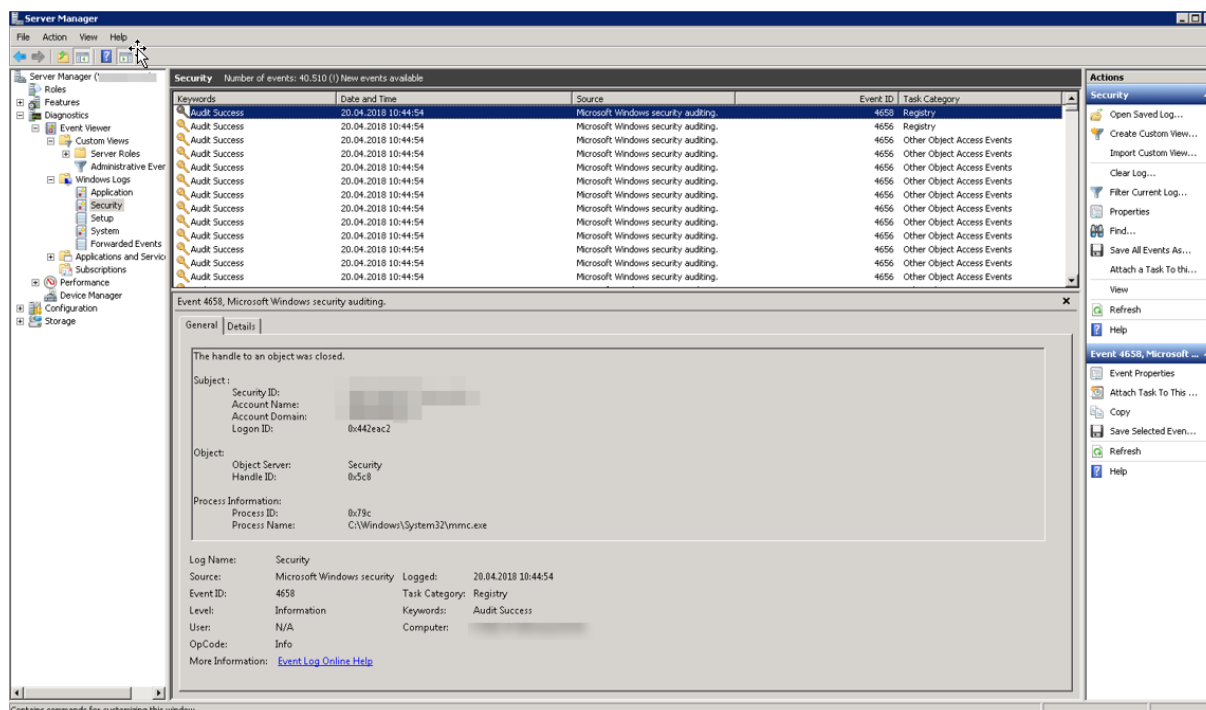




Windows-Filtering-Platform

Sollte das Security LOG mit Event-IDs 5156 volllaufen, dann kann folgendes unternommen werden.



Abschalten des Loggings über die CMD:

```
auditpol /set /subcategory:"Filtering Platform Connection" /success:disable  
/failure:enable
```

```
auditpol /set /subcategory:"Filtering Platform Connection" /success:disable
```

Abschalten des Loggings über eine Richtlinie:

POLICIES > WINDOWS SETTINGS > SECURITY SETTINGS > AUDIT POLICY > AUDIT OBJECT ACCESS settings:

Was steckt dahinter?

Die Windows Firewall Verbindungen werden durch die Aktivierung von "Filter Platform Policy Change" überwacht. Je nach Einstellung werden gescheiterte oder/auch erfolgreiche Verbindungen ins Ereignissprotokoll geschrieben. Durch die Aktivierung der Überwachung gehören diese Ereignisse nachher zu den TOP 10 der Vorkommnisse.



Windows-Filtering-Platform

Events:

- 5031 The Windows Firewall Service blocked an application from accepting incoming connections on the network.
- 5140 A network share object was accessed.
- 5150 The Windows Filtering Platform blocked a packet.
- 5151 A more restrictive Windows Filtering Platform filter has blocked a packet.
- 5154 The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
- 5155 The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
- 5156 The Windows Filtering Platform has allowed a connection.
- 5157 The Windows Filtering Platform has blocked a connection.
- 5158 The Windows Filtering Platform has permitted a bind to a local port.
- 5159 The Windows Filtering Platform has blocked a bind to a local port.



Windows-Filtering-Platform

Vorher aktiv:

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\adm_jwalter>auditpol /get /category:*
System audit policy
Category/Subcategory                                Setting
System
  Security System Extension                          Success and Failure
  System Integrity                                  Success and Failure
  IPsec Driver                                        Success and Failure
  Other System Events                               Success and Failure
  Security State Change                             Success and Failure
Logon/Logoff
  Logon                                               Success and Failure
  Logoff                                              Success and Failure
  Account Lockout                                    Success and Failure
  IPsec Main Mode                                    Success and Failure
  IPsec Quick Mode                                   Success and Failure
  IPsec Extended Mode                               Success and Failure
  Special Logon                                       Success and Failure
  Other Logon/Logoff Events                           Success and Failure
  Network Policy Server                             Success and Failure
Object Access
  File System                                         Success
  Registry                                             Success
  Kernel Object                                       Success
  SAM                                                  Success
  Certification Services                             Success
  Application Generated                              Success
  Handle Manipulation                                Success
  File Share                                           Success
  Filtering Platform Packet Drop                      Success
  Filtering Platform Connection                      Success
  Other Object Access Events                          Success
  Detailed File Share                                Success
Privilege Use
  Sensitive Privilege Use                             No Auditing
  Non Sensitive Privilege Use                         No Auditing
  Other Privilege Use Events                          No Auditing
Detailed Tracking
  Process Termination                                Success and Failure
  DPAPI Activity                                      Success and Failure
  RPC Events                                           Success and Failure
  Process Creation                                    Success and Failure
Policy Change
  Audit Policy Change                                Success and Failure
  Authentication Policy Change                       Success and Failure
  Authorization Policy Change                        Success and Failure
  MPSSVC Rule-Level Policy Change                    Success and Failure
  Filtering Platform Policy Change                    Success and Failure
  Other Policy Change Events                          Success and Failure
Account Management
  User Account Management                            Success and Failure
  Computer Account Management                        Success and Failure
  Security Group Management                          Success and Failure
  Distribution Group Management                      Success and Failure
  Application Group Management                       Success and Failure
  Other Account Management Events                     Success and Failure
DS Access
  Directory Service Changes                           Success and Failure
  Directory Service Replication                       Success and Failure
  Detailed Directory Service Replication              Success and Failure
  Directory Service Access                            Success and Failure
Account Logon
  Kerberos Service Ticket Operations                 Success and Failure
  Other Account Logon Events                         Success and Failure
  Kerberos Authentication Service                     Success and Failure
  Credential Validation                               Success and Failure

C:\Users\adm_jwalter>
```



Windows-Filtering-Platform

Nachher inaktiv:

```
Administrator: Command Prompt

C:\Users\adm_jwalter>auditpol /set /subcategory:"Filtering Platform Connection"
/success:disable /failure:enable
The command was successfully executed.

C:\Users\adm_jwalter>auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    Success and Failure
  System Integrity             Success and Failure
  IPsec Driver                 Success and Failure
  Other System Events          Success and Failure
  Security State Change        Success and Failure
Logon/Logoff
  Logon                        Success and Failure
  Logoff                       Success and Failure
  Account Lockout              Success and Failure
  IPsec Main Mode              Success and Failure
  IPsec Quick Mode             Success and Failure
  IPsec Extended Mode          Success and Failure
  Special Logon                Success and Failure
  Other Logon/Logoff Events     Success and Failure
  Network Policy Server        Success and Failure
Object Access
  File System                  Success
  Registry                     Success
  Kernel Object                Success
  SAM                          Success
  Certification Services       Success
  Application Generated        Success
  Handle Manipulation          Success
  File Share                    Success
  Filtering Platform Packet Drop Success
  Filtering Platform Connection Failure
  Other Object Access Events   Success
  Detailed File Share          Success
Privilege Use
  Sensitive Privilege Use      No Auditing
  Non Sensitive Privilege Use  No Auditing
  Other Privilege Use Events    No Auditing
Detailed Tracking
  Process Termination          Success and Failure
  DPAPI Activity               Success and Failure
  RPC Events                   Success and Failure
  Process Creation             Success and Failure
Policy Change
  Audit Policy Change          Success and Failure
  Authentication Policy Change Success and Failure
  Authorization Policy Change  Success and Failure
  MPSSUC Rule-Level Policy Change Success and Failure
  Filtering Platform Policy Change Success and Failure
  Other Policy Change Events    Success and Failure
Account Management
  User Account Management       Success and Failure
  Computer Account Management   Success and Failure
  Security Group Management     Success and Failure
  Distribution Group Management Success and Failure
  Application Group Management  Success and Failure
  Other Account Management Events Success and Failure
DS Access
  Directory Service Changes     Success and Failure
  Directory Service Replication Success and Failure
  Detailed Directory Service Replication Success and Failure
  Directory Service Access       Success and Failure
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events     Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation          Success and Failure

C:\Users\adm_jwalter>
```

Es werden ab sofort keine Logs mehr geschrieben.