Proxy

Proxy

Setting up a direct connection to the proxy server.

Proxy Server for Web Traffic

You do not need to explicitly specify the proxy settings on the LAN hosts. Specifying UTM as the default gateway for devices on the network is sufficient.

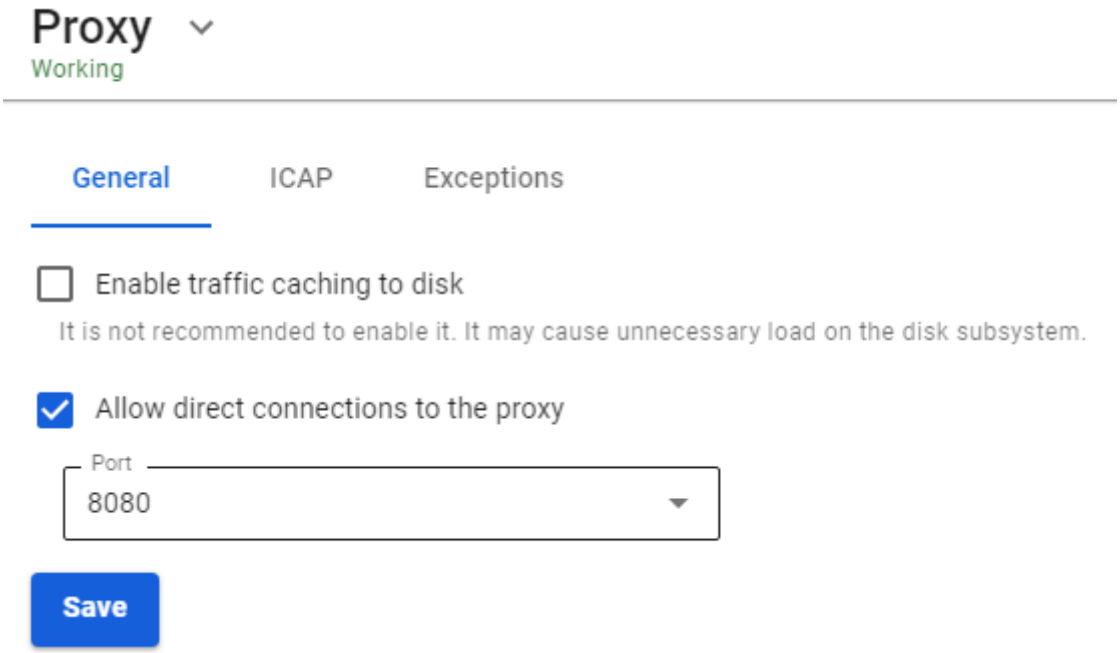
By default, caching of traffic to disk is disabled, but it is carried out in the server RAM. You can enable caching of web traffic to disk in **Services -> Proxy**, but we do not recommend doing this because of excessive load on the disk subsystem. As a rule, caching to RAM is sufficient.

Direct connections to the proxy server can be configured by checking the corresponding box in the section **Services -> Proxy** and specifying the IP address and port on the UTM side. Then these details should be specified on those LAN network devices whose web traffic needs to be passed through a proxy.

To configure HTTPS traffic filtering, you need to add a root UTM certificate to users' computers.

Read more in the article on **Setting up HTTPS filtering**.

Below is a screenshot of the **General** tab in the **Proxy** section.



Role of Proxy Server in the Operation of SafeUTM Gateway

The proxy server, in addition to proxying web traffic, plays the role of a master service for several services related to processing, monitoring, and accounting for user web traffic on the gateway, namely:

- Antivirus for web traffic (ClamAV).
- Web traffic reporting service for users.
- Content filter.

Direct Connections to Proxy Server

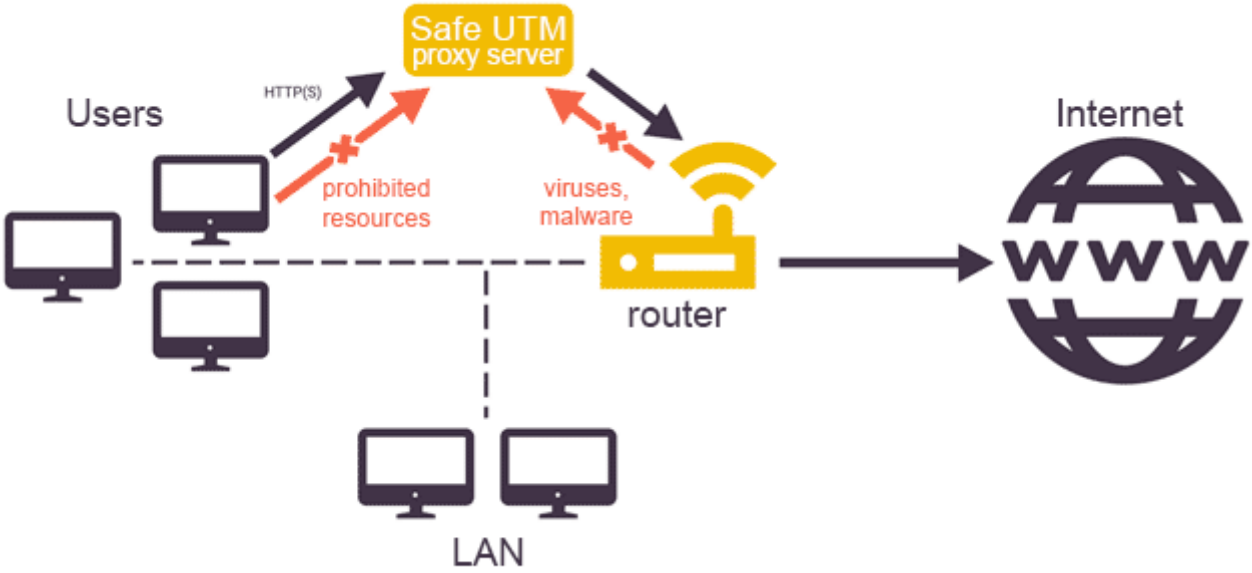
This mode is used when SafeUTM is not the default gateway for network clients.

Setting up the mode

- Specify the SafeUTM local IP address as a web proxy on the local network on client devices. It is possible to use a proxy server for all protocols.
- In the proxy settings on SafeUTM, the IP address and port for direct connections to the proxy must be specified (you can select ports from the list: 3128, 1080, 8000, 8080, 8888, 8081, 8088, and 10080).

In this mode, UTM will be able to provide hosts with web content and traffic on other ports (by default on all, if necessary, you can close the ports with a firewall), in case of necessity performing accounting (quotas), monitoring and checking web traffic for viruses, content and malicious content if the following conditions are met:

- SafeUTM server has Internet access (its external interface must be in a range that does not overlap with the local subnet and have access to the Internet).
- Authorization of the web traffic consumer host on the UTM server by one of the authorization types supported by UTM.
- Explicit indication of the web proxy address to the host (in the proxy server settings in browsers). For **Single Sign-On** authorization via Active Directory, you must specify the SafeUTM domain name in the settings, and not its IP address.



If it is not possible to specify a proxy server in the program settings for Windows or Mac OS X, then you can use third-party software to route all workstation traffic to the proxy server. For example, **Proxifier** provides such an opportunity. For more information on how to **configure Proxifier for direct connections to the proxy server,** see an article by following the **link**.

Exclusion of Resources from Proxy Server Processing

On the **Exceptions** tab, it is possible to exclude resources from processing by the proxy server and all related services (content filter, web reporting, antiviruses).

- **Source Networks:** The proxy server is excluded from processing requests from the specified internal networks or IP addresses.
- **Destination networks:** The proxy server is excluded from processing requests to external networks or IP addresses (usually addresses of websites or web services).

We strongly discourage you from excluding the ENTIRE LAN from proxy server processing.

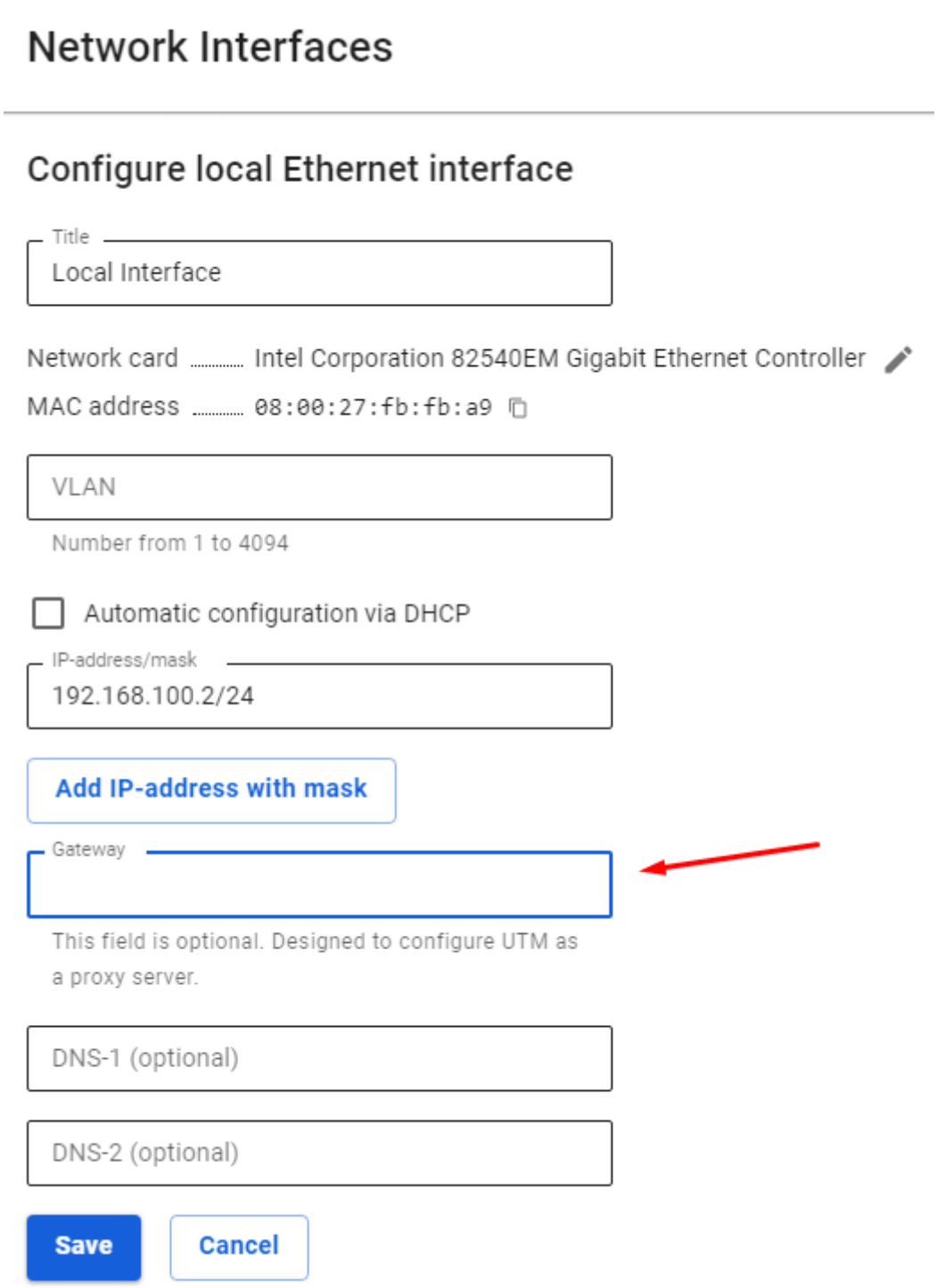
When connecting directly to a proxy server, traffic cannot be excluded from proxy processing. You need to exclude traffic in the proxy server settings on the device (in the web browser or the proxy server system settings).

Configuring Proxy with Single Interface

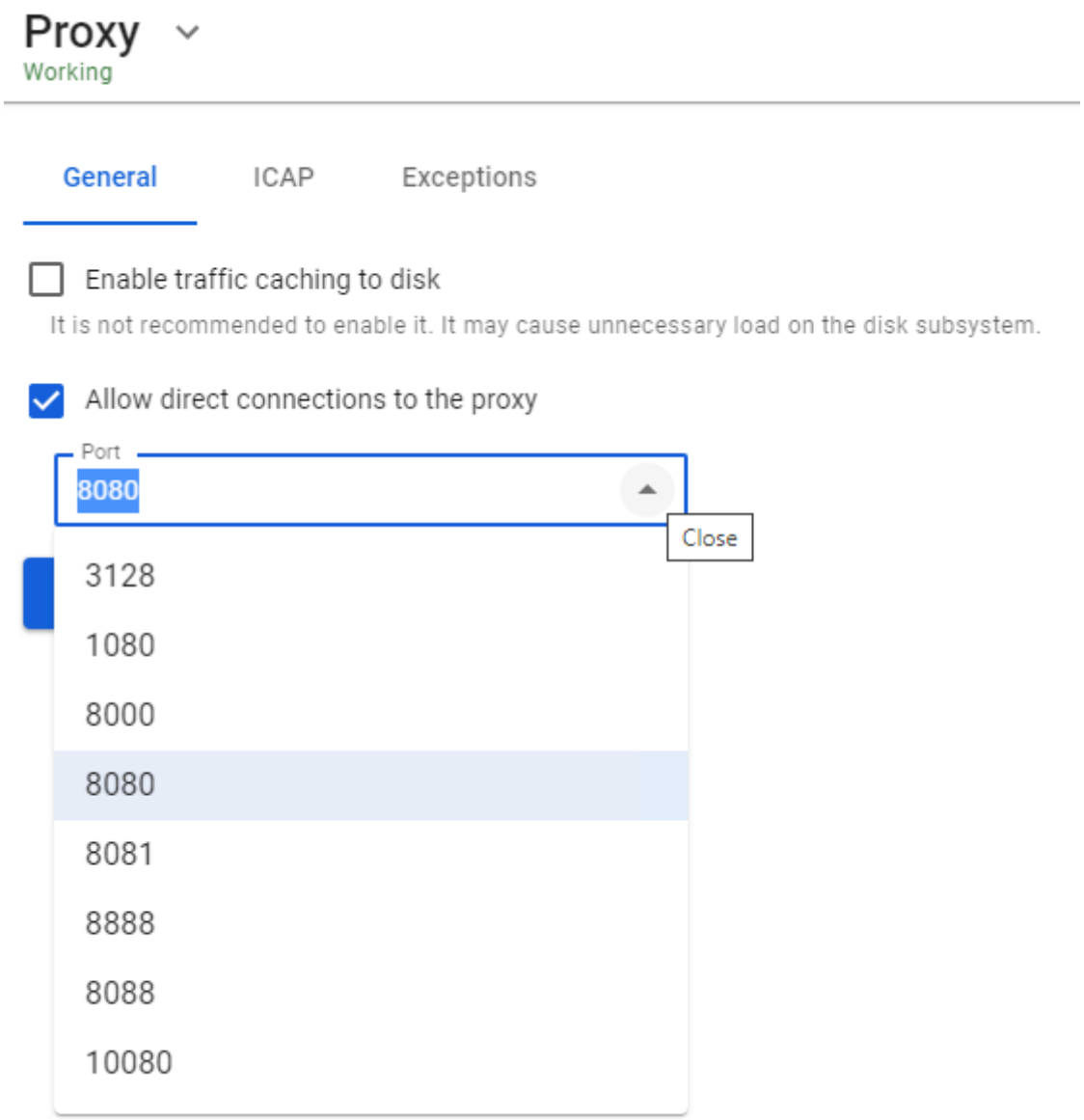
If necessary, you can use SafeUTM as a proxy server with direct connections of clients to the proxy, with a single interface.

To do this, you need to perform the following settings:

1. When creating a local interface in **Services -> Network interfaces, Gateway** needs to be specified:



2. Allow direct connections to the proxy server on the tab **Services -> Proxy** by selecting the desired port from the list:



When using SafeUTM as a proxy server with direct connections to the proxy, most of the functions will work normally, but with some peculiarities:

- In the firewall rules for users, it is necessary to specify INPUT paths instead of FORWARD.
- In-depth traffic analysis by the intrusion prevention system and the application control module will be carried out only for traffic passing through the proxy server (part of the rules will not work).
- Exceptions from the proxy server must be made by means of the browser or routes on the end devices. Settings on tab **Services -> Proxy -> Exceptions** apply only to the transparent mode of operation of the proxy server.

Exclude IP Addresses from Proxy Server Processing

Setting up exceptions for the traffic of individual users or traffic to certain Internet resources from passing and processing by a web proxy available as part of UTM.

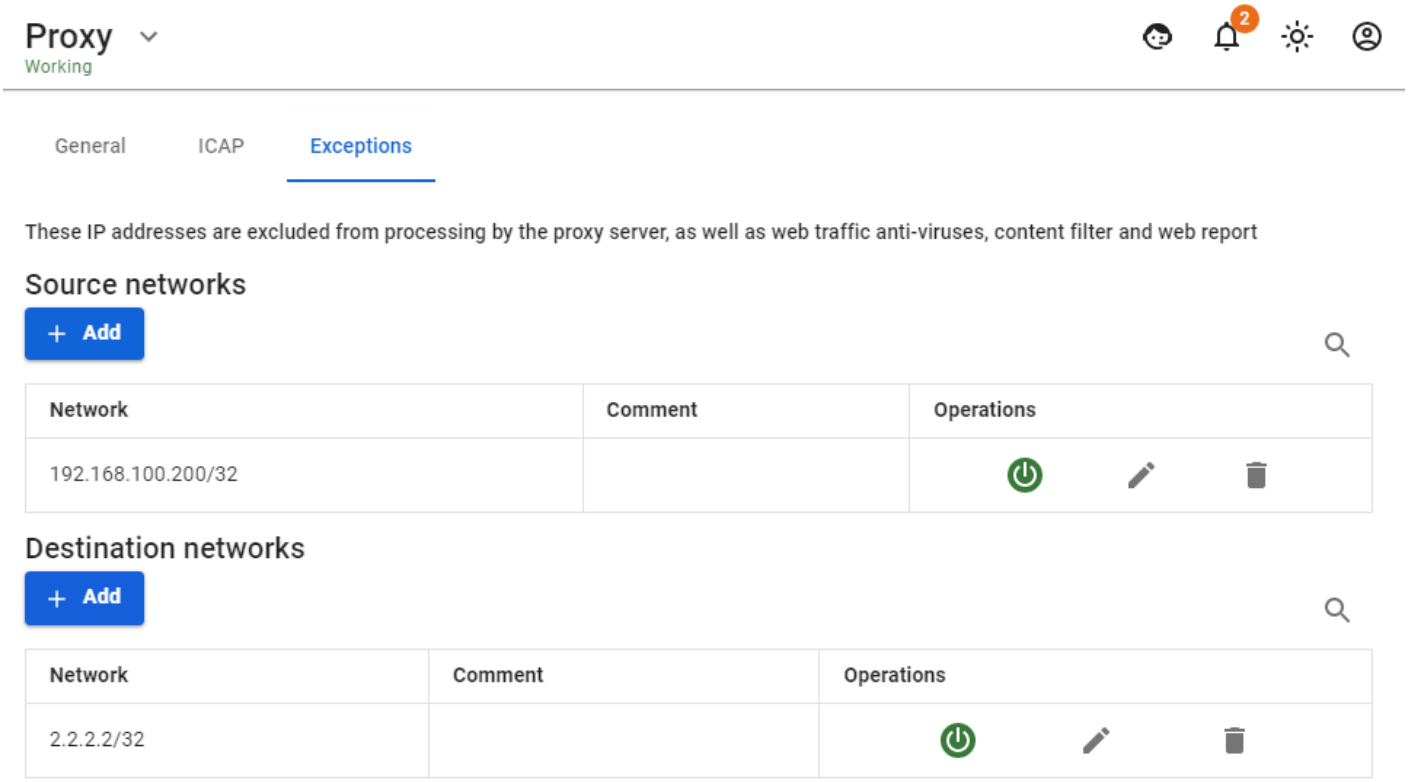
> Resource exclusions from proxy server processing only work for transparent proxy mode. With direct connections to the proxy server, it is impossible to exclude anything from proxy processing.

Two types of exceptions can be configured:

- Exclusion of traffic of local UTM network hosts directed externally from proxy processing (**Source networks**).
- Exclusion of traffic of all hosts in the local network served by UTM to certain resources in external networks (**Destination networks**).

You can only specific IP addresses or IP networks.

Traffic excluded from proxy processing will not participate in **Reports**, and also cannot be tested for viruses and processed by the **Content filter** module. At the same time, such traffic will be checked by a firewall, intrusion prevention services, and application control.



Programs Running on Protocols Other Than HTTP(S) via Web Proxy

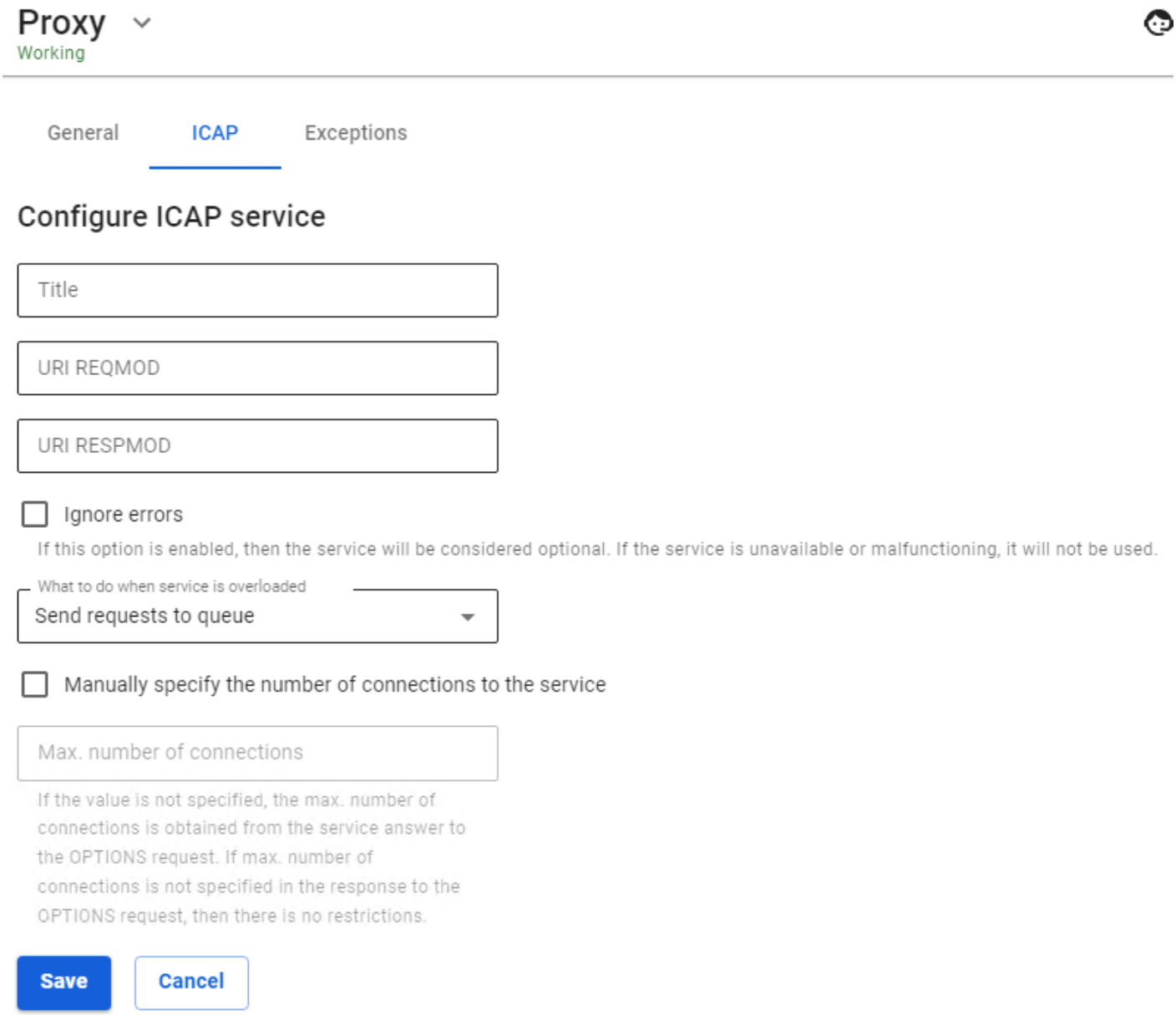
Some programs that send traffic to their servers on ports 80 and 443, but at the same time work on protocols other than HTTP(S), cannot be processed by a web proxy server on UTM with HTTPS traffic filtering enabled. The traffic of such programs should be excluded from proxy processing in the **Destination networks** field.

Connecting to External ICAP Services

Sending HTTP(S) traffic for analysis to third-party servers using ICAP protocol.

In this case, traffic to these servers (which may include DLP systems, antiviruses, and web filters) is transmitted in decrypted form.

You can configure the connection to servers via ICAP in **Services -> Proxy** on the **ICAP** tab.



It is possible to establish a connection to several ICAP services simultaneously.