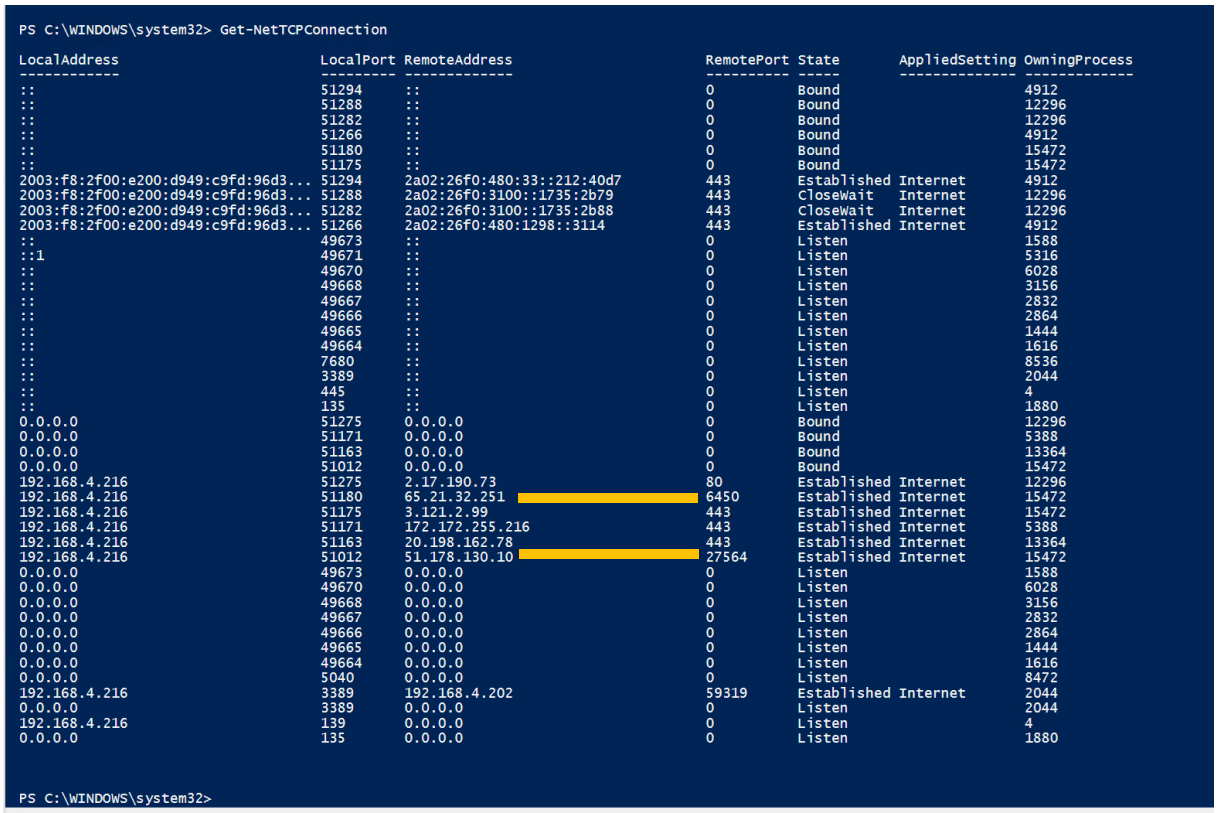
NetworkPort_Configuration

ATAS



```
PS C:\WINDOWS\system32> Get-NetTCPConnection

LocalAddress                        LocalPort RemoteAddress                       RemotePort State       AppliedSetting OwningProcess
------------                        --------- -------------                       ---------- -----       -------------- -------------
::                                  51294     ::                                  0          Bound                      4912
::                                  51288     ::                                  0          Bound                      12296
::                                  51282     ::                                  0          Bound                      12296
::                                  51266     ::                                  0          Bound                      4912
::                                  51180     ::                                  0          Bound                      15472
::                                  51175     ::                                  0          Bound                      15472
2003:f8:2f00:e200:d949:c9fd:96d3... 51294     2a02:26f0:480:33::212:40d7          443        Established Internet       4912
2003:f8:2f00:e200:d949:c9fd:96d3... 51288     2a02:26f0:3100::1735:2b79           443        CloseWait   Internet       12296
2003:f8:2f00:e200:d949:c9fd:96d3... 51282     2a02:26f0:3100::1735:2b88           443        CloseWait   Internet       12296
2003:f8:2f00:e200:d949:c9fd:96d3... 51266     2a02:26f0:480:1298::3114            443        Established Internet       4912
::                                  49673     ::                                  0          Listen                     1588
::1                                 49671     ::                                  0          Listen                     5316
::                                  49670     ::                                  0          Listen                     6028
::                                  49668     ::                                  0          Listen                     3156
::                                  49667     ::                                  0          Listen                     2832
::                                  49666     ::                                  0          Listen                     2864
::                                  49665     ::                                  0          Listen                     1444
::                                  49664     ::                                  0          Listen                     1616
::                                  7680      ::                                  0          Listen                     8536
::                                  3389      ::                                  0          Listen                     2044
::                                  445       ::                                  0          Listen                     4
::                                  135       ::                                  0          Listen                     1880
0.0.0.0                             51275     0.0.0.0                             0          Bound                      12296
0.0.0.0                             51171     0.0.0.0                             0          Bound                      5388
0.0.0.0                             51163     0.0.0.0                             0          Bound                      13364
0.0.0.0                             51012     0.0.0.0                             0          Bound                      15472
192.168.4.216                       51275     2.17.190.73                         80         Established Internet       12296
192.168.4.216                       51180     65.21.32.251                        6450       Established Internet       15472
192.168.4.216                       51175     3.121.2.99                          443        Established Internet       15472
192.168.4.216                       51171     172.172.255.216                     443        Established Internet       5388
192.168.4.216                       51163     20.198.162.78                       443        Established Internet       13364
192.168.4.216                       51012     51.178.130.10                       27564      Established Internet       15472
0.0.0.0                             49673     0.0.0.0                             0          Listen                     1588
0.0.0.0                             49670     0.0.0.0                             0          Listen                     6028
0.0.0.0                             49668     0.0.0.0                             0          Listen                     3156
0.0.0.0                             49667     0.0.0.0                             0          Listen                     2832
0.0.0.0                             49666     0.0.0.0                             0          Listen                     2864
0.0.0.0                             49665     0.0.0.0                             0          Listen                     1444
0.0.0.0                             49664     0.0.0.0                             0          Listen                     1616
0.0.0.0                             5040      0.0.0.0                             0          Listen                     8472
192.168.4.216                       3389      192.168.4.202                       59319      Established Internet       2044
0.0.0.0                             3389      0.0.0.0                             0          Listen                     2044
192.168.4.216                       139       0.0.0.0                             0          Listen                     4
0.0.0.0                             135       0.0.0.0                             0          Listen                     1880


PS C:\WINDOWS\system32>
```

PowerShell commands

```
>  Get-NetTCPConnection | Sort-Object RemoteAddress
>  Get-NetTCPConnection -State 'Established'

>  Get-NetTCPConnection -State 'Established'
   | Select-Object -Property *
   ,@{Name = 'ProcessName'
   ;Expression = {(Get-Process -Id $_.OwningProcess).Name}}
```

Dos-Cmd

```
>  netstat
>  netstat -a
>  netstat -anb
```

MT4

```
PS C:\Users\Administrator> Get-NetTCPConnection | Sort-Object owningProcess

LocalAddress                        LocalPort RemoteAddress                     RemotePort State       AppliedSetting OwningProcess
------------                        --------- -------------                     ---------- -----       -------------- -----------
85.215.234.52                       52216     2.17.190.73                       80         TimeWait                   0
2a01:239:227:2500::1                52217     2a04:4e42:8d::684                 80         TimeWait                   0
85.215.234.52                       52213     20.190.159.4                      443        TimeWait                   0
85.215.234.52                       52214     2.17.190.73                       80         TimeWait                   0
85.215.234.52                       139       0.0.0.0                           0          Listen                     4
::                                  47001     ::                                0          Listen                     4
::                                  5985      ::                                0          Listen                     4
::                                  445       ::                                0          Listen                     4
85.215.234.52                       3389      176.97.210.106                    8100       Established Internet       328
85.215.234.52                       3389      92.42.15.193                      26323      CloseWait   Internet       328
85.215.234.52                       3389      193.111.248.57                    7153       Established Internet       328
85.215.234.52                       3389      146.19.191.29                     4253       Established Internet       328
85.215.234.52                       3389      185.137.233.87                    62908      CloseWait   Internet       328
85.215.234.52                       3389      87.170.78.195                     57931      Established Internet       328
85.215.234.52                       3389      212.102.57.206                    21915      Established Internet       328
85.215.234.52                       3389      80.75.212.2                       19118      Established Internet       328
85.215.234.52                       3389      194.180.48.88                     50866      Established Internet       328
0.0.0.0                             3389      0.0.0.0                           0          Listen                     328
::                                  3389      ::                                0          Listen                     328
85.215.234.52                       3389      113.105.164.28                    17962      Established Internet       328
::                                  49665     ::                                0          Listen                     484
0.0.0.0                             49665     0.0.0.0                           0          Listen                     484
::                                  49670     ::                                0          Listen                     616
0.0.0.0                             49670     0.0.0.0                           0          Listen                     616
::                                  49664     ::                                0          Listen                     628
0.0.0.0                             49664     0.0.0.0                           0          Listen                     628
0.0.0.0                             135       0.0.0.0                           0          Listen                     844
::                                  135       ::                                0          Listen                     844
::                                  49668     ::                                0          Listen                     1044
0.0.0.0                             49668     0.0.0.0                           0          Listen                     1044
0.0.0.0                             49666     0.0.0.0                           0          Listen                     1056
::                                  49666     ::                                0          Listen                     1056
::                                  49667     ::                                0          Listen                     1572
0.0.0.0                             49667     0.0.0.0                           0          Listen                     1572
0.0.0.0                             49669     0.0.0.0                           0          Listen                     2216
::                                  49669     ::                                0          Listen                     2216
85.215.234.52                       51482     149.5.84.116                      443        Established Internet       5336
0.0.0.0                             51481     0.0.0.0                           0          Bound                      5336
0.0.0.0                             51482     0.0.0.0                           0          Bound                      5336
85.215.234.52                       51481     149.5.84.116                      443        Established Internet       5336
::                                  49729     ::                                0          Bound                      5336
85.215.234.52                       52215     51.137.3.145                      443        Established Internet       5584
0.0.0.0                             52215     0.0.0.0                           0          Bound                      5584
```

```
RemoteAddress          : 149.5.84.116
RemotePort             : 443
PSComputerName         :
CimClass               : ROOT/StandardCimv2:MSFT_NetTCPConnection
CimInstanceProperties  : {Caption, Description, ElementName, InstanceID...}
CimSystemProperties    : Microsoft.Management.Infrastructure.CimSystemProperties
ProcessName            : terminal
```

fx flat

PowerShell commands

```
>  Get-Process | Sort-Object ProcessName | Format-Table

>  Get-Process | Sort-Object ProcessName
               | Format-Table -Property Id, ProcessName
```

```
RemoteAddress          : 35.177.17.179
RemotePort             : 443
PSComputerName         :
CimClass               : ROOT/StandardCimv2:MSFT_NetTCPConnection
CimInstanceProperties  : {Caption, Description, ElementName, InstanceID...}
CimSystemProperties    : Microsoft.Management.Infrastructure.CimSystemProperties
ProcessName            : terminal
```

Vantage Market

```
PS C:> netstat -anb

Active Connections

  TCP    10.3.0.4:50160         185.97.161.50:443      ESTABLISHED
 [terminal.exe]
  TCP    10.3.0.4:50161         185.97.161.50:443      TIME_WAIT
  TCP    10.3.0.4:50162         185.97.161.50:443      TIME_WAIT
```

GbeBrokers

```
LocalAddress                          LocalPort RemoteAddress                                                  RemotePort State       AppliedSetting OwningProcess
------------                          --------- -------------                                                  ---------- -----       -------------- -------------
10.3.0.4                              50292     168.63.129.16                                                  80         TimeWait                   0
::                                    47001     ::                                                             0          Listen                     4
::                                    5985      ::                                                             0          Listen                     4
::                                    445       ::                                                             0          Listen                     4
10.3.0.4                              139       0.0.0.0                                                        0          Listen                     4
0.0.0.0                               3389      0.0.0.0                                                        0          Listen                     504
10.3.0.4                              3389      87.170.78.195                                                  65124      Established Internet       504
::                                    3389      ::                                                             0          Listen                     504
0.0.0.0                               49665     0.0.0.0                                                        0          Listen                     608
::                                    49665     ::                                                             0          Listen                     608
::                                    49670     ::                                                             0          Listen                     748
0.0.0.0                               49670     0.0.0.0                                                        0          Listen                     748
0.0.0.0                               49664     0.0.0.0                                                        0          Listen                     764
::                                    49664     ::                                                             0          Listen                     764
0.0.0.0                               135       0.0.0.0                                                        0          Listen                     976
::                                    135       ::                                                             0          Listen                     976
0.0.0.0                               50278     0.0.0.0                                                        0          Bound                      1056
10.3.0.4                              50278     169.50.82.231                                                  7443       Established Internet       1056
10.3.0.4                              50277     169.50.82.231                                                  7443       Established Internet       1056
0.0.0.0                               50277     0.0.0.0                                                        0          Bound                      1056
::                                    49666     ::                                                             0          Listen                     1084
0.0.0.0                               49666     0.0.0.0                                                        0          Listen                     1084
::                                    49667     ::                                                             0          Listen                     1728
0.0.0.0                               49667     0.0.0.0                                                        0          Listen                     1728
::                                    49668     ::                                                             0          Listen                     2412
0.0.0.0                               49668     0.0.0.0                                                        0          Listen                     2412
::                                    49669     ::                                                             0          Listen                     2800
0.0.0.0                               49669     0.0.0.0                                                        0          Listen                     2800
10.3.0.4                              50349     4.208.165.245                                                  443        Established Datacenter     3052
0.0.0.0                               50349     0.0.0.0                                                        0          Bound                      3052
10.3.0.4                              49805     168.63.129.16                                                  32526      Established Datacenter     4832
0.0.0.0                               49805     0.0.0.0                                                        0          Bound                      4832
10.3.0.4                              49786     168.63.129.16                                                  32526      Established Datacenter     5400
0.0.0.0                               49798     0.0.0.0                                                        0          Bound                      5400
0.0.0.0                               49799     0.0.0.0                                                        0          Bound                      5400
10.3.0.4                              49798     168.63.129.16                                                  80         Established Datacenter     5400
0.0.0.0                               49786     0.0.0.0                                                        0          Bound                      5400
```

ActivTrades