

Microsoft Forefront "Stirling" - Forefront Security fuer Exchange - Ueberblick und Konfiguration

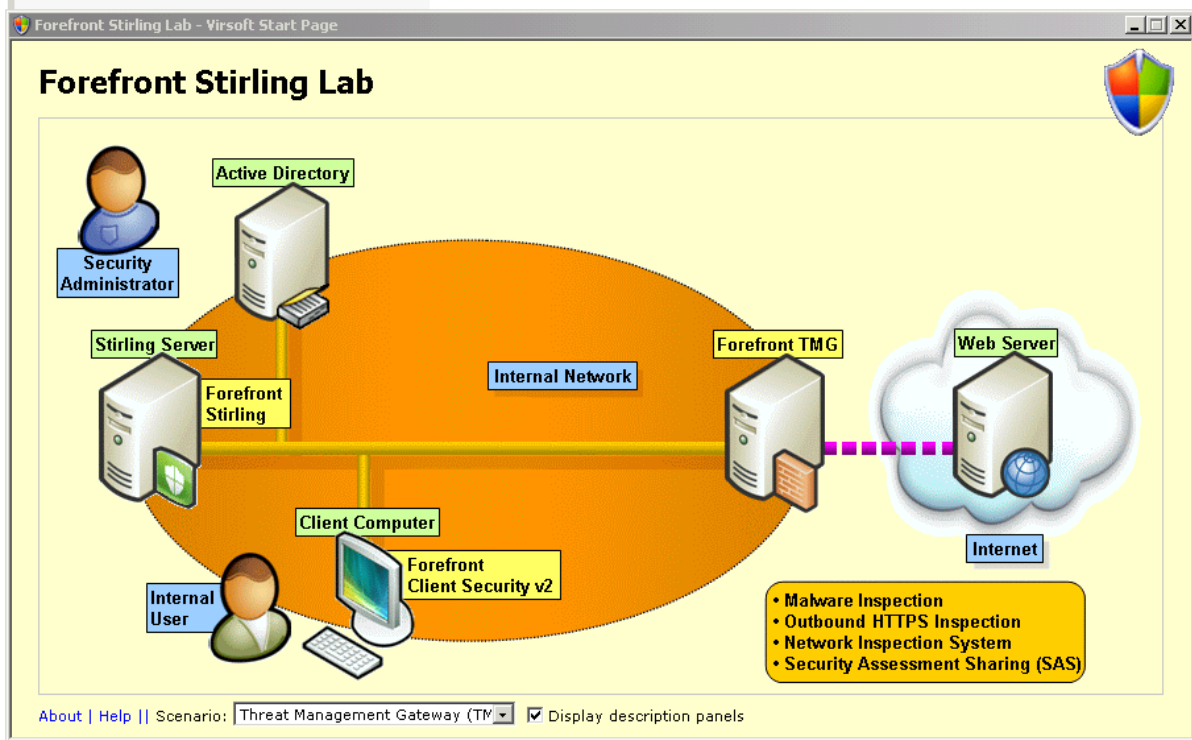
In diesem Artikel zeige ich kurz den Funktionsumfang von Forefront Security fuer Exchange und die Integration in Exchange Server 2007.

Erster Artikel Forefront Stirling im Ueberblick:

<http://www.it-training-grote.de/download/stirling-b2-1.pdf>

ich nutze wieder die herunterladbare VHD-Testumgebung von Microsoft.

Alles im Ueberblick












Was enthalten die Downloads

- . Denver
 - Domain Controller
 - Roles: DHCP server, DNS server, NPS server
 - WSUS 3.0 SP1
- . Stirling
 - System Center Operations Manager (SCOM) 2007 R2 (build 6407 - beta 1)
 - SQL Server 2005 SP3
 - Forefront Stirling (build 1677 - beta 2)
 - Outlook 2007
- . Venice
 - Forefront Client Security (build 1677 - beta 2)
 - NAP agent
 - Outlook 2007
- . Madrid
 - Exchange Server 2007 SP1 (Mailbox/Client Access/Hub Transport roles)
 - Forefront for Exchange (build 243 - beta 2)

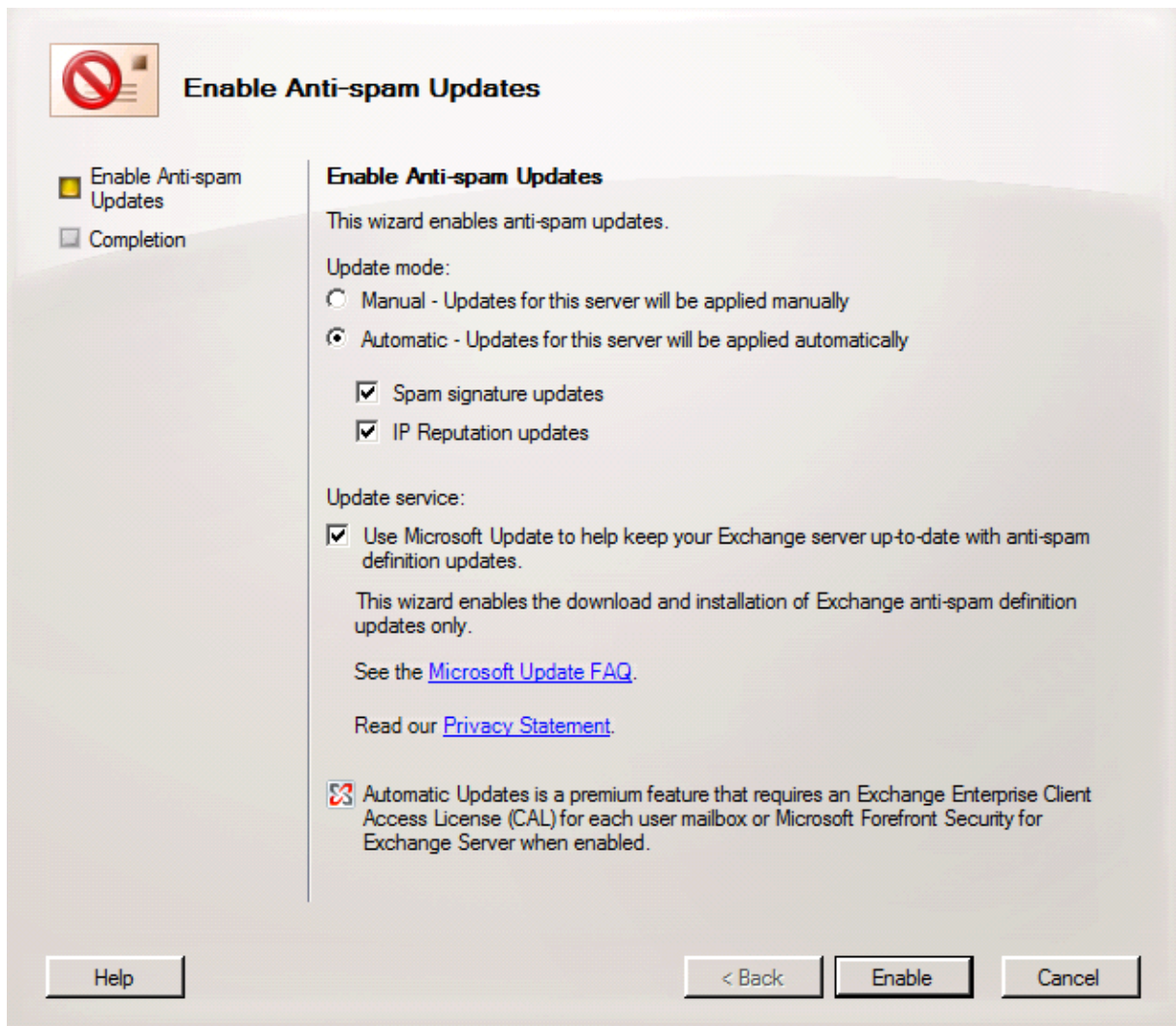
- . Sydney
 - Windows SharePoint Services (WSS) 3.0 SP1
 - Forefront for SharePoint (build 243 - beta 2)
- . Toronto
 - Exchange Server 2007 SP1 (Edge Transport role)
 - Threat Management Gateway (build 7264 - beta 2)

Exchange

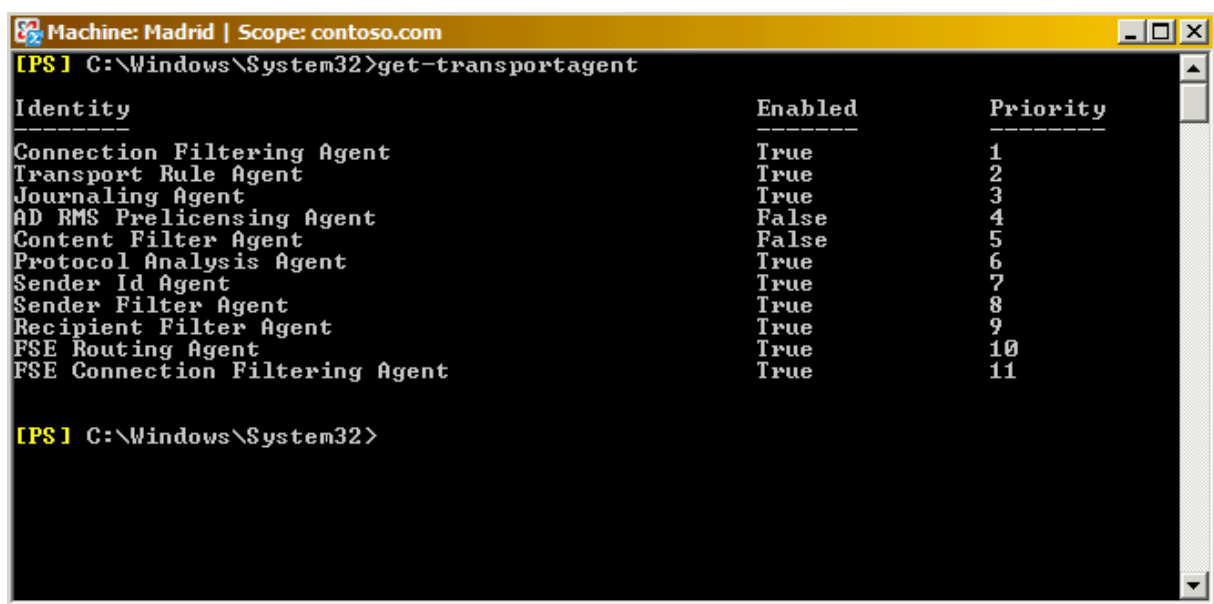
Antispam Funktionen auf dem HTS Server

Hub Transport		9 objects
Remote Domains	Accepted Domains	E-mail Address Policies
Journaling	Send Connectors	Edge Subscriptions
		Global Settings
		Anti-spam
Feature ^	Status	
 Content Filtering	Enabled	
 IP Allow List	Enabled	
 IP Allow List Providers	Enabled	
 IP Block List	Enabled	
 IP Block List Providers	Enabled	
 Recipient Filtering	Enabled	
 Sender Filtering	Enabled	
 Sender ID	Enabled	
 Sender Reputation	Enabled	

Antispam Updates



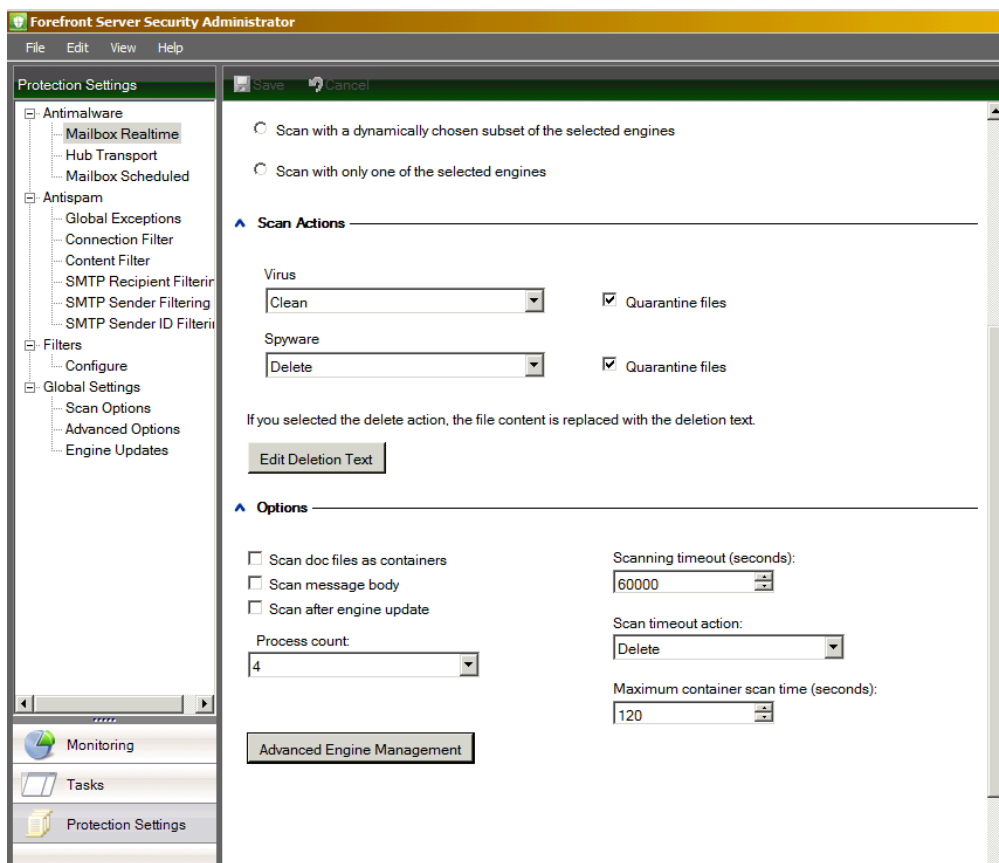
Transport Agents auf dem Exchange Server. Man sieht hier auch die installierten Transport Agents von FSE = Forefront Security fuer Exchange



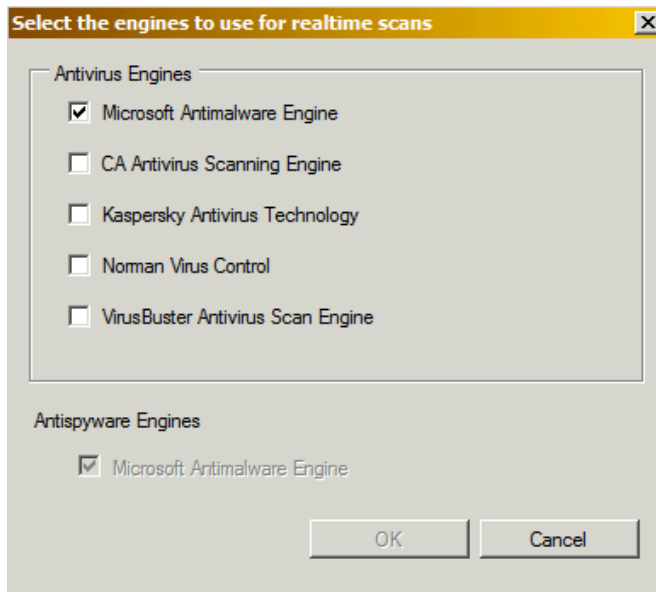
FSE Versionsnummer



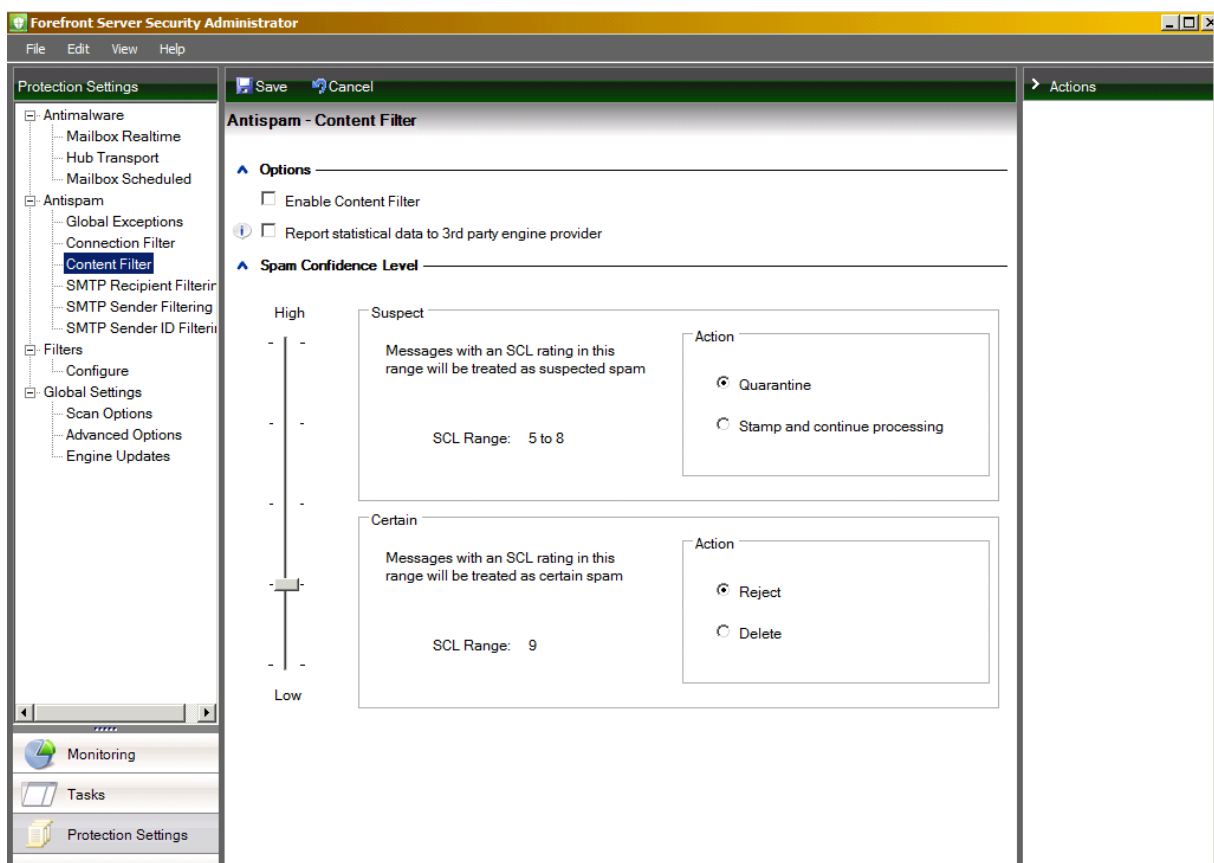
In den Protection Settings koennen grundlegende Konfigurationseinstellungen bzgl. Antimalware, Antispam und globale Einstellungen vorgenommen werden.



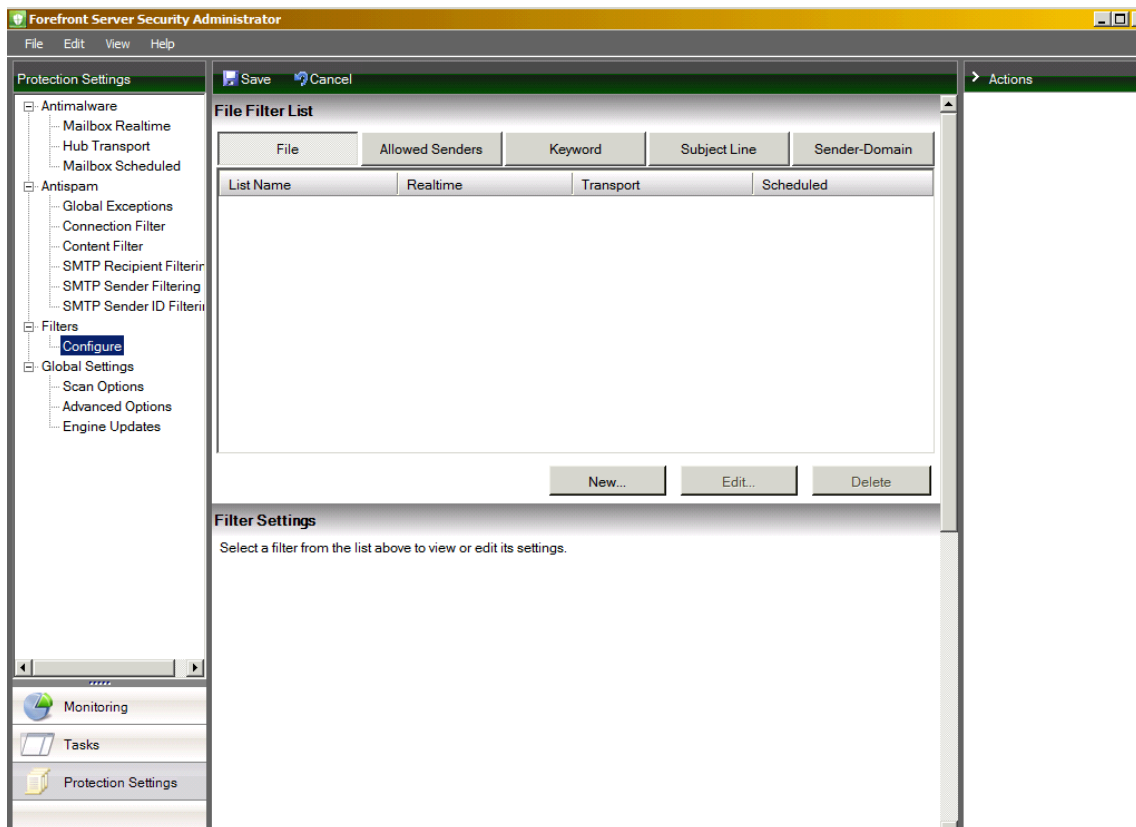
Es koennen verschiedene AntiVirus Engines ausgewaehlt werden. Als Antimalware Engine steht nur die Microsoft Antimalware Engine zur Verfuegung.



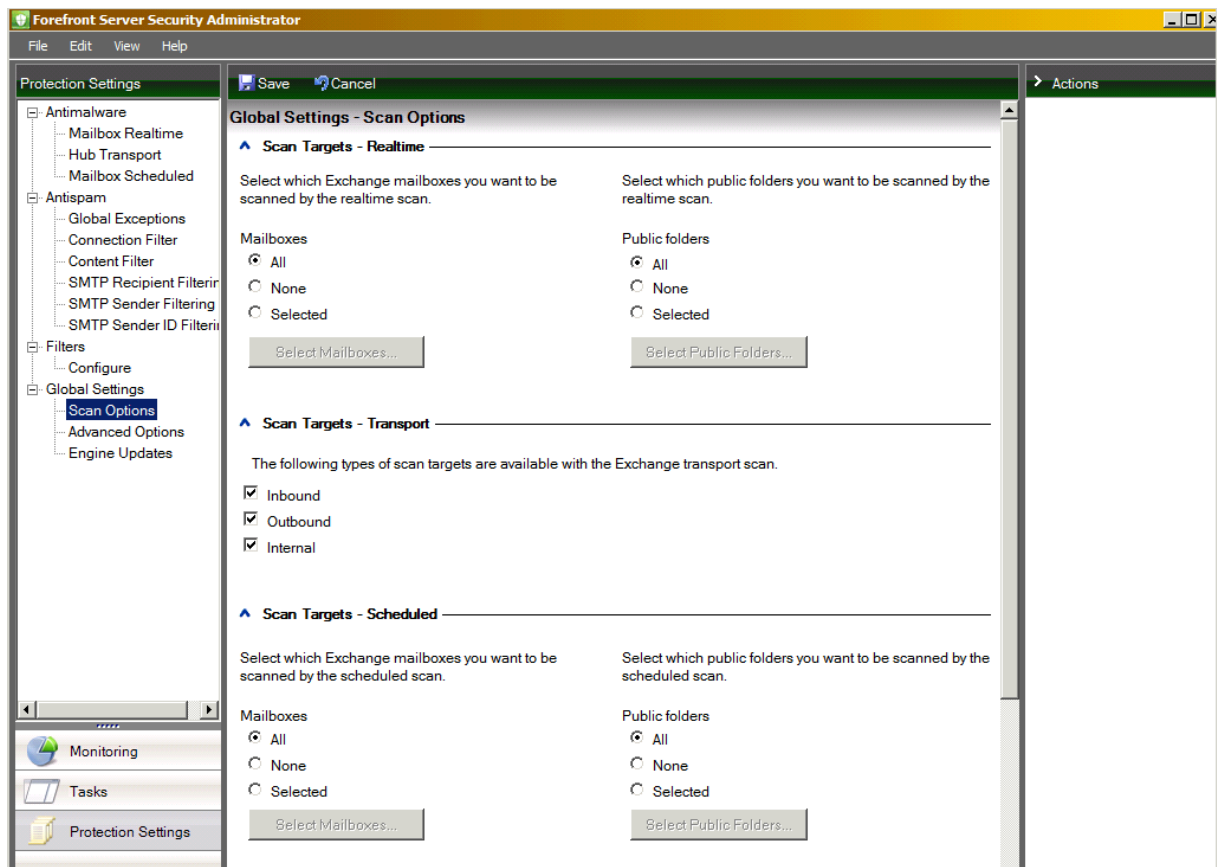
Content Filter Einstellungen fuer SCL Level



Benutzerdefinierte Filterlisten



Globale Scan-Einstellungen



Erweiterte Optionen

The screenshot displays the 'Global Settings - Advanced Options' window in the Forefront Server Security Administrator. The left-hand navigation pane shows a tree view with 'Advanced Options' selected under 'Global Settings'. The main content area is divided into several sections:

- Paths and Actions:** Includes a dropdown for 'Engine error action' (set to 'Delete'), a checkbox for 'Scan all files', a text field for 'Extension type for all deleted attachments' (set to 'txt'), and checkboxes for 'Enable inbound file filtering' and 'Enable outbound file filtering'. It also features text boxes for 'IP addresses used to identify external addresses' and 'Domain names used for identifying internal addresses', each with an 'Edit List...' button.
- Deletion Criteria:** Contains checkboxes for 'Delete corrupted compressed files', 'Delete corrupted UUEncoded files', 'Delete partial SMTP messages', and 'Delete encrypted compressed files'.
- Threshold Levels:** This section is currently collapsed.

Additional checkboxes include 'Use external "Domains.dat" file instead of value in InternalAddress parameter', 'Use reverse DNS lookup when determining whether or not a message is "inbound"', 'Quarantine corrupted compressed files', and 'Quarantine on timeout'.

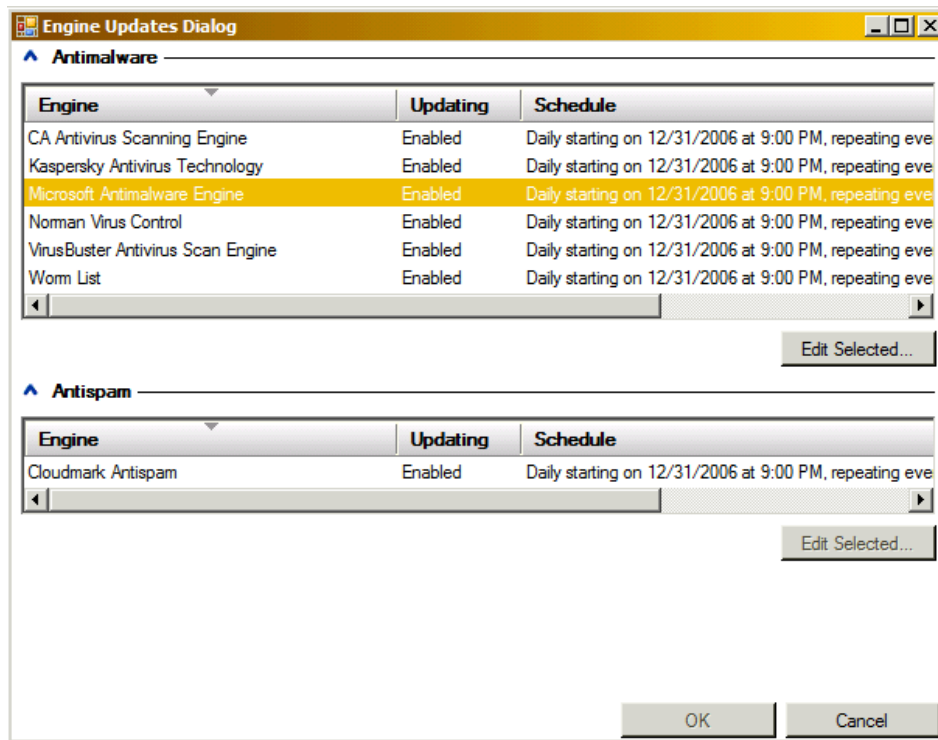
Antivirus Scan Engine Updates

The screenshot displays the 'Global Settings - Engine Updates' window in the Forefront Server Security Administrator. The left-hand navigation pane shows 'Engine Updates' selected under 'Global Settings'. The main content area includes:

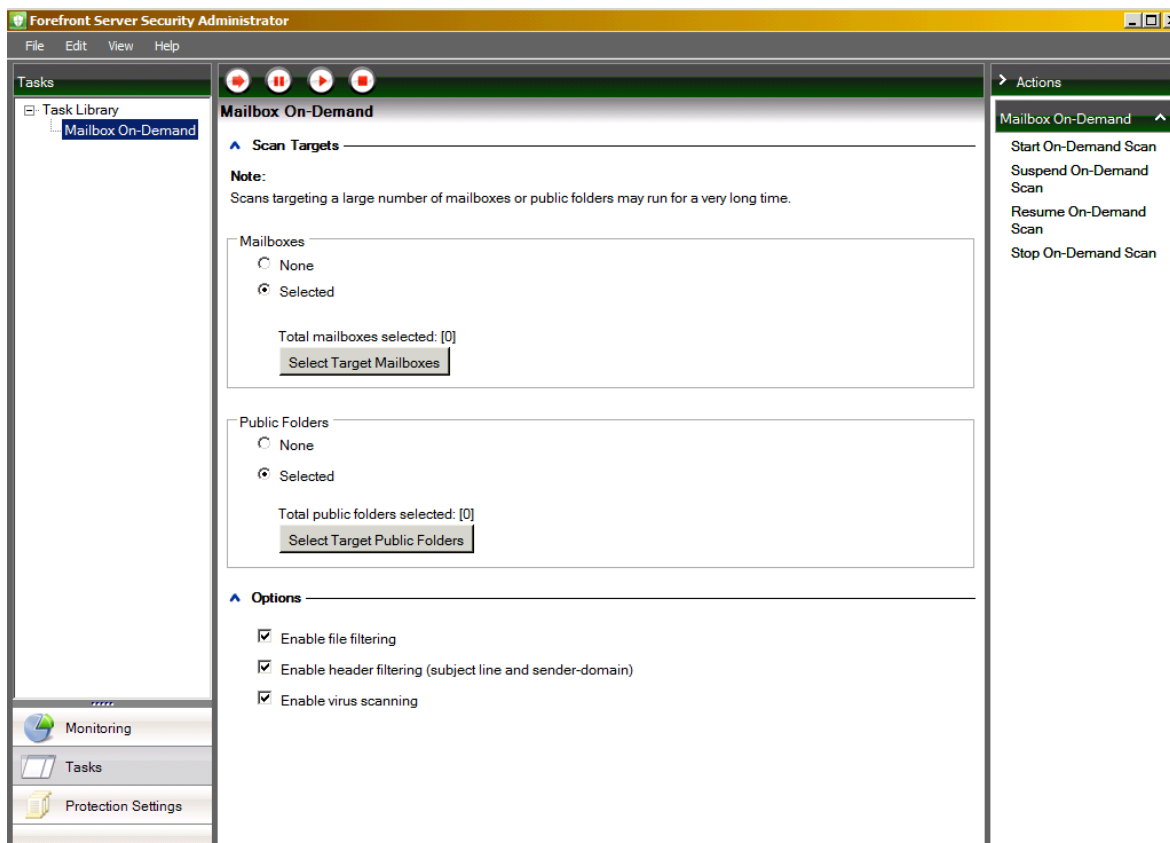
- A heading: 'Specify whether to check for updates and how often'.
- Antimalware Engine Updates:** States 'Intelligent Engine Management is enabled...' and provides a button for 'Update Engines Now'. It also shows 'Antimalware Engines: Check for updates every hour.' with an 'Advanced Engine Management' button.
- Antispam Engines:** Shows 'Antispam Engines: Check for updates every hour.'
- UNC Authentication:** Includes a checkbox to 'Enable UNC authentication using these credentials:' with a 'User:' text field and an 'Edit UNC Credentials...' button.
- Proxy Server:** Includes a checkbox to 'Enable proxy server using this location and these credentials:' with fields for 'Proxy server:', 'Port:' (set to 80), and 'User:', along with an 'Edit Proxy Server Credentials...' button.
- Additional Options:** Contains checkboxes for 'Update enabled engines on server startup' and 'Enable as an update redistribution server'.

The right-hand 'Actions' pane is active, showing 'Engine Updates' with sub-options: 'Update All Enabled Engines Now' and 'View Engine Summary'.

Update Einstellungen fuer alle Engines



Tasks



E-Mail Benachrichtigungen fuer verschiedene Ereignisse

The screenshot shows the 'Configure Notifications' window in the Forefront Server Security Administrator. The interface is divided into several sections:

- Left Navigation:** A tree view showing 'Monitoring' (Overview, Incidents, Quarantine, Dashboard) and 'Configuration' (Notifications, Incident Options, Quarantine Options).
- Top Bar:** 'Save' and 'Cancel' buttons.
- Incident Notifications Table:**

Notification	Notification Enabled For
File error	None enabled
File filter matched	None enabled
Keyword filter matched	None enabled
Sender-domain filter matched	None enabled
Spyware found	None enabled
Subject line filter matched	None enabled
Virus found	None enabled
Worm found	None enabled
Scan error	None enabled
- Event Notifications Table:**

Notification	Noti
Scan startup	None
License warning	None
License expired	None
Database size warning	None
Engine updated	None
Engine update failed	None
Engine update not found	None
Critical error	None
Health change to green	None
Health change to red	None
Health change to yellow	None
- File filter matched notification configuration:**
 - Enabled:**
 - To:**
 - Cc:**
 - Bcc:**
 - Subject:** %Product% detected a file filter match
 - Preview:**

```

%Product% has detected a file filter match.
Filter name: "%Filter%"
File name: "%File%"
State: "%State%"
Subject Line: "%Message%"
Sender: "%ISName%";%ESName%"
Scan job: "%ScanJob%"
Location: "%Company%/%Site%/%Server% (%Folder%)"
                    
```
- Right Panel:** 'Actions' menu with 'Edit selected notification' option.
- Bottom Bar:** 'Monitoring', 'Tasks', and 'Protection Settings' buttons.

Das war es dann auch schon im grossen und ganzen.