How to avoid "unstable connection"

Why this is happening?

You may have noticed some screen with the “unstable connection” warning sign. This situation happens when the real-time communication channel between the screen and the server is dropped. The real-time communication is needed in order to get screen status or other information as well as sending orders to the display (turn on, turn off, change content, get a screenshot, reboot, etc.). The main root cause of this issue is the firewall configuration and can be solved easily most of the time.

Firewalls known to be concerned by this problem + solutions

Fortinet Fortigate

Fortigates have a default setting of five minute TTL’s for TCP sessions; active sessions that have no packet movement simply get dropped. That parameter cannot be adjusted via the web interface, you have to use the CLI. Here’s an example of how to adjust the TTL to 86400 seconds for the concerned rule, along with a default of ten minutes for everything else:

```
config system session-ttl
    set default 600
        config port
            edit 123
                set protocol 6
                set timeout 86400
                set end-port 80
                set start-port 80
            next
        end
end
```

The “123” after the edit simply means the rule number; it has nothing to do with the port which is set within the rule as a range. The protocol is 6 for TCP.

Stonesoft

The problem on stonesoft firewall can easily be fixed by turning off the **“Deep Inspection”** and switching the **“Connection tracking mode”** to **“Loose”**

With certain Proximus routers

Switching the connection of screens to https instead of http fixes the problem.

Bluecoat Proxy / Firewall

It has been noticed that bluecoat proxy antivirus module regularly close the channel to do its scanning job. If turning off the antivirus is not an option for you, consider to switch the connection of screens to https instead of http fixes the problem.

Other firewalls?

Please consider trying to adjust or disable following modules for the zebrix create rule:

- http antivirus module - WebFilter / contentFiltering - DLP module - SSL Inpection - Deep Packet Inspection - Connection Tracking - transparent proxy - adjusting TTL (Time-to-live) or Timeout.

Alternatively, you can try to https instead of http or http over TCP6001 instead of http over TCP80 (Firewall might be more permissive)