Sentinel Product Line IP Address Filtering

The Sensaphone Sentinel line of products relies on DNS resolution to ensure access to required resources for monitoring, logging, and generating alarms. IP-based filtering will cause your device to go offline when changes are made to upstream addresses for our infrastructure.

Our recommended configuration for the Sentinel line of products requires unrestricted outbound access on TCP port 443 for communications with our infrastructure. Your device must be able to successfully resolve DNS to guarantee that it can reach required resources. Hostname based filtering can be implemented if required by your security policy. The hostnames used by the Sentinel product line to access Sensaphone infrastructure are listed below:

Sensaphone Infrastructure (TCP port 443)

- `stud1.sensaphone.net`
- `stud2.sensaphone.net`
- `stud3.sensaphone.net`
- `stud4.sensaphone.net`
- `hitch1.sensaphone.net`
- `hitch2.sensaphone.net`
- `hitch3.sensaphone.net`
- `hitch4.sensaphone.net`

Your Sentinel/Sentinel Pro must be able to successfully resolve DNS for any of these addresses to ensure uninterrupted device functionality and fail-over, in case of upstream infrastructure changes.

Alternatively, if your security policy allows, your Sentinel product can be placed in your network DMZ (Demilitarized Zone), allowing unrestricted access to the internet while maintaining separation from your internal network. Refer to your firewall or security appliance documentation for further information.

Sentinel Family Product Line

- Sentinel
- Sentinel Pro
- Stratus EMS