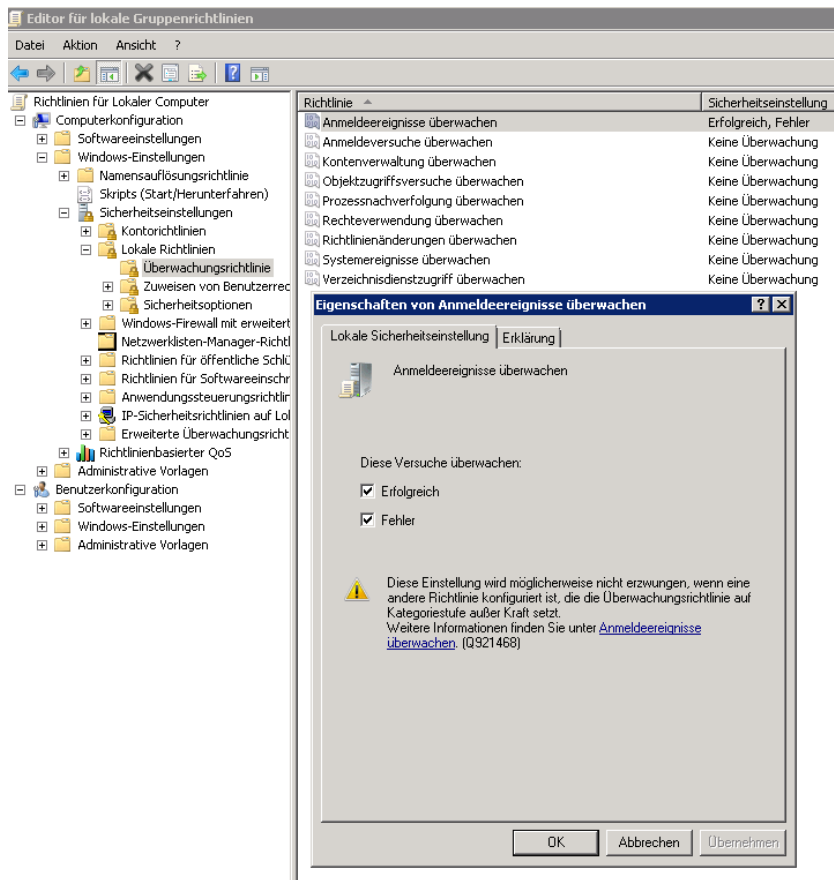
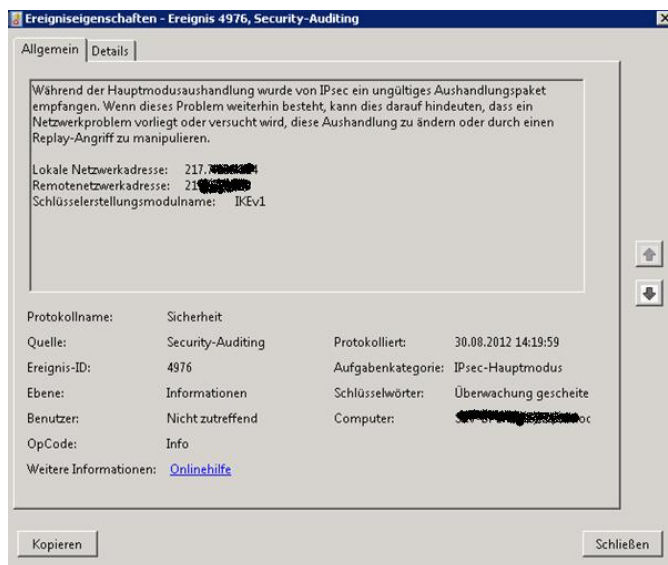


Forefront TMG IPSEC Debugging

Windows Anmeldeereignisse ueberwachen aktivieren



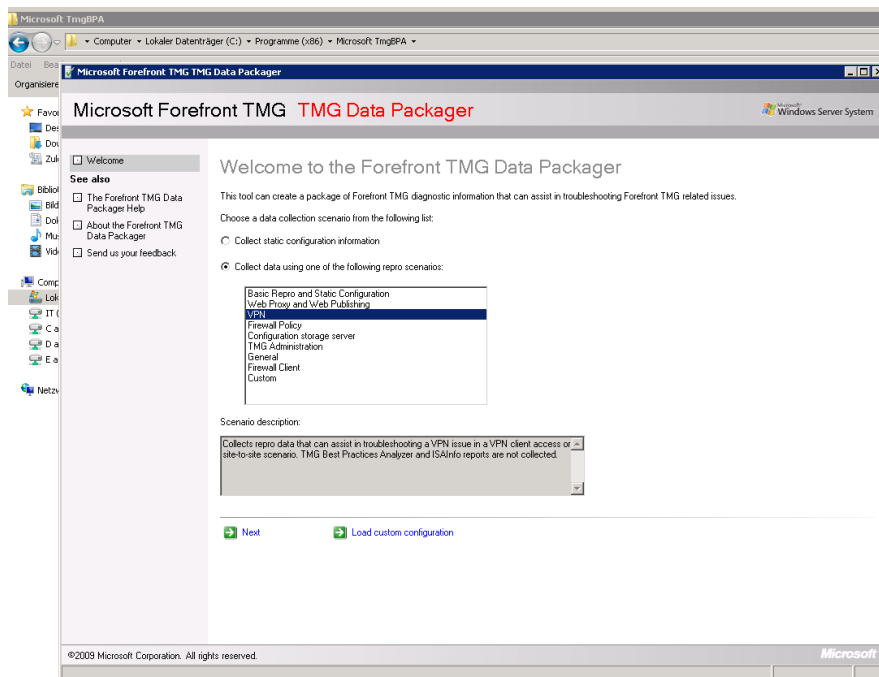
Danach werden im Security Log zusätzliche Informationen angezeigt



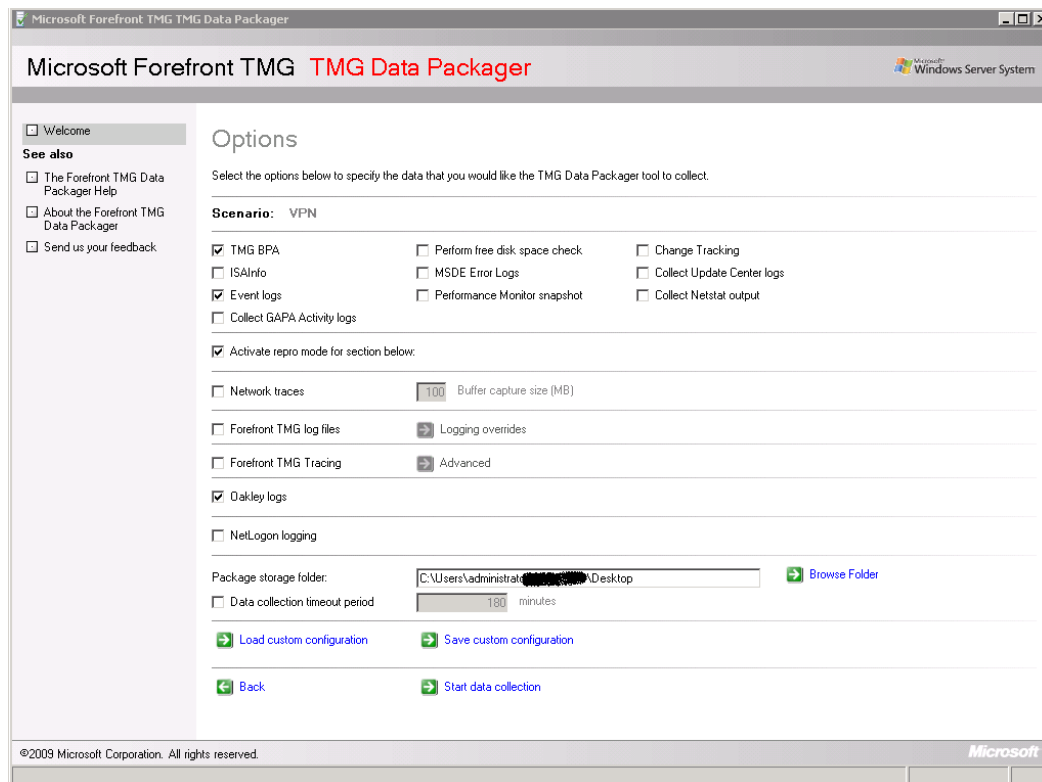
TMG BPA installieren

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.

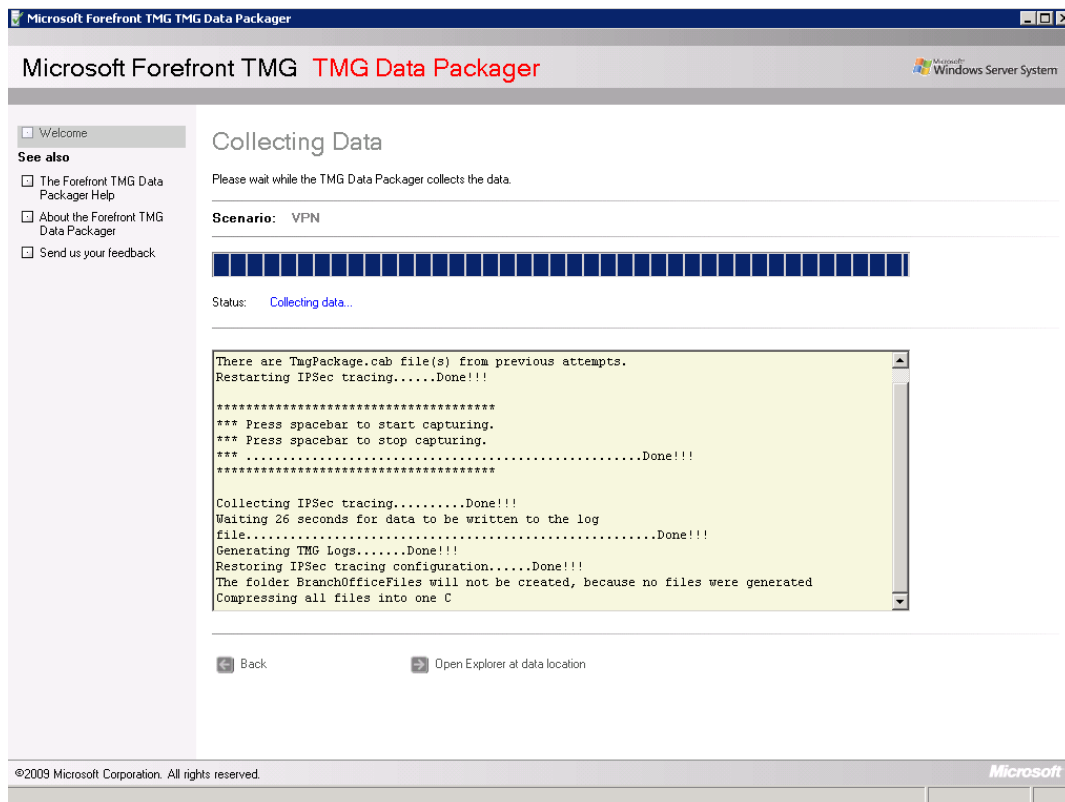
TMG Data Packager ausfuehren. Repro Mode VPN Szenario auswaehlen. VPN Verbindungsversuche erneut durchfuehren, damit die entsprechenden Daten gesammelt werden.



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

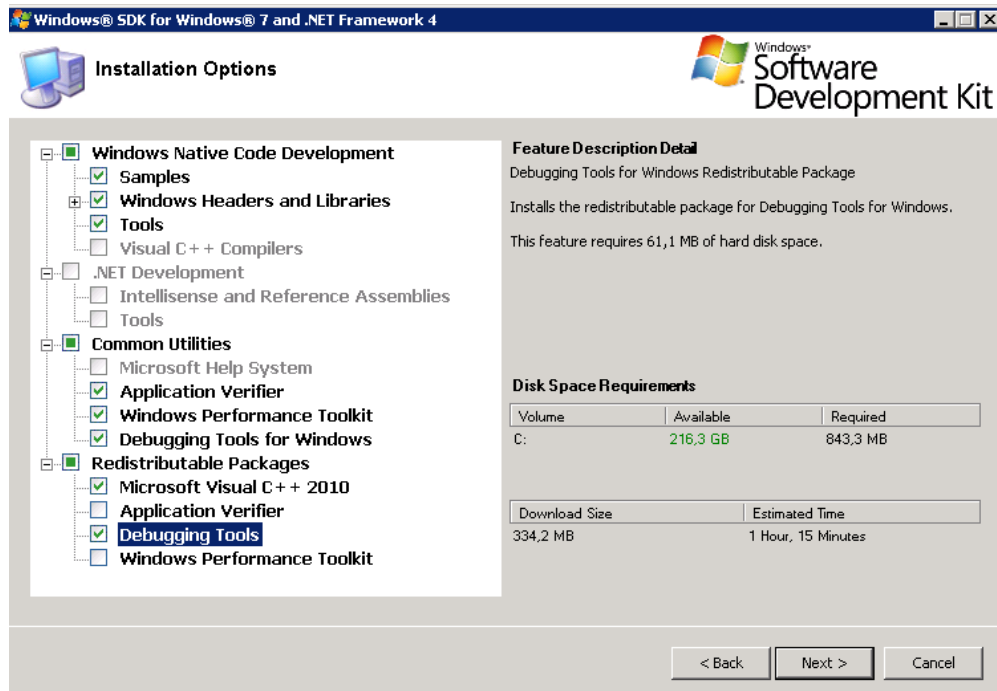


Der Trace kann jetzt manuell gestartet und gestoppt werden. TMG Data Packager erzeugt ein CAB File welches u. a. auch die IKEEXT.ETL Datei enthaelt.

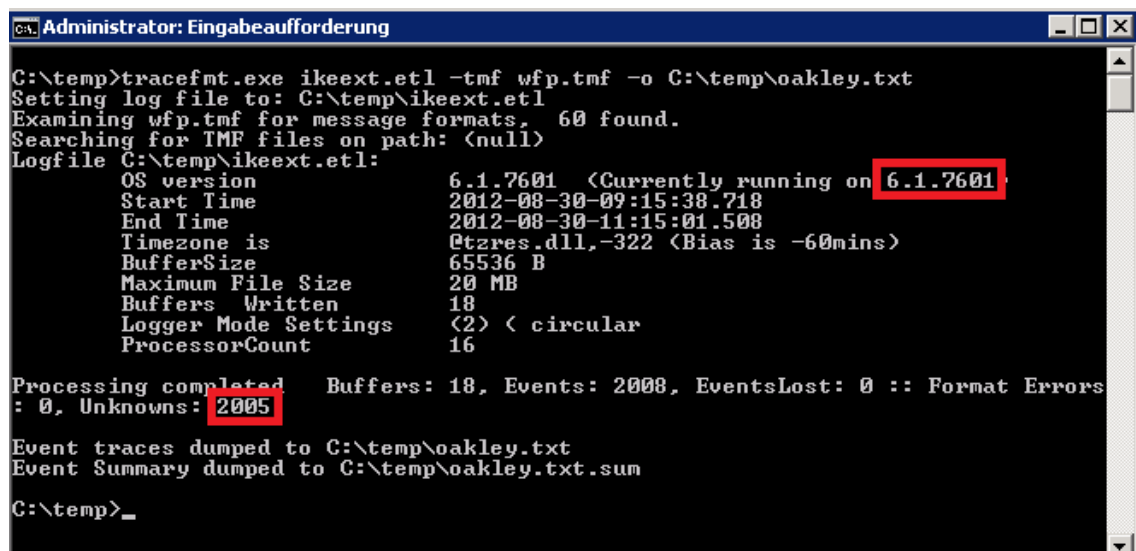


Windows SDK downloaden und installieren

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!

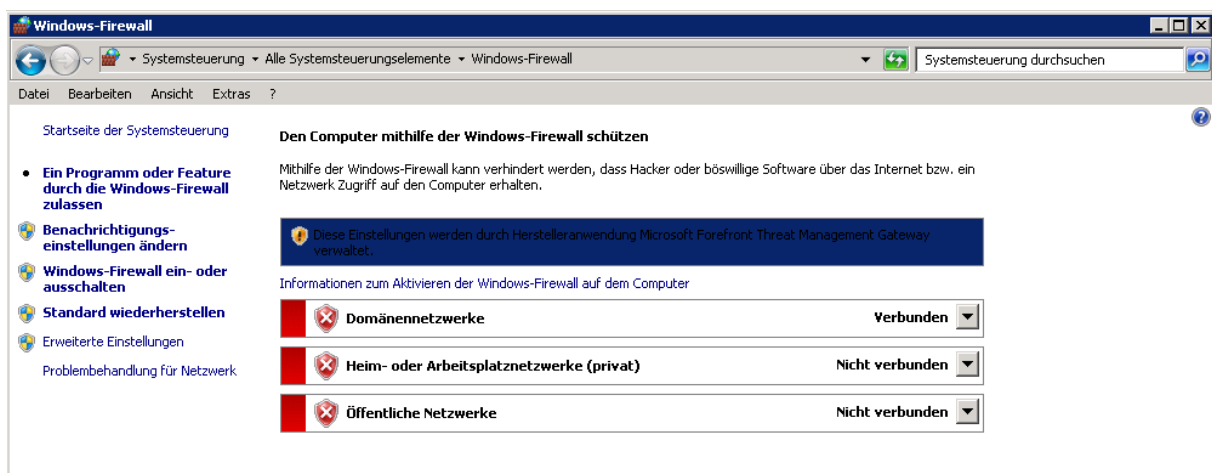
WFP Einfuehrung

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.

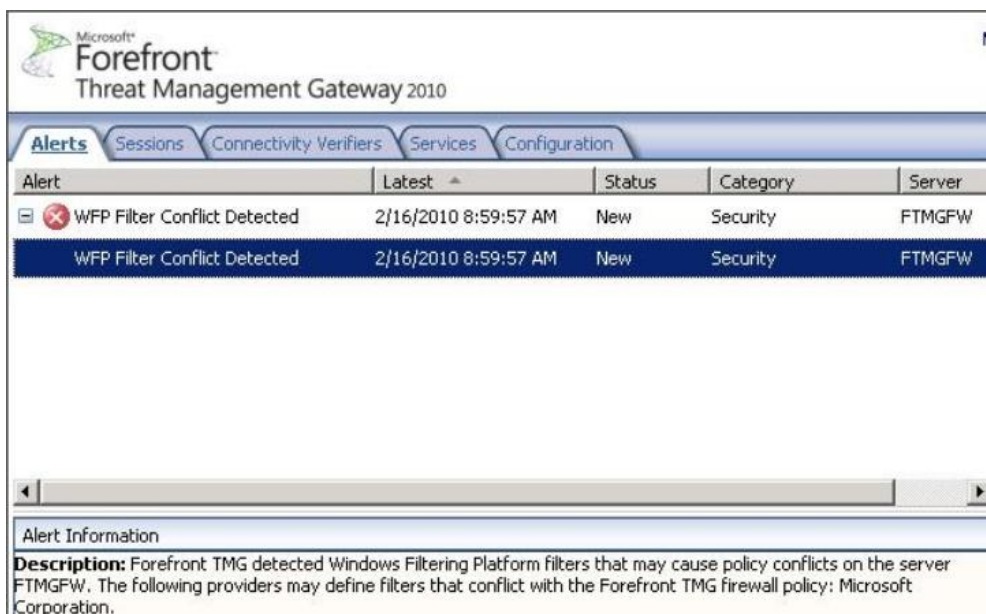
Weitere Informationen:

<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

```
Administrator: Eingabeaufforderung

C:\Users\administrator.C...>netsh ipsec dynamic show mmsas all
IPsec-Hauptmodus-Sicherheitszuordnungen sind nicht verfügbar.

C:\Users\administrator.C...>netsh ipsec dynamic show mmsas all
IPsec-Hauptmodus-Sicherheitszuordnungen sind nicht verfügbar.

C:\Users\administrator.C...>netsh ipsec dynamic show mmsas all
IKE-Hauptmodus-Sicherheitszuordnungen auf 30.08.2012 14:42:35
-----
Cookiepaar           : e3daa3745c48e46d:63619b27b41e26b4
Sicherheitsmethoden  : KEINER/SHA1/2/3600
Authentifizierungsmodus: Vorinstallierter Schlüssel
Quelle                : 217.71.11.14      , Port 500
Kennung              : 217.71.11.14
Ziel                 : 217.71.11.159   , Port 500
Kennung              : 217.71.11.159

C:\Users\administrator.C...>
```

Quick Mode established

```
Administrator: Eingabeaufforderung

IPsec-Schnellmodus-Sicherheitszuordnungen sind nicht verfügbar.

C:\Users\administrator.C...>netsh ipsec dynamic show qmsas all

Schnellmodus-Sicherheitszuordnungen
-----

Transportfilter

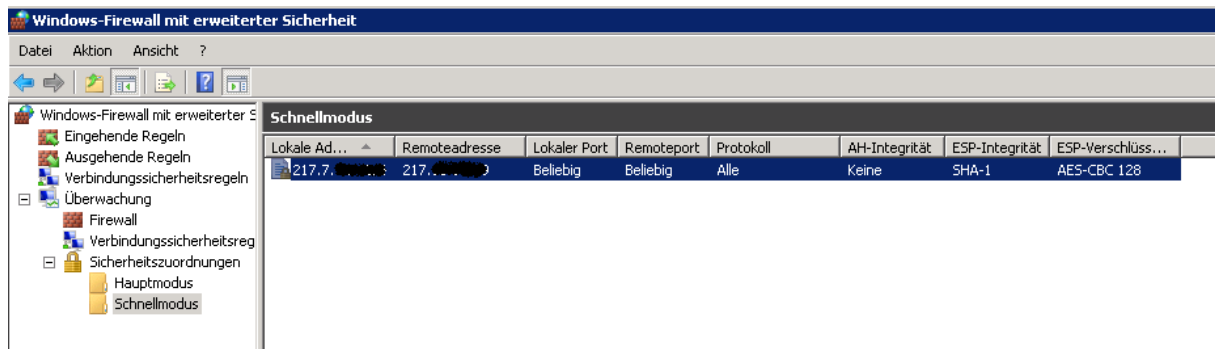
Quelladresse          : 217.71.11.14
Zieladresse           : 217.71.11.159
Protokoll             : BELIEBIG
Quellport             : 0
Zielport              : 0
Ziel                  : Eingehend

Verwendetes Angebot

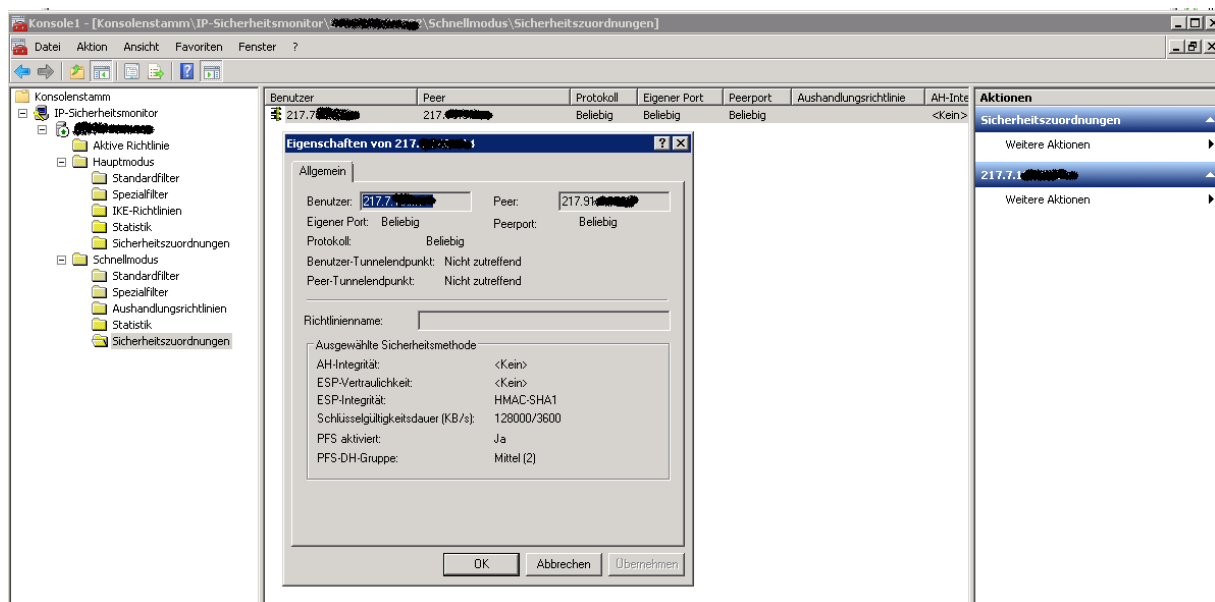
  AH(h/r)  ESP-Uer.(h/r)  ESP-Int  PFS-DH-Gruppe
-----
  Kein     Kein          SHA1     Medium (2)

C:\Users\administrator.C...>
```

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.

The screenshot shows the Microsoft Network Monitor 3.4 interface. The left pane displays the network tree with 'My Traffic' selected. The main pane shows a list of network frames. The selected frame is an IKEEXT packet (Frame 6335) with the following details:

- Frame Number: 6335
- Time Date Local Adjusted: 20-25-08 30.08.2012
- Time Offset: 108.5609133
- Process Name: IKEEXT
- Source: 10.10.10.10
- Destination: 10.10.10.10
- Protocol Name: ESP
- Description: ESP-SP1 = 0x7611be21, Seq = 0x0

The packet details pane shows the following information:

- Udp: SrcPort = ISAKMP/IKE(500), DstPort = ISAKMP/IKE(500), Length = 64
- Ike: version 1.0, Informational, Payloads = HDR*, HASH, Flags = ..E, Length = 64
- InitiatorCookie: 7B 3A 6A B8 AC 61 79 B8
- ResponderCookie: 63 15 46 1D 75 6F AD 0A
- NextPayload: Hash (HASH), 8(0x08)
- Version: 1.0
- MajorVersion: (0001....) 1
- MinorVersion: (....0000) 0
- ExchangeType: Informational, S(0x05)
- FlagsVer: ..E
- MessageID: 2717562720 (0xA1FAB760)
- Length: 76 (0x4C)

Die IKEEXT.ETL Datei kann auch mit Netmon geoeffnet werden

The screenshot shows the Microsoft Network Monitor 3.4 interface with the 'Open' dialog box open. The dialog box is titled 'Ikeext.etl' and shows the file 'Ikeext.etl' in the 'temp' directory. The file is dated '30.08.2012 11:15' and has a 'Performance An...' extension. The 'Dateiname' field is set to 'Ikeext' and the 'Dateityp' is set to 'All Supported Captures (*.cap;*.pcap;*.etl)'. The 'Öffnen' (Open) button is highlighted.

Voraussetzung: Full Parser Support aktivieren

