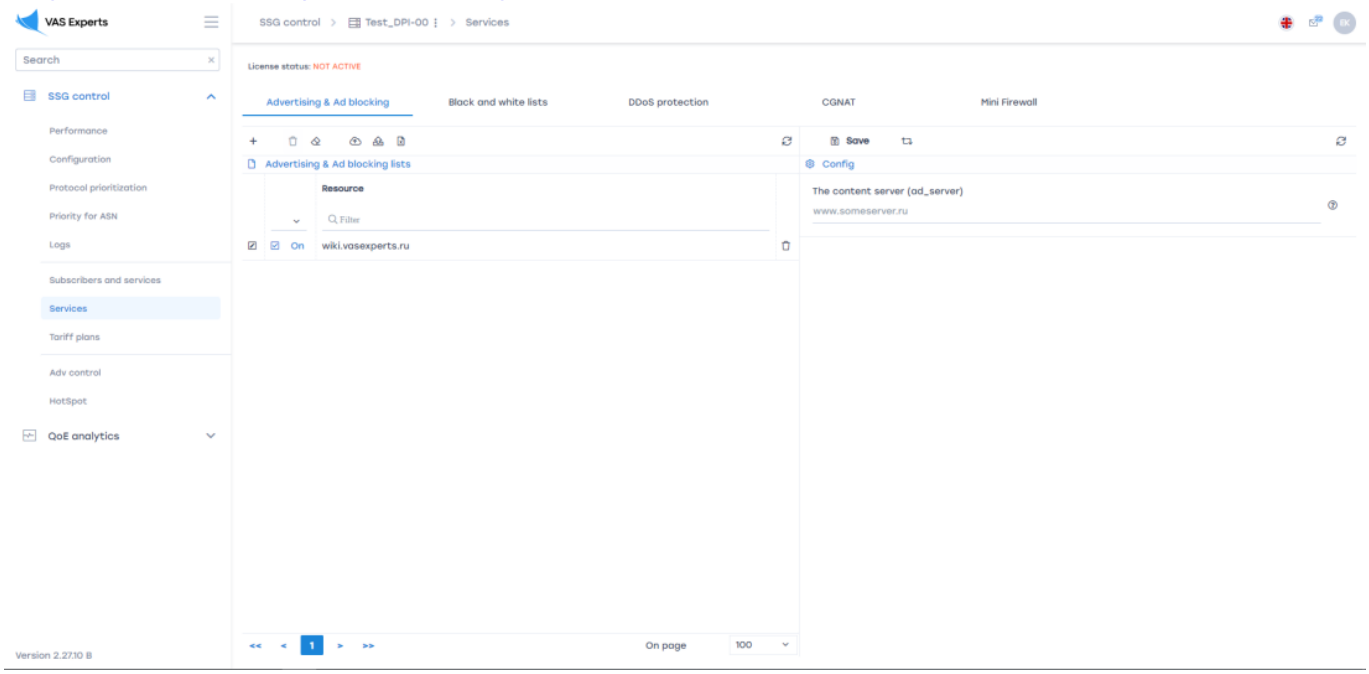
Содержание

Services 3

Services

- Blacklist/Whitelist
- PCAP entry
- Mini Firewall
- Entry L2 BRAS
- L3 BRAS Entry
- CG NAT
- Protection against DOS and DDOS attacks
- Caching
- Subscriber notification
- Ad blocking and replacing
- Reward Program

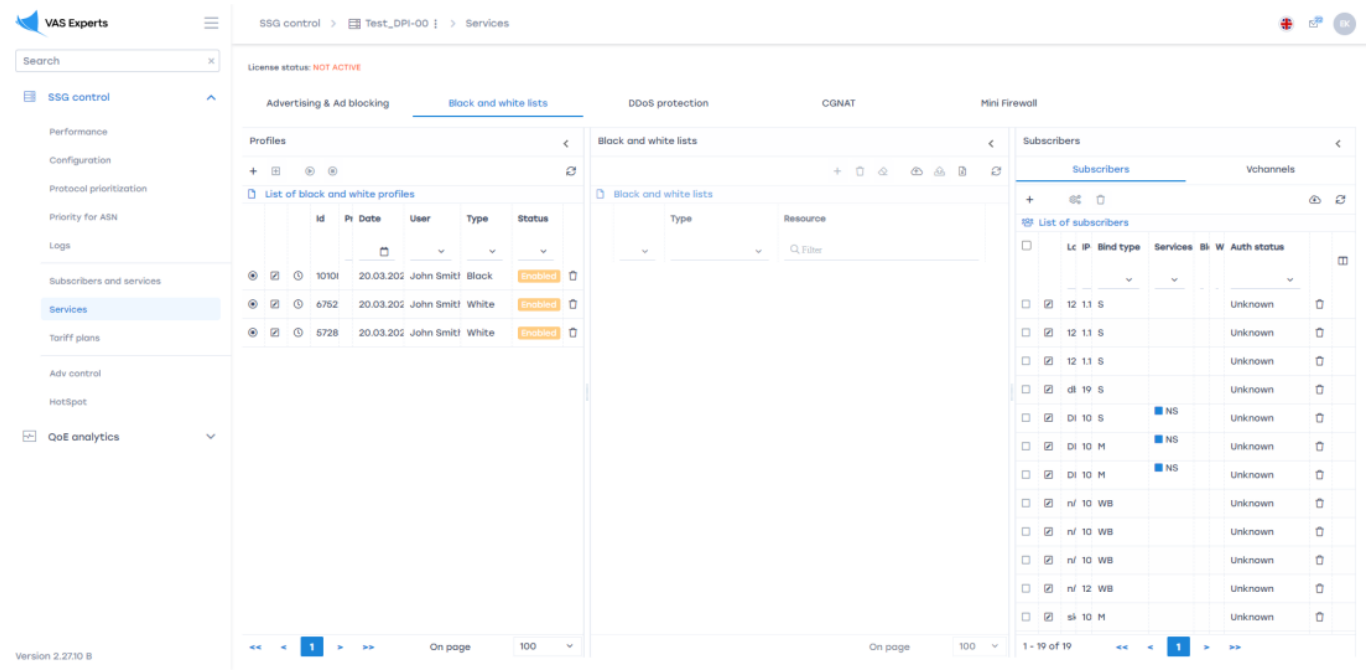
To go to the section, open the "Manage services" menu and click "Services".



Block lists/Allow lists

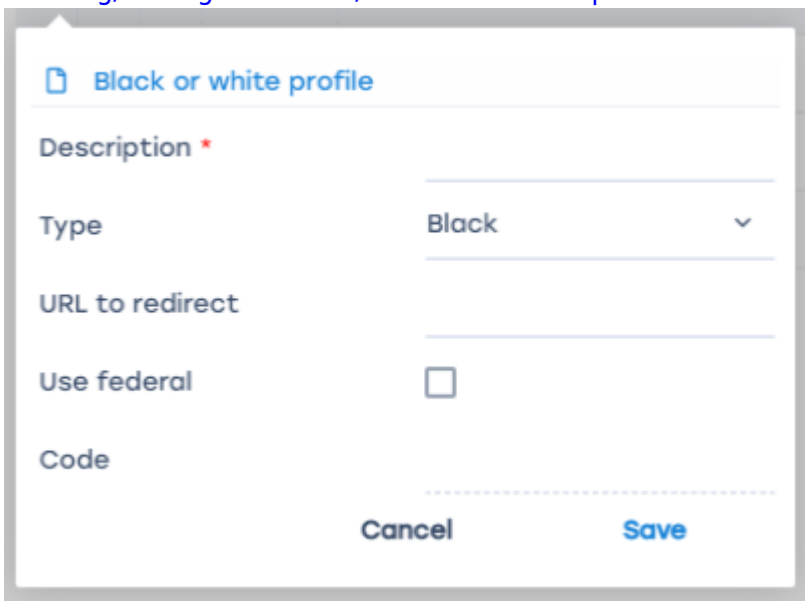
This section appeared in version 2.1.5.

The section looks like the picture below.



Block list/Allow list profiles

Here you can create block list/allow list service profiles, as well as edit and delete them. The form for creating/editing a blocklist/allow list service profile is shown in the figure below.



The form allows you to enter the following parameters:

- Profile name
- Select profile type (Block list/Allow list)
- URL to redirect

You can only manage Block list/Allow list service profiles for one selected equipment.

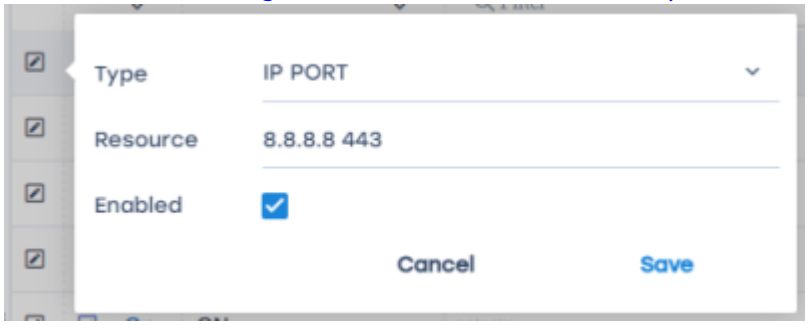
Subscribers of Block/Allow Lists

It is described in detail in the section Subscribers and Services

Block list/Allow list Resources

Here you can add resources to the selected Block list/Allow list profile. As well as edit and delete resources added to the profile.

The resource editing form in the Block/Allow Lists profile is shown in the figure below.

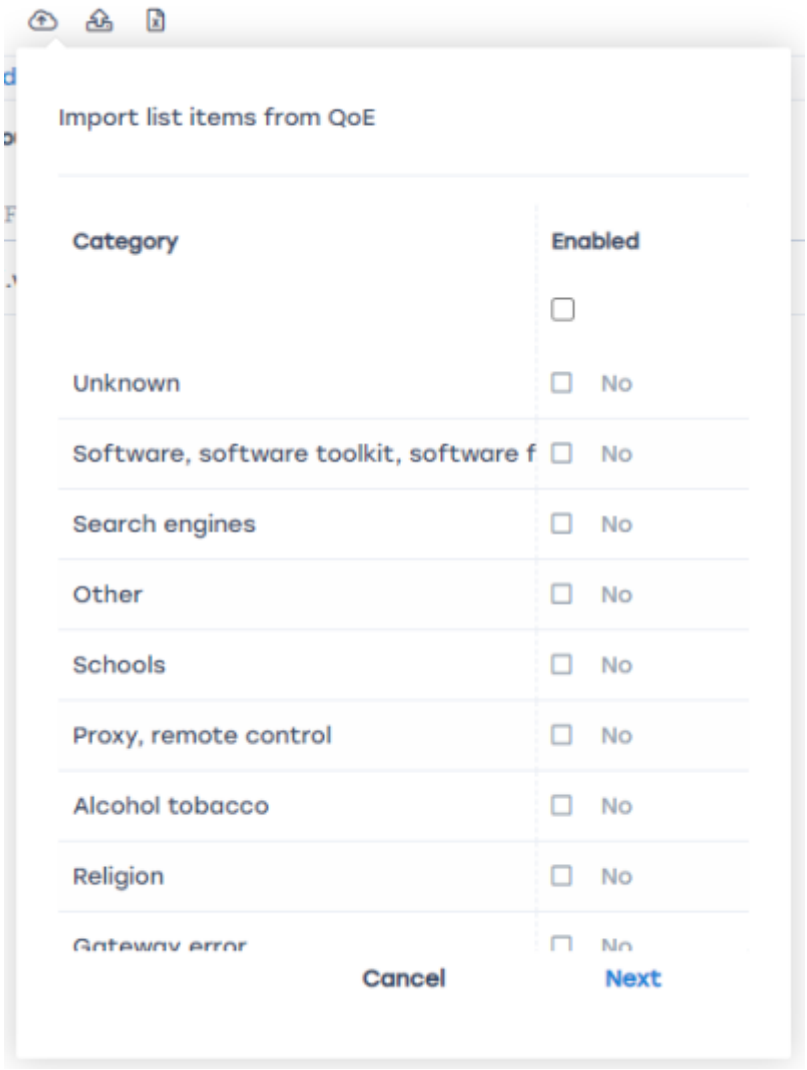


The form allows you to enter the following parameters:

- Resource type (SNI, URL, IP, CN)
- Resource
- Status (Enabled / Disabled)

Import resources by category from QoE

The form for importing resources by category from QoE is shown in the figure below.



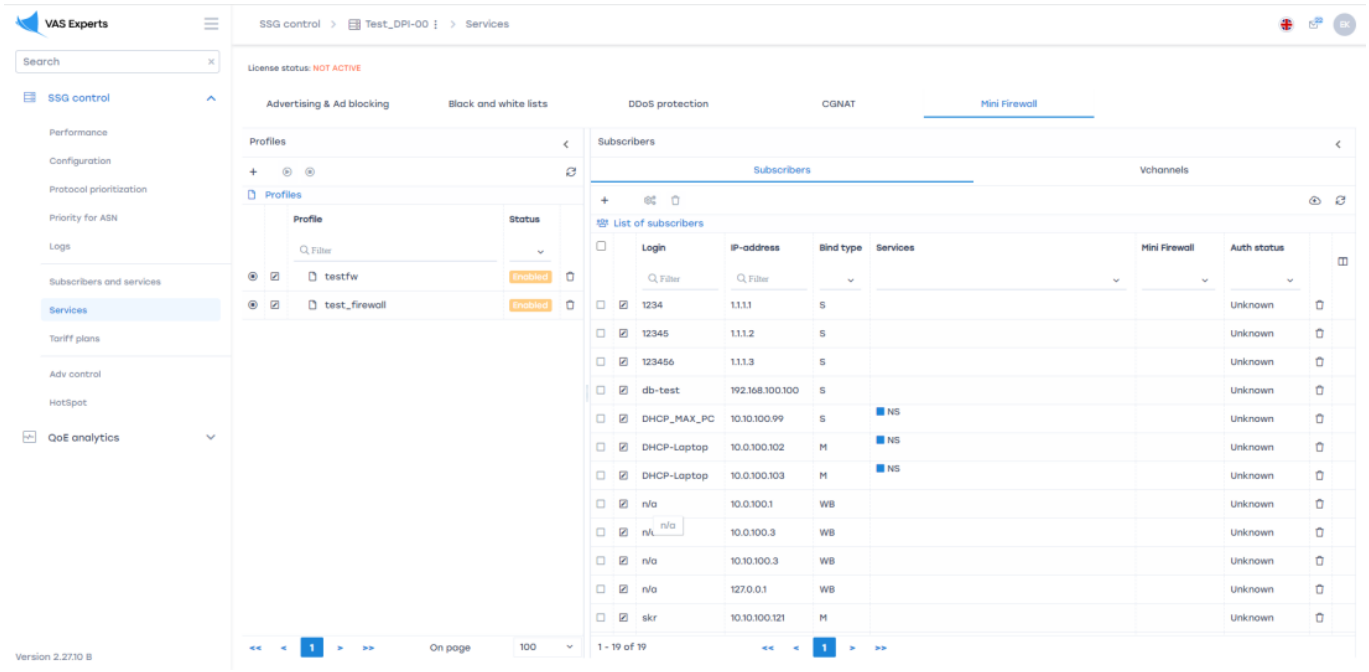
PCAP entry

In developing.

Mini Firewall

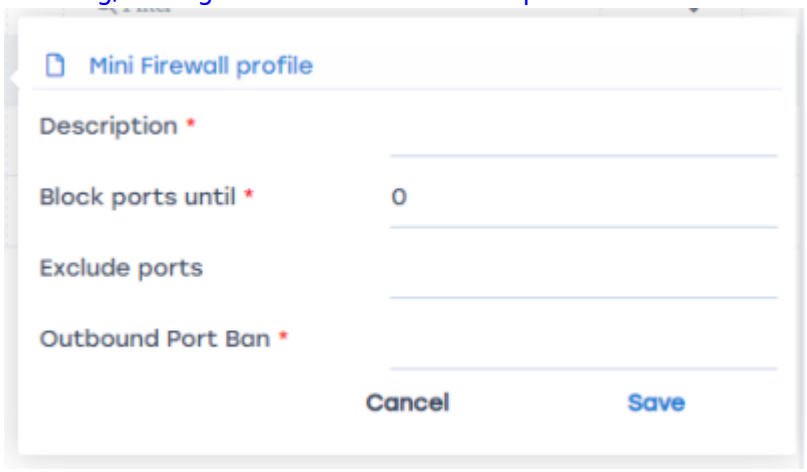
This section appeared in version 2.x.x.

The appearance of the section is shown in the image below.



Mini Firewall Profiles

Here you can create profiles for the Mini Firewall service, as well as edit and delete them. The form for creating/editing a Mini Firewall service profile is shown in the figure below.



The form allows you to enter the following parameters:

- Profile name
- Block ports up to (**max_port**) - Port number below which access is blocked
- Exclude ports (**port_holes**) - List of ports that are allowed to access bypassing the **max_port** restriction
- Deny outgoing ports (**out_port**) - list of ports to which outgoing traffic is closed

You can only manage block list/allow list service profiles for one selected equipment.

Connecting / disconnecting a profile to subscribers

It is described in detail in the section Subscribers and services

L2 BRAS

In developing.

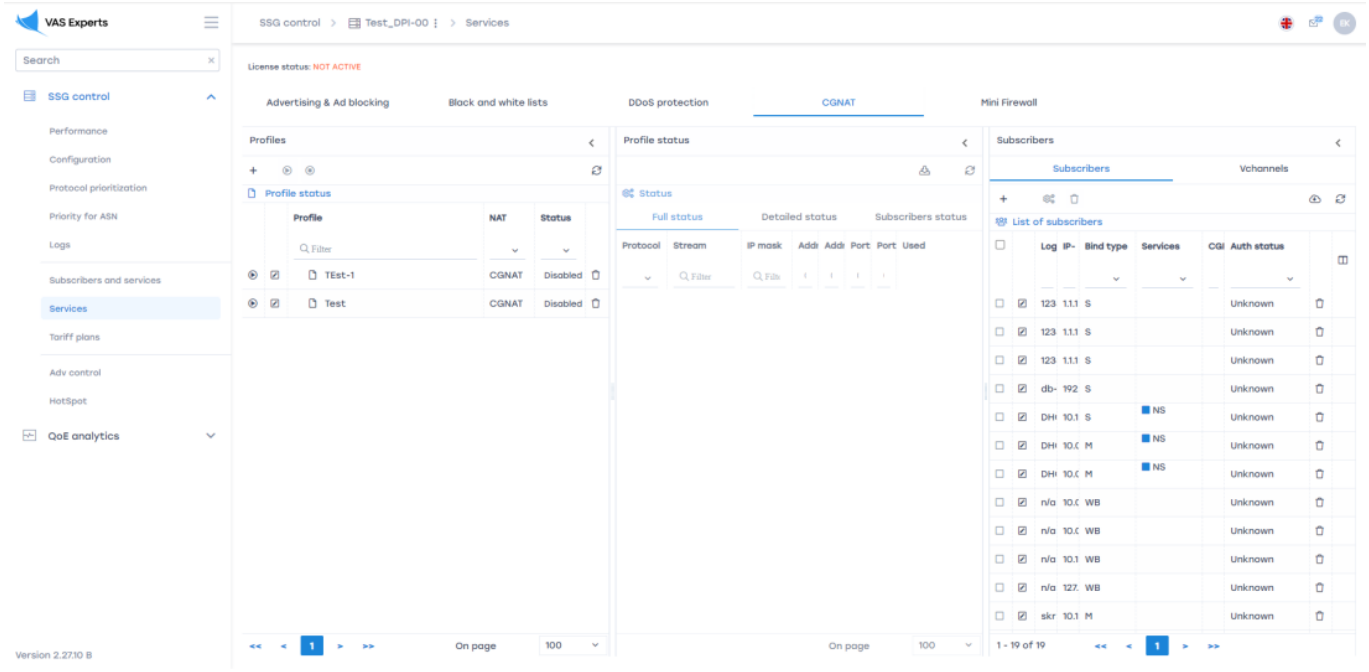
L3 BRAS

In developing.

CG NAT

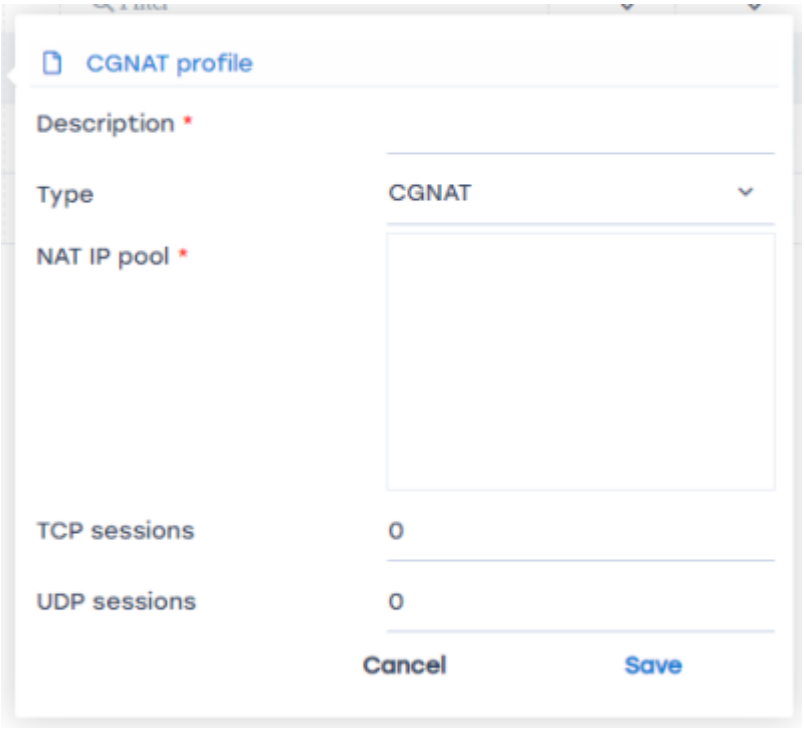
This section appeared in version 2.4.0.

The appearance of the section is shown in the image below.



CG NAT profiles

Here you can create profiles for the CG NAT service, as well as edit and delete them. The form for creating/editing a CG NAT service profile is shown in the figure below.



The form allows you to enter the following parameters:

- Profile name
- Select profile type (CGNAT / 1:1)
- Nat IP pool (CIDR)
- Number of TCP and UDP sessions (if profile type is CGNAT)

You can only manage block list/allow list service profiles for one selected equipment.

General profile status

This tab displays the general status of the profile:

- Protocol used
- Thread number
- Max IP
- Total number of addresses
- Used number of addresses (for profile type 1:1)
- Total number of ports (for CGNAT profile type)
- Number of ports used (for CGNAT profile type)

Detailed profile status

This tab displays detailed status by profile:

- Protocol used

- Thread number
- Max IP
- White IP address from the pool
- Total number of ports
- Number of ports used

Detailed profile status

This tab displays detailed status by profile:

- Protocol used
- Thread number
- Max IP
- White IP address from the pool
- Total number of ports
- Number of ports used

Profile subscriber status

This tab displays detailed status by profile:

- Gray IP address of the subscriber
- White IP address of the subscriber
- Number of subscriber TCP sessions
- Number of UDP sessions of the subscriber

Connecting / disconnecting a profile to subscribers

It is described in detail in the section Subscribers and services

Protection against DOS and DDOS attacks

In developing.

Caching

In developing.

Notifying subscribers

In developing.

Blocking and replacing ads

In developing.

Bonus program

In developing.