

These analysed events occurred when a block connection firewall rule was triggered for chrome.exe. Key information from these events include:

- Application Name: The application attempting the connection, in this case chrome.exe
- Direction: In this case outbound, meaning the host initiated the connection
- Source/Destination Address: IPv6 addresses for host and destination
- Source/Destination Port: Source Port is a custom port, while destination is 443, which is for HTTPS. This is expected from an attempted connection from a browser
- Protocol being 17 seems unusual as this stands for UDP while HTTPS is generally a TCP process. This is likely because the connection could not establish the TCP handshake due to the connection being blocked by the firewall

```
Application Information:
    Process ID:          18232
    Application Name:     \device\harddiskvolume3\program file
s\google\chrome\application\chrome.exe

Network Information:
    Direction:           Outbound
    Source Address:
1
    Source Port:          63035
    Destination Address:
    Destination Port:     443
    Protocol:             17
    Interface Index:      11
```

Figure 1: Example Connection Blocked Event (Source/Destination Addresses Covered Up)