

Блокировка служб телеметрии Windows

MikroTik / RouterOS

Рассмотрим 2 варианта возможных блокировок данной службы с помощью Mikrotik роутера:

1. Необходимо вписать в фаервол следующие правила:

```
/ip firewall address-list add list=MStelemetry
address=111.221.29.177
/ip firewall address-list add list=MStelemetry
address=111.221.29.253
/ip firewall address-list add list=MStelemetry
address=131.253.40.37
/ip firewall address-list add list=MStelemetry
address=134.170.30.202
/ip firewall address-list add list=MStelemetry
address=134.170.115.60
/ip firewall address-list add list=MStelemetry
address=134.170.165.248
/ip firewall address-list add list=MStelemetry
address=134.170.165.253
/ip firewall address-list add list=MStelemetry
address=134.170.185.70
/ip firewall address-list add list=MStelemetry
address=137.116.81.24
/ip firewall address-list add list=MStelemetry
address=137.117.235.16
/ip firewall address-list add list=MStelemetry
address=157.55.129.21
/ip firewall address-list add list=MStelemetry
address=157.55.133.204
/ip firewall address-list add list=MStelemetry
address=157.56.121.89
/ip firewall address-list add list=MStelemetry
address=157.56.91.77
/ip firewall address-list add list=MStelemetry
address=168.63.108.233
/ip firewall address-list add list=MStelemetry
address=191.232.139.254
/ip firewall address-list add list=MStelemetry
address=191.232.80.58
/ip firewall address-list add list=MStelemetry
address=191.232.80.62
```

```
2. /ip firewall address-list add list=MStelemetry
address=191.237.208.126
/ip firewall address-list add list=MStelemetry
address=204.79.197.200
/ip firewall address-list add list=MStelemetry
address=207.46.101.29
/ip firewall address-list add list=MStelemetry
address=207.46.114.58
/ip firewall address-list add list=MStelemetry
address=207.46.223.94
/ip firewall address-list add list=MStelemetry
address=207.68.166.254
/ip firewall address-list add list=MStelemetry
address=212.30.134.204
/ip firewall address-list add list=MStelemetry
address=212.30.134.205
/ip firewall address-list add list=MStelemetry
address=23.102.21.4
/ip firewall address-list add list=MStelemetry
address=23.99.10.11
/ip firewall address-list add list=MStelemetry
address=23.218.212.69
/ip firewall address-list add list=MStelemetry
address=64.4.54.22
/ip firewall address-list add list=MStelemetry
address=64.4.54.32
/ip firewall address-list add list=MStelemetry
address=64.4.6.100
/ip firewall address-list add list=MStelemetry
address=65.39.117.230
/ip firewall address-list add list=MStelemetry
address=65.52.100.11
/ip firewall address-list add list=MStelemetry
address=65.52.100.7
/ip firewall address-list add list=MStelemetry
address=65.52.100.9
/ip firewall address-list add list=MStelemetry
address=65.52.100.91
/ip firewall address-list add list=MStelemetry
address=65.52.100.92
/ip firewall address-list add list=MStelemetry
address=65.52.100.93
/ip firewall address-list add list=MStelemetry
address=65.52.100.94
```

```
3. /ip firewall address-list add list=MStelemetry
   address=65.52.108.29

4. /ip firewall address-list add list=MStelemetry
   address=65.55.108.23
   /ip firewall address-list add list=MStelemetry
   address=65.55.138.114
   /ip firewall address-list add list=MStelemetry
   address=65.55.138.126
   /ip firewall address-list add list=MStelemetry
   address=65.55.138.186
   /ip firewall address-list add list=MStelemetry
   address=65.55.252.63
   /ip firewall address-list add list=MStelemetry
   address=65.55.252.71
   /ip firewall address-list add list=MStelemetry
   address=65.55.252.92
   /ip firewall address-list add list=MStelemetry
   address=65.55.252.93
   /ip firewall address-list add list=MStelemetry
   address=65.55.29.238
   /ip firewall address-list add list=MStelemetry
   address=65.55.39.10
   /ip firewall address-list add list=MStelemetry
   address=191.232.139.2
   /ip firewall address-list add list=MStelemetry
   address=64.4.23.0-64.4.23.255
   /ip firewall address-list add list=MStelemetry
   address=111.221.64.0-111.221.127.255
   /ip firewall address-list add list=MStelemetry
   address=157.55.235.0-157.55.235.255
   /ip firewall address-list add list=MStelemetry
   address=157.55.56.0-157.55.56.255
   /ip firewall address-list add list=MStelemetry
   address=157.55.52.0-157.55.52.255
   /ip firewall address-list add list=MStelemetry
   address=157.55.130.0-157.55.130.255
   /ip firewall address-list add list=MStelemetry
   address=65.55.223.0-65.55.223.255
   /ip firewall address-list add list=MStelemetry
   address=213.199.179.0-213.199.179.255
   /ip firewall address-list add list=MStelemetry
   address=195.138.255.0-195.138.255.255
   /ip firewall filter add chain=forward dst-address-
   list=MStelemetry action=reject comment="Reject MS Telemetry"
```

Мы можем использовать Layer7 для блокировки

2.1 Создаем регулярное выражение в Layer7:

```
/ip firewall layer7-protocol add name=NoZond regexp="^.+  
(vortex.data.microsoft.com|vortex-win.data.microsoft.com|  
telecommand.telemetry.microsoft.com|telecommand.telemetry  
.microsoft.com.nsatc.net|oca.telemetry.microsoft.com|  
oca.telemetry.microsoft.com  
.  
nsatc.net|sqm.telemetry.microsoft.com|  
sqm.telemetry.microsoft.com.nsatc.net|wats  
o  
n.telemetry.microsoft.com|  
watson.telemetry.microsoft.com.nsatc.net|redir.metaser  
v  
ices.microsoft.com|choice.microsoft.com|  
choice.microsoft.com.nsatc.net|df.teleme  
t  
ry.microsoft.com|reports.wes.df.telemetry.microsoft.com|  
wes.df.telemetry.microso  
f  
t.com|services.wes.df.telemetry.microsoft.com|  
sqm.df.telemetry.microsoft.com|tel  
e  
metry.microsoft.com|watson.ppe.telemetry.microsoft.com|  
telemetry.appex.bing.net|  
t  
elemetry.urs.microsoft.com|telemetry.appex.bing.net|settings-  
sandbox.data.microsoft.com|vortex-sandbox.data.microsoft.com|  
survey.watson.microsoft.com|watson.live.com|watson.mi  
crosoft.com|statsfe2.ws.microsoft.com|  
corpext.msitadfs.glbdns2.microsoft.com|com  
p  
atexchange.cloudapp.net|cs1.wpc.v0cdn.net|a-0001.a-msedge.net|  
statsfe2.update.microsoft.com.akadns.net|  
diagnostics.support.microsof  
t.com|corp.sts.microsoft.com|statsfe1.ws.microsoft.com|  
pre.footprintpredict.com|  
i  
1.services.social.microsoft.com|  
i1.services.social.microsoft.com.nsatc.net|feedb  
a  
ck.windows.com|feedback.microsoft-hohm.com|  
feedback.search.microsoft.com|rad.msn.com|preview.msn.com|  
ad.doubleclick  
k.net|ads.msn.com|ads1.msads.net|ads1.msn.com|a.ads1.msn.com|
```

```
a.ads2.msn.com|adne  
x  
us.net|adnxs.com|az361816.vo.msecnd.net|  
az512334.vo.msecnd.net).*$"
```

Добавляем правило в Firewall, не забывая поместить его выше разрешающих:

```
ip firewall filter add chain=forward action=reject reject-  
with=tcp-reset protocol=tcp layer7-protocol=NoZond  
ip firewall filter add chain=forward action=drop protocol=udp  
layer7-protocol=NoZond
```

Windows Update при этом доступен и работает.