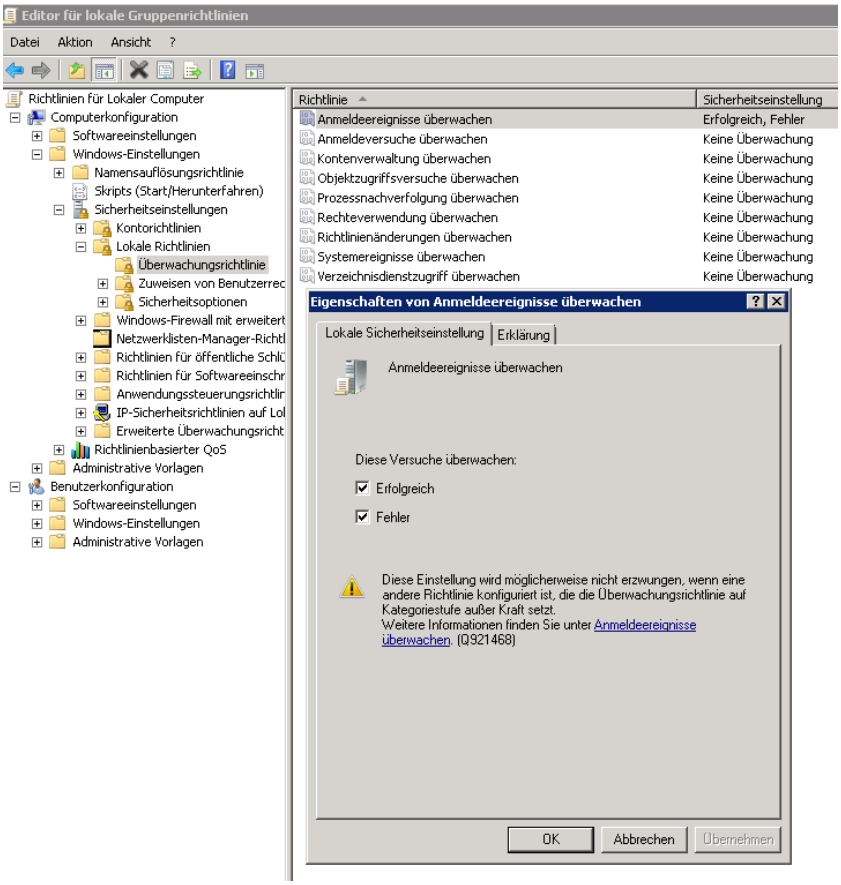
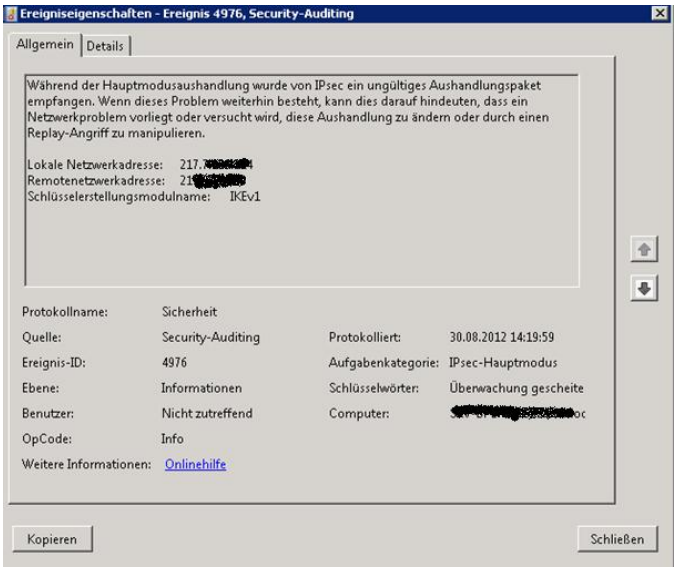
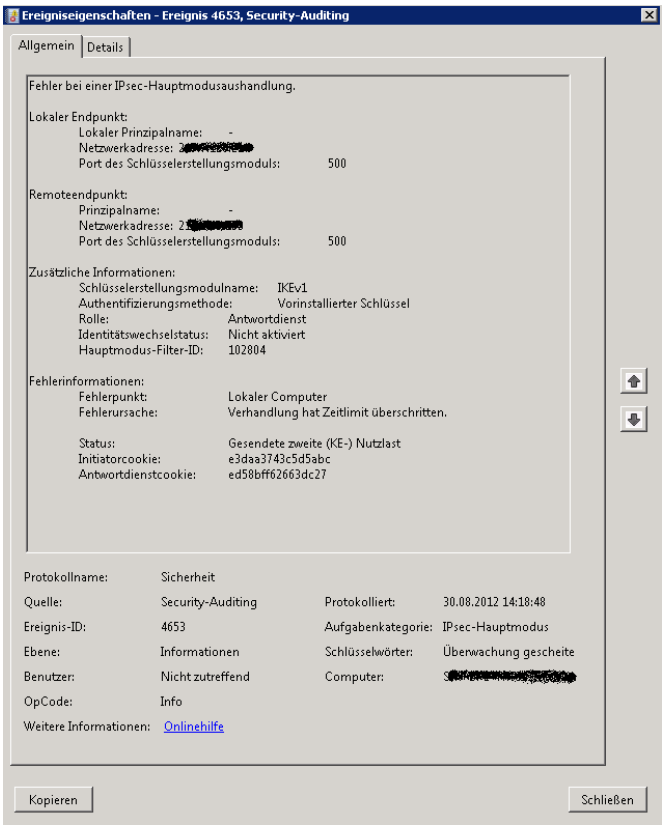
Forefront TMG IPSEC Debugging

Windows Anmeldeereignisse ueberwachen aktivieren

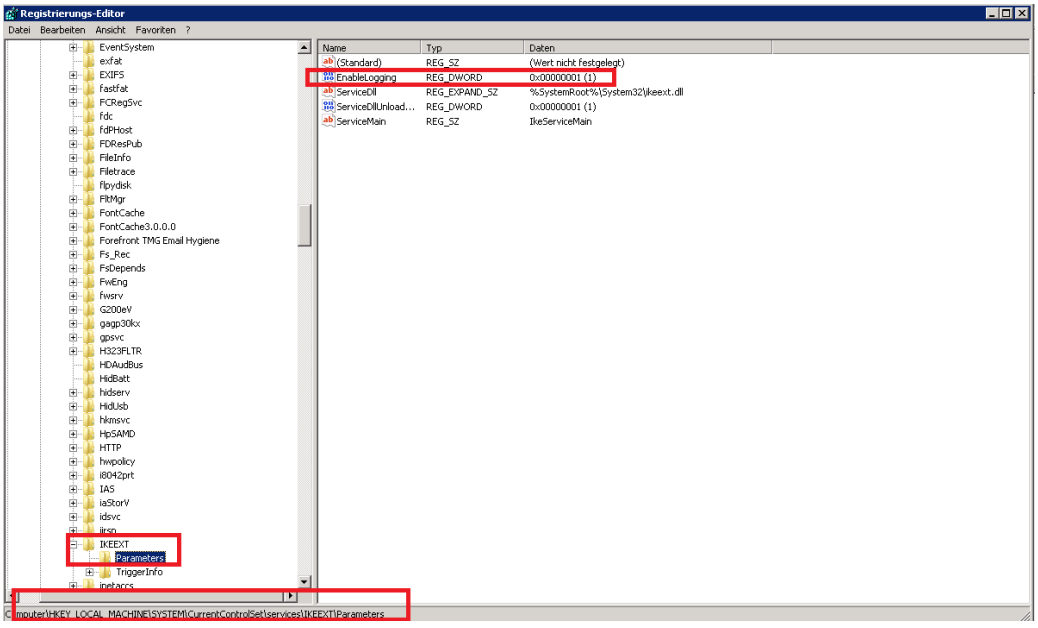


Danach werden im Security Log zusaetzliche Informationen angezeigt





IKE Logging aktivieren



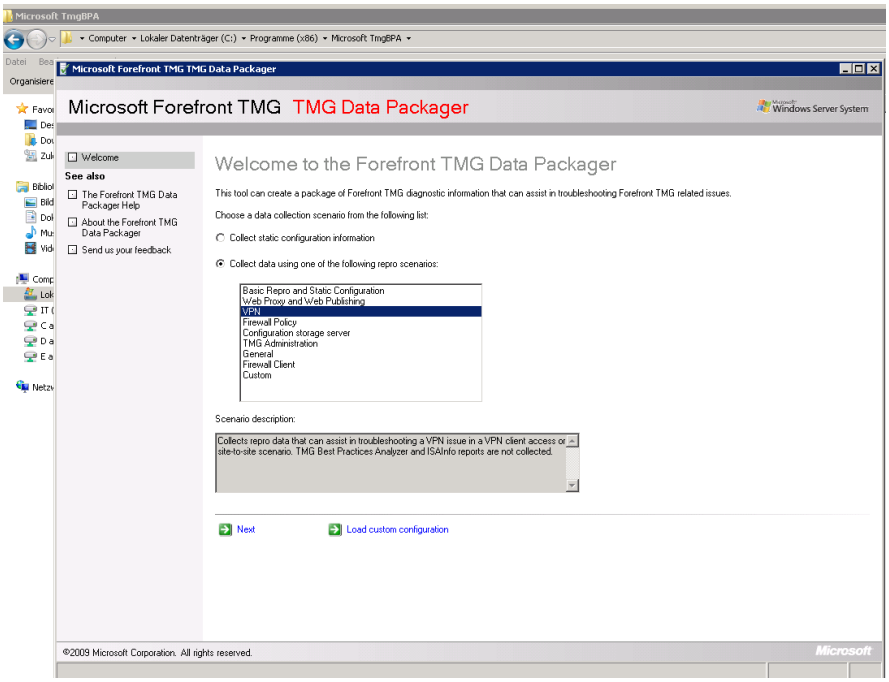
Dienst IKEEXT (IKE- und AuthIP IPsec-Schlüsselerstellungsmodule) stoppen und starten (wichtig nicht neustarten).
Achtung: Nach Beendigung des Debugging nicht vergessen das IKE Logging wieder zu deaktivieren

Das erzeugt die Datei IKEEXT.DLL. Nutzbar **NUR** fuer Windows Server 2008 weil nur in dieser Version die WFP.TMF Datei fuer die lesbare Aufbereitung des binaeren .ETL File enthalten ist.

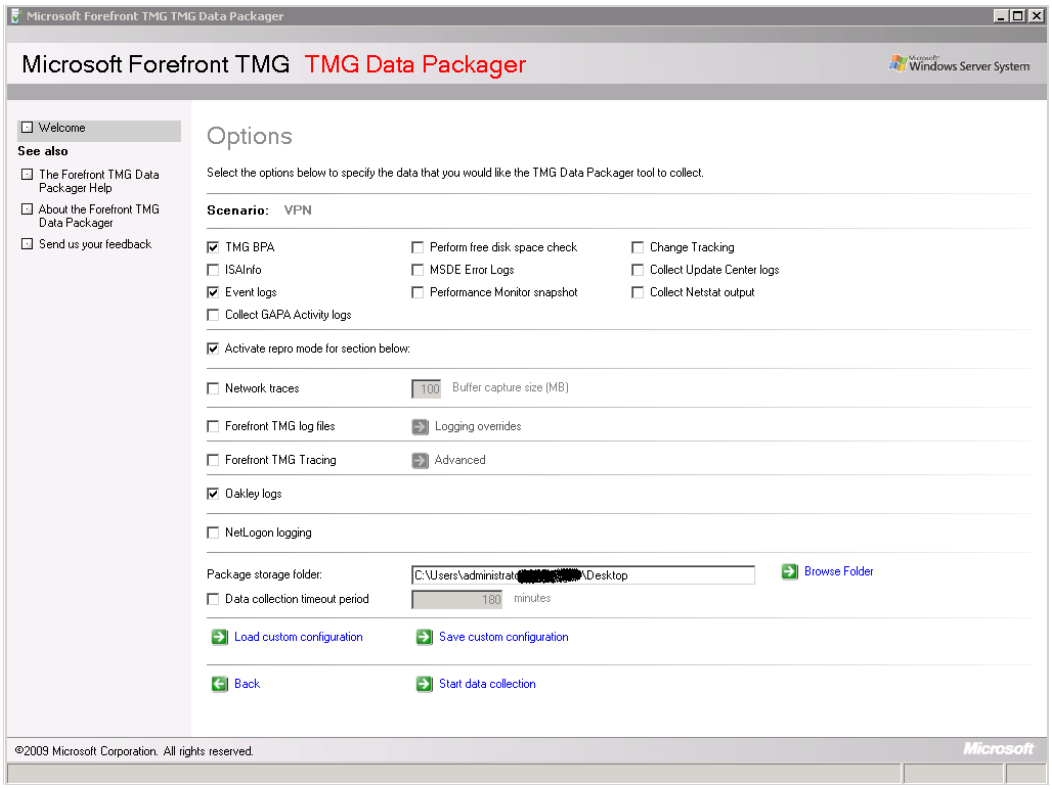
TMG BPA installieren

Der TMG BPA enthaelt im Installationsverzeichnis den TMG Data Packager welcher im VPN Repro Modus Logdateien erzeugen kann. Der TMG Data Packager kann fuer einen bestimmten Zeitraum aktiviert werden um VPN Verbindungsversuche aufzuzeichnen. Das Setzen des IKE Logging wie weiter oben beschrieben ist nicht notwendig.

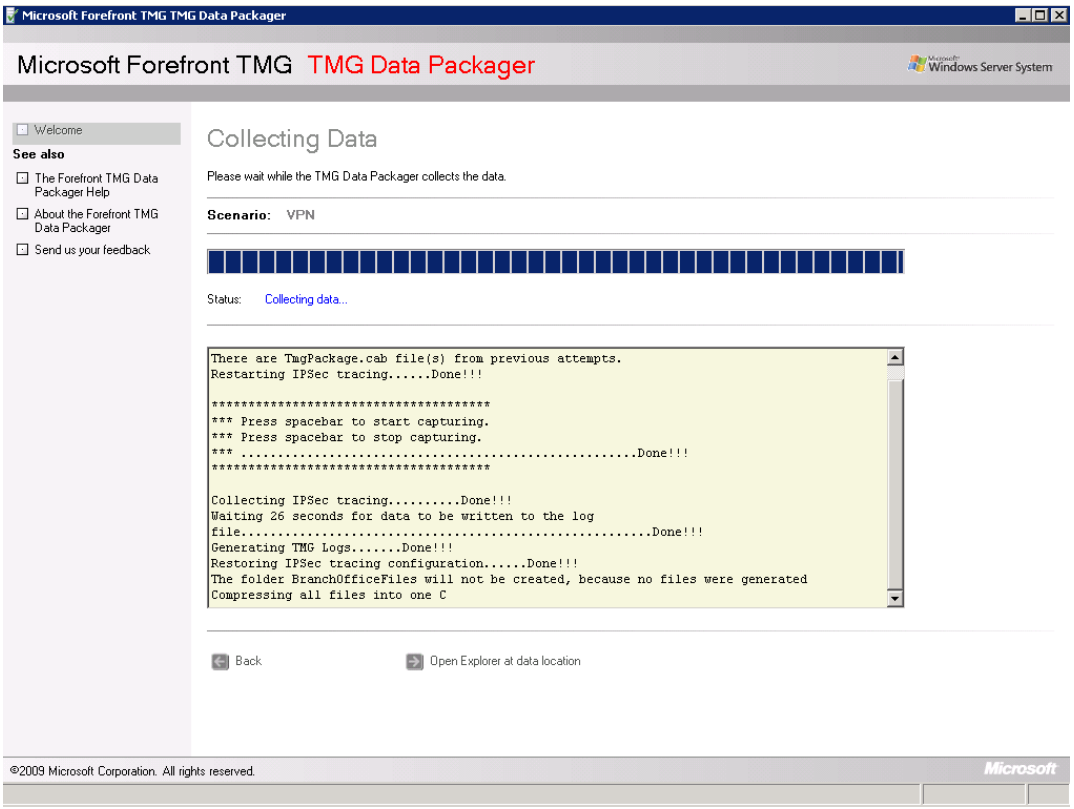
TMG Data Packager ausfuehren. Repro Mode VPN Szenario auswaehlen. VPN Verbindungsversuche erneut durchfuehren, damit die entsprechenden Daten gesammelt werden.



Modify options anklicken. Oakley Logs auswaehlen. Andere Optionen koennen abgewaehlt werden.

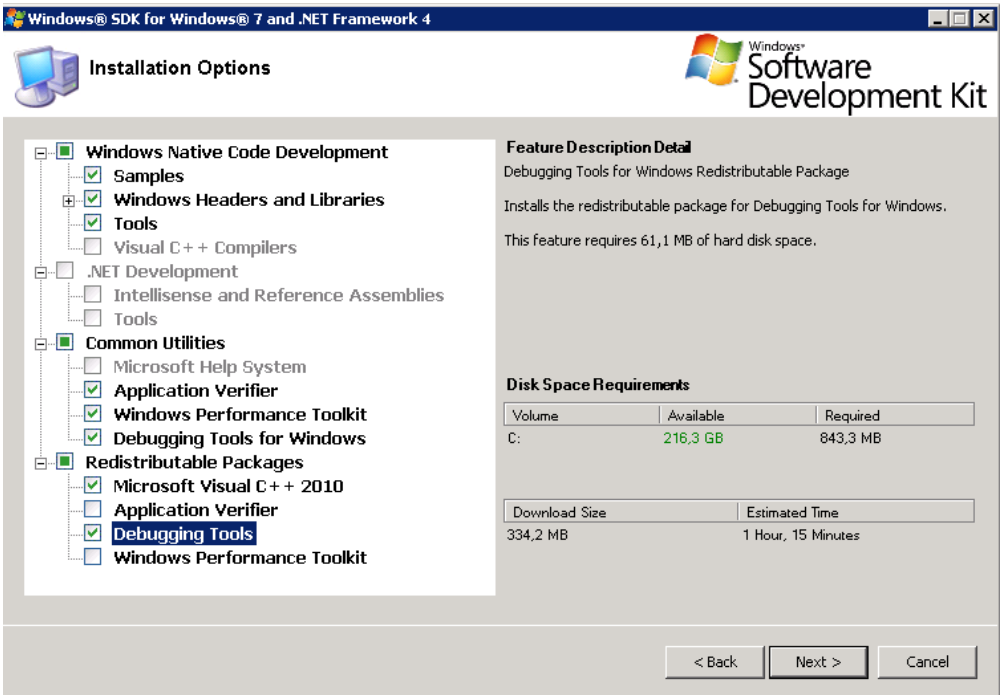


Der Trace kann jetzt manuell gestartet und gestoppt werden. TMG Data Packager erzeugt ein CAB File welches u. a. auch die IKEEXT.ETL Datei enthaelt.



Windows SDK downloaden und installieren

Das Windows SDK enthaelt die TRACEFMT.EXE Datei in 64 Bit fuer die Auswertung des IKEEXT.ETL Files in ein Textfile.



Die TRACEFMT Datei liegt in C:\Program Files\Microsoft SDKs\Windows\v7.1\Bin
Ausfuehrung von *TRACEFMT.EXE IKEEXT.ETL –TMF WFP.TMF –O C:\TEMP\OAKLEY.TXT* (funktioniert nur in Windows Server 2008)

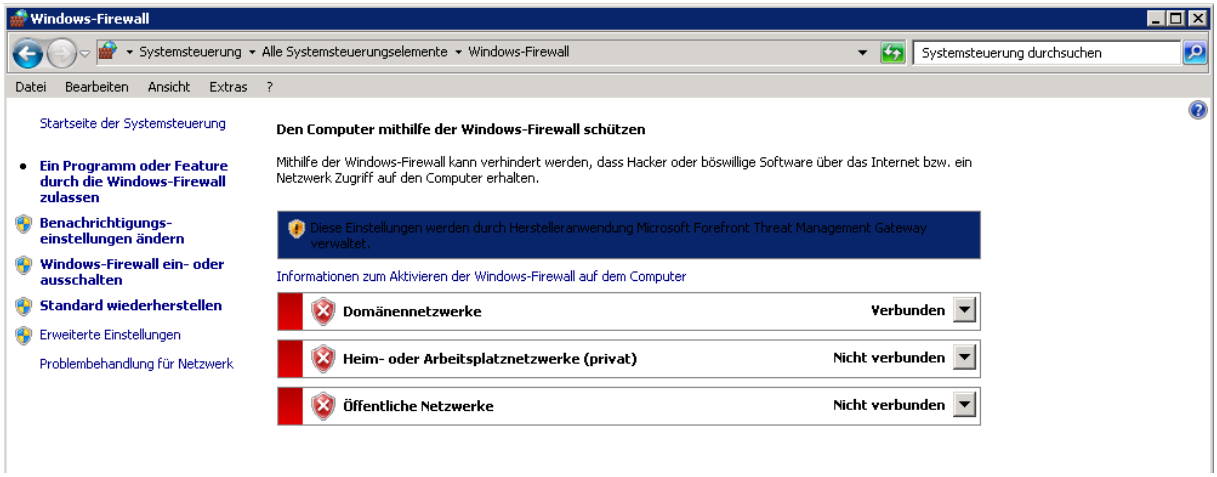
Hinweis: Die Datei WFP.TMF kann nur von einem Windows Server 2008 SP2 geladen werden. Eine Aufuehrung auf Windows Server 2008 R2 funktioniert liefert aber keine lesbare Auswertung.
http://blogs.technet.com/b/yuridiogenes/archive/2010/03/30/how-tmg-data-packager-can-assist-you-troubleshooting-vpn-site-to-site-issues.aspx
Die WFP.TMF Datei fuer Windows Server 2008 R2 steht nur intern bei Microsoft zur Verfuegung!

WFP Einfuehrung

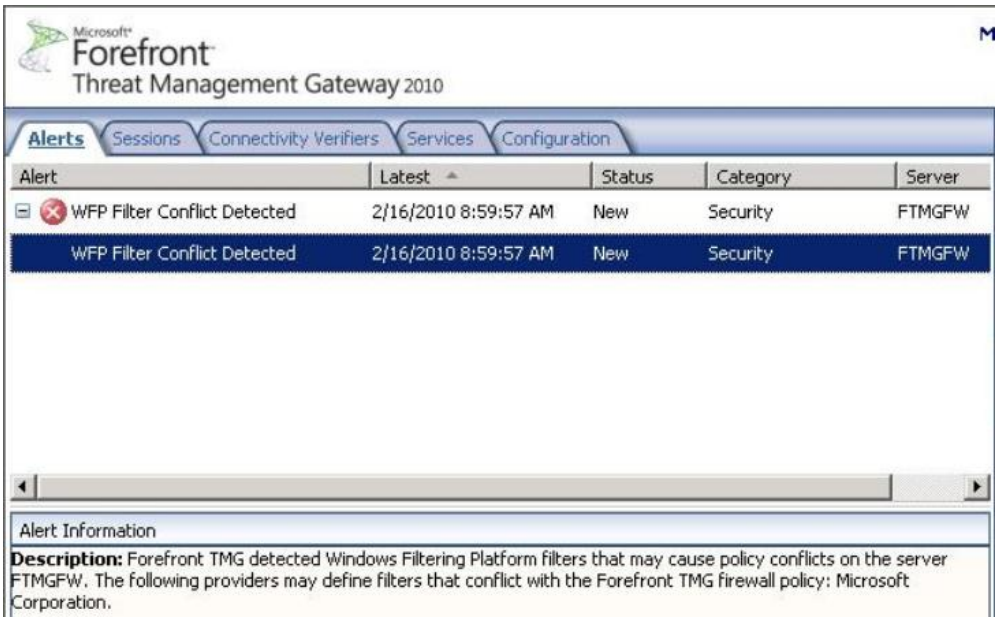
Die Windows Filtering Plattform wird seit Windows Vista / 2008 als Schnittstelle / Filter von Windows verwendet um TCP/IP Pakete zu filtern, Verbindungen zu authorisieren und z. B. IPSEC Verbindungen zu filtern/steuern. Third party Hersteller koennen WFP verwenden um Ihre Produkte in Windows zu integrieren.

Weitere Informationen:
http://msdn.microsoft.com/en-us/library/windows/hardware/gg463267.aspx

Ein Ergebnis der WFP Integration von TMG in Windows ist diese Meldung in den Eigenschaften der Windows Firewall, dass TMG Kontrolle ueber die Windows Firewall uebernimmt und diese u. a. auch fuer die IPSEC Verbindungsanforderungen nutzt (IPSEC Phase 1 und Phase 2).



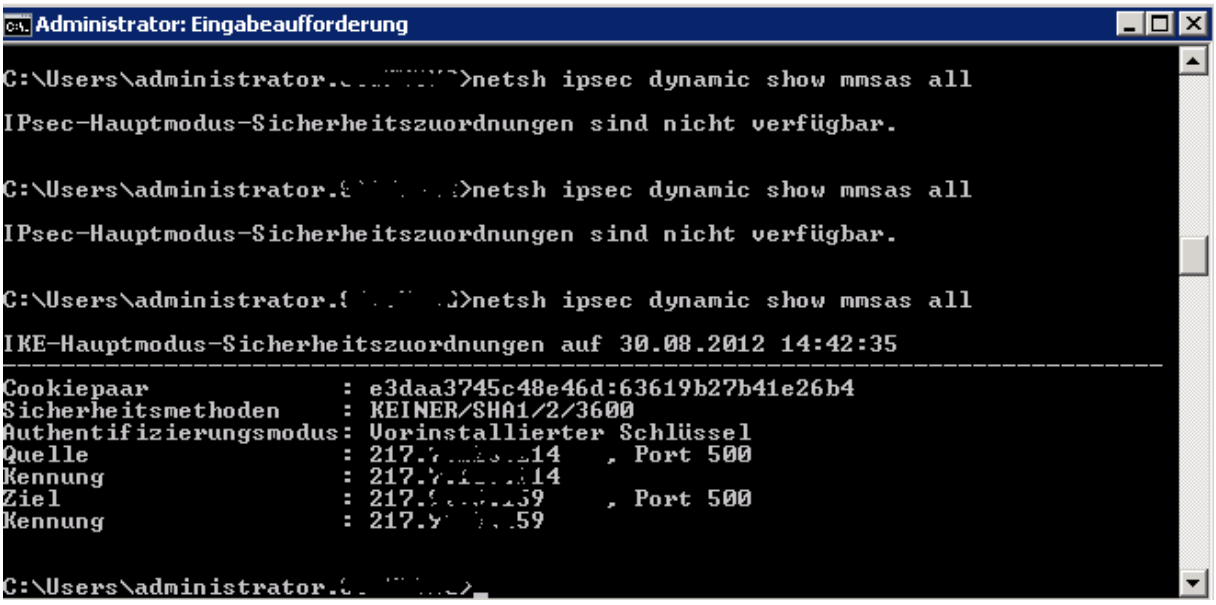
WFP ist unter anderem auch fuer die klassische WFP Meldung in TMG verantwortlich:



http://blogs.technet.com/b/yuridiogenes/archive/2010/02/16/wfp-filter-conflict-detected-alert-after-installing-forefront-tmg-2010.aspx

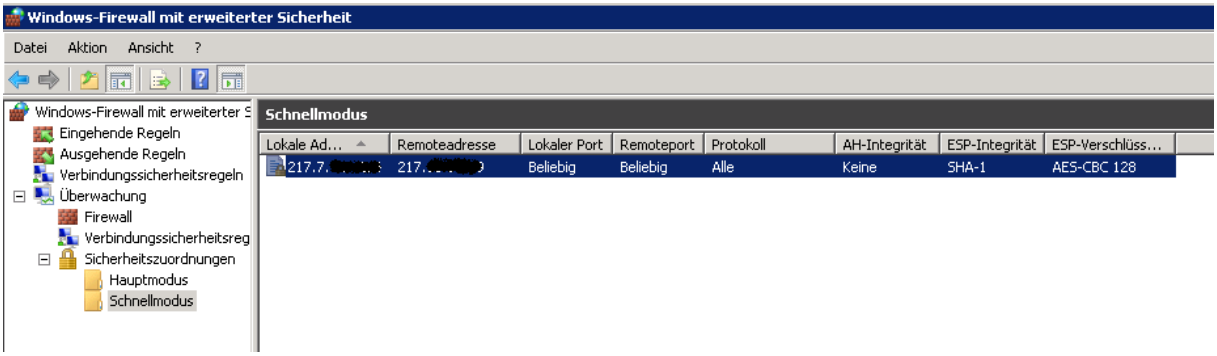
IPSEC Main und Quick Mode Verbindungen mit NETSH anzeigen

Main Mode established

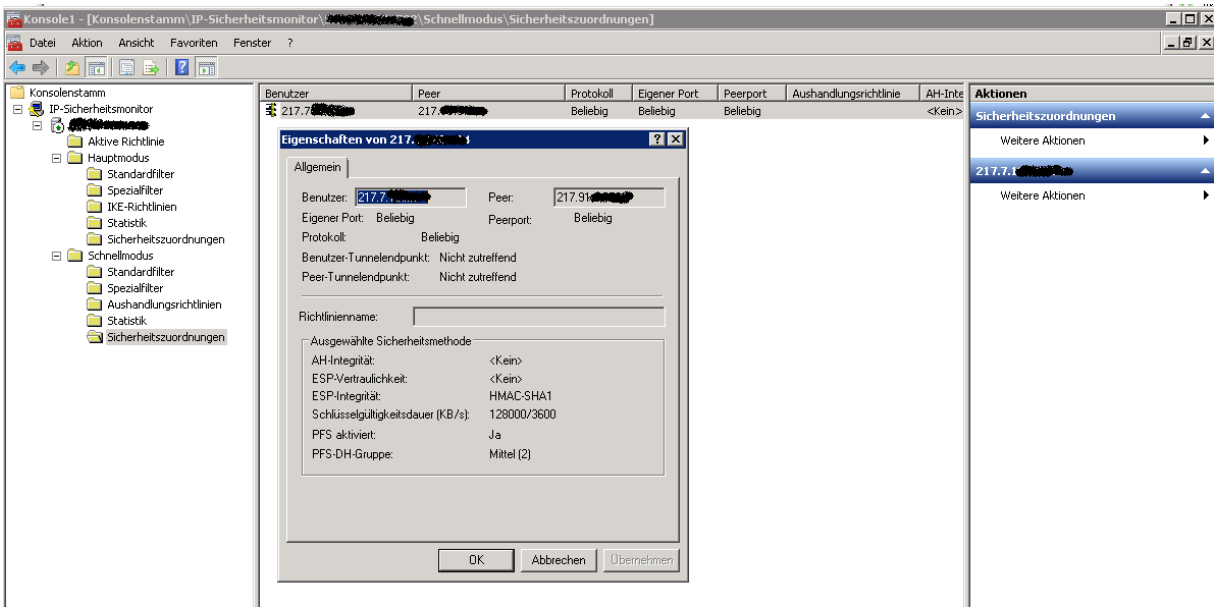


Quick Mode established

Anzeige der IPSEC Phase 1 und 2 Verbindungen in der Windows Firewall mit erweiterter Sicherheit

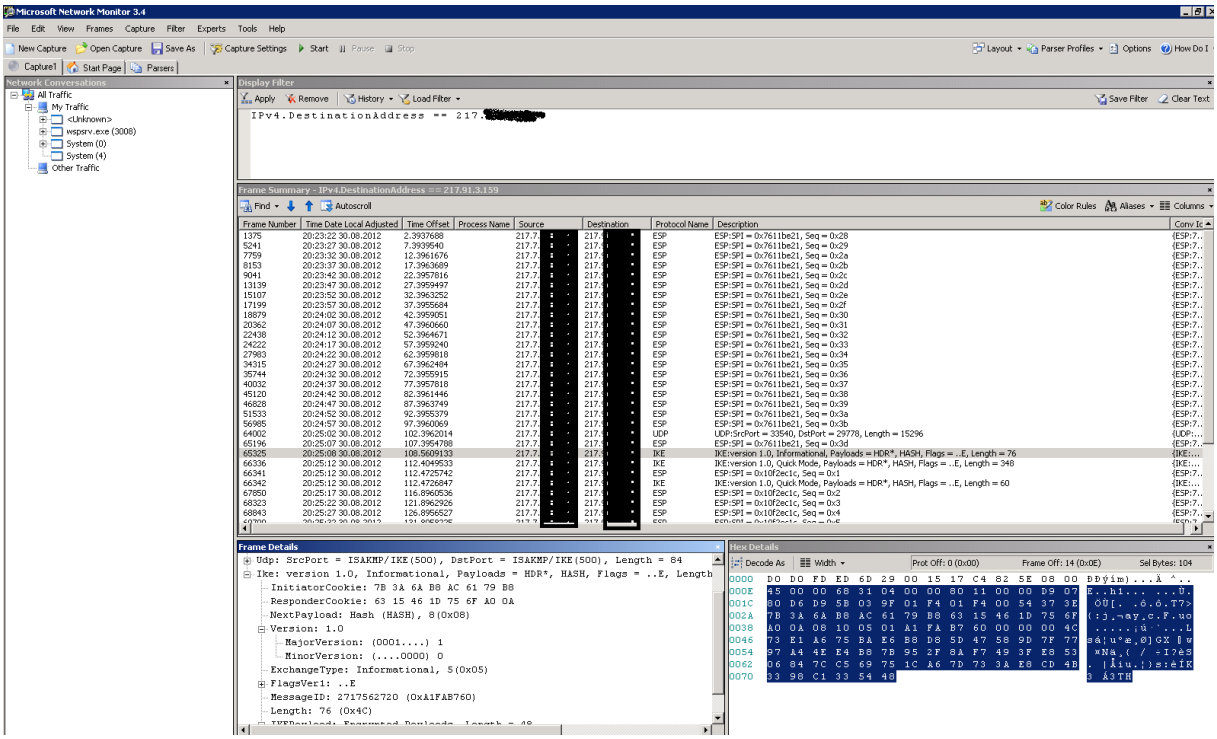


Der gute (alte) IPSEC Monitor liefert auch noch ein paar Informationen ☺

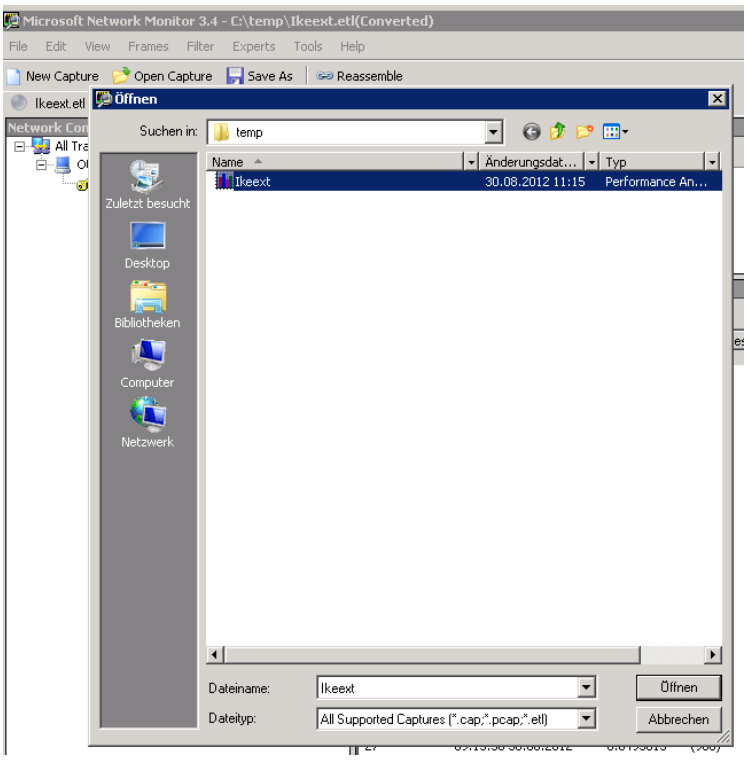


Netmon

Fuer eine detaillierte Analyse der IPSEC Verbindungen bietet sich auch der Microsoft Netzwerkmonitor an.



Die IKEEXT.ETL Datei kann auch mit Netmon geoeffnet werden



Voraussetzung: Full Parser Support aktivieren