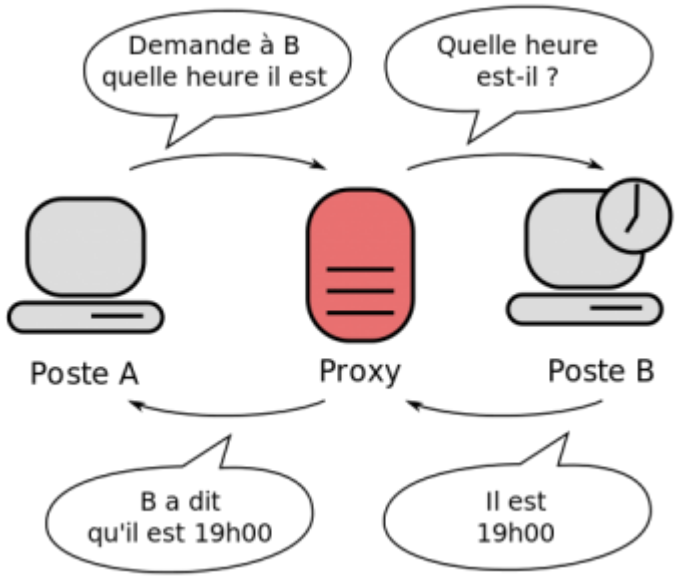
Why is it not recommended to use a zebrix screen through a proxy?

Reminder of the role of a proxy

“A proxy is a computer software component that acts as an intermediary by placing itself between two hosts to facilitate or monitor their exchanges.” - wikipedia definition



Proxy servers are used in particular to provide the following functions:

- acceleration of navigation: cache memory, data compression, filtering of ads or heavy content (java, flash) ;
- logging of requests;
- security of the Internet user: antivirus;
- content and site filtering (white list, black list, banning by keywords, by file type).

Why is the use of a zebrix screen through a proxy not recommended?

The proxy is a security device mainly intended to protect the company from risky behaviors (voluntary or involuntary) that employees could adopt: surfing on risky sites, downloading malicious files, visiting forbidden websites from the workplace.

The control, caching and compression mechanisms of the proxy alter the http connection and do not always work well with equipment that uses the http protocol as a generic TCP channel.

Zebrix relies on HTML5 and its new standards, for example websockets and SSE connections, which have the particularity of opening HTTP channels with infinite timeouts. Proxies or pro security

modules integrated in some firewalls are unfortunately not tolerant of these new mechanisms (the proxy will tend to cut the connections to do its caching work, the same for antivirus and content filtering modules, tracking connection modules will tend to redefine their own timeout...).

What are the known problems when using a proxy with zebrix?

The problems found differ depending on the proxy technology used and its settings. However, the following recurring problems have been reported:

- Unreliable connection status (the screen appears disconnected when it is connected or vice versa)
- Content update takes several minutes when it should be instantaneous
- Updating of dynamic data sources (datasource) is not done or is done with a significant delay.
- Video playback does not work
- Displaying security messages (from the proxy) on top of the zebrix application
- Requests for a username and password instead of the zebrix application
- screenshot function not working
- etc.

Using zebrix through a proxy is not recommended or even discouraged

The right way to go

Open port 80 or 443 to the zebrix server IP:

screenv2.zebrix.net - 46.105.174.70

Source IP address	Source port	Destination IP address	Destination port
any	**any**	**46.105.174.70 (screenv2.zebrix.net)**	**TCP 80 or 443**

In this configuration, zebrix screens do not have access to the entire internet, it is a very targeted port opening to the zebrix servers. For an optimal level of security, partitioning the displays within a VLAN (without access from or to the LAN) is also a good practice. In this context, not using a proxy does not degrade the security level of your company.

What to do if it is not possible to bypass the proxy

If the proxy is unavoidable on the default port http (80) or https (443), it is possible to connect to zebrix through TCP port 6001 or 6002. Again, since the port opening in your firewall is very restrictive, it will not degrade the security level of your network

Source IP address	Source port	Destination IP address	Destination port
any	**any**	**46.105.174.70 (screenv2.zebrix.net)**	**TCP 6001-6002**

What if I want to display web content (web area) that requires going through a proxy?

It is possible to configure a proxy server in the external players and add an exception on *.zebrix.net, the communication to zebrix will be done without proxy. The rest of the loaded web content will be regulated by the proxy.