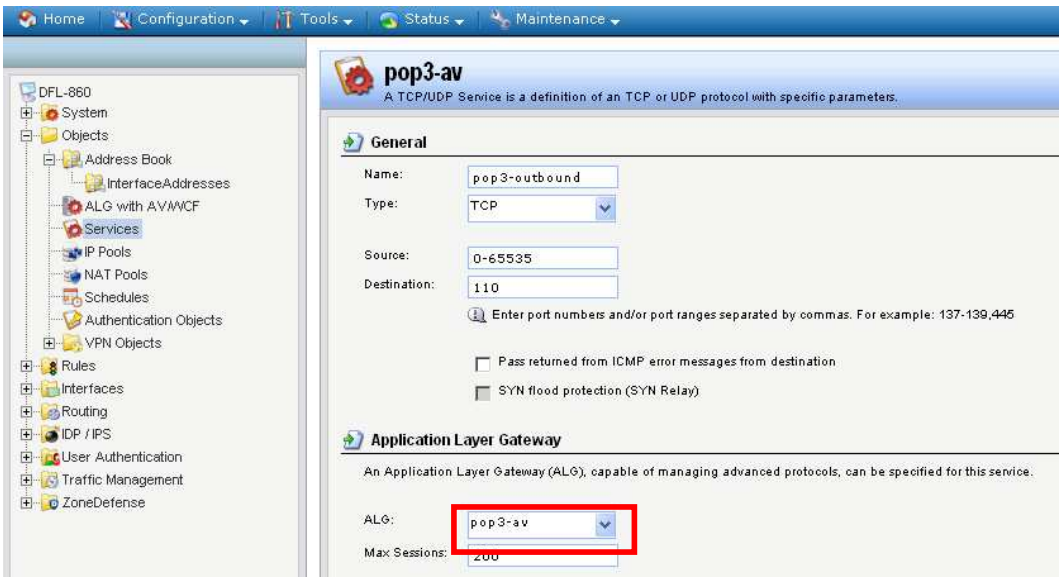


Bestätigen Sie die Einstellungen mit OK.

2. Anlegen eines Service Objekts:

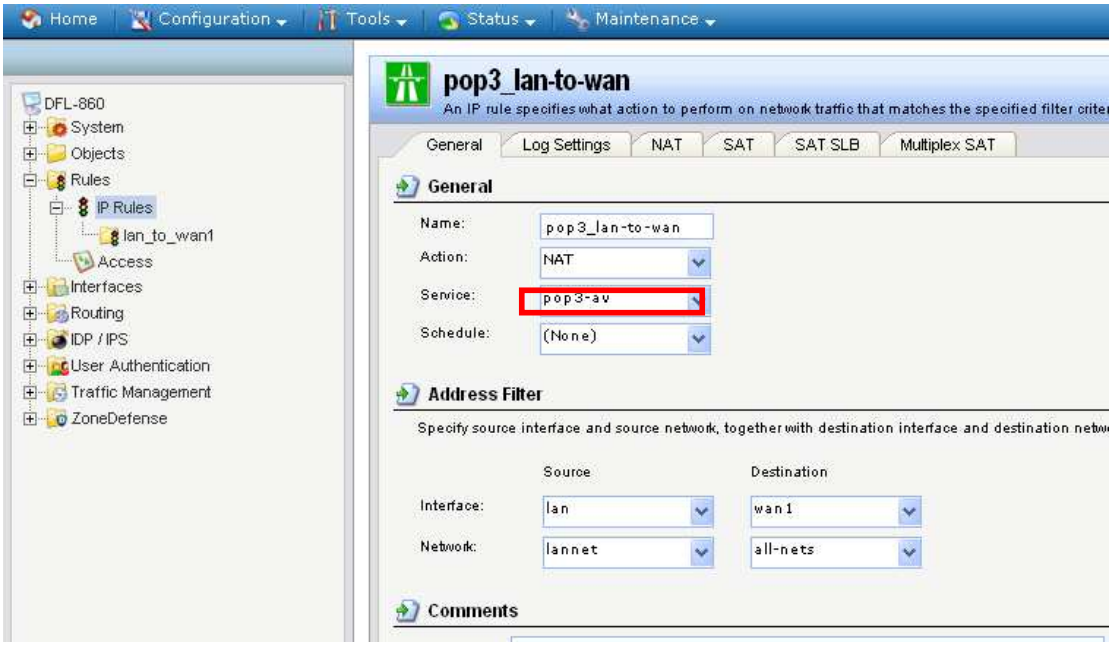
Wechseln Sie in den Menüpunkt:
Objects -> Services.
Fügen Sie über „Add“ ein neues TCP/UDP Service Objekt hinzu.

Konfiguration des Service Objekts:
Neben der Namensvergabe und den Porteinstellungen sollte unter „ALG“ das vorher angelegte ALG Objekt (hier: POP3) ausgewählt werden.

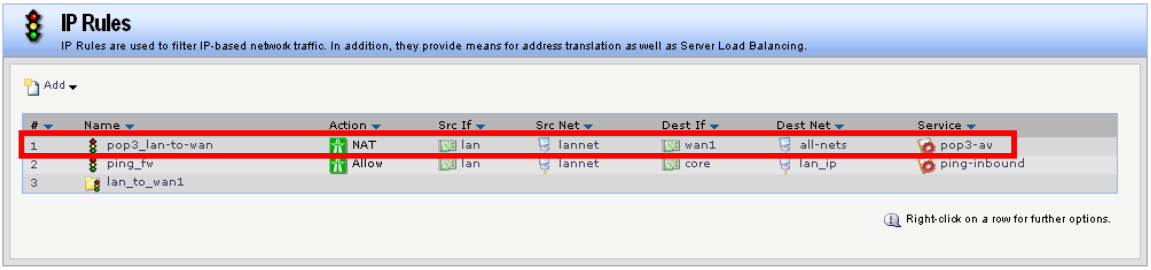


Bestätigen Sie die Einstellungen mit OK.

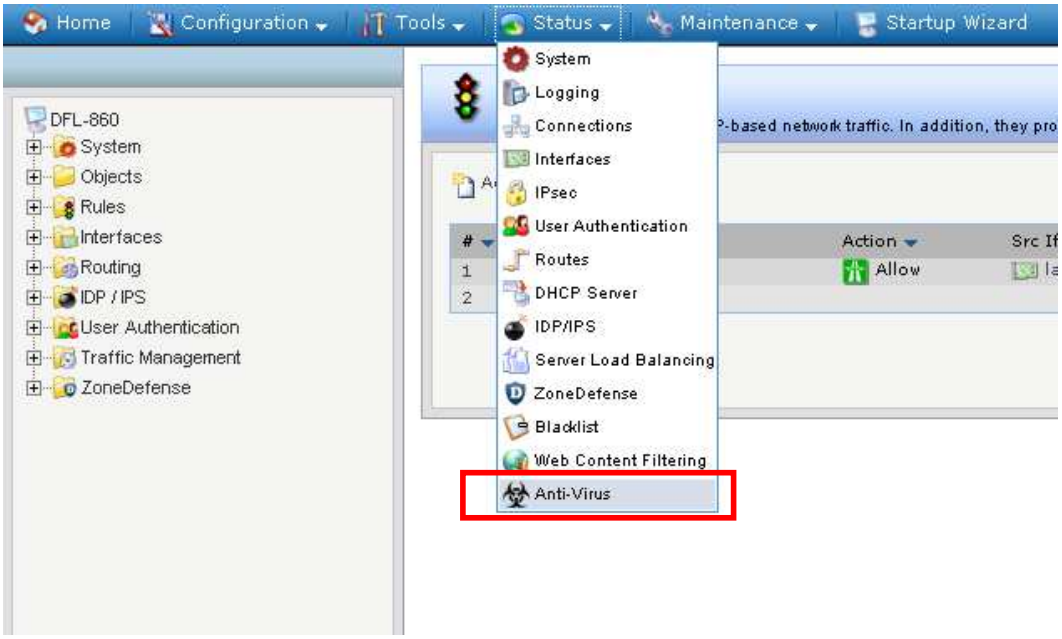
3. Einrichtung von IP-Rules
Wechseln Sie nun in den Menüpunkt:
Rules -> IP Rules.
Fügen Sie über „Add“ IP-Rule eine neue IP Rule hinzu.
Diese sollte wie folgend konfiguriert werden.
Beachten Sie bitte, dass als Service das oben angelegte Service Objekt (hier: pop3-av) welches bereits mit dem entsprechenden ALG verknüpft wurde.



Die Regel sollte wie unten aufgeführt aussehen:



Sie können den Status von Antivir über den Menüpunkt
Status -> Anti-Virus
überprüfen:



Der LOG Eintrag zu einem in einer Email erkannten Virus: