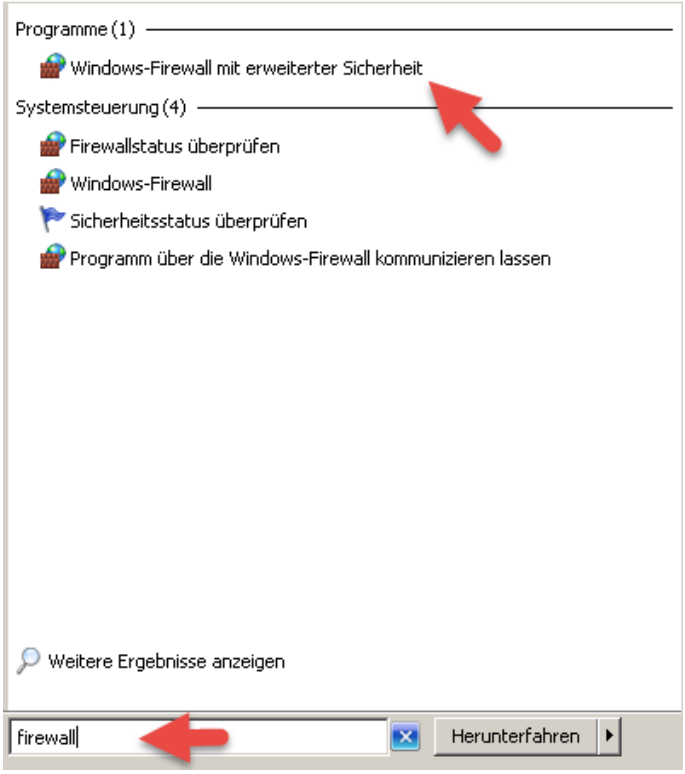
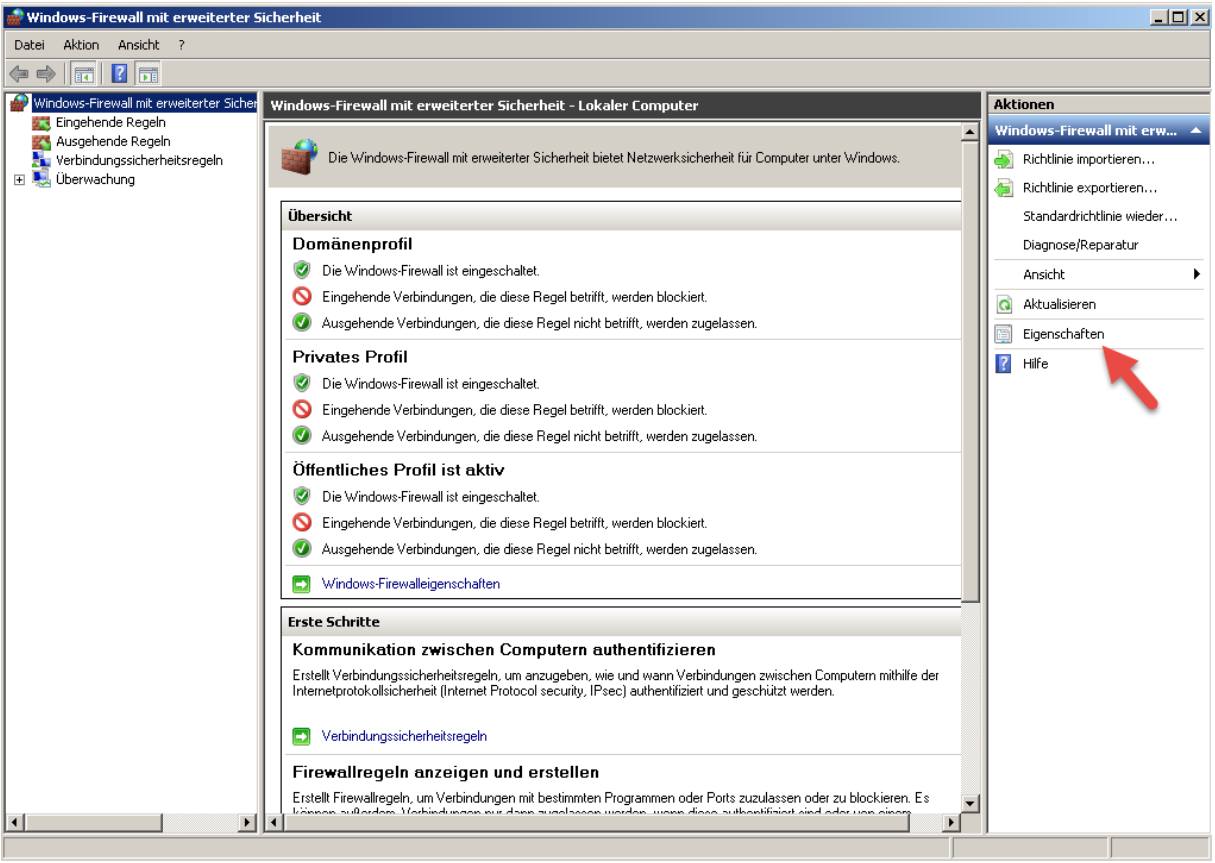
Windows Firewall - Protokollierung aktivieren

Zur Einsicht in die Tätigkeit (geblockte und durchgelassene Pakete) der Windows Firewall schalten wir die Protokollierung wie folgt ein.

Über **Start > Suchfeld** und dem Begriff **Firewall** öffnen wir die erweiterte Sicherheit.

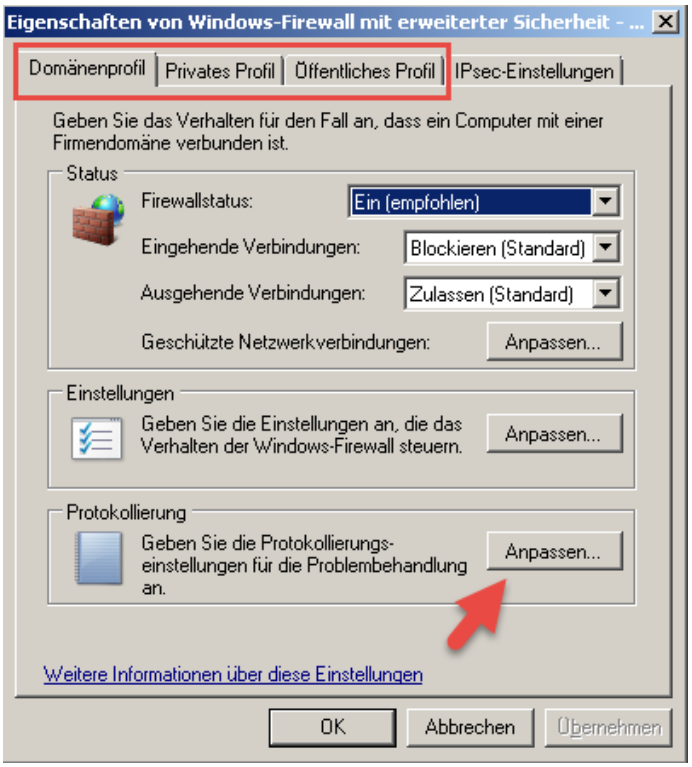


Auf der rechten Seite klicken wir auf Eigenschaften.

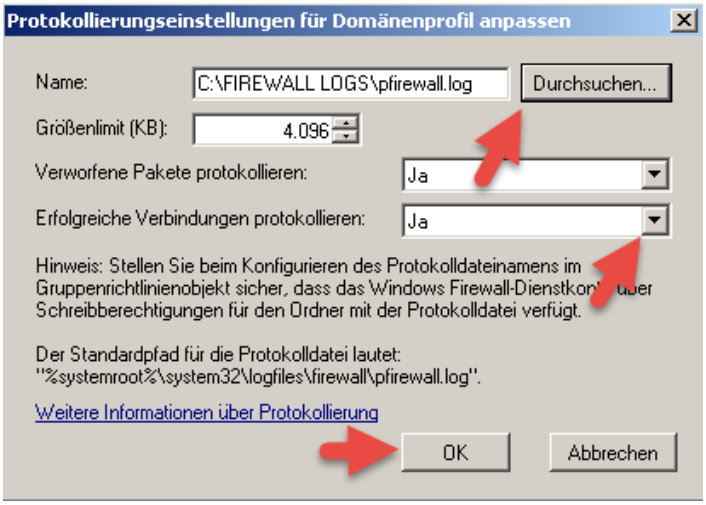


Windows Firewall - Protokollierung aktivieren

Entscheiden uns zwischen den jeweils zu protokollierenden **Profilen** und klicken unten rechts auf **Anpassen**.



Passen über Durchsuchen den Protokollpfad an. In diesem Beispiel entscheide ich mich für **C:\FIREWALL LOGS** und aktiviere über das **Drop-Down Menü** das Logging für die **verworfenen Pakete** und die **erfolgreichen Verbindungen**.



Mit einem Klick auf **OK** ist das Logging aktiviert.

Das **Log-File** sieht wie folgt aus:

pfirewall - Editor

Datei Bearbeiten Format Ansicht ?

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype
icmpcode info path


                                                                                                    2015-02-12 21:49:44 ALLOW
ICMP fe80::d4c8:1a70:b92:b0dc ff02::16 - - 0 - - - - 143 0 - SEND
2015-02-12 21:49:44 ALLOW UDP 0.0.0.0 255.255.255.255 68 67 0 - - - - - - - SEND
2015-02-12 21:49:44 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - RECEIVE
2015-02-12 21:49:44 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - RECEIVE
2015-02-12 21:49:44 ALLOW UDP fe80::d4c8:1a70:b92:b0dc ff02::1:3 59700 5355 0 - - - - - - - SEND
2015-02-12 21:49:44 DROP ICMP 192.168.17.254 192.168.17.129 - - 48 - - - - 8 0 - RECEIVE
2015-02-12 21:49:44 ALLOW UDP 0.0.0.0 255.255.255.255 68 67 0 - - - - - - - SEND
2015-02-12 21:49:44 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - RECEIVE
2015-02-12 21:49:44 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - RECEIVE
2015-02-12 21:49:44 ALLOW 2 127.0.0.1 224.0.0.22 - - 0 - - - - - - - SEND
2015-02-12 21:49:44 ALLOW ICMP ::1 ff02::16 - - 0 - - - - 143 0 - SEND
2015-02-12 21:49:44 ALLOW UDP ::1 ::1 63555 63555 0 - - - - - - - SEND
2015-02-12 21:49:44 ALLOW UDP fe80::d4c8:1a70:b92:b0dc ff02::1:3 54334 5355 0 - - - - - - - SEND
2015-02-12 21:49:44 ALLOW UDP 127.0.0.1 239.255.255.250 63556 1900 0 - - - - - - - SEND
2015-02-12 21:49:44 ALLOW UDP 127.0.0.1 239.255.255.250 63556 1900 0 - - - - - - - RECEIVE
2015-02-12 21:49:44 ALLOW ICMP :: ff02::1:ff92:b0dc - - 0 - - - - 135 0 - SEND
2015-02-12 21:49:44 ALLOW ICMP fe80::d4c8:1a70:b92:b0dc ff02::2 - - 0 - - - - 133 0 - SEND
2015-02-12 21:49:45 ALLOW UDP fe80::d4c8:1a70:b92:b0dc ff02::1:3 63440 5355 0 - - - - - - - SEND
2015-02-12 21:49:45 DROP UDP fe80::2161:3f1d:7489:623e ff02::1:3 53083 5355 138 - - - - - - - RECEIVE
2015-02-12 21:49:45 DROP UDP 192.168.17.1 224.0.0.252 49218 5355 118 - - - - - - - RECEIVE
2015-02-12 21:49:45 DROP UDP 192.168.17.1 224.0.0.252 49218 5355 118 - - - - - - - RECEIVE
2015-02-12 21:49:45 ALLOW UDP fe80::d4c8:1a70:b92:b0dc ff02::1:3 51542 5355 0 - - - - - - - SEND
2015-02-12 21:49:45 ALLOW UDP 192.168.17.254 192.168.17.129 67 68 0 - - - - - - - RECEIVE
2015-02-12 21:49:45 ALLOW UDP fe80::d4c8:1a70:b92:b0dc ff02::1:3 59737 5355 0 - - - - - - - SEND
2015-02-12 21:49:45 ALLOW ICMP fe80::d4c8:1a70:b92:b0dc ff02::1 - - 0 - - - - 136 0 - SEND
2015-02-12 21:49:46 ALLOW UDP fe80::d4c8:1a70:b92:b0dc ff02::1:3 58023 5355 0 - - - - - - - SEND
2015-02-12 21:49:48 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - RECEIVE
2015-02-12 21:49:48 DROP UDP 0.0.0.0 255.255.255.255 68 67 328 - - - - - - - RECEIVE
2015-02-12 21:49:48 DROP UDP 0.0.0.0 255.255.255.255 68 67 354 - - - - - - - RECEIVE
2015-02-12 21:49:48 DROP UDP 0.0.0.0 255.255.255.255 68 67 354 - - - - - - - RECEIVE
2015-02-12 21:49:48 ALLOW UDP fe80::d4c8:1a70:b92:b0dc ff02::1:3 52712 5355 0 - - - - - - - SEND
```