Table of Contents

General description

The Allow-list specifies the only available for a subscriber sites and pages. Its functionality includes redirection of a subscriber to the specified page on attempt to get resources outside this list. Redirection is only possible for HTTP requests, all HTTPS requests outside the access list are blocked without redirection. Most operating systems and browsers request HTTP resources at startup to determine if the Internet is available and to find the Captive Portal page.

Application example:

1. Captive Portal with access to payment systems
   In this case, the subscriber, when trying to access the Internet, is redirected to a page with a notification about the lack of funds and is given the opportunity to deposit them into the account. If necessary, further transfer to the sites of payment systems or banks is possible.
2. Captive Portal for public Wi-Fi networks
   SSG provides redirecting to the Captive Portal which handles user authorization by phone number (either SMS or Caller ID).
   Automation of this process and configuration of the Wi-fi portal is implemented using the HotSpot section of the GUI.

Performance Features:

1. Service 5 and 16 (Allow Lists and Captive Portal) regulate access to TCP-based protocols only. To allow only HTTP, HTTPs protocols, it is necessary to combine the allow-lists with protocol restriction list.
2. The allow list is formed on the basis of URL, SNI, CN, IP, which allows to include sites accessible via HTTPS, HTTP and specific local resources into the allowed resources.
3. Service 5 requires mandatory establishment of TCP connection for redirection, i.e. for private IP addresses it is necessary to provide Internet access and assign NAT service.
4. Service 16 does not require a TCP connection. SSG responds to TCP SYN requests and performs HTTP redirect in case of access to resources outside the access list.