2024

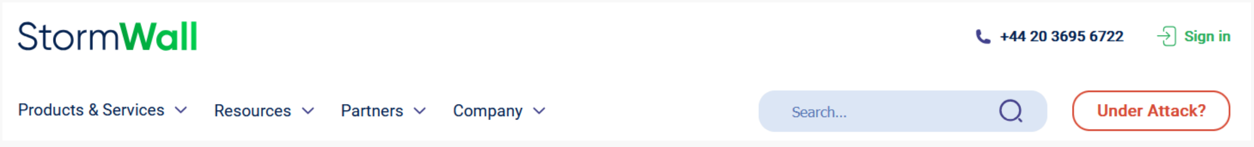
User Guide

Getting Started

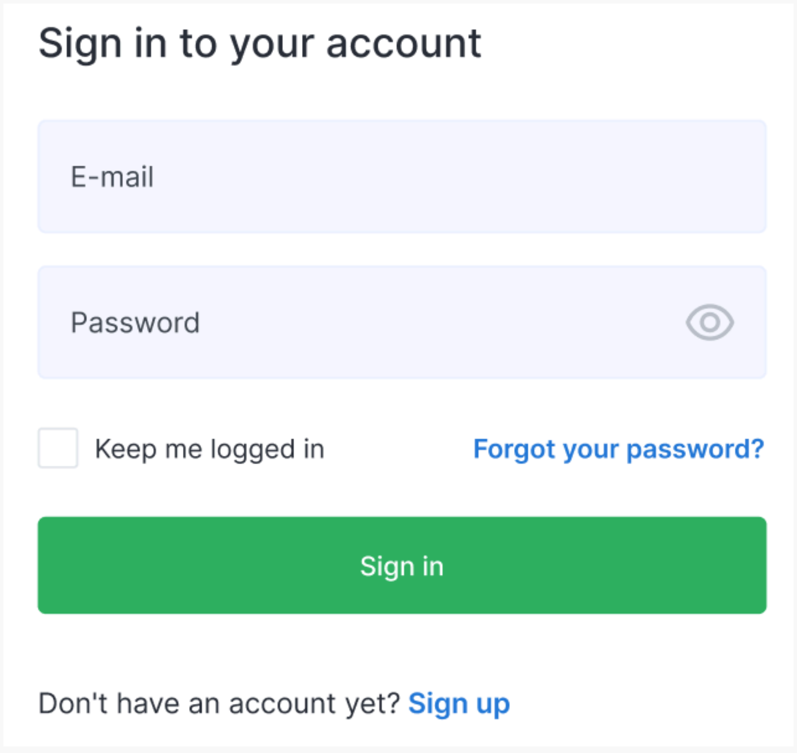
How to Register for Your StormWall Client Portal?

To access StormWall protection, registration as a new user is required.

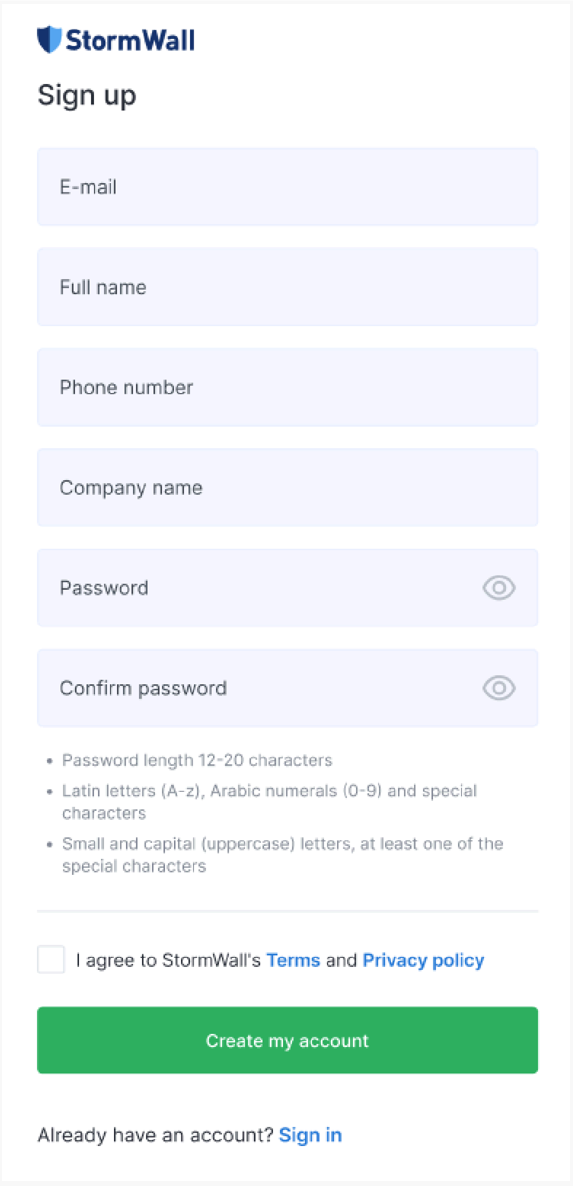
Start by navigating to the StormWall website, then find the **Sign in** button located in the top right corner of the homepage.



Click on the **Sign in** button to open the form.



Inside the form, locate and click on the **Sign up** button to initiate the signup process.



StormWall

Sign up

E-mail

Full name

Phone number

Company name

Password

Confirm password

- Password length 12-20 characters
- Latin letters (A-z), Arabic numerals (0-9) and special characters
- Small and capital (uppercase) letters, at least one of the special characters

□ I agree to StormWall's Terms and Privacy policy

Create my account

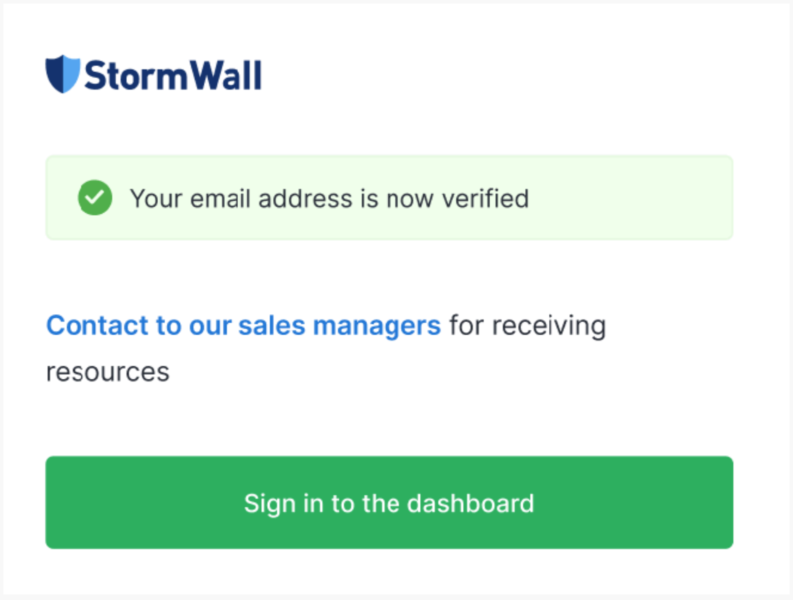
Already have an account? Sign in

Fill out the registration form:

- E-mail;
- Full name;
- Phone number (optional);
- Company name;
- Password: Choose a secure password;
- Confirm password: Re-enter your chosen password.

Make sure to review the Terms of Service and the Personal Data Processing Agreement; after reviewing, consent by ticking the appropriate box. To complete your registration, click the **Register** button.

To finalize your registration, please check your email for a confirmation message. Follow the link provided in the email to activate your account. Upon clicking the link, you will receive a notification confirming the successful completion of your registration process.

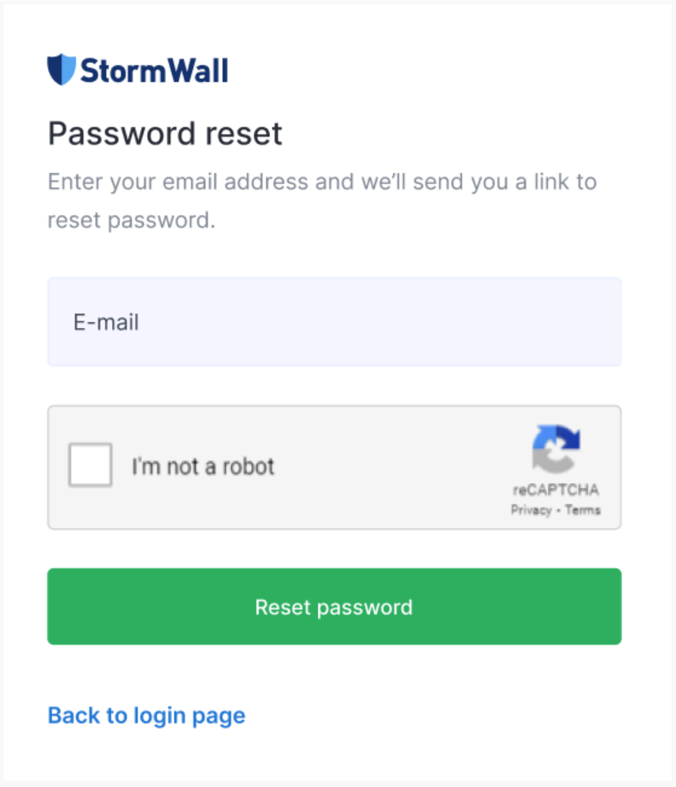


✓ Your email address is now verified

Contact to our sales managers for receiving resources

If you've previously registered but have forgotten your password, please follow these steps:

- Navigate to the password reset form on the right side of the screen to establish a new password.
- Input your email address and verify your identity by completing the Captcha challenge.

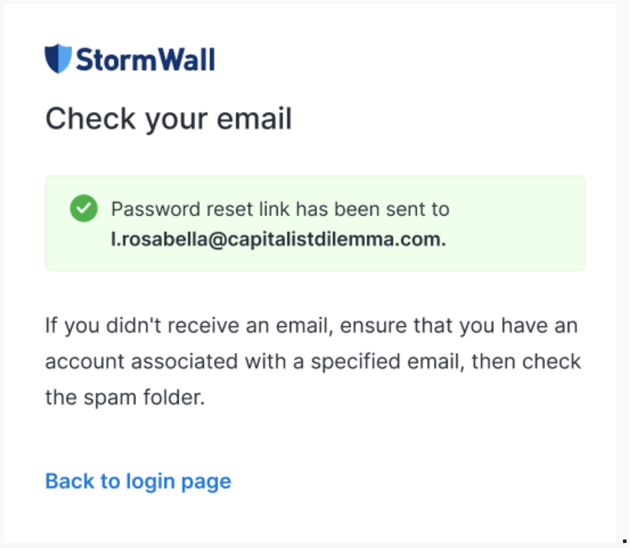


Password reset

Enter your email address and we'll send you a link to reset password.

- Click the **Reset Password** button.

You will receive an email at your registered address containing detailed instructions on how to proceed with resetting your password.



Check your email

Password reset link has been sent to **l.rosabella@capitalistdilemma.com.**

If you didn't receive an email, ensure that you have an account associated with a specified email, then check the spam folder.

Great!

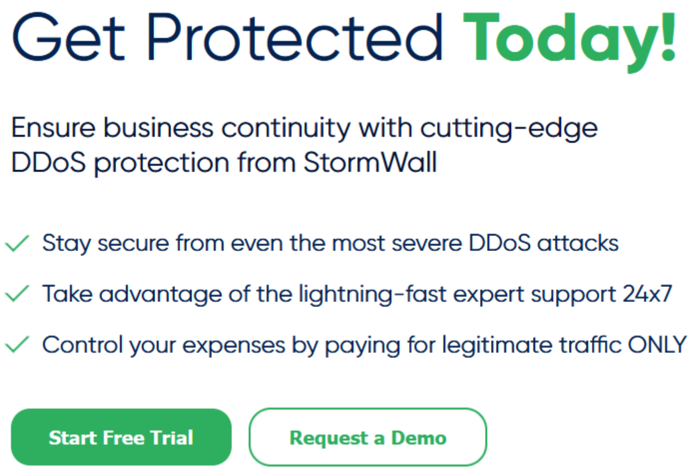
You have successfully completed the registration process on the StormWall website.

You are now able to log into your account and start making use of our services. Our personal account features allow you to manage your account effortlessly, as well as conveniently configure services and process payments.

For further details on the features available to you, please visit the **Client Panel** section.

How to Enable Service Testing?

To familiarize yourself with the product before subscribing, click the **Start Free Trial** button.

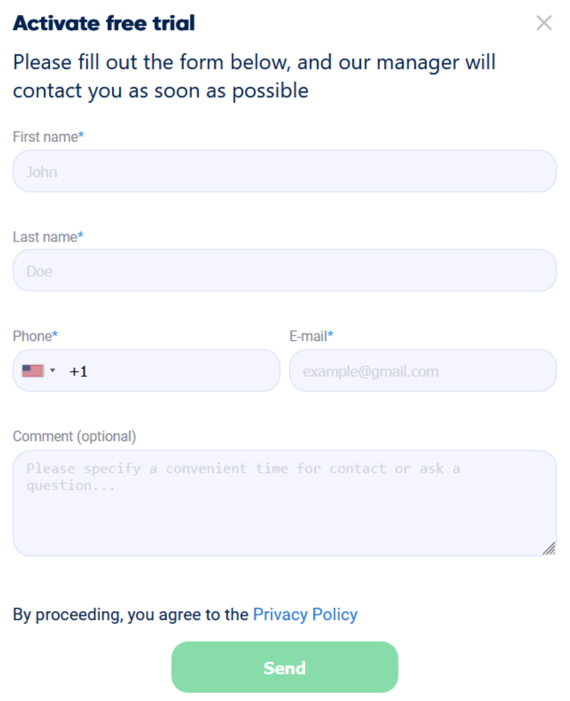


Get Protected **Today!**

Ensure business continuity with cutting-edge
DDoS protection from StormWall

- ✓ Stay secure from even the most severe DDoS attacks
- ✓ Take advantage of the lightning-fast expert support 24x7
- ✓ Control your expenses by paying for legitimate traffic ONLY

Fill out the form and wait for our call.



Activate free trial

Please fill out the form below, and our manager will contact you as soon as possible

First name*

John

Last name*

Doe

Phone*

+1

E-mail*

example@gmail.com

Comment (optional)

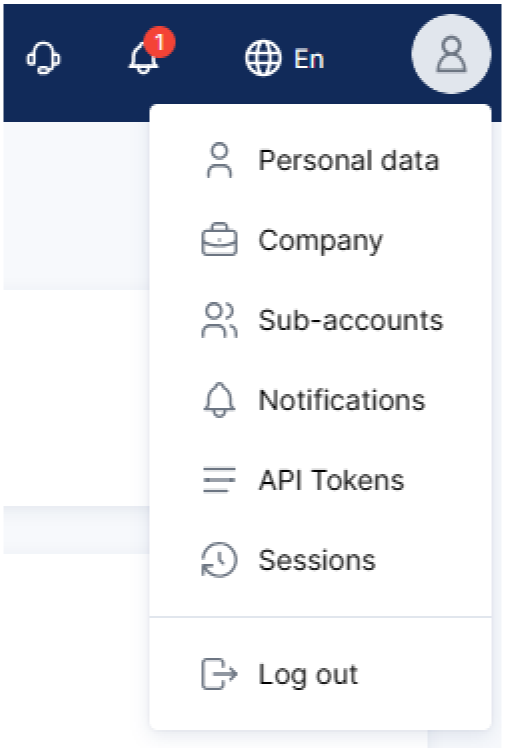
Please specify a convenient time for contact or ask a question...

By proceeding, you agree to the Privacy Policy

If you encounter difficulties in connecting services, please contact customer support.

User Data

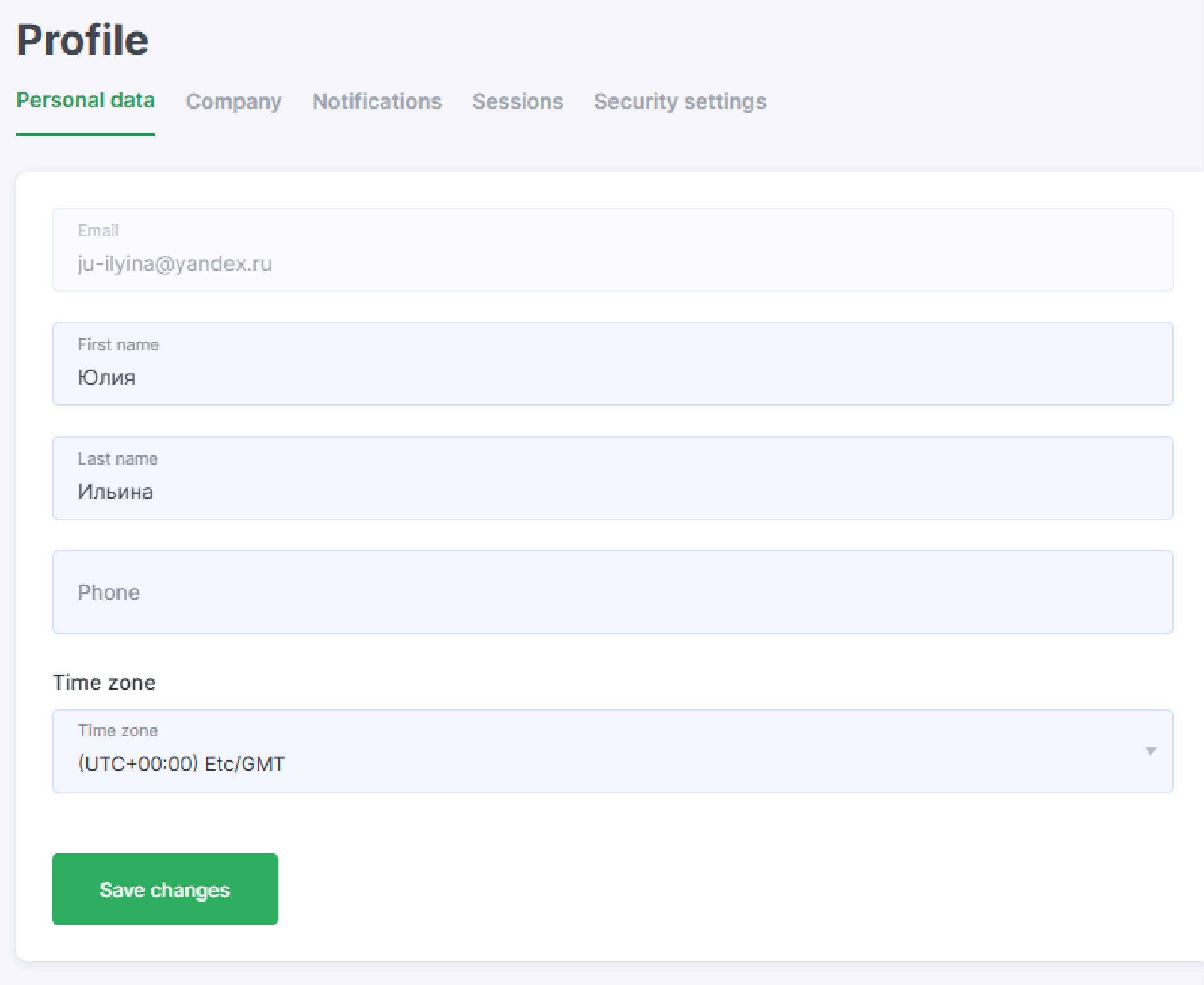
To access your user data, select the account icon situated in the upper right corner of the screen.



Personal Information

Personal data

After clicking the account icon in the top right corner of the screen, choose **Personal Information** from the dropdown menu that appears.



Profile

Personal data | Company | Notifications | Sessions | Security settings

Email: ju-ilyina@yandex.ru

First name: Юлия

Last name: Ильина

Phone

Time zone

Time zone: (UTC+00:00) Etc/GMT

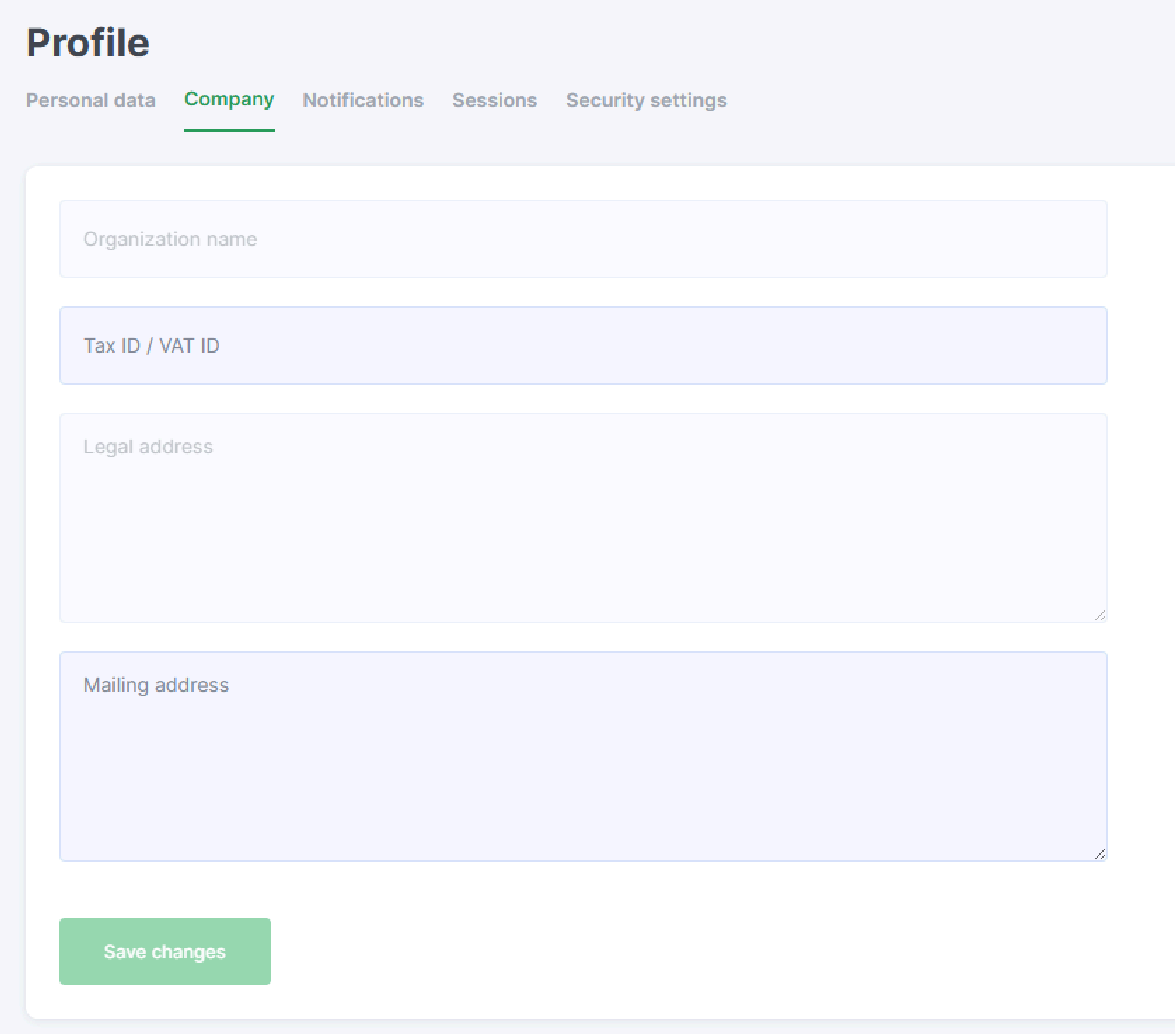
Please fill out the following fields in the form:

- E-mail;
- First name;
- Last name;
- Phone;
- Time Zone;
- Time Format.

After completing the form, click on the **Save** button to confirm the changes.

Company

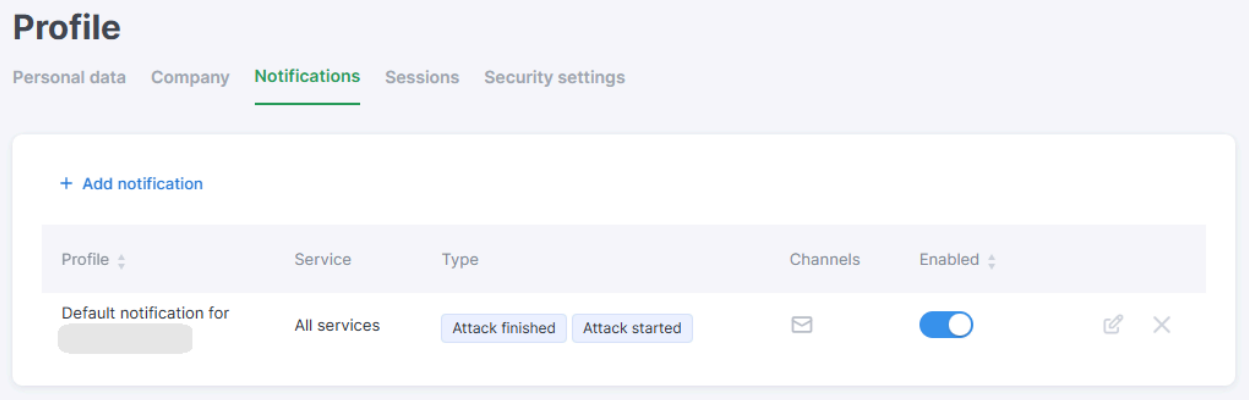
On the **Company** tab, enter your company details.



After entering the information, click the **Save change** button.

Notifications

On the **Notifications** tab, you will see all notifications related to each of your services.



Profile

Personal data Company Notifications Sessions Security settings

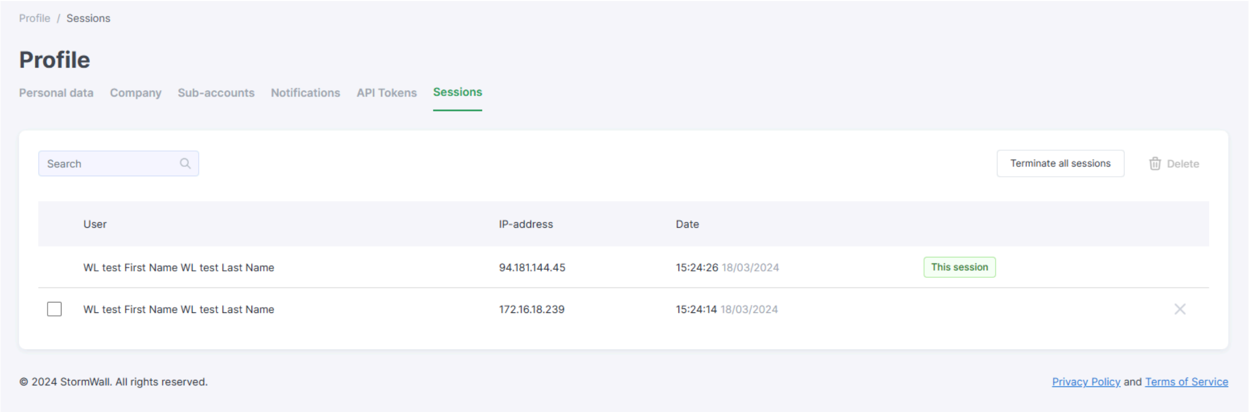
+ Add notification

Profile	Service	Type	Channels	Enabled	
Default notification for [redacted]	All services	Attack finished Attack started	✉	●	

You can create, edit, and delete notifications. To manage notifications, please refer to the instructions.

Sessions

Access the **Sessions** tab to view a table that lists all active and historical user sessions.



	User	IP-address	Date	
	WL test First Name WL test Last Name	94.181.144.45	15:24:26 18/03/2024	This session
□	WL test First Name WL test Last Name	172.16.18.239	15:24:14 18/03/2024	×

© 2024 StormWall. All rights reserved.

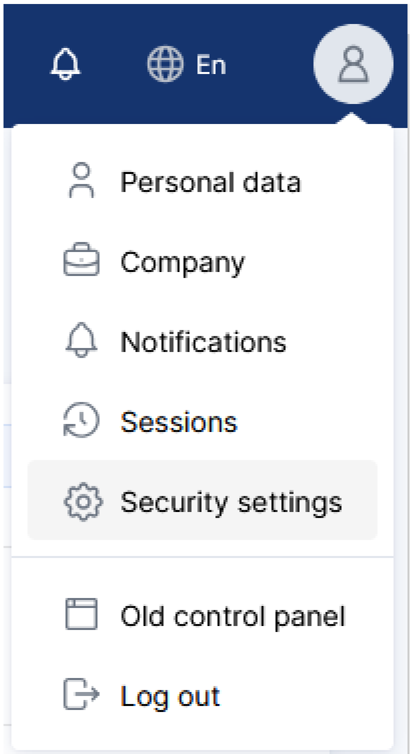
Privacy Policy and Terms of Service

You can terminate a session by marking the checkbox in the corresponding session row and pressing the **Delete** button. The user associated with the terminated session will be required to log in again on the website.

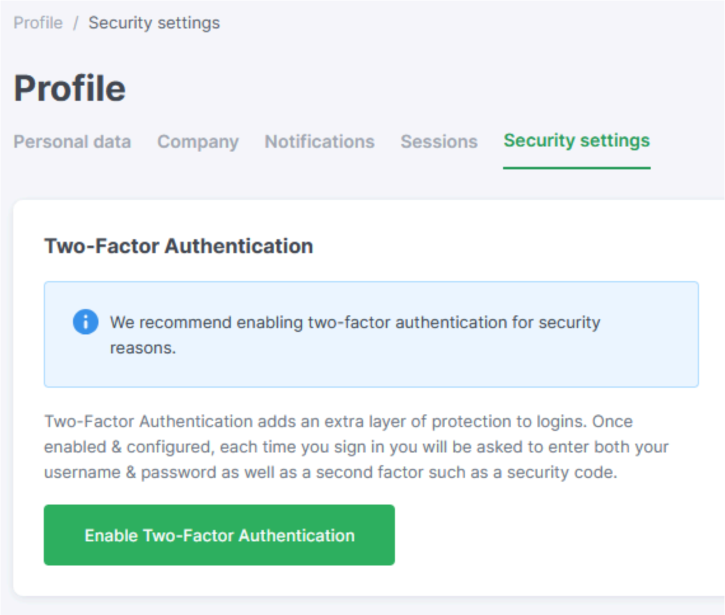
Should you notice any suspicious activity, opt for the **Terminate all sessions** button to ensure security.

Security Settings

Open the **Security Settings** tab.



We recommend enabling two-factor authentication. To do this, you will need to install any authenticator app on your smartphone, such as **Google Authenticator** or **Duo**.

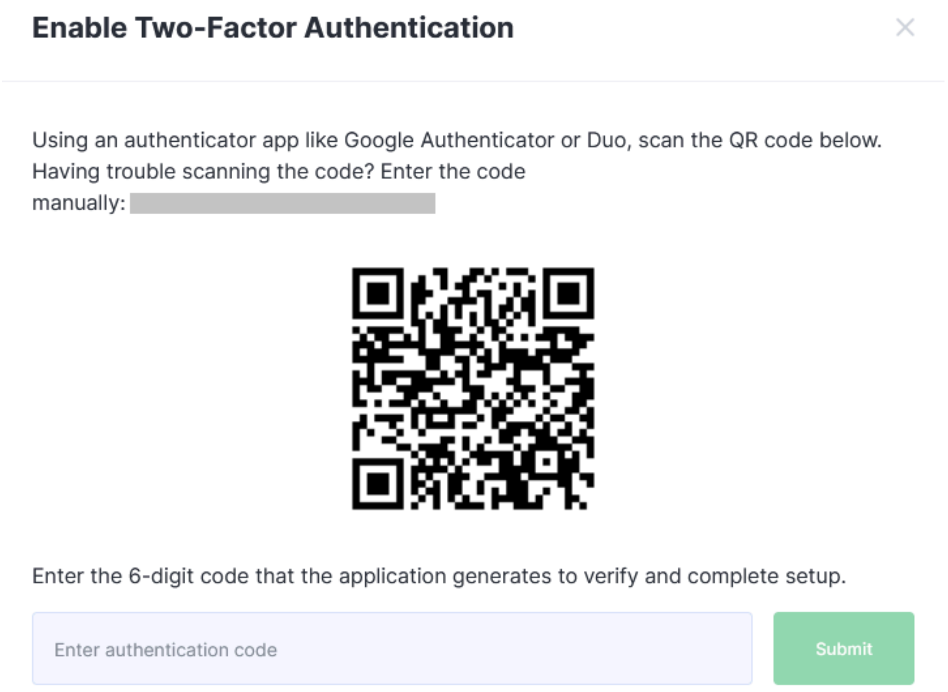


Two-Factor Authentication

We recommend enabling two-factor authentication for security reasons.

Two-Factor Authentication adds an extra layer of protection to logins. Once enabled & configured, each time you sign in you will be asked to enter both your username & password as well as a second factor such as a security code.

To enhance your account security, click the **Enable Two-Factor Authentication** button.



Enable Two-Factor Authentication

Using an authenticator app like Google Authenticator or Duo, scan the QR code below. Having trouble scanning the code? Enter the code manually: [redacted]

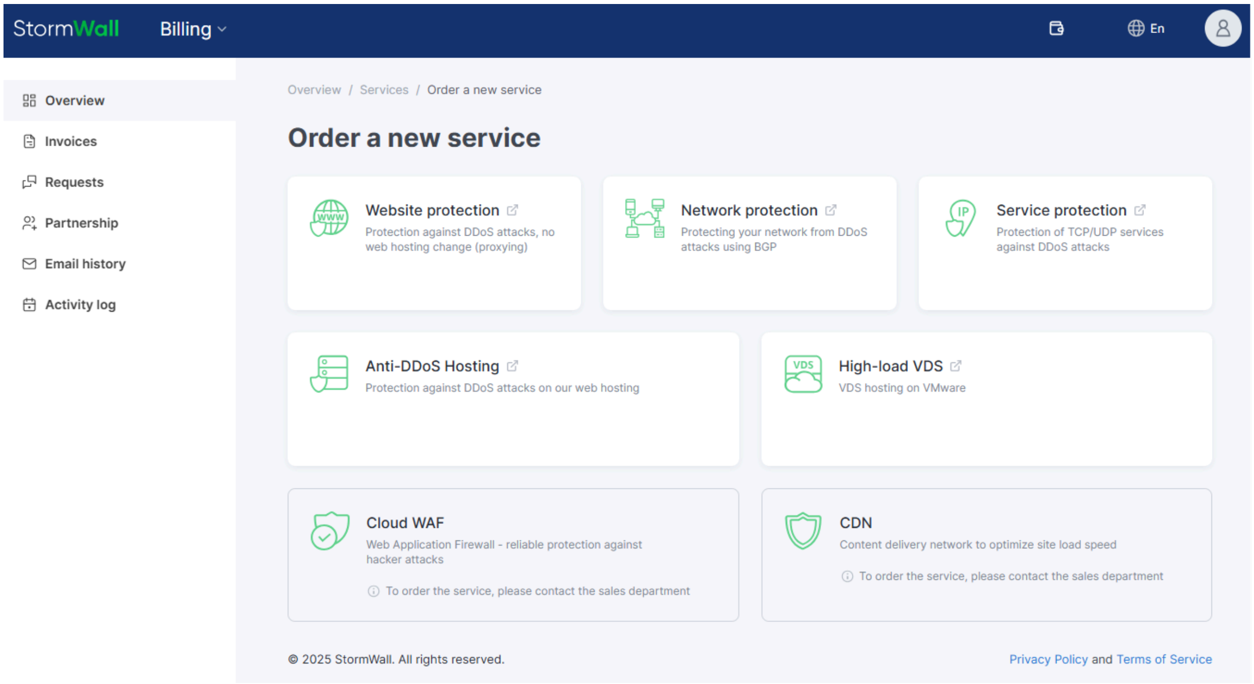
Enter the 6-digit code that the application generates to verify and complete setup.

Follow the on-screen instructions and click **Submit** after entering the code from the authenticator app on your smartphone.

Billing

How to Connect Your Service

Log in to your account on the StormWall website. In the top panel, select the **Billing** option. This will open a menu in the left panel. In the opened panel, select the service and click on its name.



Order a new service

Website protection
Protection against DDoS attacks, no web hosting change (proxying)

Network protection
Protecting your network from DDoS attacks using BGP

Service protection
Protection of TCP/UDP services against DDoS attacks

Anti-DDoS Hosting
Protection against DDoS attacks on our web hosting

High-load VDS
VDS hosting on VMware

Cloud WAF
Web Application Firewall - reliable protection against hacker attacks
To order the service, please contact the sales department

CDN
Content delivery network to optimize site load speed
To order the service, please contact the sales department

© 2025 StormWall. All rights reserved.

Privacy Policy and Terms of Service

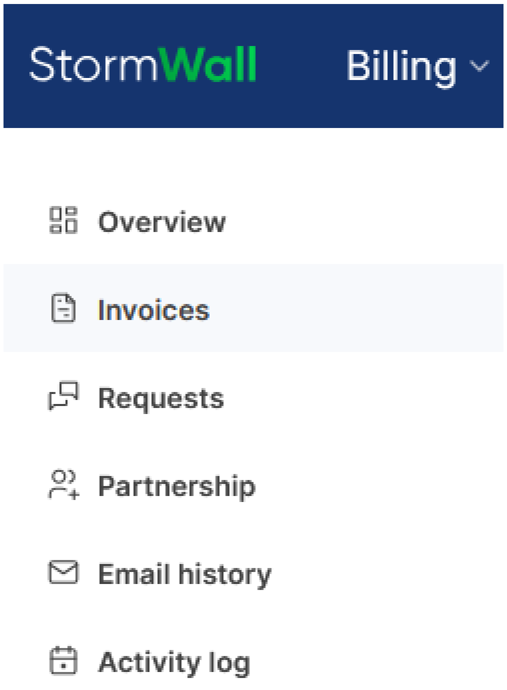
You will be redirected to the service order page on the website. Please review the available pricing plans.

To order a service with the **Standard (Personal)** or **Business (Business One)** plan, simply fill out the form that appears after clicking the **Order** button.

If you choose the **Enterprise (Enterprise One)** plan, a support specialist will contact you after you submit the form.

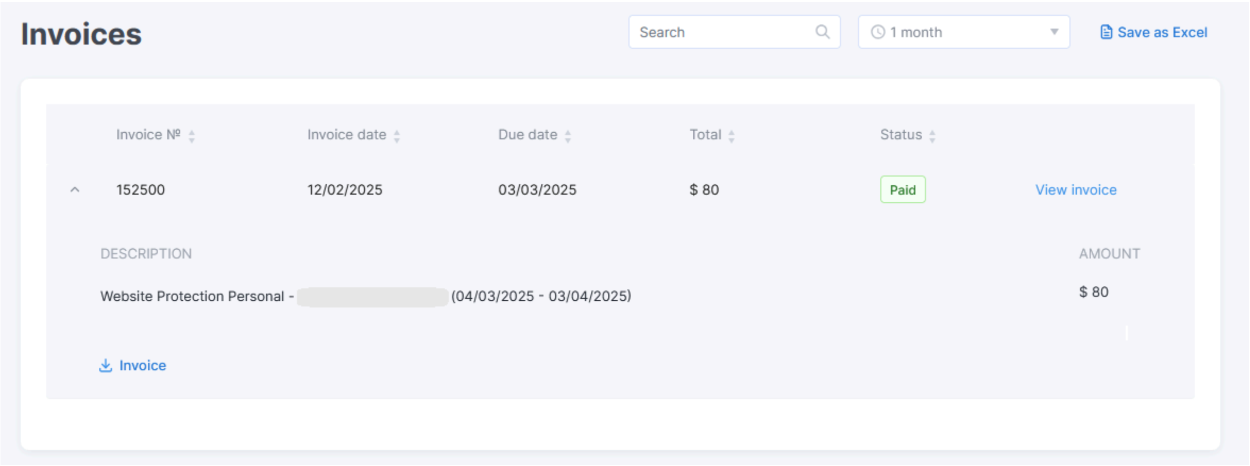
How to Pay for Protection

To pay for protection, first, log into your personal account on the StormWall website. Then, select **Billing** from the top panel. This action will open the menu on the left panel.



When an unpaid bill appears, an icon will be displayed next to the **Invoices** field.

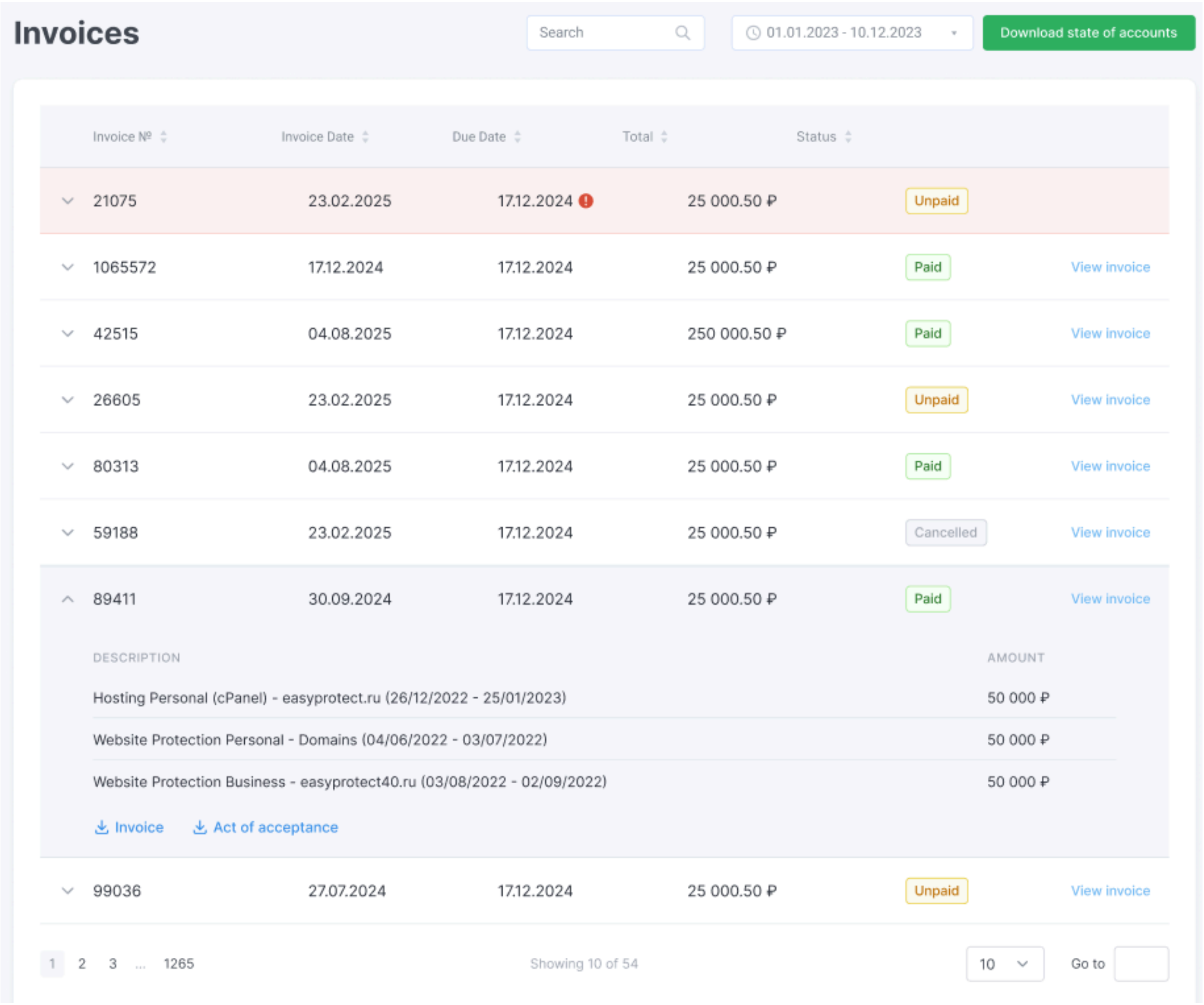
Select the **Invoices** menu item to view a list of your invoices. If no invoices have been issued yet, the area will be empty.



Invoice №	Invoice date	Due date	Total	Status	
152500	12/02/2025	03/03/2025	$ 80	Paid	View invoice

DESCRIPTION	AMOUNT
Website Protection Personal - [redacted] (04/03/2025 - 03/04/2025)	$ 80

Invoice



Invoices

Search

01.01.2023 - 10.12.2023

Download state of accounts

Invoice №	Invoice Date	Due Date	Total	Status	
21075	23.02.2025	17.12.2024 !	25 000.50 ₽	Unpaid	
1065572	17.12.2024	17.12.2024	25 000.50 ₽	Paid	View invoice
42515	04.08.2025	17.12.2024	250 000.50 ₽	Paid	View invoice
26605	23.02.2025	17.12.2024	25 000.50 ₽	Unpaid	View invoice
80313	04.08.2025	17.12.2024	25 000.50 ₽	Paid	View invoice
59188	23.02.2025	17.12.2024	25 000.50 ₽	Cancelled	View invoice
89411	30.09.2024	17.12.2024	25 000.50 ₽	Paid	View invoice

DESCRIPTION	AMOUNT
Hosting Personal (cPanel) - easyprotect.ru (26/12/2022 - 25/01/2023)	50 000 ₽
Website Protection Personal - Domains (04/06/2022 - 03/07/2022)	50 000 ₽
Website Protection Business - easyprotect40.ru (03/08/2022 - 02/09/2022)	50 000 ₽

Invoice   Act of acceptance

99036	27.07.2024	17.12.2024	25 000.50 ₽	Unpaid	View invoice

1 2 3 ... 1265   Showing 10 of 54   10   Go to

Click on the «arrow» icon in the invoice field to expand its contents. Then, press the **View Invoice** button within the field of the selected item to open it in a separate window.

You can download the invoice using the form's tools - utilize the **Save as Excel** or **Invoice** buttons for this action.

Payment Methods

Choose a Payment Method:

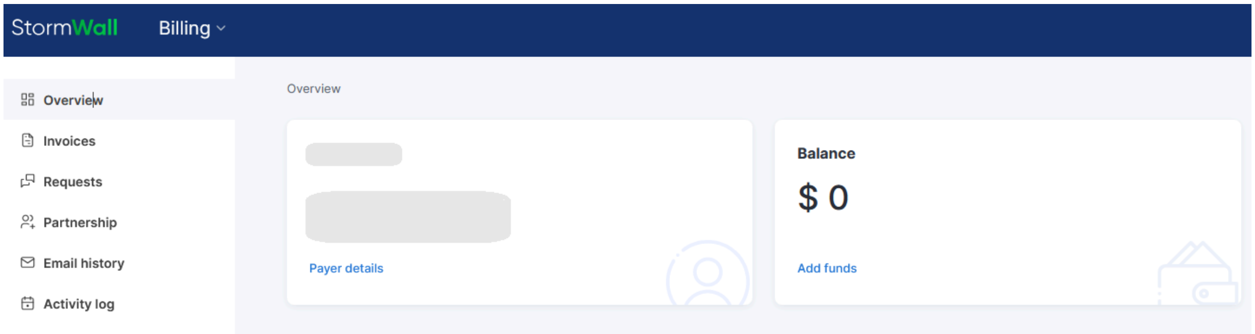
- **Credit Balance:** You can pay for the service from your credit balance after pre-funding it. To do this, select "Pay from credit balance" when making a payment.

- **Other Payment Methods:** You can pay for the service using a bank card, bank transfer, or online payment systems.

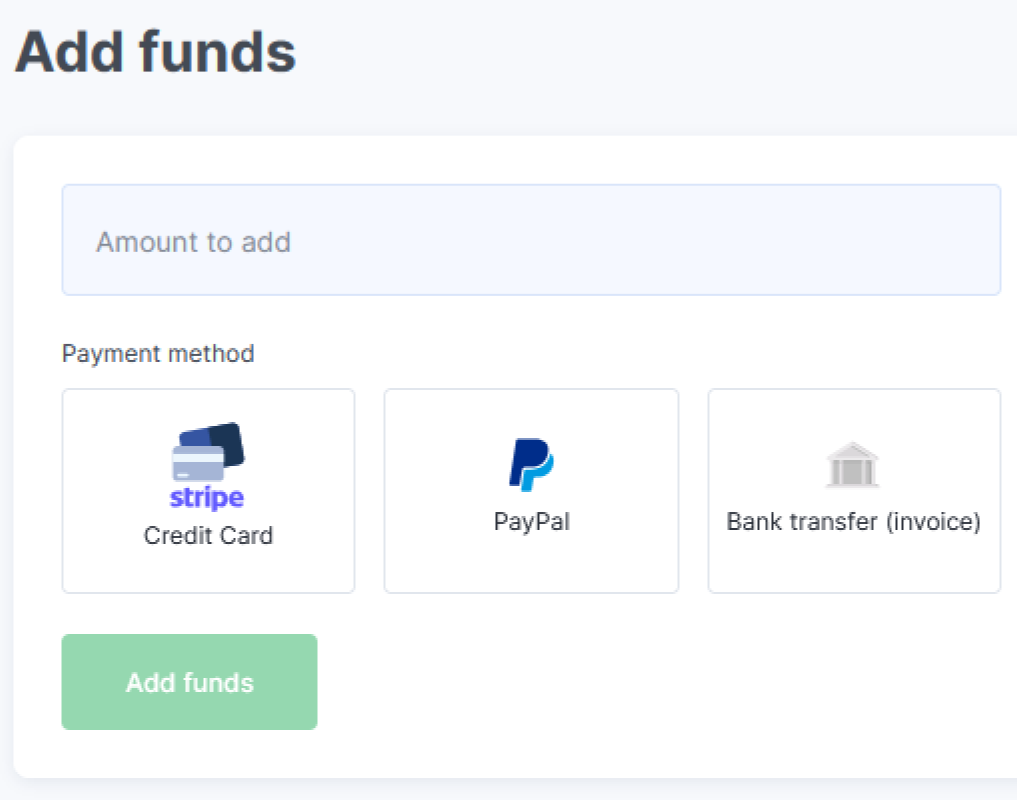
Payment from Credit Balance

The credit balance in your account allows you to top up your account in advance and then pay for services from it. This payment method helps avoid minor transactions using bank cards and accounts.

To top up your credit balance, fill out the form on the **Billing** tab.



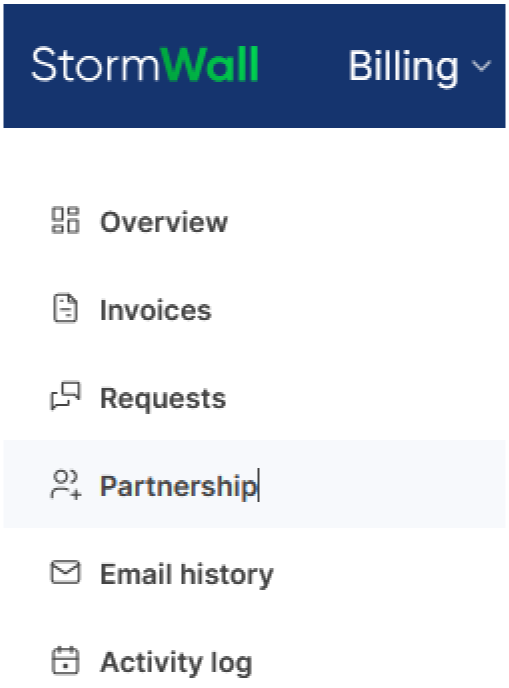
In the **Balance** area, click on the **Add funds** button.



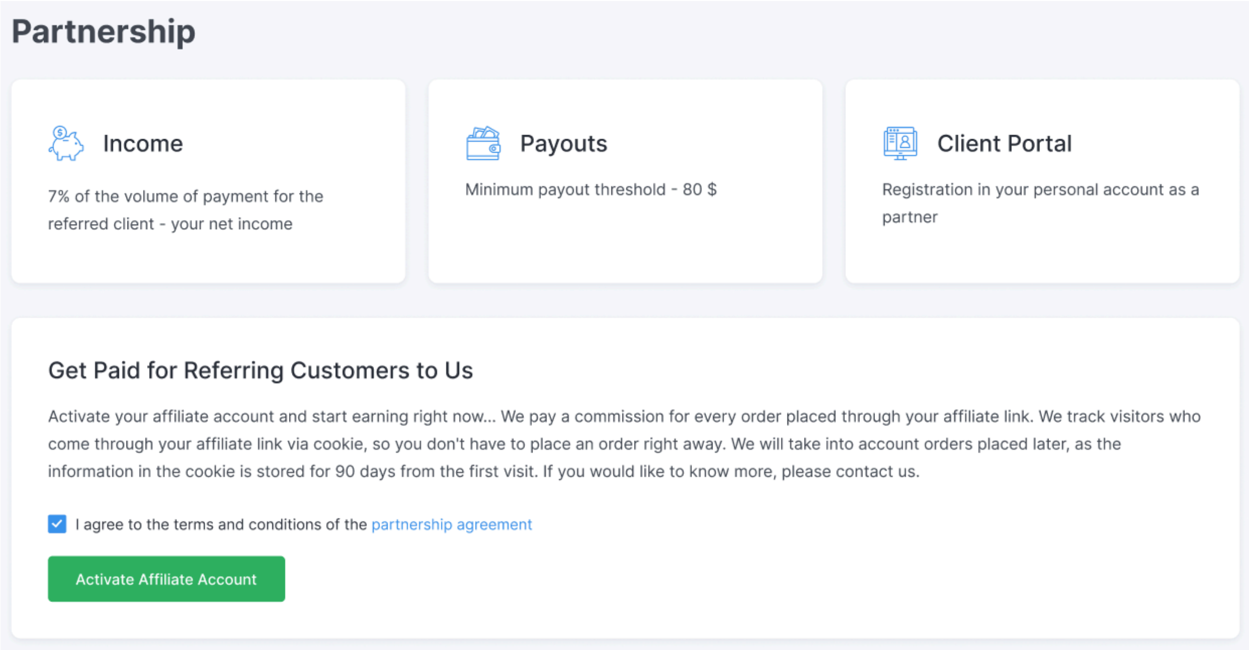
Select the amount and the payment method, then click on the **Add funds** button and wait to be redirected to the payment gateway. Complete the transaction according to the payment method you have chosen.

How to Participate in an Affiliate Program?

In the top menu bar, navigate to the **Billing** tab.



In the menu that opens on the left, select the **Partnership** option.



Partnership

Income

7% of the volume of payment for the referred client - your net income

Payouts

Minimum payout threshold - 80 $

Client Portal

Registration in your personal account as a partner

Get Paid for Referring Customers to Us

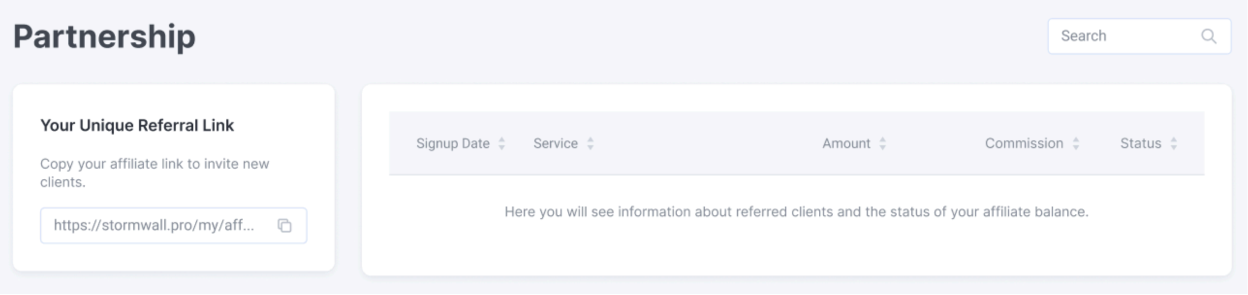
Activate your affiliate account and start earning right now... We pay a commission for every order placed through your affiliate link. We track visitors who come through your affiliate link via cookie, so you don't have to place an order right away. We will take into account orders placed later, as the information in the cookie is stored for 90 days from the first visit. If you would like to know more, please contact us.

☑ I agree to the terms and conditions of the partnership agreement

Activate Affiliate Account

In the window that opens, review the information about [partner program]() and click on the **Activate Affiliate Account** button.

After activation, a code will appear which you can use to attract customers.



Partnership

Search

Your Unique Referral Link

Copy your affiliate link to invite new clients.

https://stormwall.pro/my/aff...

Signup Date	Service	Amount	Commission	Status

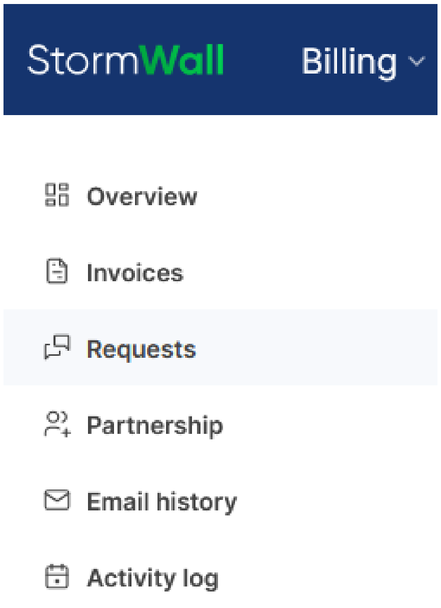
Here you will see information about referred clients and the status of your affiliate balance.

You can find detailed information on the website.

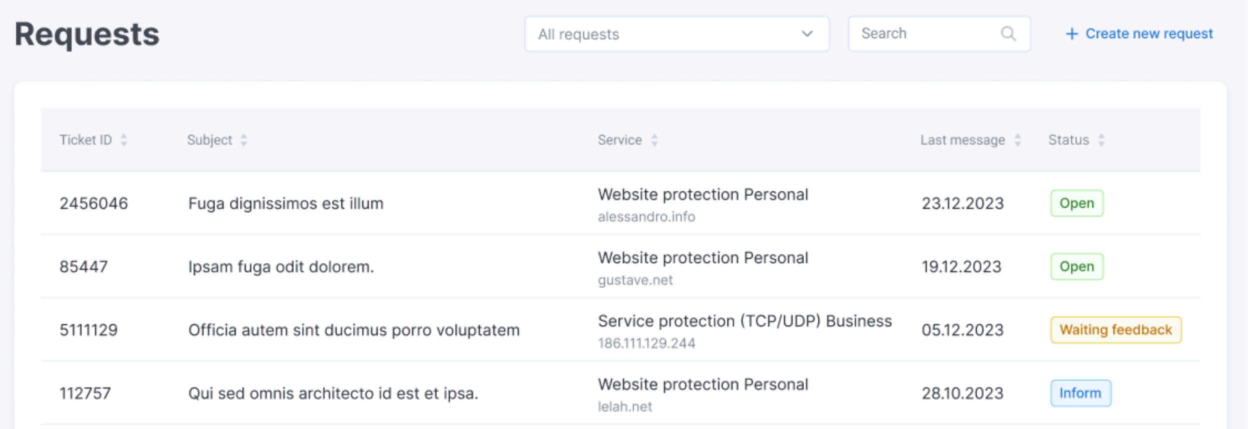
How to Contact Technical Support?

In the top menu bar, navigate to the **Billing** tab.

In the menu that opens on the left, select the **Requests** item.



In the window that opens, you will see a history of inquiries to technical support. Use the filtering and search features to find the inquiries you need.

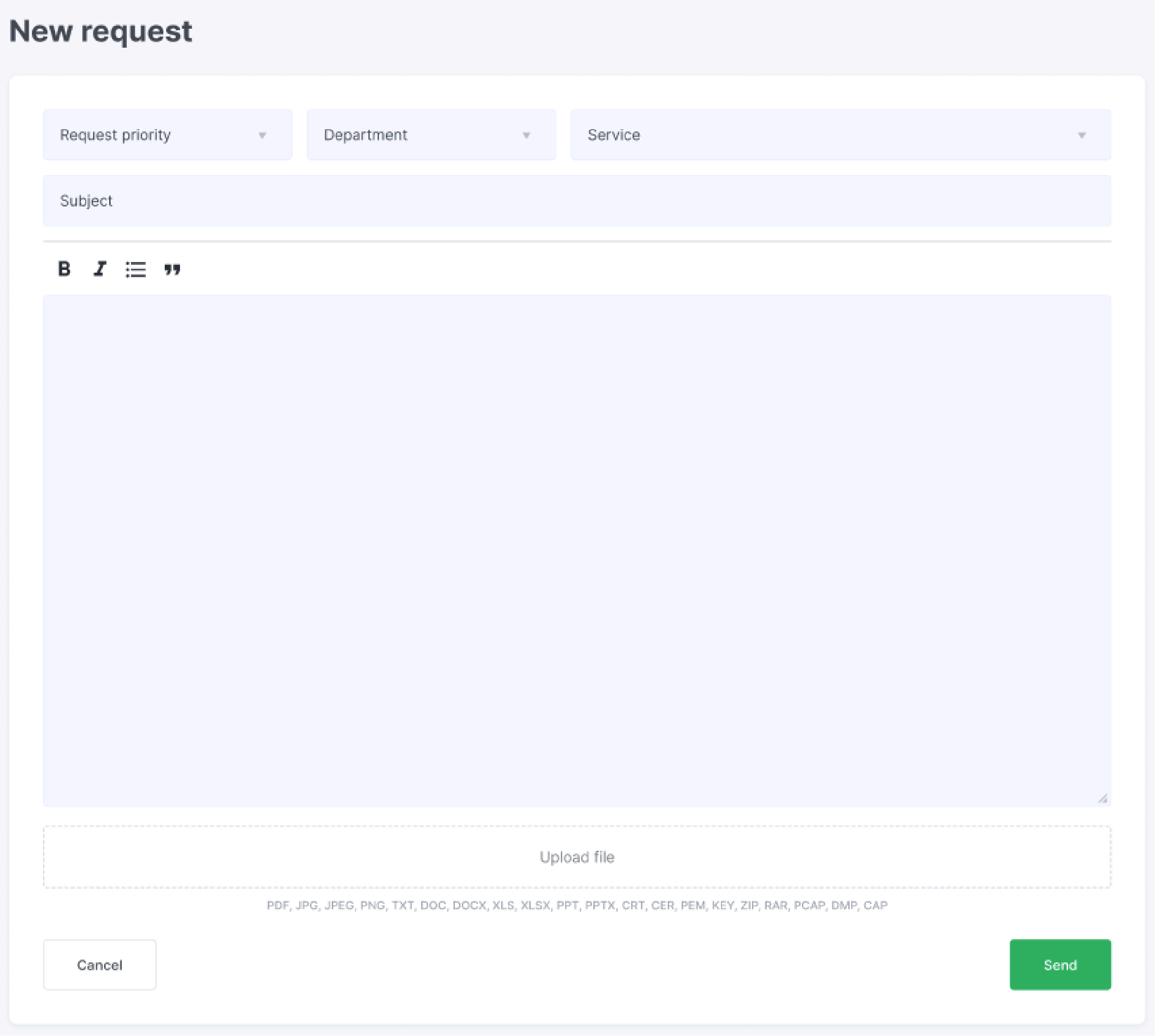


Requests

All requests | Search | + Create new request

Ticket ID	Subject	Service	Last message	Status
2456046	Fuga dignissimos est illum	Website protection Personal alessandro.info	23.12.2023	Open
85447	Ipsam fuga odit dolorem.	Website protection Personal gustave.net	19.12.2023	Open
5111129	Officia autem sint ducimus porro voluptatem	Service protection (TCP/UDP) Business 186.111.129.244	05.12.2023	Waiting feedback
112757	Qui sed omnis architecto id est et ipsa.	Website protection Personal lelah.net	28.10.2023	Inform

Click on the **Create new request** button to contact support.



New request

Request priority ▾ | Department ▾ | Service ▾

Subject

Upload file

PDF, JPG, JPEG, PNG, TXT, DOC, DOCX, XLS, XLSX, PPT, PPTX, CRT, CER, PEM, KEY, ZIP, RAR, PCAP, DMP, CAP

Fill out the form by selecting:

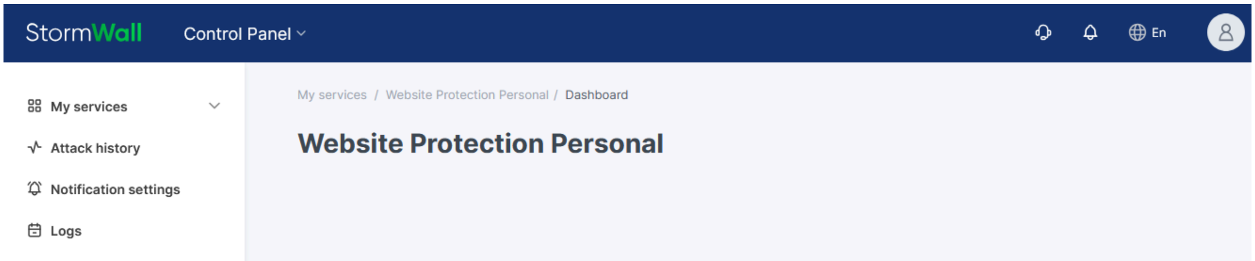
- Request priority (how urgently you need a resolution);
- Department (to whom the inquiry is addressed);
- Service (which service the inquiry concerns);
- Subject (a brief summary of the inquiry);
- Text (describe the issue in as much detail as possible);
- File (attach a file if necessary).

After filling out the form, click the **Send** button.

Control Panel

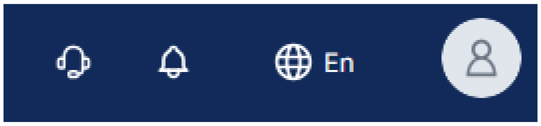
How to Manage Your Account?

After successfully logging in, you'll be directed to the main page, which is the client panel. The central module displays the services you've connected. If you haven't connected any services yet, this area will be empty.

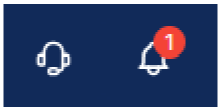

StormWall
Control Panel
En
My services
Attack history
Notification settings
Logs
My services / Website Protection Personal / Dashboard
Website Protection Personal

In the top right corner of the window, you'll find buttons for:

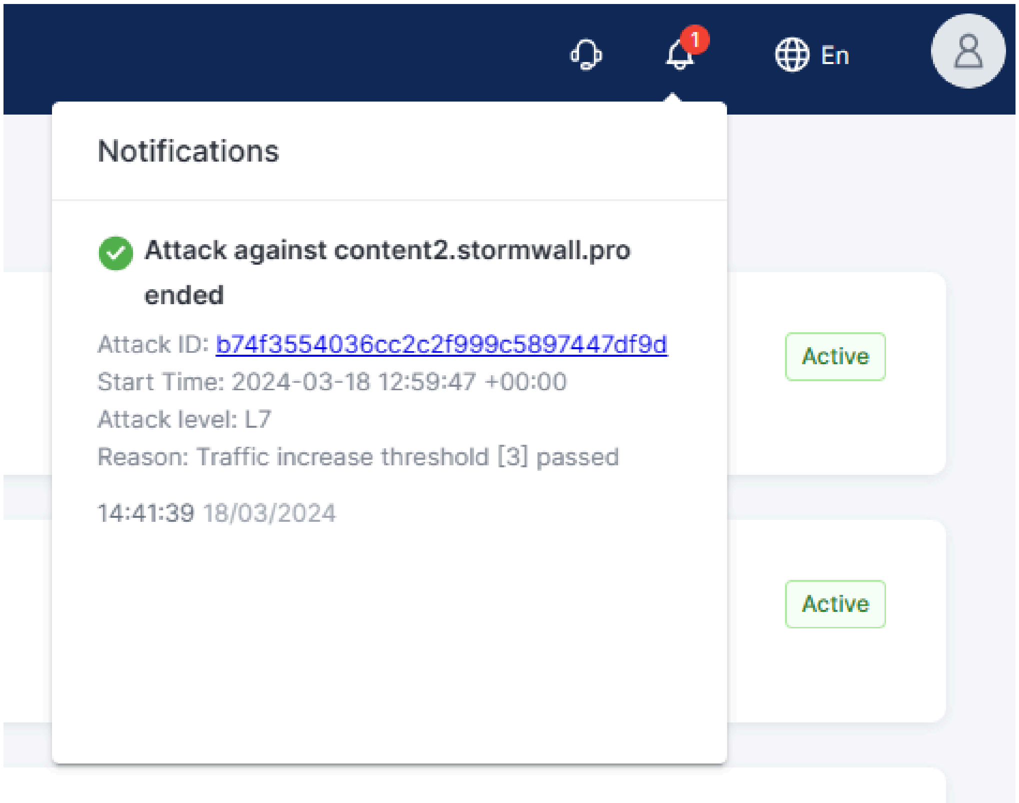
- Contacting technical support;
- Notifications;
- Language switch;
- Personal account access.



When a new notification arrives, a number will appear on its icon to indicate the count of new notifications.



Click on the icon, and you will see a message. This could be information about an attack or details regarding the successful verification of the selected notification method (Telegram or Webhook).



Notifications

✓ **Attack against content2.stormwall.pro ended**

Attack ID: b74f3554036cc2c2f999c5897447df9d
Start Time: 2024-03-18 12:59:47 +00:00
Attack level: L7
Reason: Traffic increase threshold [3] passed

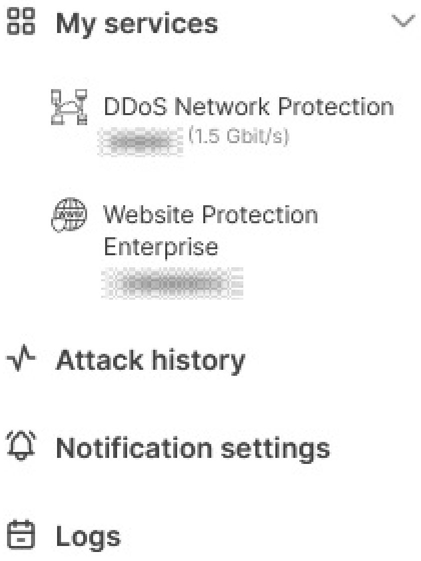
14:41:39 18/03/2024

In the top left corner, there's a page switcher that allows you to navigate between different sections:

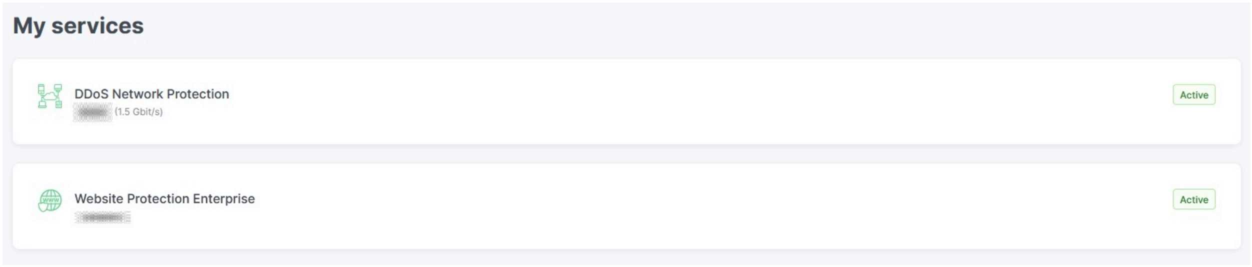
- Users;
- Billing;
- Control Panel.

On the left side, you will find a menu with the following options:

- My Services;
- Attack History;
- Notification Settings;
- Logs.

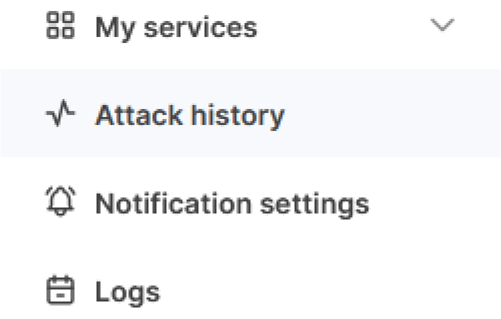


In the central module, the services you have connected are displayed. If you haven't yet connected any of the company's products, this area will be empty. Click on the service line to view information about it.

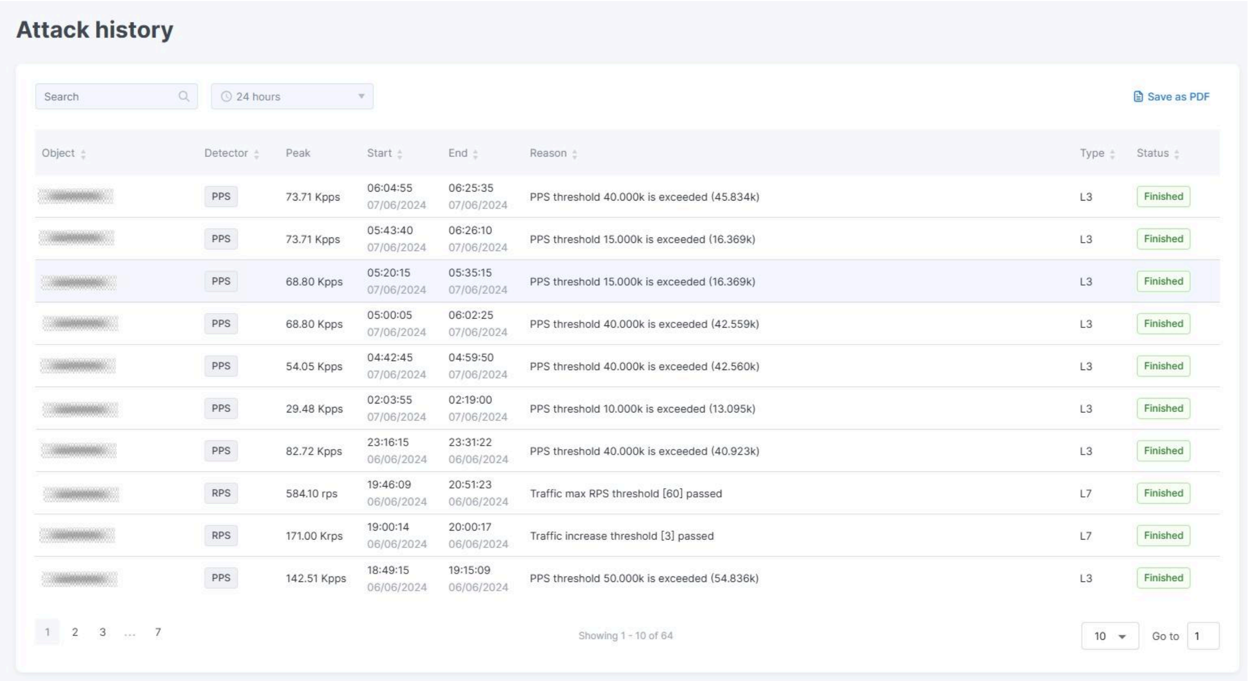


Attack History

In the left sidebar of the client panel, select the **Attack History** option.



On the opened page, there is a table with data on all attacks on each of the objects.



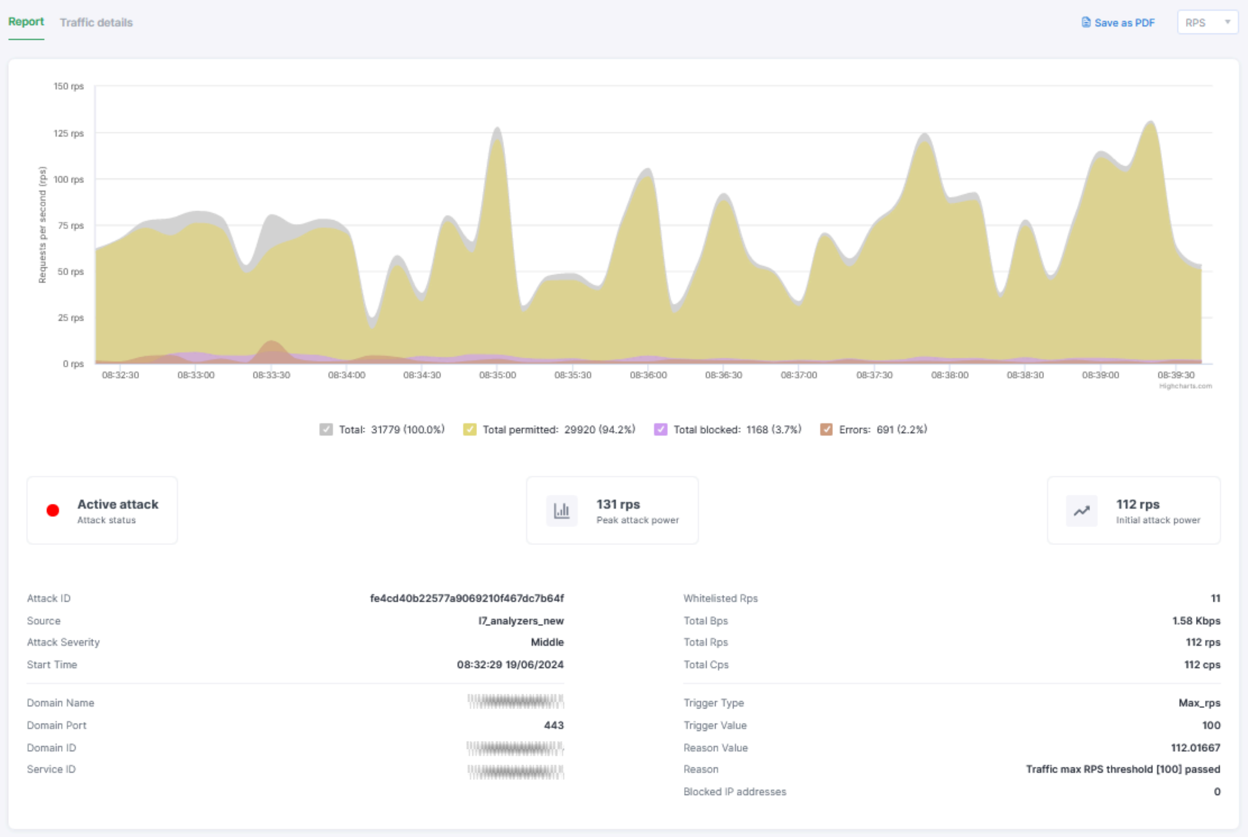
Attack history

Search | 24 hours | Save as PDF

Object	Detector	Peak	Start	End	Reason	Type	Status
[redacted]	PPS	73.71 Kpps	06:04:55 07/06/2024	06:25:35 07/06/2024	PPS threshold 40.000k is exceeded (45.834k)	L3	Finished
[redacted]	PPS	73.71 Kpps	05:43:40 07/06/2024	06:26:10 07/06/2024	PPS threshold 15.000k is exceeded (16.369k)	L3	Finished
[redacted]	PPS	68.80 Kpps	05:20:15 07/06/2024	05:35:15 07/06/2024	PPS threshold 15.000k is exceeded (16.369k)	L3	Finished
[redacted]	PPS	68.80 Kpps	05:00:05 07/06/2024	06:02:25 07/06/2024	PPS threshold 40.000k is exceeded (42.559k)	L3	Finished
[redacted]	PPS	54.05 Kpps	04:42:45 07/06/2024	04:59:50 07/06/2024	PPS threshold 40.000k is exceeded (42.560k)	L3	Finished
[redacted]	PPS	29.48 Kpps	02:03:55 07/06/2024	02:19:00 07/06/2024	PPS threshold 10.000k is exceeded (13.095k)	L3	Finished
[redacted]	PPS	82.72 Kpps	23:16:15 06/06/2024	23:31:22 06/06/2024	PPS threshold 40.000k is exceeded (40.923k)	L3	Finished
[redacted]	RPS	584.10 rps	19:46:09 06/06/2024	20:51:23 06/06/2024	Traffic max RPS threshold [60] passed	L7	Finished
[redacted]	RPS	171.00 Krps	19:00:14 06/06/2024	20:00:17 06/06/2024	Traffic increase threshold [3] passed	L7	Finished
[redacted]	PPS	142.51 Kpps	18:49:15 06/06/2024	19:15:09 06/06/2024	PPS threshold 50.000k is exceeded (54.836k)	L3	Finished

1 2 3 ... 7 Showing 1 - 10 of 64 10 Go to 1

Use the **Search** field to filter attacks, as well as the time filter. You can also sort the table elements by clicking on the "arrow" icon next to the column header. To save the data in a file format, click the **Save as PDF** button. To view detailed information about an attack, click on its row in the table. A report area will open.



☑ Total: 31779 (100.0%) ☑ Total permitted: 29920 (94.2%) ☑ Total blocked: 1168 (3.7%) ☑ Errors: 691 (2.2%)

● **Active attack**
Attack status

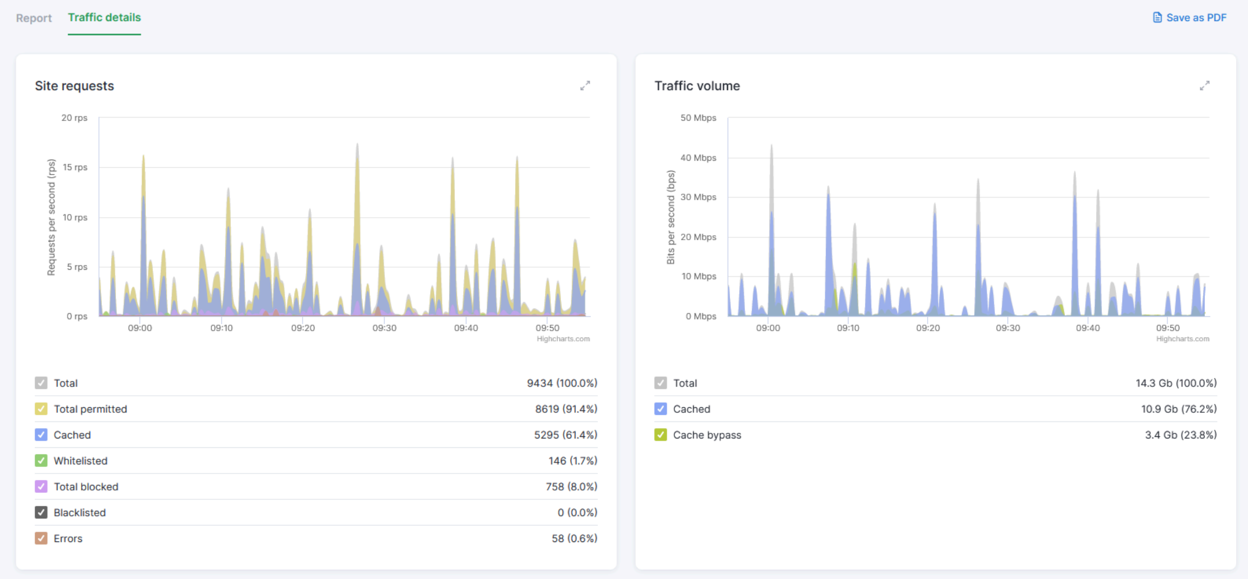
131 rps
Peak attack power

112 rps
Initial attack power

Attack ID	fe4cd40b22577a9069210f467dc7b64f
Source	l7_analyzers_new
Attack Severity	Middle
Start Time	08:32:29 19/06/2024
Domain Name	[redacted]
Domain Port	443
Domain ID	[redacted]
Service ID	[redacted]

Whitelisted Rps	11
Total Bps	1.58 Kbps
Total Rps	112 rps
Total Cps	112 cps
Trigger Type	Max_rps
Trigger Value	100
Reason Value	112.01667
Reason	Traffic max RPS threshold [100] passed
Blocked IP addresses	0

To view additional information, go to the **Traffic Details** tab. You can exclude an object from the chart by unchecking the box next to its name. The set of information fields depends on the type of service.

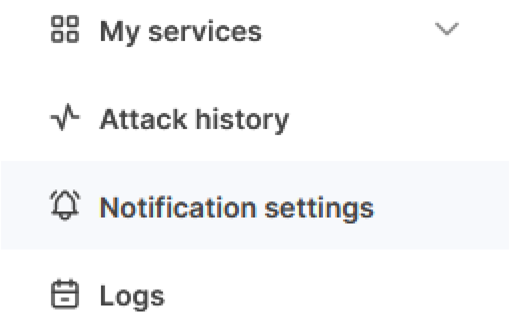


☑ Total	9434 (100.0%)
☑ Total permitted	8619 (91.4%)
☑ Cached	5295 (61.4%)
☑ Whitelisted	146 (1.7%)
☑ Total blocked	758 (8.0%)
☑ Blacklisted	0 (0.0%)
☑ Errors	58 (0.6%)

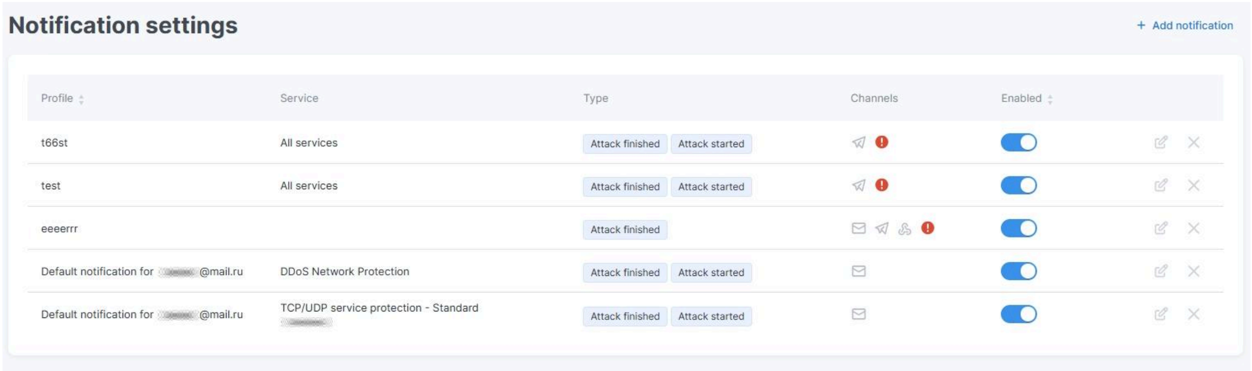
☑ Total	14.3 Gb (100.0%)
☑ Cached	10.9 Gb (76.2%)
☑ Cache bypass	3.4 Gb (23.8%)

Notification Settings

In the left sidebar of the client panel, select the **Notification Settings** option.



On the page that opens, there is a table listing previously configured notifications. In the last column of the table, each notification has buttons for editing and deleting.

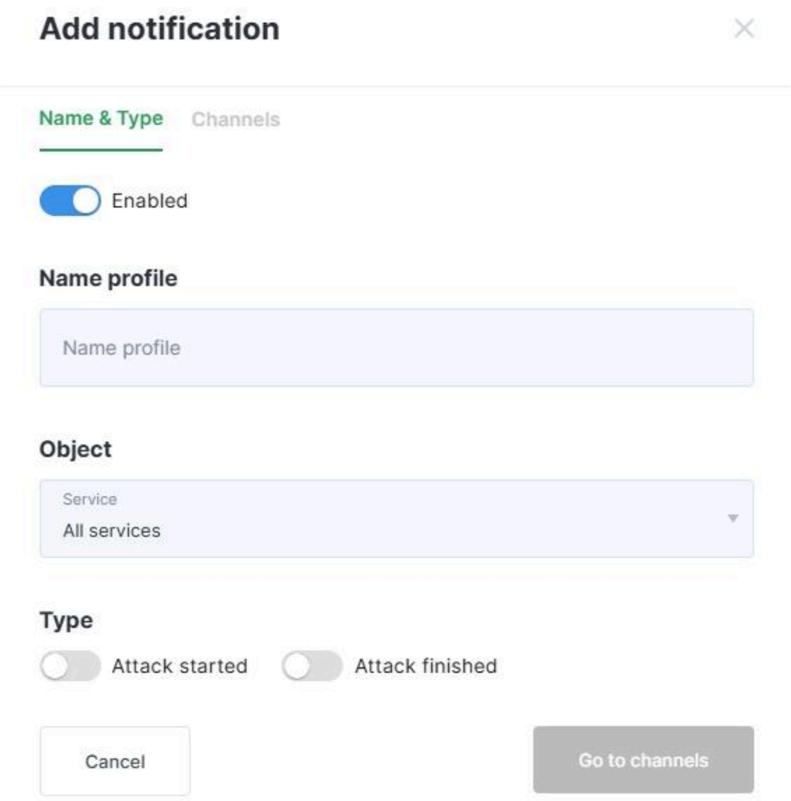


Notification settings

+ Add notification

Profile	Service	Type	Channels	Enabled	
t66st	All services	Attack finished Attack started	✈ !	●	✎ ✕
test	All services	Attack finished Attack started	✈ !	●	✎ ✕
eeeerrr		Attack finished	✉ ✈ ⚙ !	●	✎ ✕
Default notification for [redacted]@mail.ru	DDoS Network Protection	Attack finished Attack started	✉	●	✎ ✕
Default notification for [redacted]@mail.ru	TCP/UDP service protection - Standard [redacted]	Attack finished Attack started	✉	●	✎ ✕

To set up a new notification, click the **Add Notification** button. A configuration dialog box will open.



Add notification

Name & Type | Channels

Enabled

Name profile

Name profile

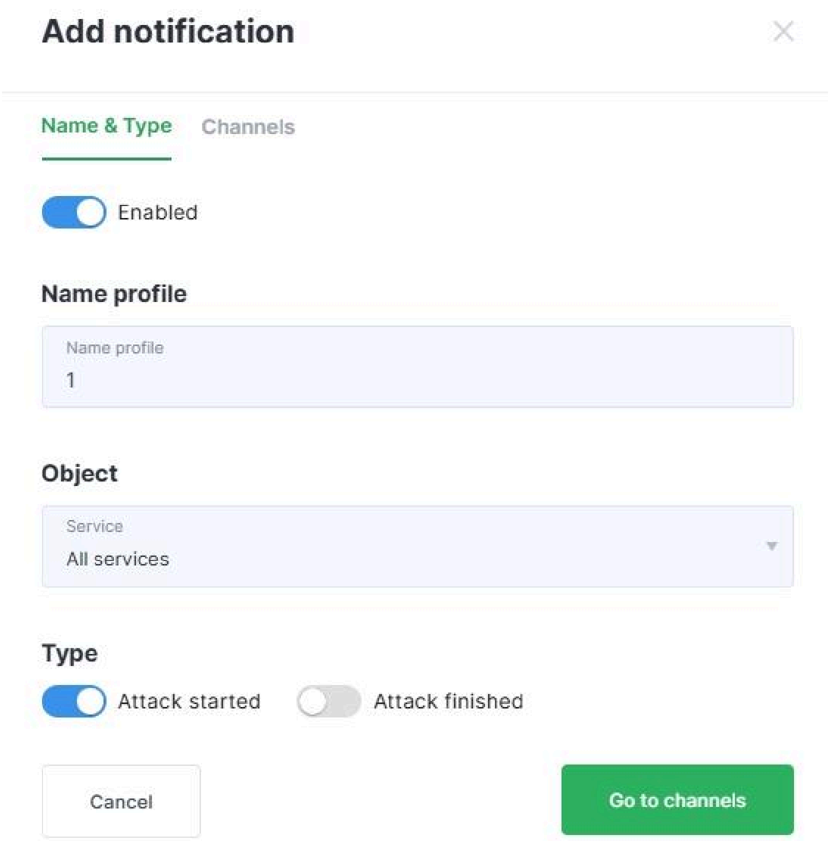
Object

Service
All services

Type

Attack started | Attack finished

After filling in the mandatory **Name&Type** field and selecting the notification type, the **Go to Channels** button becomes active.



Enabled

Name profile

Name profile
1

Object

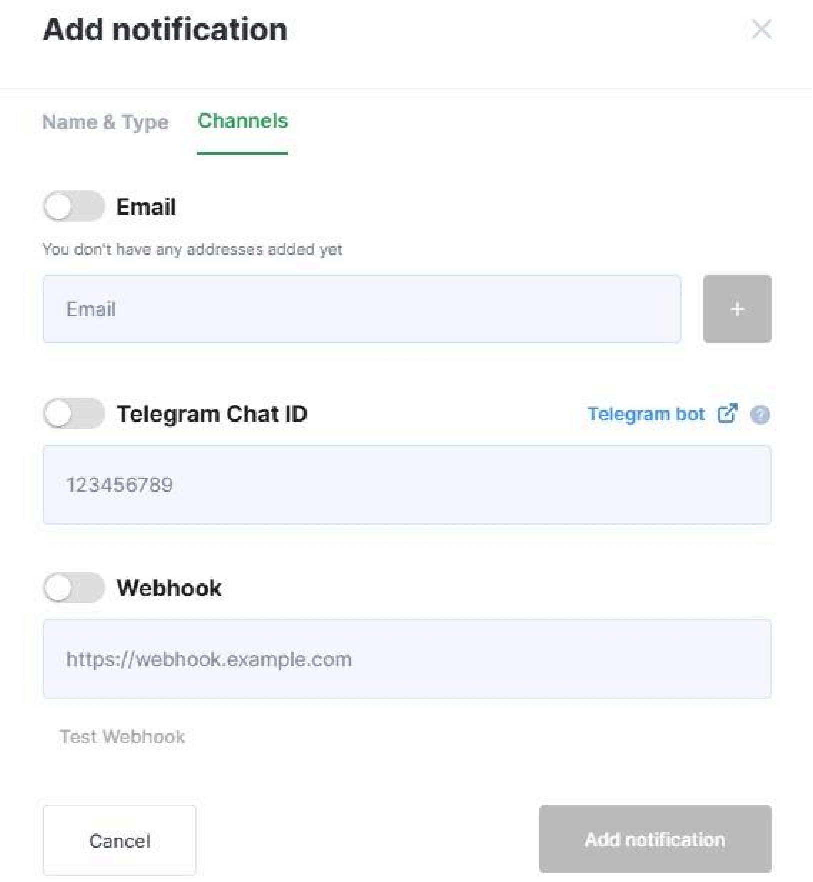
Service
All services

Type

Attack started

Attack finished

Click the **Go to Channels** button. You can return to the current form later to make changes.



Add notification

Email

You don't have any addresses added yet

Email

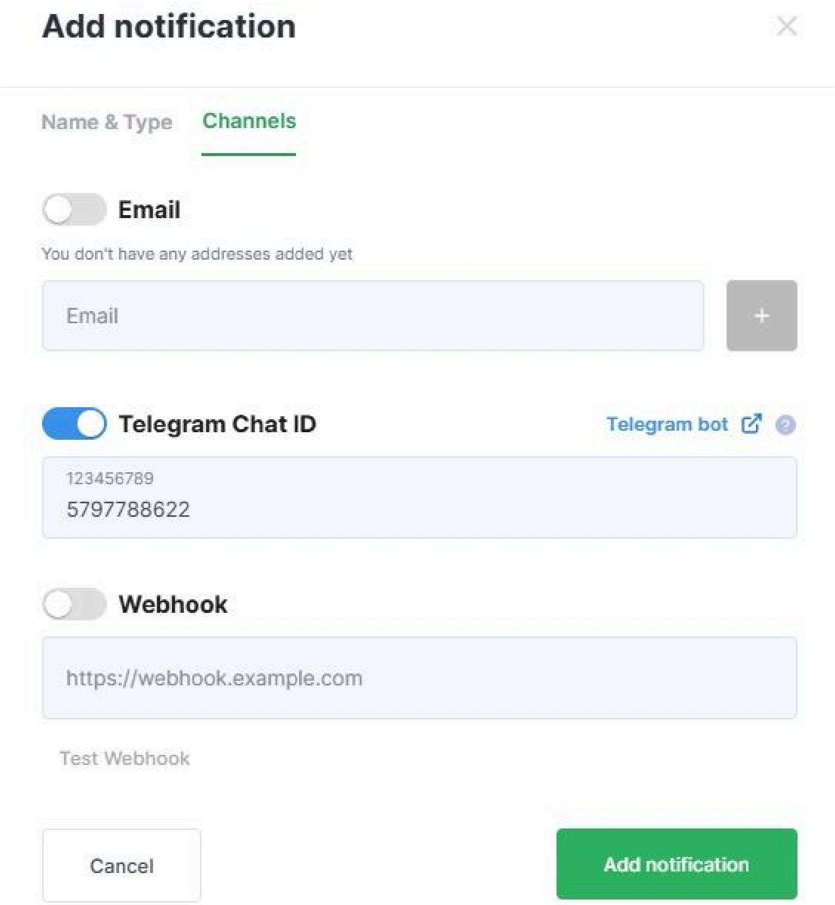
Telegram Chat ID

123456789

Webhook

https://webhook.example.com

Fill in one or more channels for sending notifications. To set up notifications in Telegram, click the **Telegram bot** button to open the bot page. Type and send the «/start» command. A code will be sent in the reply message, which you should enter in the **Telegram Chat ID** area.



Email

You don't have any addresses added yet

Email

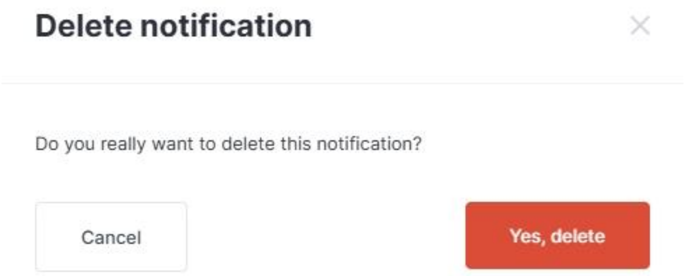
Telegram Chat ID

123456789
5797788622

Webhook

https://webhook.example.com

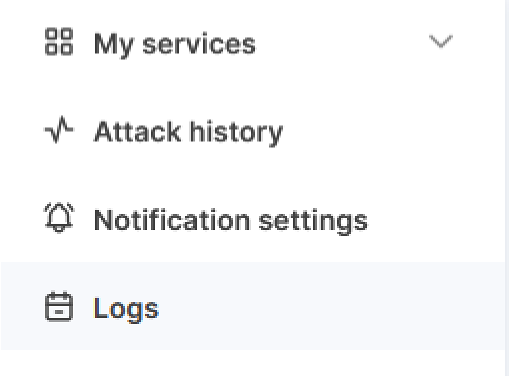
Click the **Add Notification** button to save the entered data. The created notification will appear in the table. To edit a notification, click the «pencil» button in the object field. The fields of the form that opens match those of the new notification creation form. To delete a notification, click the **X** button in the object field and confirm the action in the dialog box.



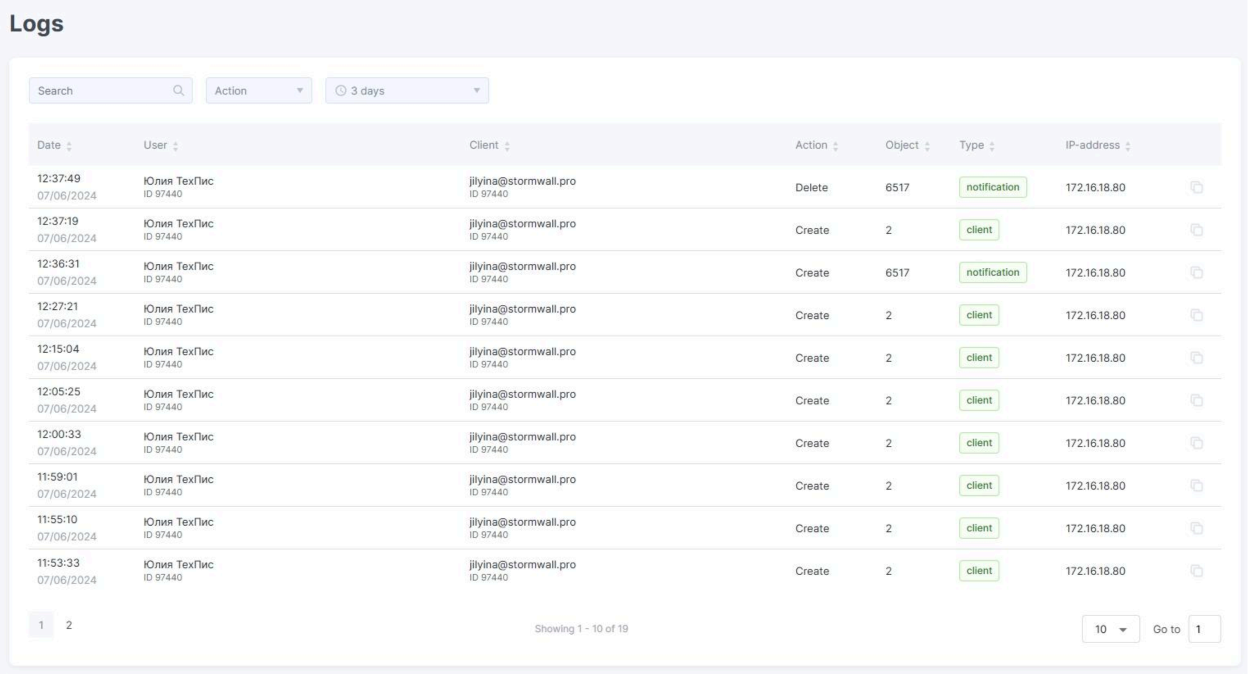
Do you really want to delete this notification?

Logs

In the left sidebar of the client panel, select the **Logs** option.



On the page that opens, there is a table with data about all the actions of the account's users. Use the **Search** field to filter and the time filter for more specific queries. You can also filter by user action by selecting it from the **Action** dropdown menu. In the last column of the table, each entry has a «Copy» icon for copying all the information.



Date	User	Client	Action	Object	Type	IP-address
12:37:49 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Delete	6517	notification	172.16.18.80
12:37:19 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Create	2	client	172.16.18.80
12:36:31 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Create	6517	notification	172.16.18.80
12:27:21 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Create	2	client	172.16.18.80
12:15:04 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Create	2	client	172.16.18.80
12:05:25 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Create	2	client	172.16.18.80
12:00:33 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Create	2	client	172.16.18.80
11:59:01 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Create	2	client	172.16.18.80
11:55:10 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Create	2	client	172.16.18.80
11:53:33 07/06/2024	Юлия ТехПис ID 97440	jilyina@stormwall.pro ID 97440	Create	2	client	172.16.18.80

Users

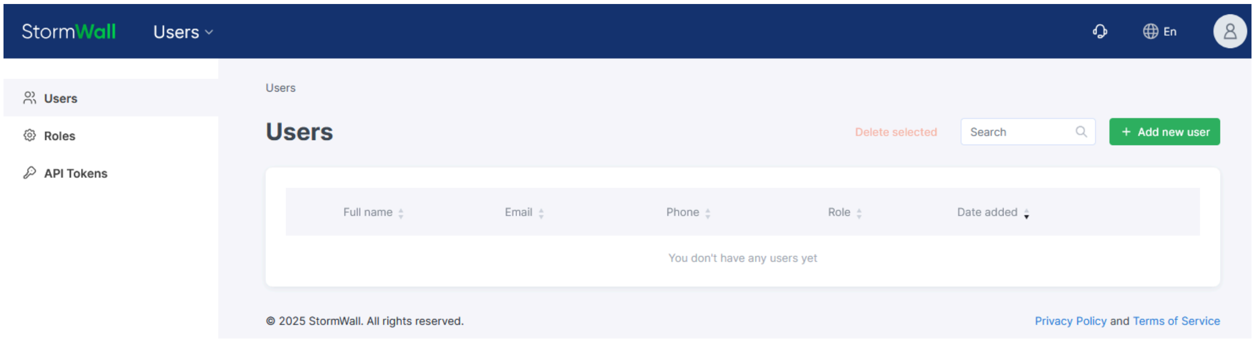
Log in to your personal account on the StormWall website.

In the top panel, select the **Users** section. The following menu will open in the left panel:

- **Users**
- **Roles**
- **Tokens**

Users

On the **Users** page, you can create, edit, or delete sub-accounts.



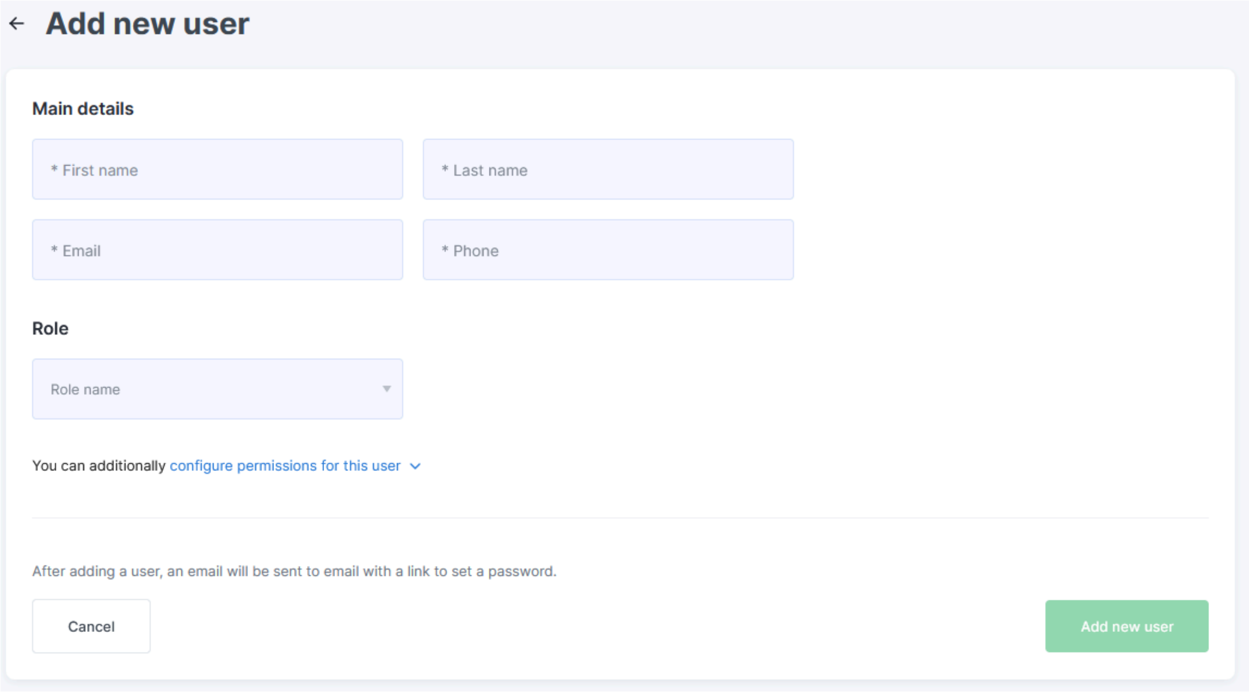
You don't have any users yet

© 2025 StormWall. All rights reserved.

Privacy Policy and Terms of Service

Creation

To create a sub-account, click the **Add User** button.



You can additionally configure permissions for this user

After adding a user, an email will be sent to email with a link to set a password.

Fill in the required fields in the form:

- First Name
- Last Name
- Email
- Phone
- Role (select from the dropdown list).

You can fine-tune the user's permissions by expanding the **configure permissions for this user...** and selecting the necessary rights.

After completing the configuration, click the **Add new user** button.

Note: If the «Single Sign-On (SSO)» permission is enabled, a ticket created by the user will appear as created by the main account.

Editing

To change the parameters of a sub-account, click the edit icon in its row.

A form for modifying the data will open.

You can reset the password and update the data. To confirm the changes, click the **Save** button.

Deletion

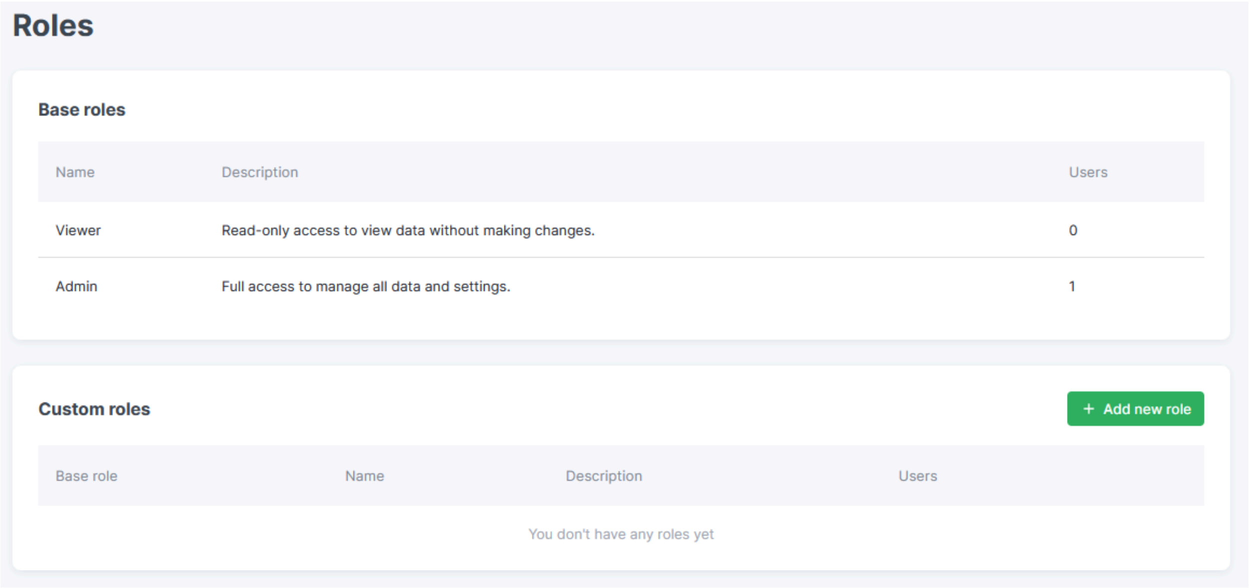
To delete users, select the accounts and click the **Delete Selected** button. To delete a single entry, click the **X** symbol in its row.

If an error message appears when creating a sub-account, it may indicate that the specified email address already has its own account. In this case, use a different email address.

Roles

On the **Roles** page, you can create, edit, or delete additional user roles.

For example, you can create a custom role and assign it only the right to receive notifications.



Roles

Base roles

Name	Description	Users
Viewer	Read-only access to view data without making changes.	0
Admin	Full access to manage all data and settings.	1

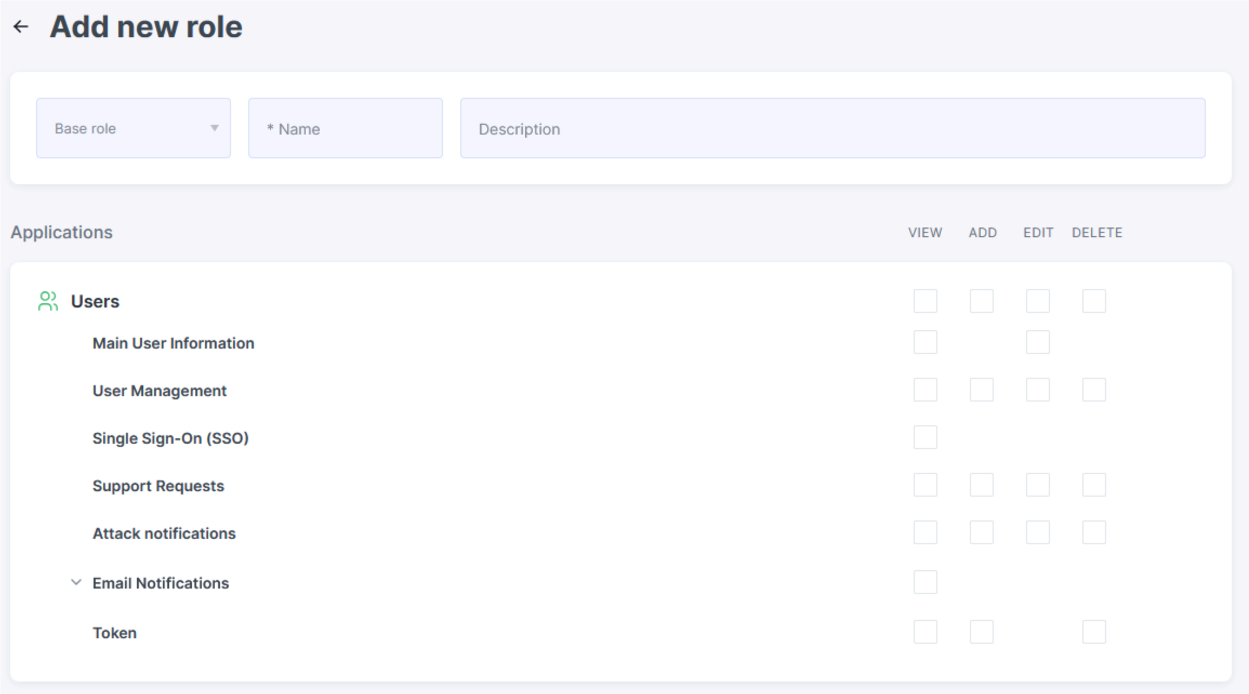
Custom roles

Base role	Name	Description	Users

You don't have any roles yet

Creation

New roles are based on default roles. To create a new role, click the **Add new role** button.



← Add new role

Base role ▾ | * Name | Description

Applications	VIEW	ADD	EDIT	DELETE
Users	□	□	□	□
Main User Information	□		□	
User Management	□	□	□	□
Single Sign-On (SSO)	□			
Support Requests	□	□	□	□
Attack notifications	□	□	□	□
Email Notifications	□			
Token	□	□		□

Fill in the required fields in the form:

- Base Role
- Name

Optionally, add a description for the role.

Select access levels for the role by checking the following options:

- VIEW
- ADD
- EDIT
- DELETE

After completing the configuration, click the **Create** button (under forms).

Editing

To modify the parameters of a role, click the edit icon in its row.

A form for editing the data will open.

After making changes, click the **Save Changes** button to save the data.

Deletion

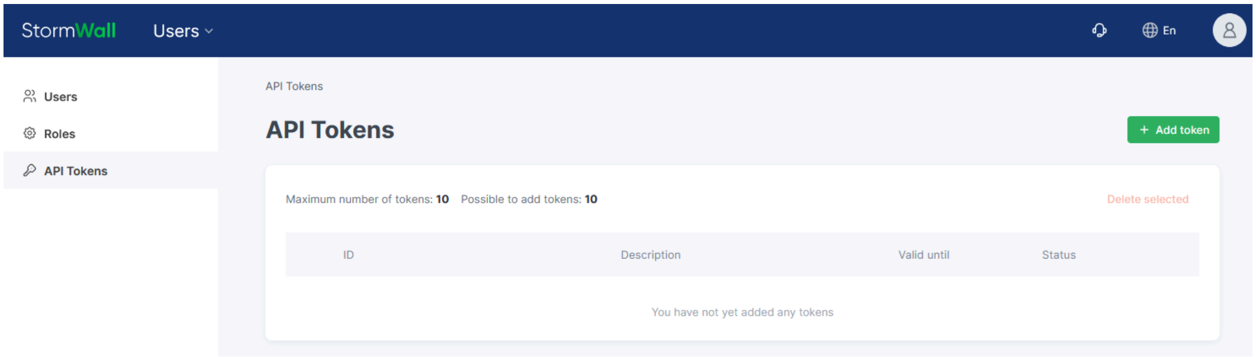
To delete a role, click the **X** symbol in its row.

Confirm the deletion in the dialog box by clicking the **Yes, delete** button.

Tokens

On the **Tokens** page, you can create and delete tokens.

The service generates an API token for an application to use when requesting information from the service. For more detailed information about using the API, refer to the relevant section of the instructions.



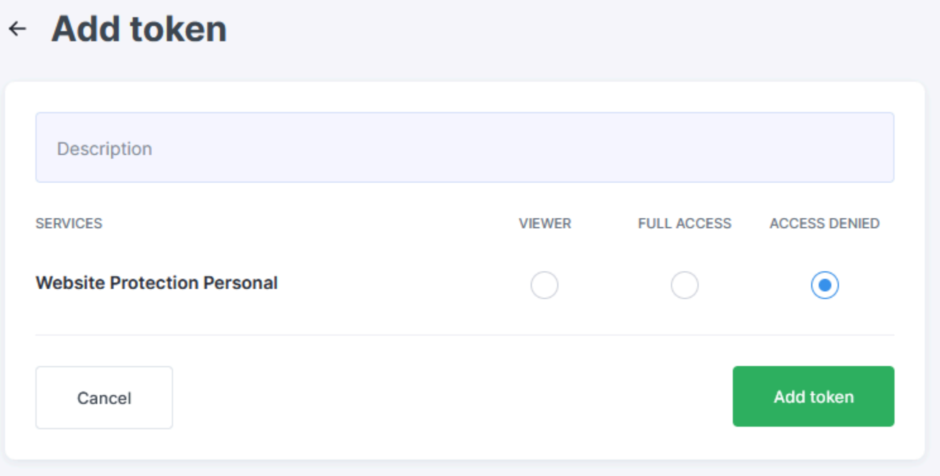
Maximum number of tokens: **10** Possible to add tokens: **10**

ID	Description	Valid until	Status

You have not yet added any tokens

Creation

To create a new token, click the **Add Token** button.



SERVICES	VIEWER	FULL ACCESS	ACCESS DENIED
Website Protection Personal	○	○	●

Define the access level for each service. After completing the configuration, click the **Add Token** button.

Copy the generated token and store it securely.

Note: Tokens cannot be edited, but you can delete them and create new ones. Tokens do not apply to services added after their creation. To work with new services, a new token must be created.

Deletion

To delete a token, click the **X** symbol in its row.

Confirm the deletion in the dialog box by clicking the **Yes, delete** button.

Website protection

How the Service Works

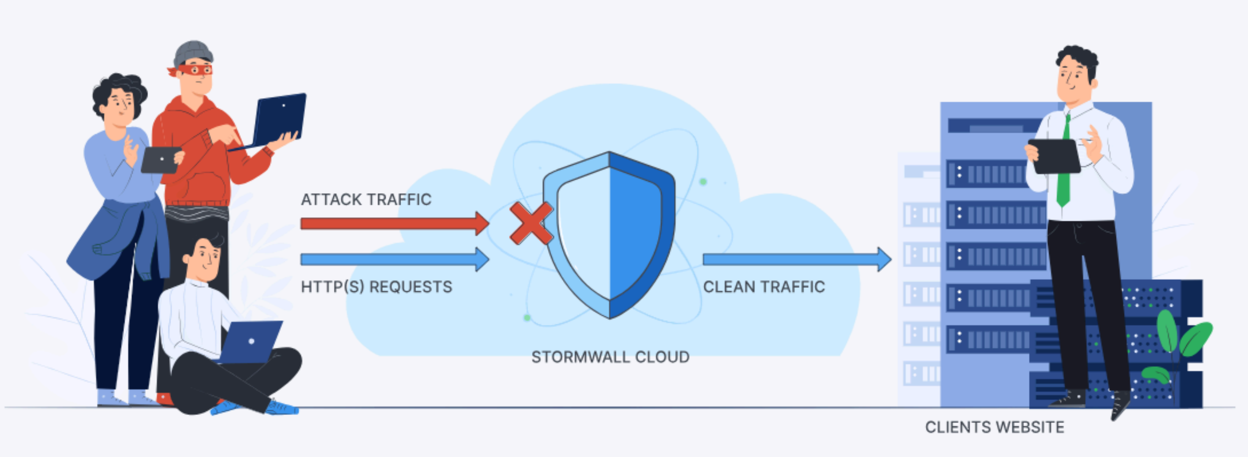
The «StormWall for Web» service safeguards against attacks through proxying, allowing your site to retain its current hosting.

Every online resource has a limit to the number of requests it can handle simultaneously. During an attack, this limit is exceeded, causing the resource's operation to slow down or halt entirely. By utilizing our protection, you ensure that your resource remains operational even under the most severe attacks.

Workflow Algorithm:

1. You receive a protected address in the StormWall cloud.
2. The DNS record of your site is redirected to this protected address.
3. Traffic from site visitors is filtered and optimized.
4. Attack traffic is blocked.
5. Only safe traffic is directed to your server, with real visitor IP addresses maintained in the HTTP header.

This approach ensures that legitimate traffic reaches your site without interruption, while malicious traffic is identified and blocked before it can cause harm.

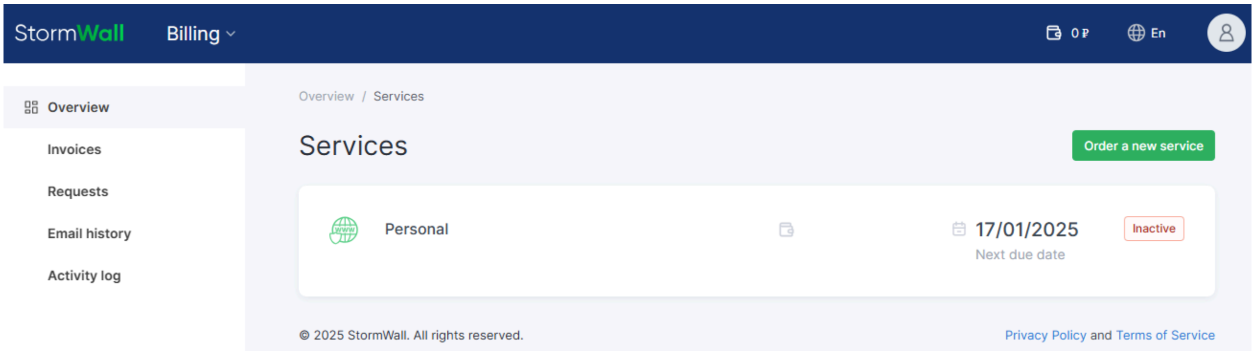


Order

To set up website protection:

1. Log in to your **Client Portal** on the website;

2. On the top panel of the site, select the **Billing** tab and click on the **Order a new service** button;



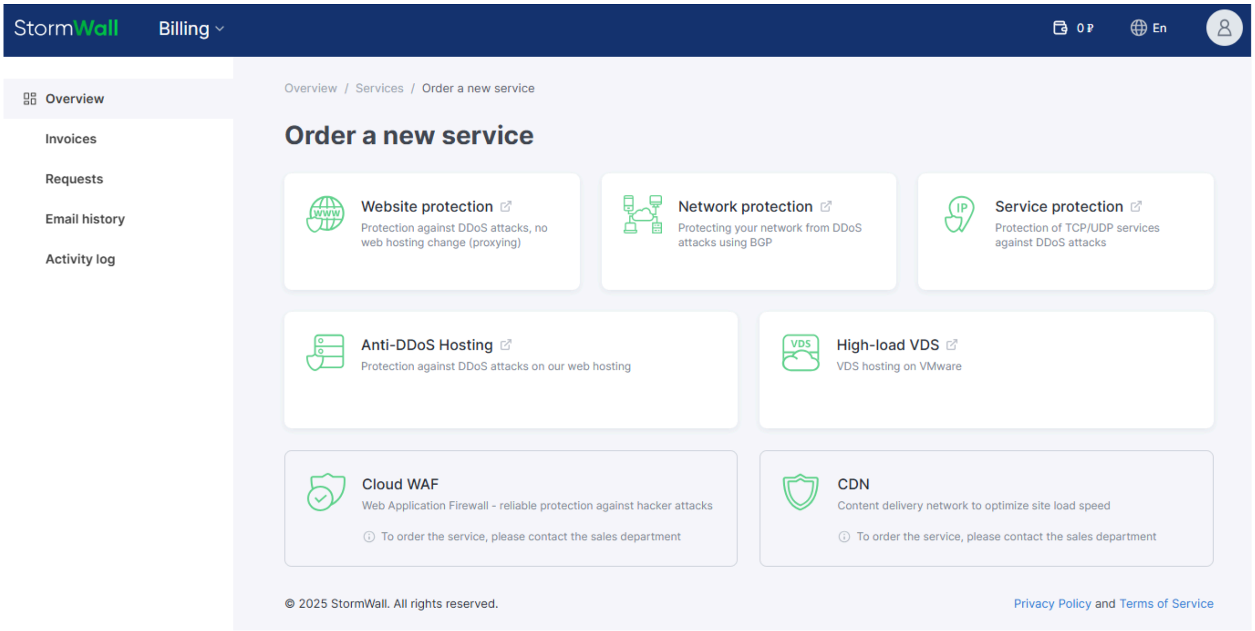
Services

Personal — 17/01/2025 Next due date — Inactive

© 2025 StormWall. All rights reserved.

Privacy Policy and Terms of Service

3. In the tab that opens, select the **Website Protection** item;



Order a new service

Website protection
Protection against DDoS attacks, no web hosting change (proxying)

Network protection
Protecting your network from DDoS attacks using BGP

Service protection
Protection of TCP/UDP services against DDoS attacks

Anti-DDoS Hosting
Protection against DDoS attacks on our web hosting

High-load VDS
VDS hosting on VMware

Cloud WAF
Web Application Firewall - reliable protection against hacker attacks
To order the service, please contact the sales department

CDN
Content delivery network to optimize site load speed
To order the service, please contact the sales department

© 2025 StormWall. All rights reserved.

Privacy Policy and Terms of Service

4. You will be redirected to a website page with a detailed description of the service.
5. Review the information about the service and the pricing plans:
   - Personal;
   - Business ONE;
   - Enterprise ONE.

Please note that protection without certificate disclosure is only available on the «Enterprise» plan.

If none of the available pricing plans meet your requirements, please contact us — we will make a special offer for you.

Activation

After connecting and paying for the service, there are a few steps left to complete the configuration.

We have allocated a secured IP address for you. You now need to change the A-record of your domain in DNS to this secured IP address.

For the protection system to work correctly, you need to add our outgoing addresses to your trusted list: remove all restrictions in the Firewall and at the Web server level. Here are our outgoing network ranges:

- 185.121.240.0/22
- 193.84.78.0/24
- 103.134.155.0/24
- 188.0.150.0/24
- 193.104.120.0/24

You can use the following commands:

```
iptables -I INPUT -s 185.121.240.0/22 -j ACCEPT

iptables -I INPUT -s 193.84.78.0/24 -j ACCEPT

iptables -I INPUT -s 103.134.155.0/24 -j ACCEPT

iptables -I INPUT -s 188.0.150.0/24 -j ACCEPT

iptables -I INPUT -s 193.104.120.0/24 -j ACCEPT
```

If attackers know the direct IP of your web server, we recommend blocking connections to ports 80 and 443 for all networks except for local connections and connections from our networks:

```
iptables -I INPUT -p tcp -m multiport —dports 80,443 -j DROP

iptables -I INPUT -i lo -j ACCEPT

iptables -I INPUT -s 185.121.240.0/22 -j ACCEPT

iptables -I INPUT -s 193.84.78.0/24 -j ACCEPT

iptables -I INPUT -s 103.134.155.0/24 -j ACCEPT

iptables -I INPUT -s 188.0.150.0/24 -j ACCEPT

 iptables -I INPUT -s 193.104.120.0/24 -j ACCEPT

iptables -I INPUT -s 127.0.0.1 -j ACCEPT

iptables -I INPUT -s IP.your.web.server -j ACCEPT

iptables -I INPUT -m conntrack —ctstate RELATED,ESTABLISHED -j ACCEPT
```

After this, you need to restart your web server process. Information about real IP addresses of users when protection is enabled is passed in the HTTP headers X-Real-IP and X-Forwarded-For. To display real IP addresses, you need to configure mod_rpaf for Apache web servers, mod_remoteip for Apache > 2.3, or http_real_ip for Nginx, so that your web server can correctly process these headers.

Nginx Configuration

In the configuration file /etc/nginx/nginx.conf, under the http or server section, add:

```
set_real_ip_from 185.121.240.0/22;

set_real_ip_from 193.84.78.0/24;
set_real_ip_from 103.134.155.0/24;

set_real_ip_from 188.0.150.0/24;

set_real_ip_from 193.104.120.0/24;

real_ip_header X-Forwarded-For.
```

Save the configuration file and restart Nginx with:

```
service nginx restart
```

Apache Configuration (mod_rpaf)

In the module's configuration file, enter the following settings.

In the module configuration file, add:

```
RPAFenable On

RPAFsethostname On

RPAFproxy_ips 127.0.0.0 185.121.240.0/22 193.84.78.0/24 103.134.155.0/24 188.0.150.0/24 193.104.120.0/24

RPAFheader X-Forwarded-For
```

Apache Configuration (mod_remoteip)

In the module's configuration file, enter the following settings:

```
RemoteIPHeader X-Forwarded-For

RemoteIPInternalProxy 127.0.0.1 185.121.240 185.121.241 185.121.242 185.121.243 103.134.155 188.0.150 193.84.78 193.104.120
```

Save the configuration file and restart Apache with:

```
service apache2 restart
```

For IIS configuration, follow the steps in this guide: https://techcommunity.microsoft.com/t5/iis-support-blog/how-to-use-x-forwarded-for-header-to-log-actual-client-ip/ba-p/873115.

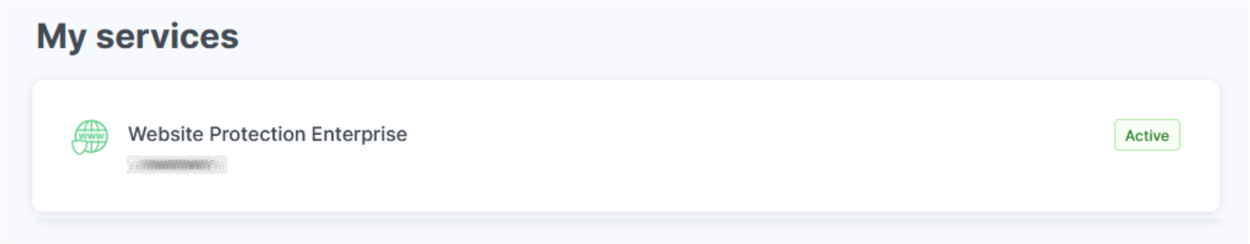
If you need assistance with these settings, please let us know. Also, be aware of the following:

- If SSL (HTTPS) is used on your site, you can configure it in detail in your account.
- If you use WebSockets, inform us which ports need to be opened on our side.
- You may also use our DNS servers; please inform us in advance through a ticket.
- When using site protection, do not disclose the direct IP address of the server. Mail sending should be done through an external relay. For protecting other applications, use our service protection service.

For any setup difficulties, please contact us via chat on the website or through the inquiry form in your account.

Configuring protection settings

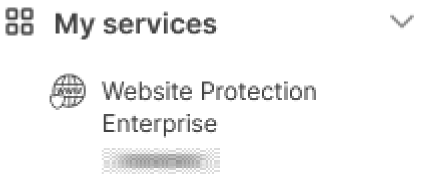
After the service is connected, it will show up on the main page of your account and under **My Services**. To start configuring it, simply click on the service name to access the settings area.



My services

Website Protection Enterprise
[redacted]

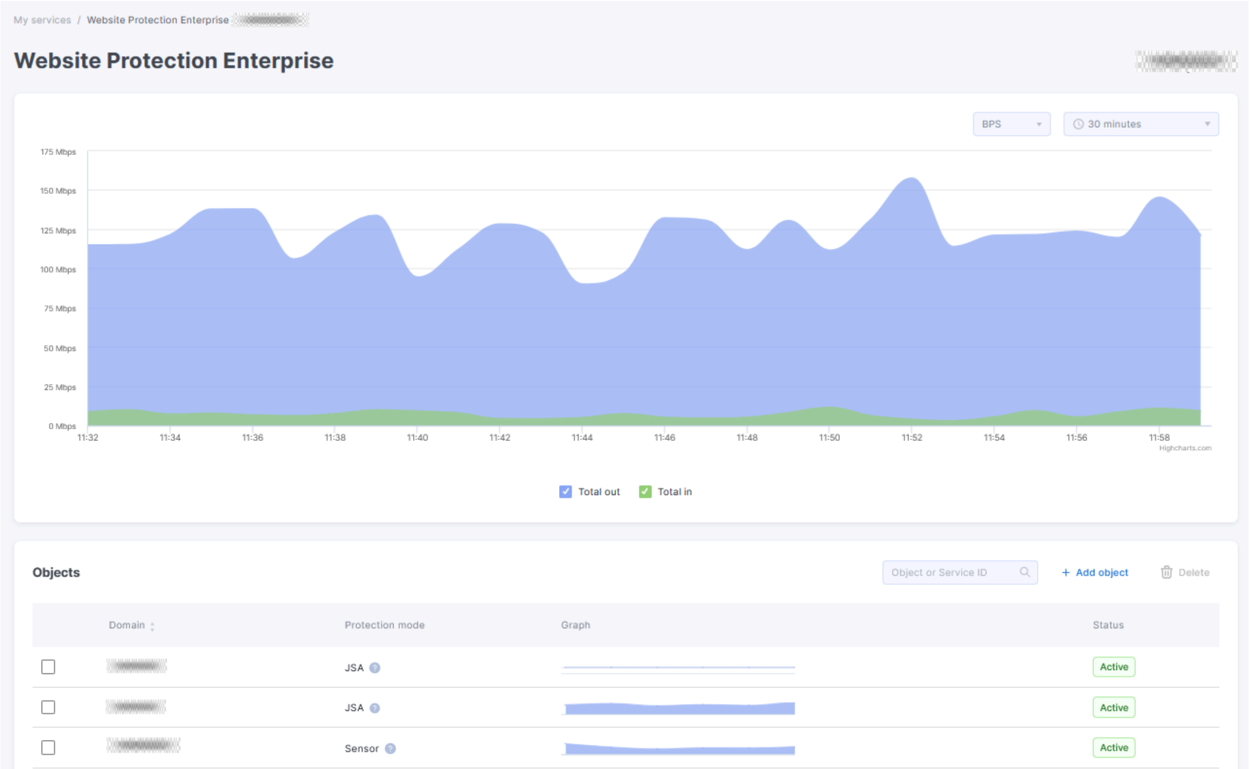
Active



My services

Website Protection Enterprise
[redacted]

On the page that opens, select the object you are interested in and click on its line with a graph thumbnail next to it.



My services / Website Protection Enterprise [redacted]

Website Protection Enterprise [redacted]

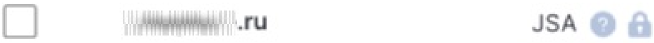
BPS ▾ 30 minutes ▾

Objects

Object or Service ID + Add object Delete

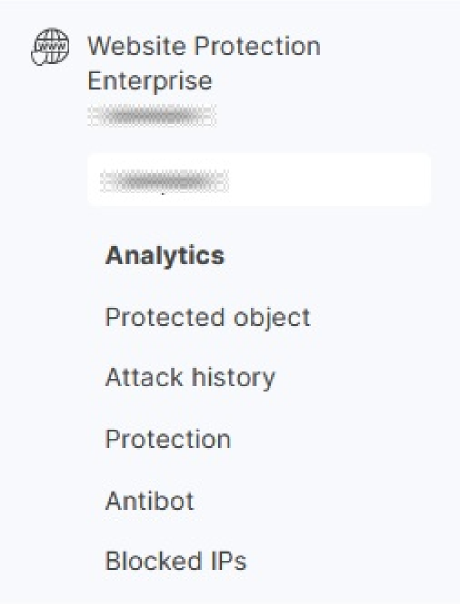
	Domain	Protection mode	Graph	Status
□	[redacted]	JSA		Active
□	[redacted]	JSA		Active
□	[redacted]	Sensor		Active

Please note - an icon in the shape of a padlock in the table row indicates that the domain has a restriction on changing its protection.



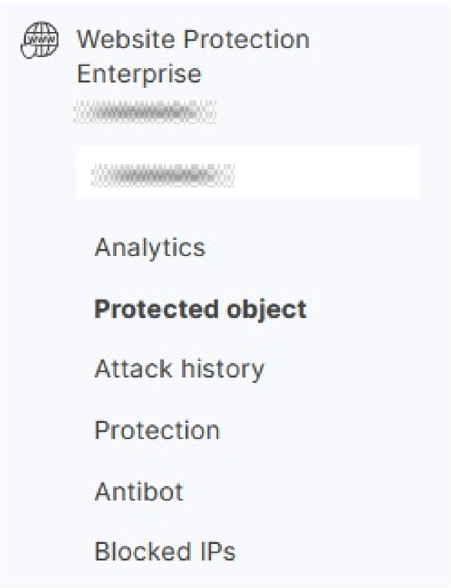
□ [redacted].ru JSA

After selecting a domain on the left side of the screen, a menu will open where the current selection is **Analytics**.



Protected object

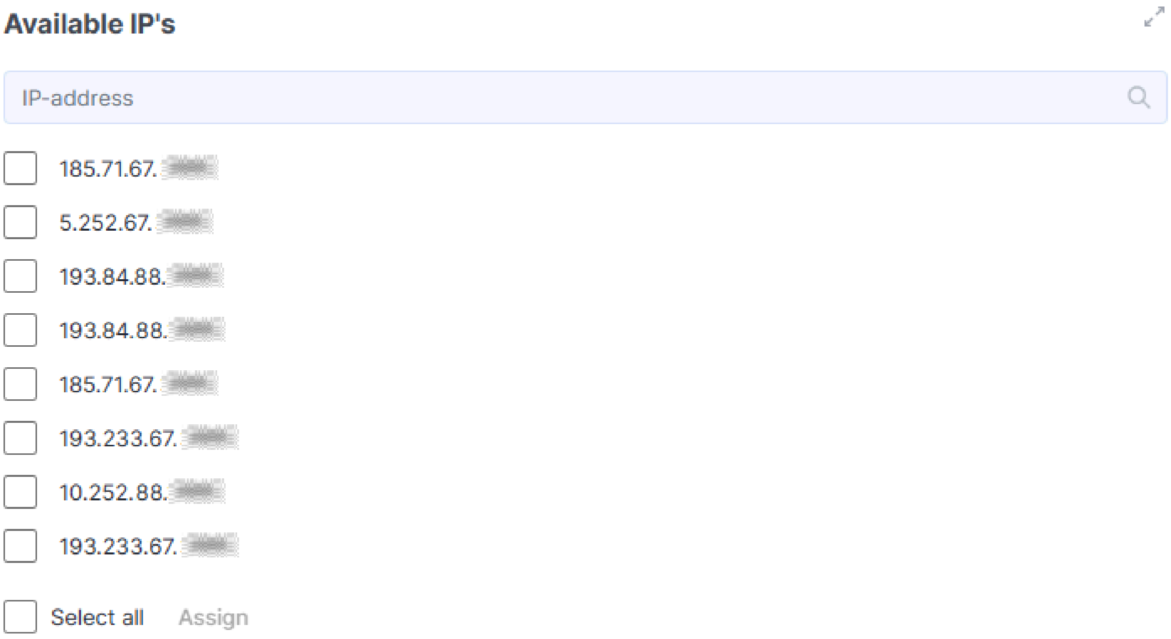
In the left menu, select the **Protected object** item.



On the page that opens, customizable parameters are presented for you to configure according to your needs or preferences:

- Available IP’s

On the page that opens, you will find configurable parameters, including **Available IP’s**. To assign an IP address from the list of options provided to you, select it by checking the box at the beginning of the row, and then click on the **Assign** button. We will provide you with several IP addresses and you will be able to assign them to your domains yourself.



Available IP's

IP-address

□ 185.71.67.[redacted]

□ 5.252.67.[redacted]

□ 193.84.88.[redacted]

□ 193.84.88.[redacted]

□ 185.71.67.[redacted]

□ 193.233.67.[redacted]

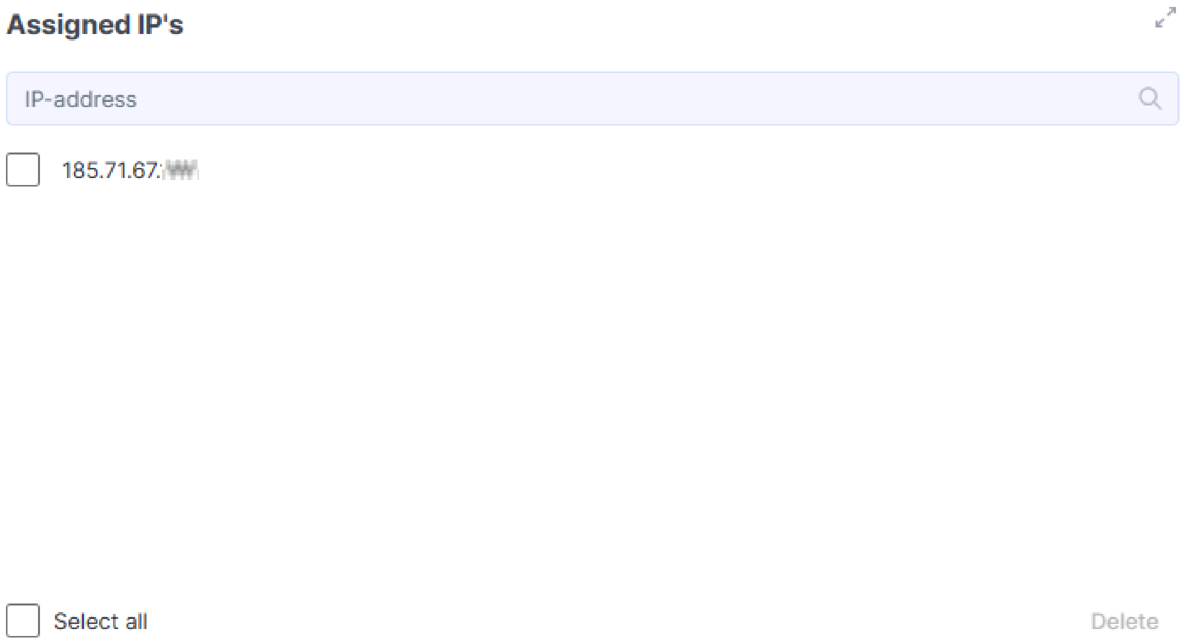
□ 10.252.88.[redacted]

□ 193.233.67.[redacted]

□ Select all Assign

- Assigned IP’s

You can remove IP addresses from the list of assigned ones. To do this, select the address you no longer need by checking the box at the beginning of its row, and then click on the **Delete** button.



Assigned IP's

IP-address

□ 185.71.67.[redacted]

□ Select all

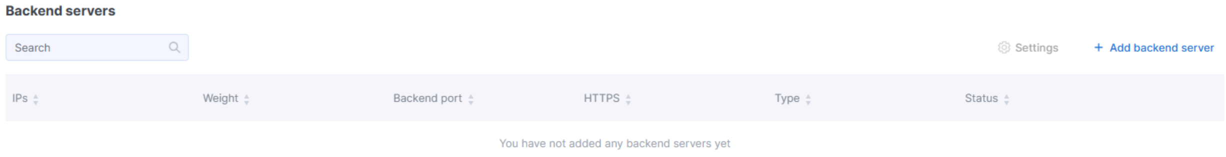
Delete

- **Backend servers**

By default, the service provides a traffic balancing feature. To configure it, you can specify several internal (backend) servers. Each of them must be assigned a weight coefficient and designated as either «active» or «backup».

In normal operation, load balancing will be performed by the active backend servers. If an active server fails, a backup server will take its place.

You can also specify the protocol used to access the backend servers: HTTP (port 80) or HTTPS (port 443).



Backend servers

Search

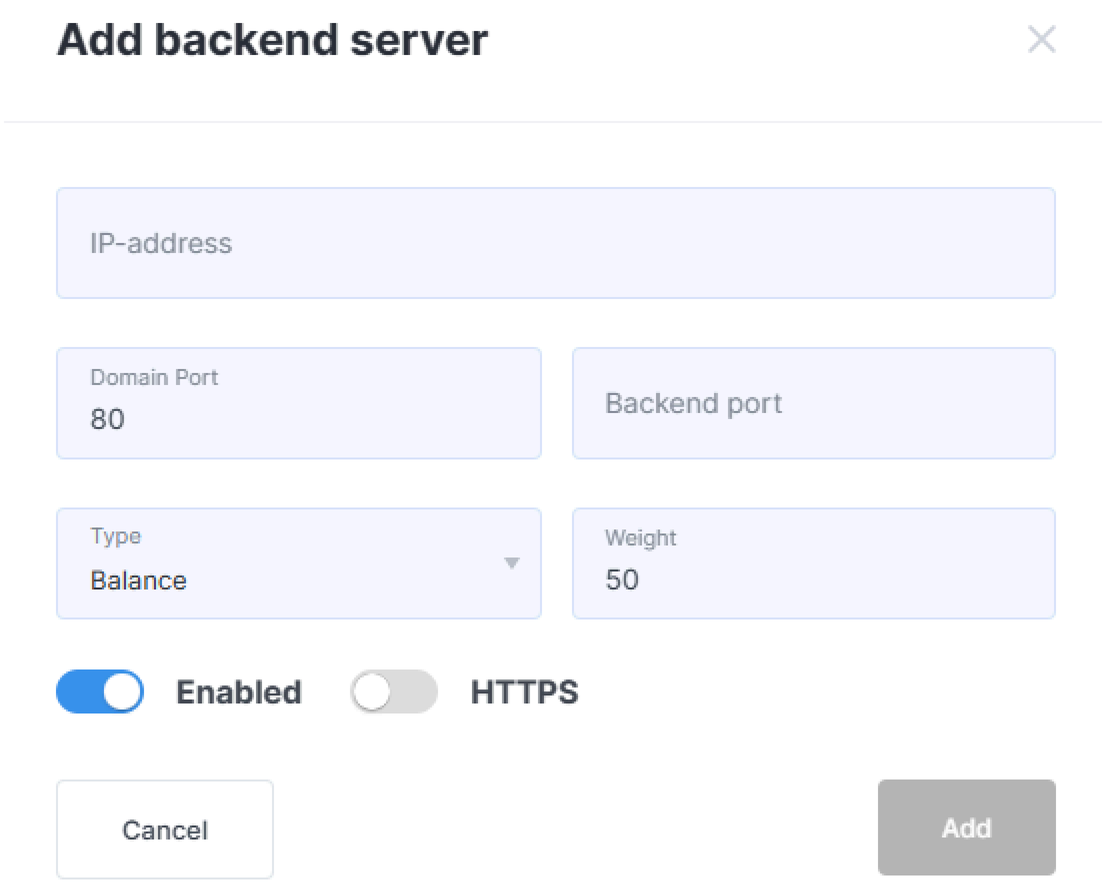
Settings

+ Add backend server

IPs	Weight	Backend port	HTTPS	Type	Status

You have not added any backend servers yet

To add a backend server, click on the **Add backend server** button. Fill out the form and press the **Add** button. You can modify the created backend server using the **Settings** button.



Add backend server

IP-address

Domain Port: 80

Backend port

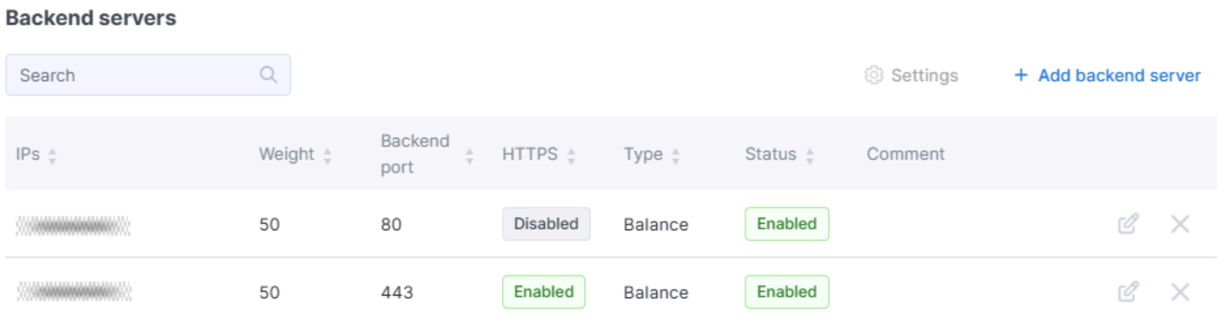
Type: Balance

Weight: 50

Enabled: on

HTTPS: off

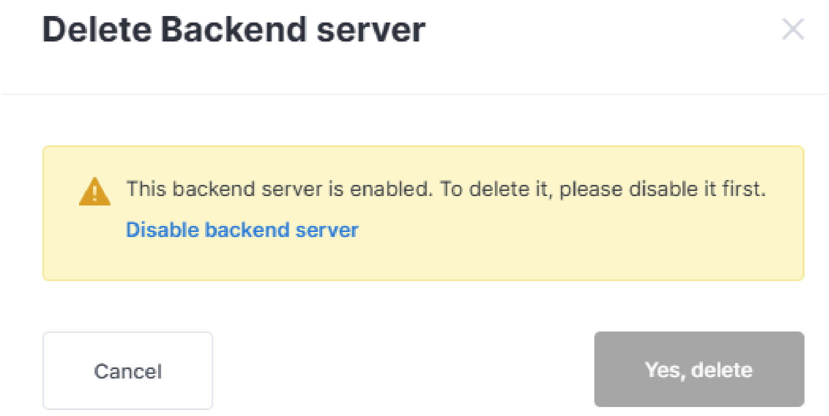
Added objects will appear in the table. Using the buttons on the right side of each row, you can modify or delete a backend server.



Backend servers

IPs	Weight	Backend port	HTTPS	Type	Status	Comment
[redacted]	50	80	Disabled	Balance	Enabled	
[redacted]	50	443	Enabled	Balance	Enabled	

The edit form is identical to the backend addition form. A warning will appear when attempting to delete an enabled backend.


Delete Backend server

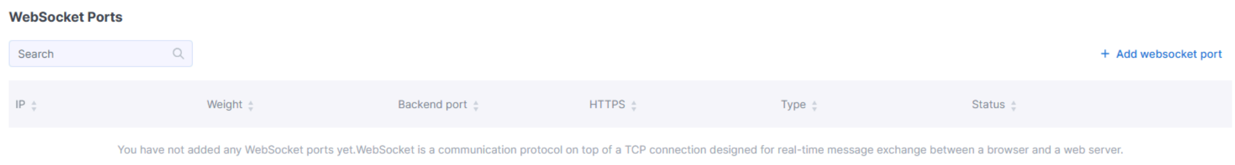
This backend server is enabled. To delete it, please disable it first.

Click the **Disable backend server** button, then confirm its deletion.

- **WebSocket Ports**

Configure settings to protect your website from DDoS attacks through WebSocket protocol vulnerabilities.

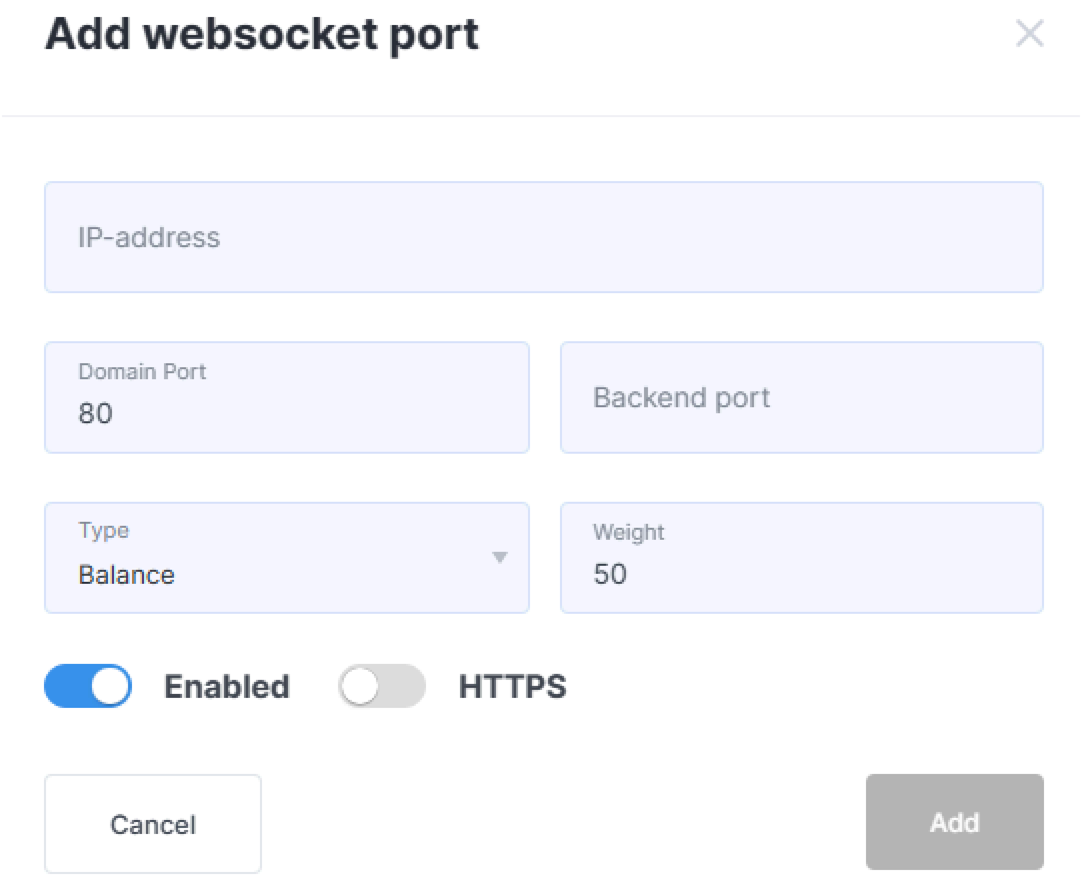
- If your site uses standard ports for the WebSocket protocol (80 and 443), no special server protection settings are required.
- If non-standard ports are used for this protocol, a special configuration is necessary by specifying these ports. If necessary, you can also configure load balancing between backend servers.


WebSocket Ports

IP	Weight	Backend port	HTTPS	Type	Status

You have not added any WebSocket ports yet.WebSocket is a communication protocol on top of a TCP connection designed for real-time message exchange between a browser and a web server.

Click on the **Add websocket port** button. Fill out the form and then press the **Add** button to complete the process. If the **Add websocket port** button is not active, it means that the maximum number of ports has been reached.



Add websocket port

IP-address

Domain Port: 80

Backend port

Type: Balance

Weight: 50

Enabled ● HTTPS ○

- **SSL certificate**

You can obtain a free SSL certificate (from Let’s Encrypt) or install your own. You can also enable or disable redirection from HTTP to HTTPS (or vice versa), which will reduce the load on the end server.

- **Own Certificate**

To check SSL traffic, you need to specify the public key certificate and the private key. On the screen, they will be displayed in a truncated form (to prevent copying). You also need to enter the root and intermediate CA certificates (if applicable).

If you are using your own certificate, you will need to update it yourself when it expires.

Please note: all SSL certificates must start with "BEGIN CERTIFICATE" and end with "END CERTIFICATE". Typically, the certificate validator sends this set of files marked "For Apache/Nginx". The private key of the domain starts with the header "BEGIN RSA PRIVATE KEY".

Before copying the certificate into the form field, make sure that the **Let's Encrypt Certificate** switch is set to OFF.

If you receive a certificate validity error message, you need to check the following:

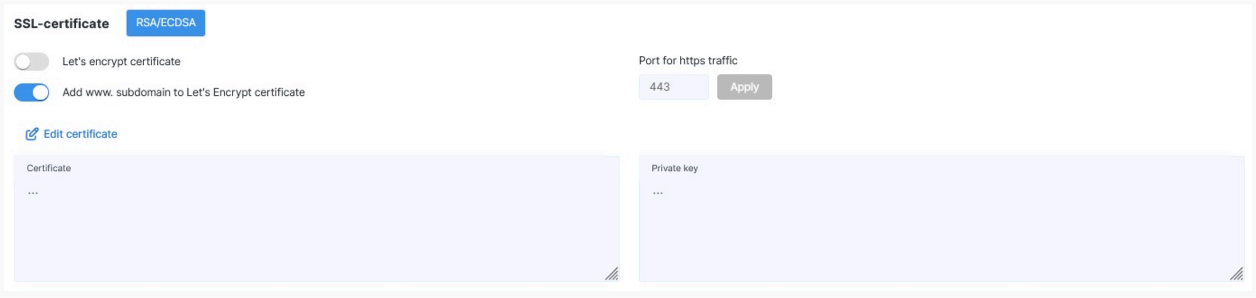
- Verify the certificate fields (Common Name, SANs, Valid)
- Use openssl to compare the hashes of the certificate and the key
- Check the entire certificate chain to ensure it validates correctly.

- **Free New Certificate**

If you do not have a certificate or do not wish to enter its data into the personal account, you can activate the **Let's Encrypt Certificate** option. In this case, client keys are generated and a public key certificate is issued for the protected server. The certificate and key will be re-generated and replaced automatically three days before their expiration date.

To use such a certificate, the primary "A" record of the domain, as well as its www.* record, must point to the obtained protected IP address.

The certificate will be automatically installed within a few minutes. If you receive a DNS record mismatch error, please wait a bit – the domain zone update can take from 15 minutes to several hours, depending on the previously specified TTL value in the domain's A record and the settings of internet providers.



SSL-certificate RSA/ECDSA

○ Let's encrypt certificate

● Add www. subdomain to Let's Encrypt certificate

Edit certificate

Certificate ...

Port for https traffic 443 Apply

Private key ...

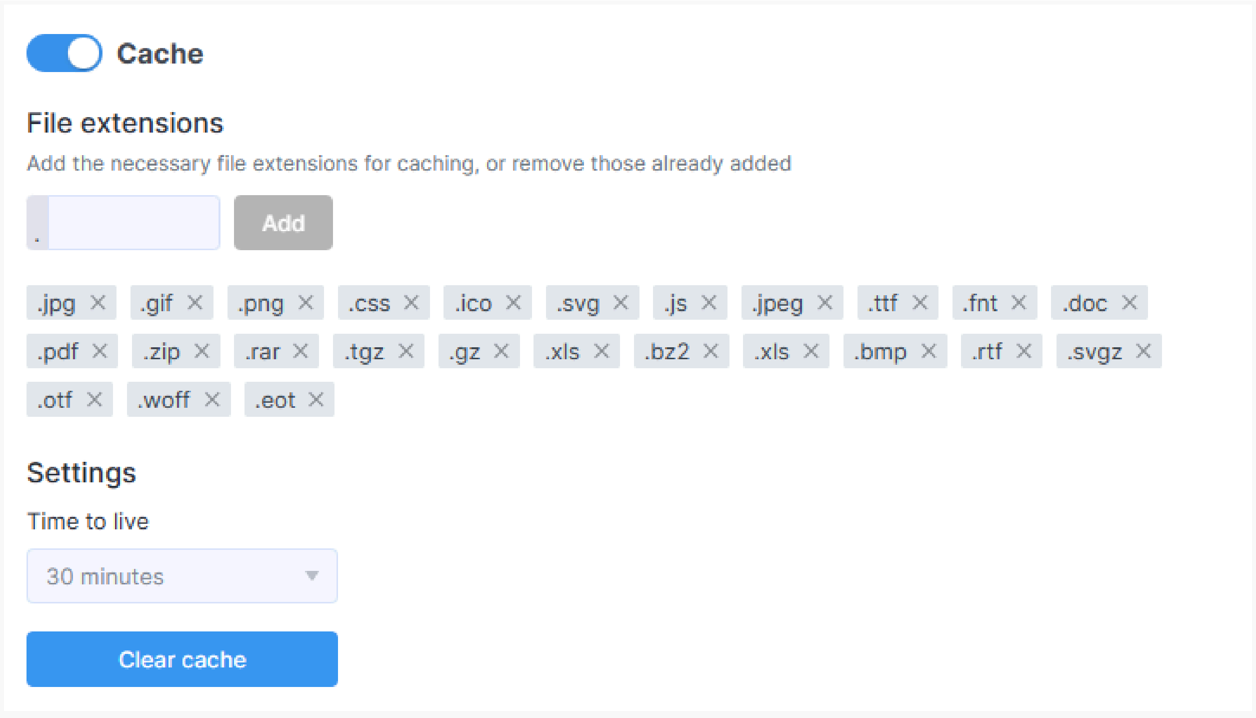
- **Cache**

Thanks to caching, your website will not only be more reliable but also faster.

Caching of static content will be performed in the RAM of caching servers at StormWall scrubbing centers, which significantly reduces the load on the end server.

You can independently set the cache lifetime and the types of files that will be subject to caching. If you need other parameters (geographical restrictions or anything else), please contact technical support.

To enable caching, select the cache lifetime and file extensions, and then set the **Cache** slider to the ON position.



Cache

File extensions

Add the necessary file extensions for caching, or remove those already added

.jpg ✕ .gif ✕ .png ✕ .css ✕ .ico ✕ .svg ✕ .js ✕ .jpeg ✕ .ttf ✕ .fnt ✕ .doc ✕
.pdf ✕ .zip ✕ .rar ✕ .tgz ✕ .gz ✕ .xls ✕ .bz2 ✕ .xls ✕ .bmp ✕ .rtf ✕ .svgz ✕
.otf ✕ .woff ✕ .eot ✕

Settings

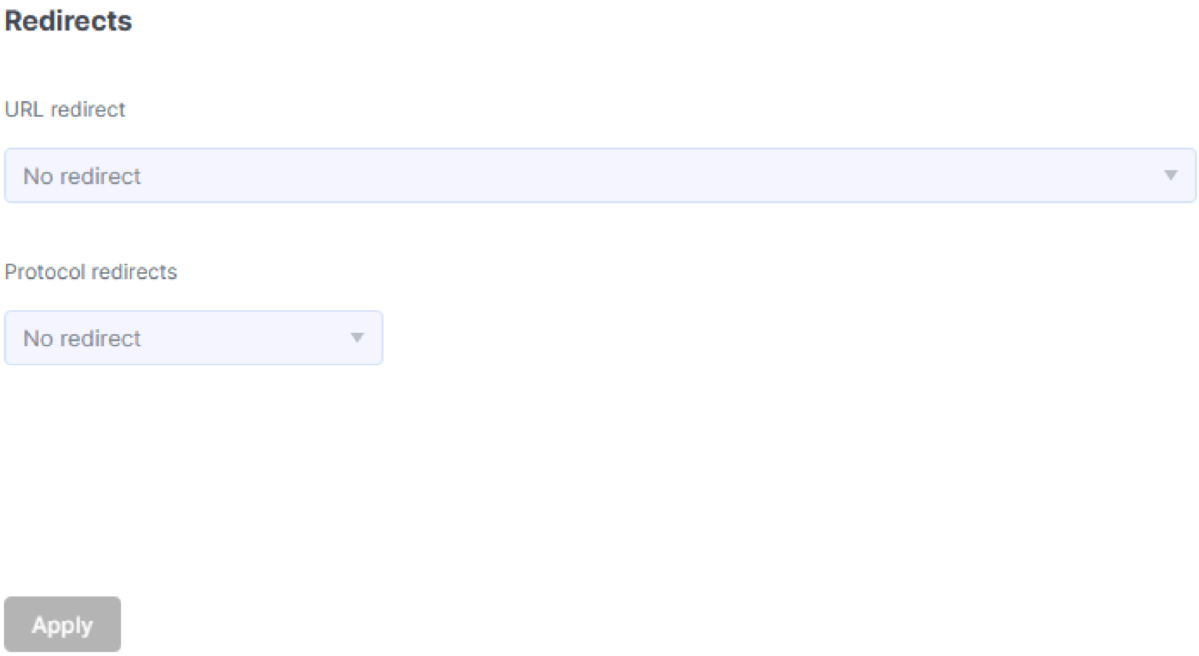
Time to live: 30 minutes

When you press the **Clear cache** button, all data will be reloaded from the resources anew.

- Redirects

Configure the rules for redirecting traffic between different addresses.

For example, here you can set up a redirect from «http» to «https».



Redirects

URL redirect

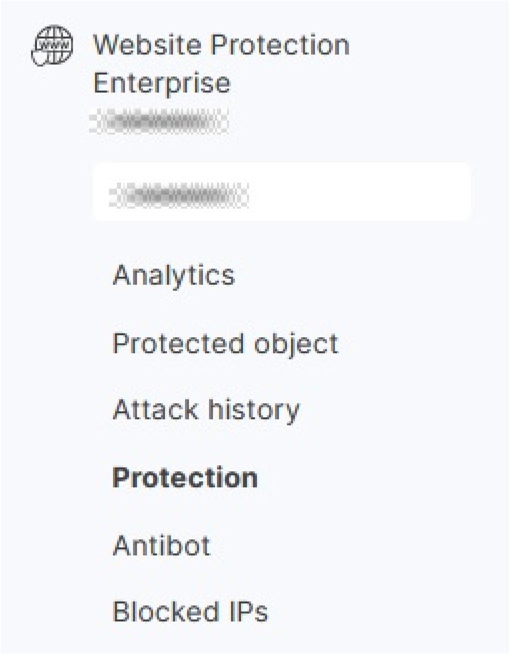
No redirect

Protocol redirects

No redirect

Protection

In the left menu, select the **Protection** item.



On the page that opens, you can configure the parameters:

- **Protection mode**

1. Sensor

   The sensor monitors the total number of requests, spikes, and errors while the filters remain in a passive state. If an attack is detected, the sensor activates the filters to suppress it. The sensor's response time typically does not exceed 1 minute, but it may vary depending on the intensity of the attack.

2. Redirect

   For visitor requests, additional redirection to the requested location is applied.

3. JS validation

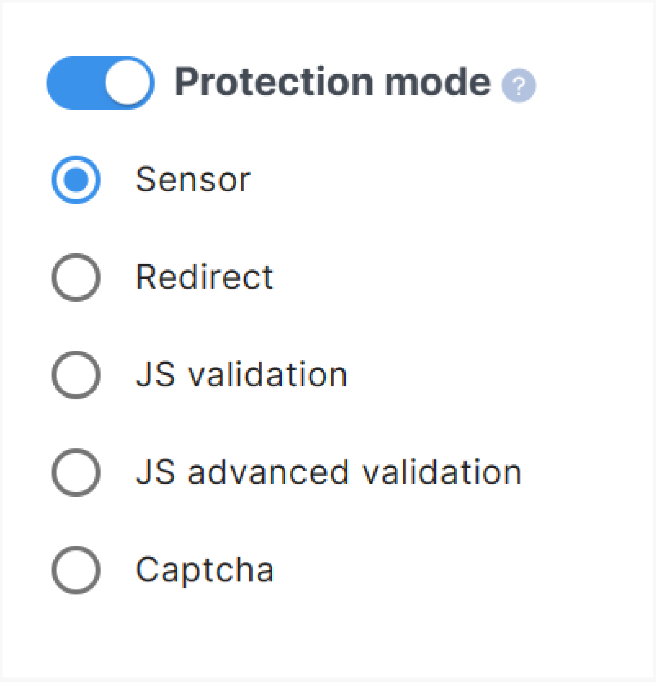
   For requests from regular IP addresses, validation is performed using JavaScript.

4. JS advanced validation

   For requests from regular IP addresses, advanced validation using JavaScript is applied.

5. Captcha

   A request to the site will require passing a Captcha for validation.



Protection mode ?

● Sensor

○ Redirect

○ JS validation

○ JS advanced validation

○ Captcha

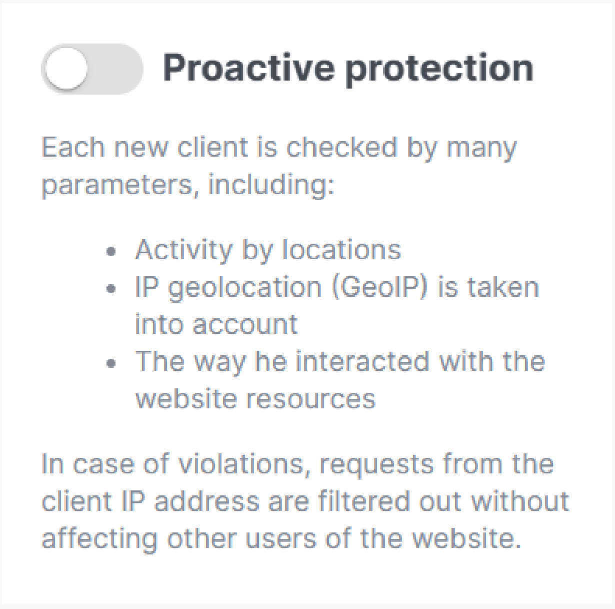
- Proactive protection

The protection is based on the use of a positive usage model. Any users whose behavior does not conform to this model can be blocked or subjected to additional checks (depending on the settings established).

When proactive protection is activated in sensor mode, all requests are not filtered, but each new visitor is checked against many parameters:

- Visited site locations;
- Whether keepalive connections were used;
- Presence of attacks on other sites;
- Whether request limits are exceeded;
- Which User Agents are used;
- Other signs.

In case violations are detected, the user's behavior is monitored. Selective validation allows not to switch the entire configuration into active mode.



Proactive protection

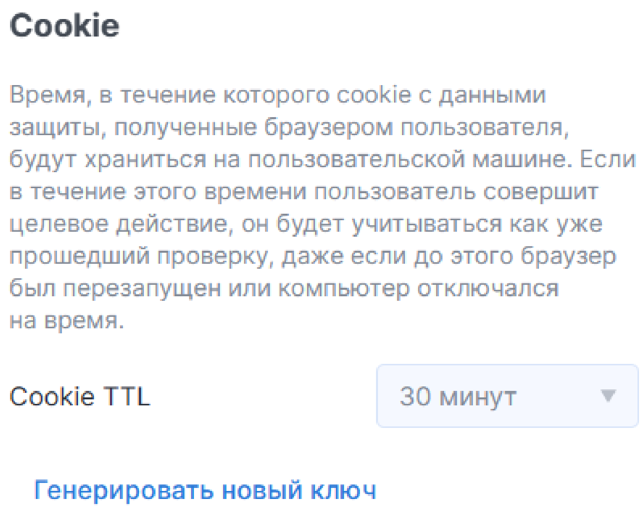
Each new client is checked by many parameters, including:

- Activity by locations
- IP geolocation (GeoIP) is taken into account
- The way he interacted with the website resources

In case of violations, requests from the client IP address are filtered out without affecting other users of the website.

- Cookie

You can set the lifetime of a visitor's session. Once the specified time expires, the user will undergo revalidation. By clicking the **Generate New Security Key** button, each of the active users will be revalidated.



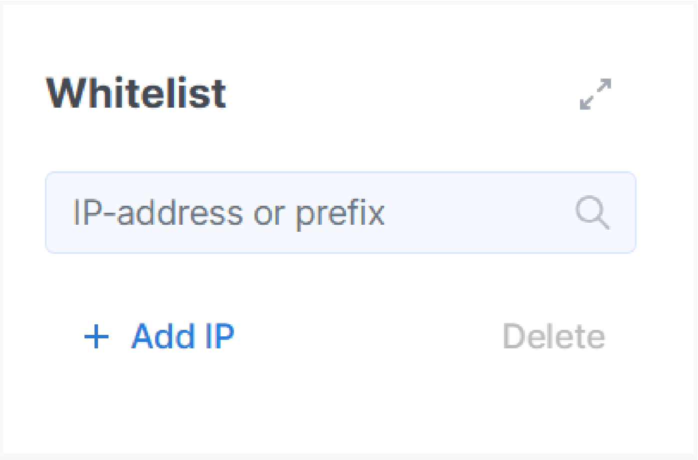
Cookie

Время, в течение которого cookie с данными защиты, полученные браузером пользователя, будут храниться на пользовательской машине. Если в течение этого времени пользователь совершит целевое действие, он будет учитываться как уже прошедший проверку, даже если до этого браузер был перезапущен или компьютер отключался на время.

Cookie TTL 30 минут

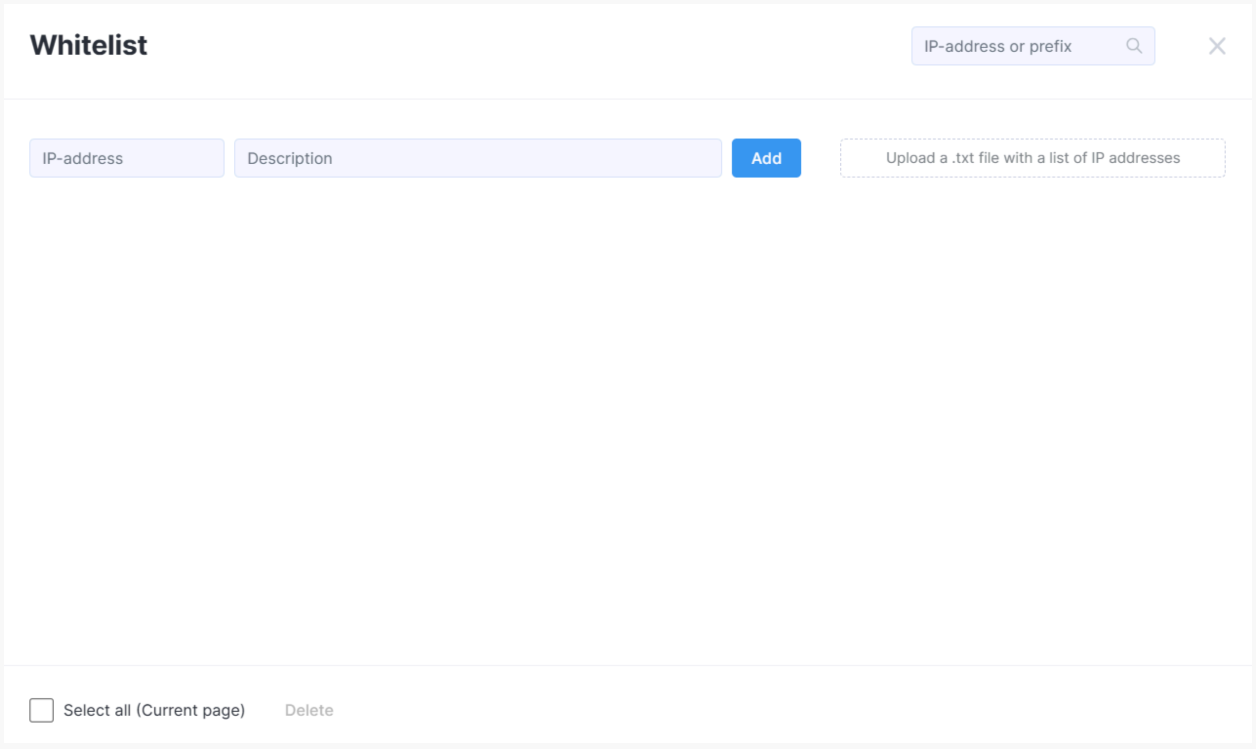
- Whitelist

  Requests from the addresses specified here will be transmitted without filtering.

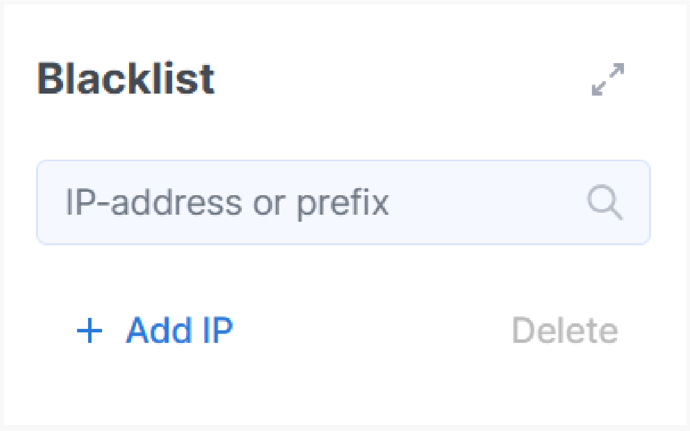


Click on the **Add IP** button and fill out the form to add a new address to the list. You can upload addresses in a ".txt" file format, with each address printed on a separate line.

You can add addresses one at a time (for example, 8.8.8.8) or enter a network with a mask into the list (for example, 8.8.8.0/24).

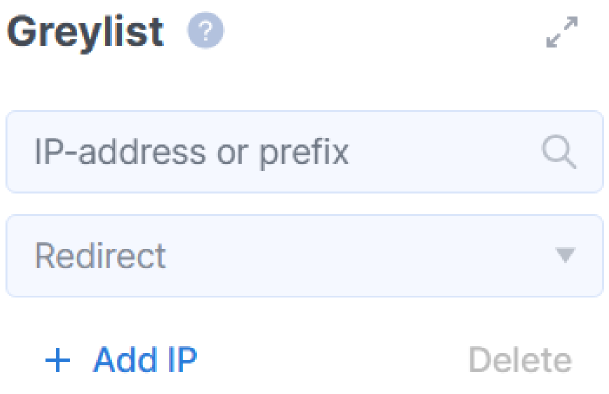

Whitelist
IP-address or prefix
IP-address
Description
Add
Upload a .txt file with a list of IP addresses
□ Select all (Current page)
Delete

- Blacklist
  A user with an address from this list will receive an «HTTP 403 Forbidden» error when trying to access your resource. You can add a new address to the list in a manner similar to the «Whitelist».



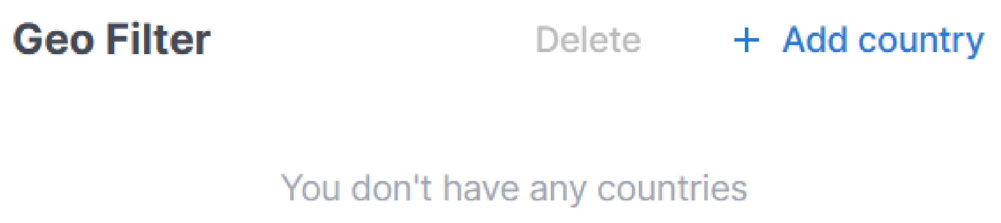
- Greylist

For individual IPs or subnets specified in this list, you can assign a unique protection method, different from that for other addresses. You can add a new address to the list following the same procedure as for the «Whitelist».



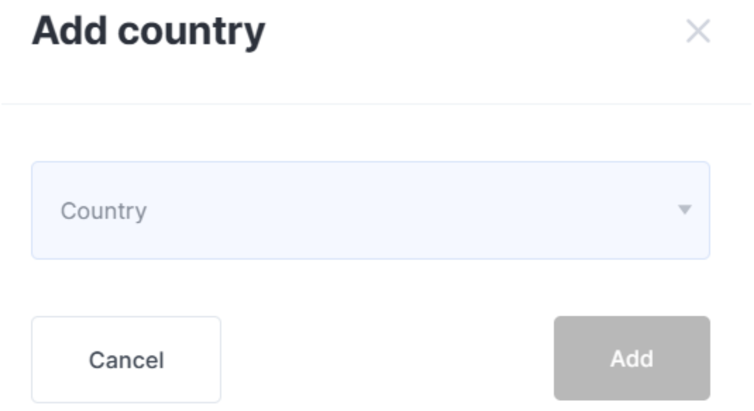
- Geolocation Filter

Here, you can restrict access to your resource based on the visitor's country of origin.



You don't have any countries

Click on the **Add country** button and fill out the form. The countries are provided in a dropdown list.



It is permissible to add no more than 15 countries in one rule when using L3 and L7 filtering without SSL decryption. For L7 filtering with SSL decryption, there are no restrictions on the number of countries.

- Exceptions by location

  For certain requests, it is possible to disable the use of interactive checks. For example, if only bots or mobile applications access a specific server resource, having a check in place could lead to disruptions in the client service's operation. Specify such local resources in the **Location Exceptions** section.

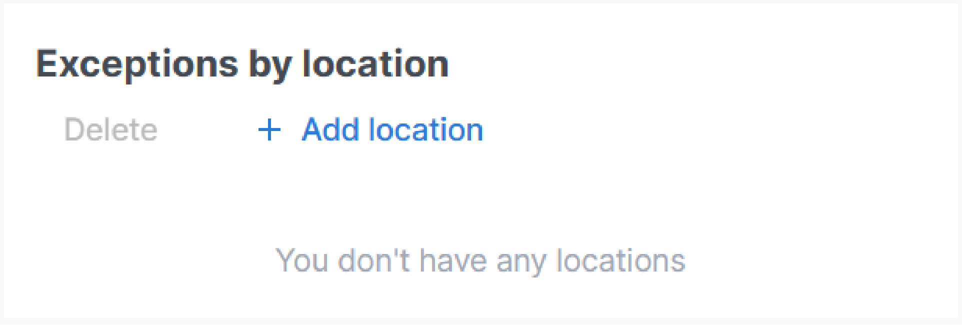
  A request will be sent to the whitelist if its path to your resource contains a segment specified in this setting.

For example, when adding the path «/location» to the whitelist, requests such as the following will be executed without additional checks:

- site.com/location
- site.com/location/
- site.com/location.php
- site.com/location.php?id=123
- site.com/admin/location

Meanwhile, requests such as the following will be processed according to general rules:

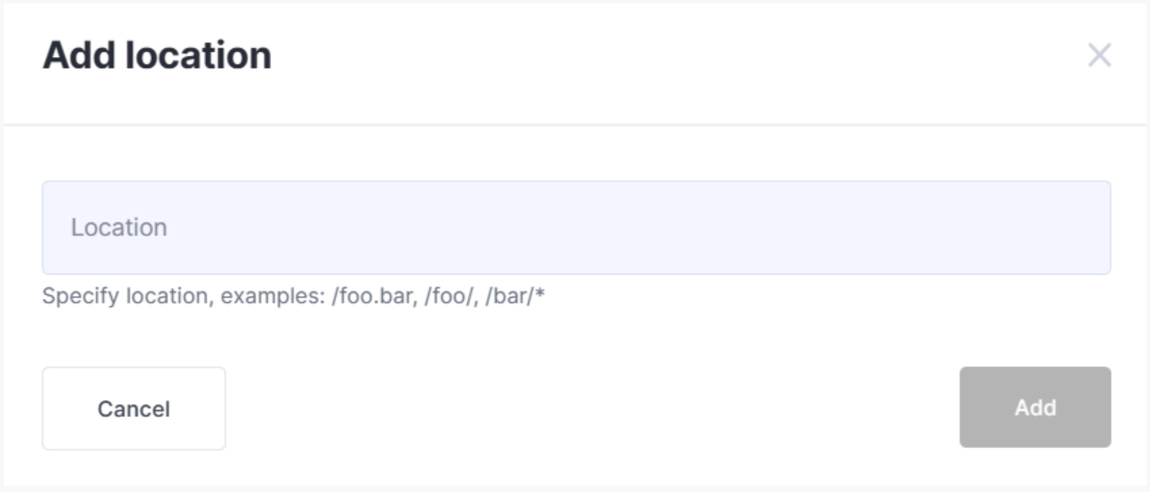
- site.com/some-other-location
- site.com/en_location.php



Exceptions by location

You don't have any locations

Click on the **Add location** button and fill out the form that appears.


Add location

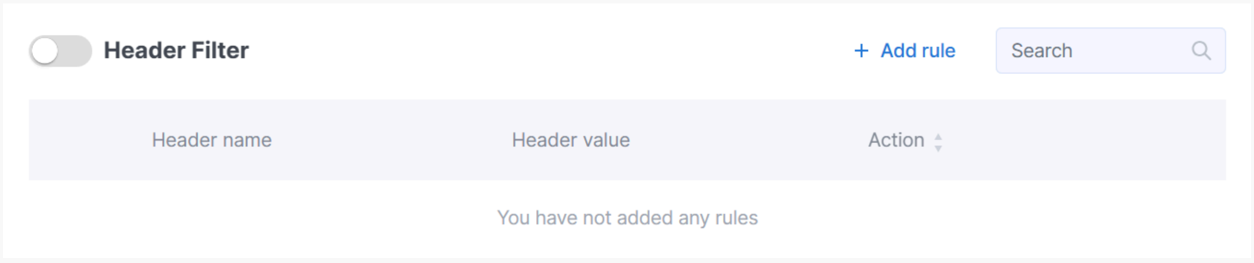
Location

Specify location, examples: /foo.bar, /foo/, /bar/*

- Header Filter

  You can create rules to block requests with a specific header as well as rules that allow them.

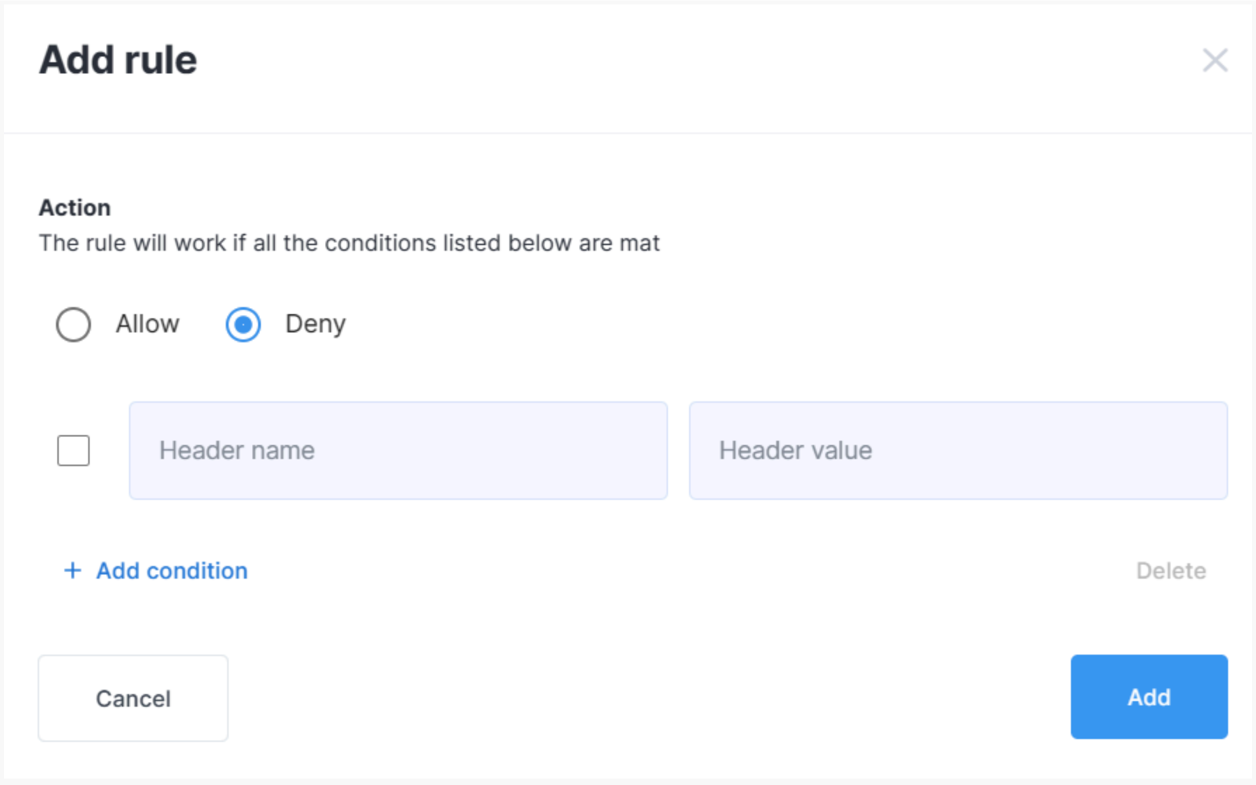
  This functionality will be relevant when using APIs (requests are made by a separate application). You can specify either a single header or a combination of several.



Header name	Header value	Action

You have not added any rules

Click on the **Add rule** button and fill out the form.



Add rule

Action

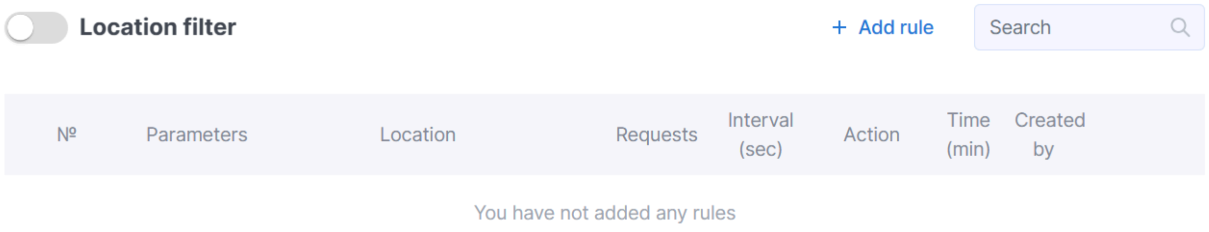
The rule will work if all the conditions listed below are mat

○ Allow ● Deny

□ Header name | Header value

- Location filter

  You can set up filtering for different locations of your resource.

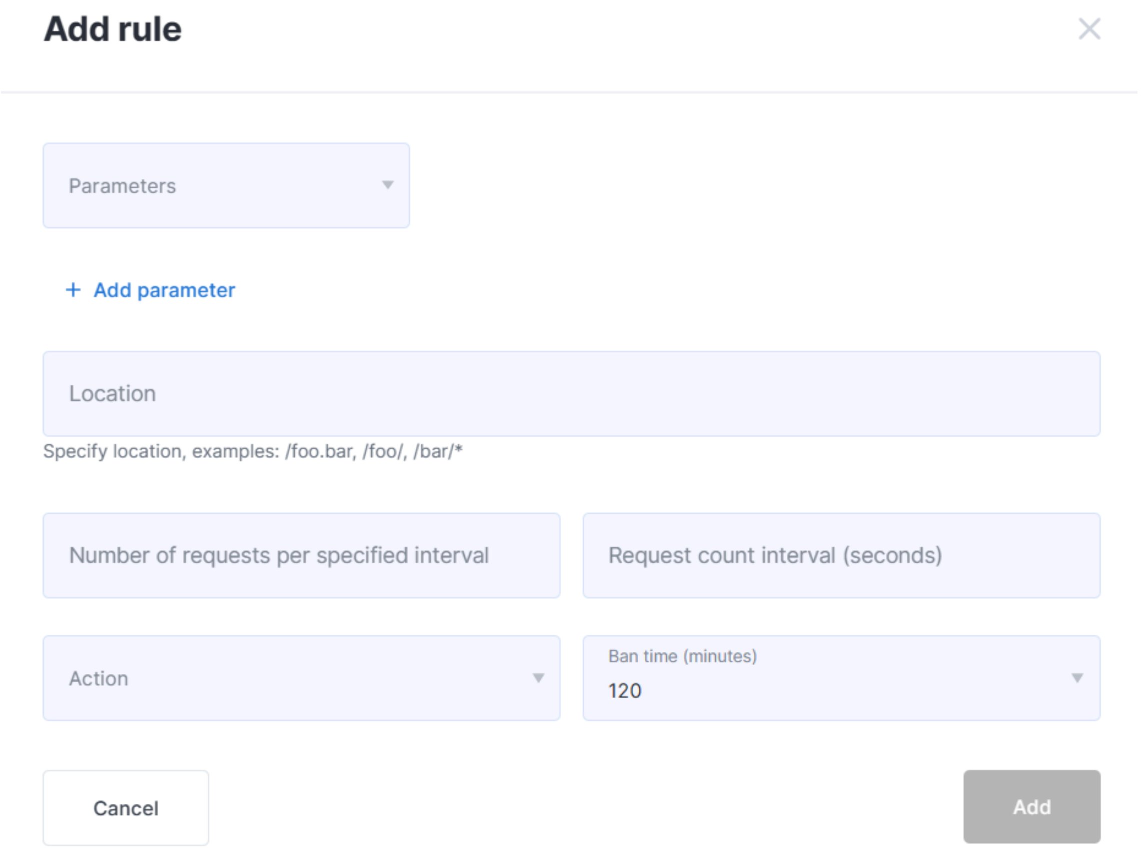


Location filter

№	Parameters	Location	Requests	Interval (sec)	Action	Time (min)	Created by

You have not added any rules

Click on the **Add rule** button and complete the form.



Add rule

Parameters

+ Add parameter

Location

Specify location, examples: /foo.bar, /foo/, /bar/*

Number of requests per specified interval

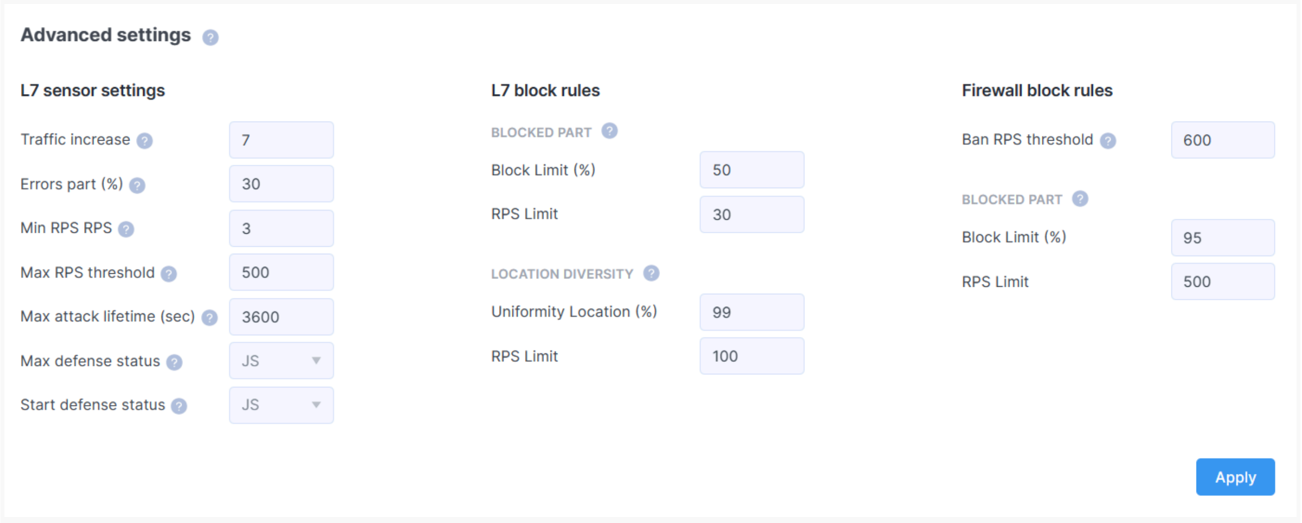
Request count interval (seconds)

Action

Ban time (minutes): 120

- Advanced settings

Experienced users can independently configure a wide range of sensor parameters.



Advanced settings

L7 sensor settings

Traffic increase	7
Errors part (%)	30
Min RPS RPS	3
Max RPS threshold	500
Max attack lifetime (sec)	3600
Max defense status	JS
Start defense status	JS

L7 block rules

BLOCKED PART	
Block Limit (%)	50
RPS Limit	30
LOCATION DIVERSITY	
Uniformity Location (%)	99
RPS Limit	100

Firewall block rules

Ban RPS threshold	600
BLOCKED PART	
Block Limit (%)	95
RPS Limit	500

You have the option to configure:

- ○ **L7 sensor setting**

In the first column, you can adjust parameters for attack detection:

- **Traffic Increase**: The factor by which the number of requests must increase over a short period of time to switch to active protection mode.

  For example, the number «3» in this field will mean that the protection will be activated if the number of requests triples over the last 15 minutes.

- **Errors Part**: The percentage of erroneous requests that, once reached, will trigger the filters to switch to active mode.

  For example, the number «30» in this area means that if the proportion of errors with «500» series codes exceeds the set value (30%), protective measures will be activated.

- **Set Min RPS**: The value below which «Traffic Increase» and «Errors Part» checks will not be performed.
- **Max RPS Threshold**: The number of requests that, when exceeded, triggers the switch to active mode.
- **Max Attack Lifetime (sec)**: The time after the start of an attack after which the filter will attempt to switch back to sensor mode.

  Here, you can specify the duration for which countermeasures against an attack are activated upon its detection, regardless of whether it has ceased or is continuing. This is a relevant parameter for combating attacks that are sporadic over time.

- **Max Defence Status**: The maximum type of protection during automatic trigger operations.
- **Start Defence Status**: The type of protection that will be set when the filter initially switches from sensor mode to active mode.

- **L7 block rules**

  In the second column, you can set values to detect bot activity.

  If a certain IP address sends more requests than specified in the «RPS Limit» field, and a higher percentage of those are blocked than the percentage specified in the «Block Limit» («Uniformity Location»), then that IP address will be added to a «grey» list of addresses.

  - Blocked part
    - Block Limit (%)
    - RPS Limit
  - Location diversity
    - Uniformity Location (%)
    - RPS Limit
- **Firewall block rules**

  In the third column, the parameters of the firewall are presented.

  Here, you can configure threshold values at the network level to block traffic from certain nodes, subnets, and networks without activating application-level filtering mechanisms.

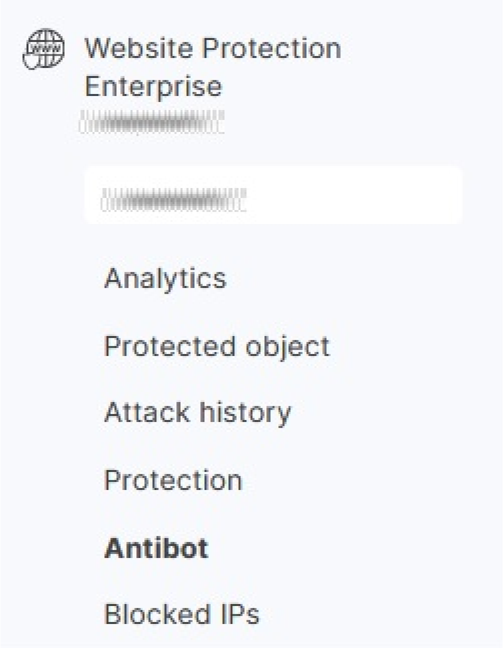
  - Ban RPS threshold

    If a parameter is exceeded, then the IP address is blocked without additional checks.
  - Blocked part L3 (%)

    If the «RPS Limit» value is exceeded and the proportion of blocked requests from that IP address surpasses the «Block Limit», then the address is blocked.
    - Block Limit (%)
    - RPS Limit

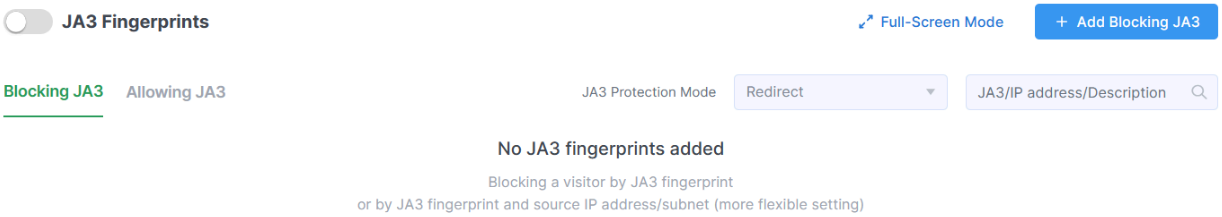
Antibot

In the left menu, select the **Antibot** item.



On the page that opens, customizable parameters are presented:

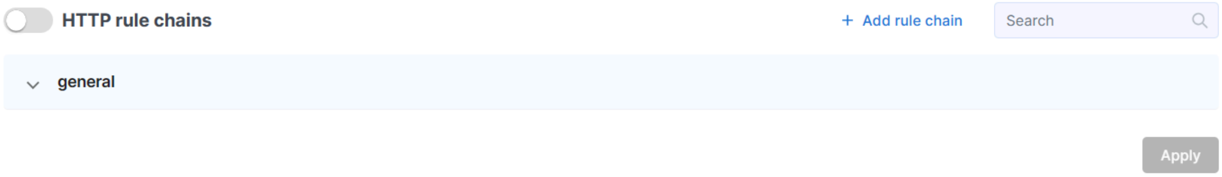
- JA3 Fingerprints



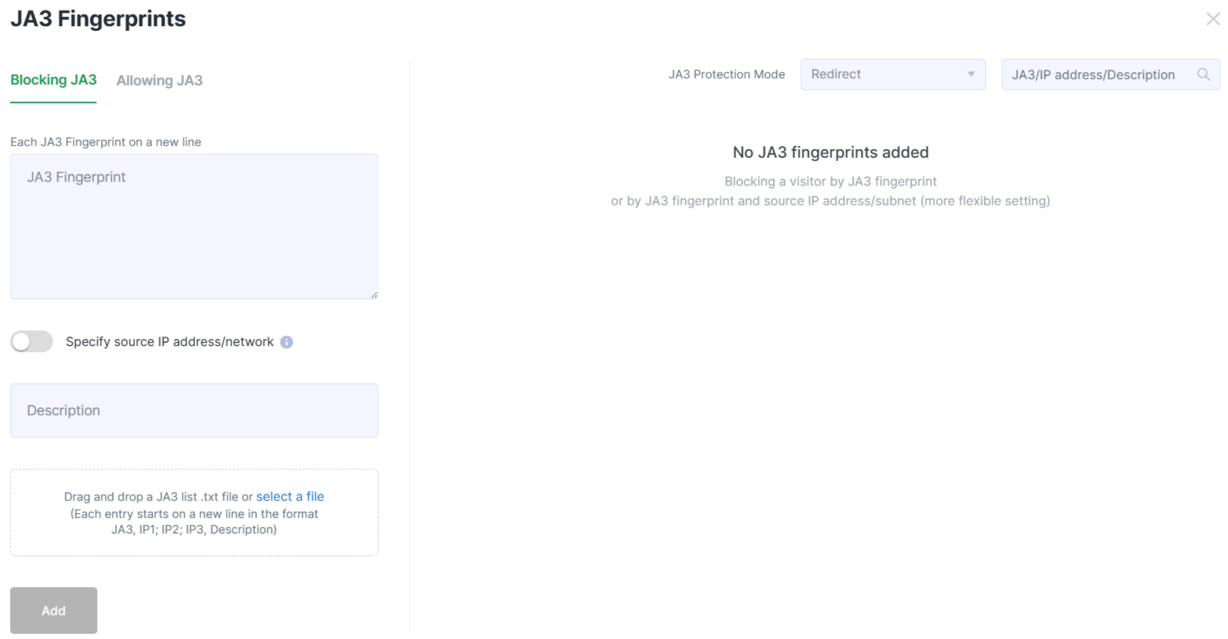
No JA3 fingerprints added

Blocking a visitor by JA3 fingerprint
or by JA3 fingerprint and source IP address/subnet (more flexible setting)

- HTTP rule chains



To configure JA3 blocks and permissions, click on the **Add Blocking JA3** button or the **Full-screen Mode** button.



JA3 Fingerprints

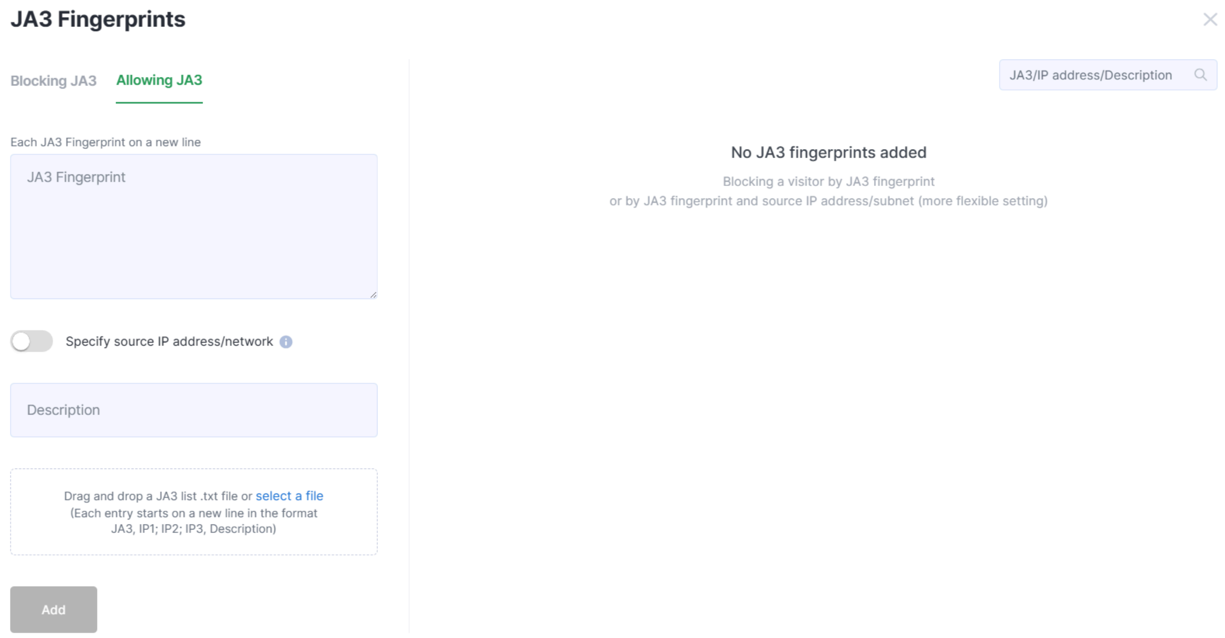
Blocking JA3
Allowing JA3
Each JA3 Fingerprint on a new line
JA3 Fingerprint
Specify source IP address/network
Description
Drag and drop a JA3 list .txt file or select a file
(Each entry starts on a new line in the format
JA3, IP1; IP2; IP3, Description)
Add
JA3 Protection Mode
Redirect
JA3/IP address/Description

No JA3 fingerprints added

Blocking a visitor by JA3 fingerprint or by JA3 fingerprint and source IP address/subnet (more flexible setting)

Fill out the form that opens to configure JA3 blocks, uploading data in a ".txt" file format if necessary. Then, click on the **Add** button.

To configure JA3 permissions, navigate to the **JA3 Fingerprints** tab.



JA3 Fingerprints

Blocking JA3
Allowing JA3
Each JA3 Fingerprint on a new line
JA3 Fingerprint
Specify source IP address/network
Description
Drag and drop a JA3 list .txt file or select a file
(Each entry starts on a new line in the format
JA3, IP1; IP2; IP3, Description)
Add
JA3/IP address/Description

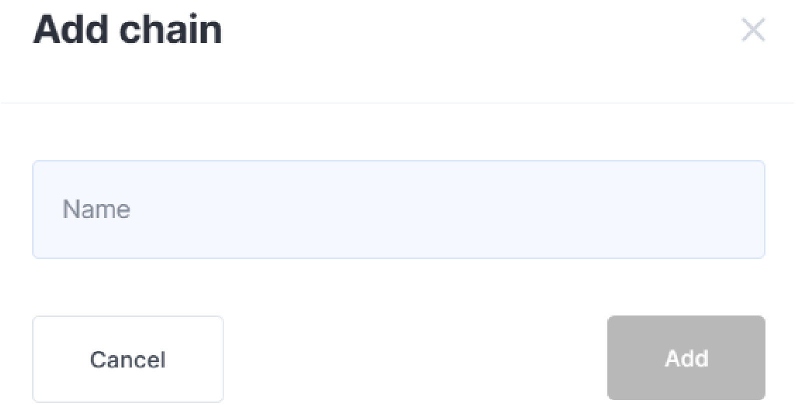
No JA3 fingerprints added

Blocking a visitor by JA3 fingerprint or by JA3 fingerprint and source IP address/subnet (more flexible setting)

Fill it out and click on the **Add** button.

You can create chains of HTTP request processing and check their compliance with multiple parameters simultaneously, followed by specifying actions to be taken on the requests. You can check for the presence or absence of certain headers, cookies, and much more. By creating chains of rules, you can achieve a variety of access differentiation combinations - by addresses, packet states, and other characteristics.

Then, click on the **Add rule chain** button in the **HTTP Rule Chains** area.

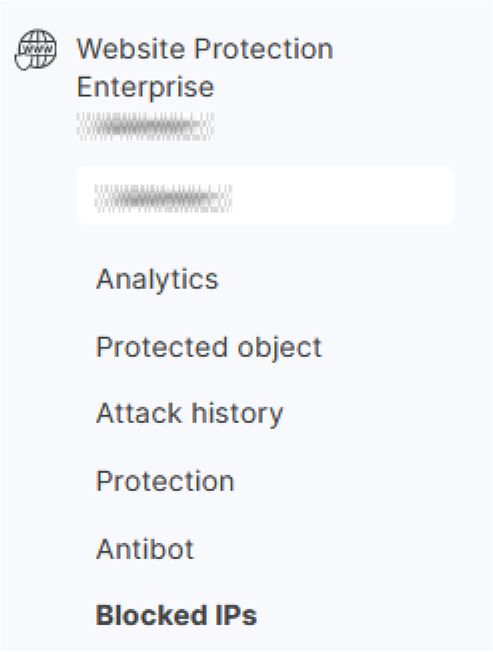


Fill in the field and click on the **Add** button. In the form that opens, create a rule.

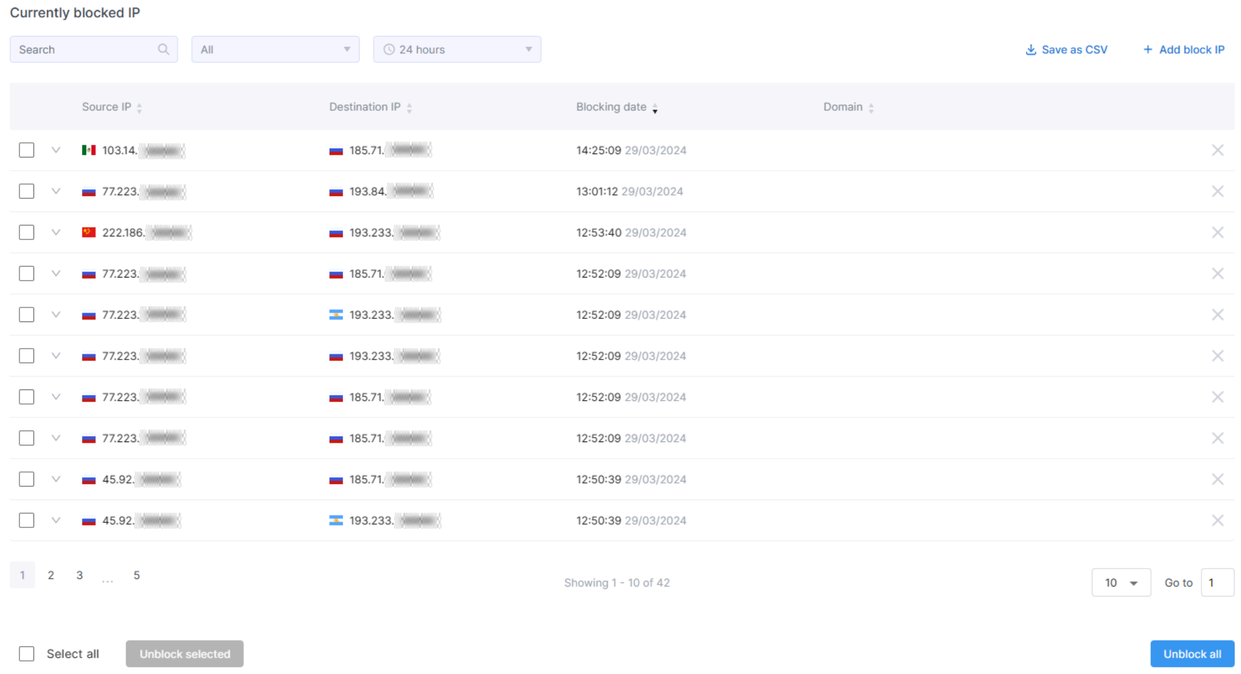
For example, you can create a rule named «hidden_key» where you specify the action «BLOCK» for the «POST» method and the location «/api/*» if the condition is met, and «NEXT RULE» if it is not met.

Blocked IP's

In the left menu, select the **Blocked IP's** item.



The page that opens will show you the IP addresses that are currently blocked, and below that, you'll find a form displaying the history of blocks. You can remove specific IP addresses from the block list by ticking their boxes and pressing the **Unblock selected** button. Additionally, you have the option to clear the list entirely by using the **Unblock all** button.



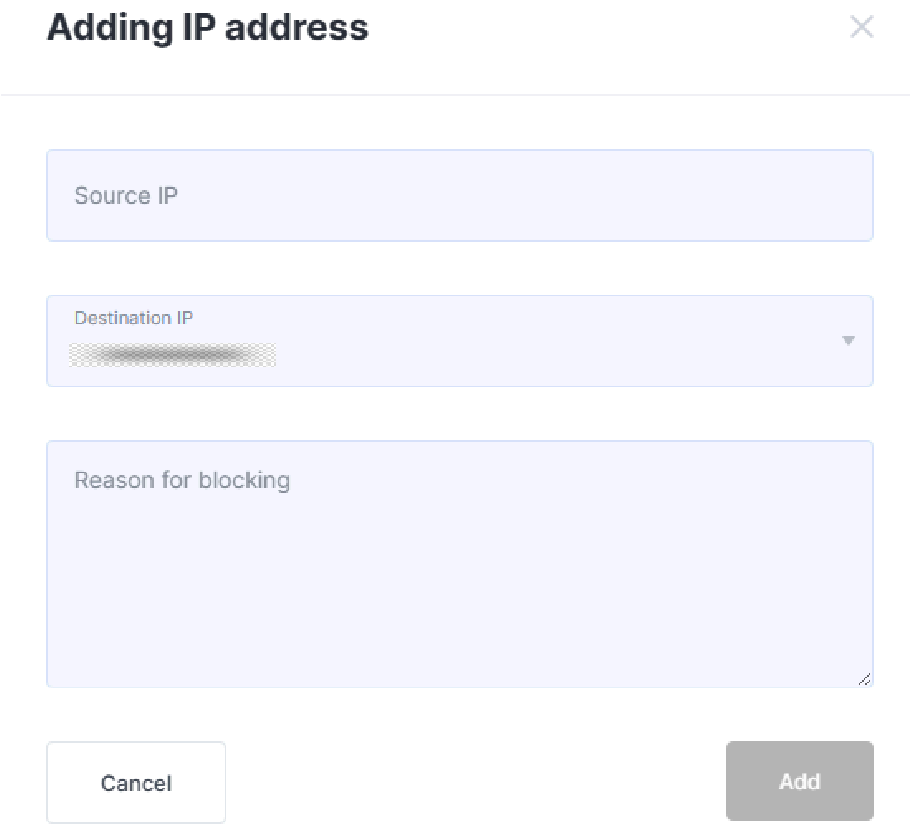
Currently blocked IP

		Source IP	Destination IP	Blocking date	Domain	
□	∨	103.14.[redacted]	185.71.[redacted]	14:25:09 29/03/2024		×
□	∨	77.223.[redacted]	193.84.[redacted]	13:01:12 29/03/2024		×
□	∨	222.186.[redacted]	193.233.[redacted]	12:53:40 29/03/2024		×
□	∨	77.223.[redacted]	185.71.[redacted]	12:52:09 29/03/2024		×
□	∨	77.223.[redacted]	193.233.[redacted]	12:52:09 29/03/2024		×
□	∨	77.223.[redacted]	193.233.[redacted]	12:52:09 29/03/2024		×
□	∨	77.223.[redacted]	185.71.[redacted]	12:52:09 29/03/2024		×
□	∨	77.223.[redacted]	185.71.[redacted]	12:52:09 29/03/2024		×
□	∨	45.92.[redacted]	185.71.[redacted]	12:50:39 29/03/2024		×
□	∨	45.92.[redacted]	193.233.[redacted]	12:50:39 29/03/2024		×

Showing 1 - 10 of 42

Utilize the search and filters by time and data type to narrow down the selection of addresses. You can save the records into a file by clicking the **Save as CSV** button. To block an IP address, press the **Block IP** button and fill out the form that opens:

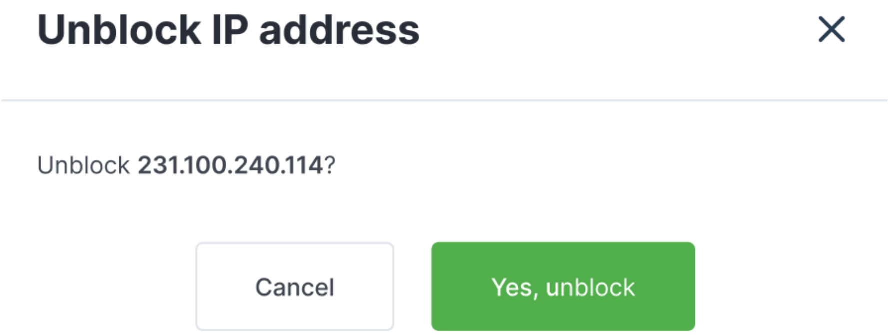
- Source IP address - the one you want to block;
- Destination IP address - your address that you want to protect;
- Reason for blocking - an optional field.



Destination IP [redacted]

After filling out the form, click the **Add** button.

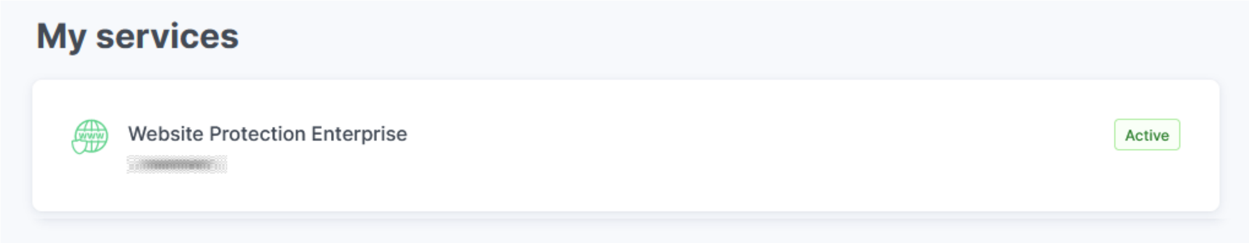
You can remove an address from the list of blocked addresses at any time. Click on the delete icon in the field and confirm the action.



Unblock **231.100.240.114**?

Monitoring Tools

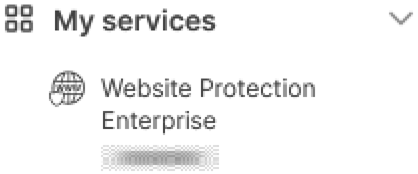
Open the service page - click on its name on the main page of the account or in the list **My Services** in the left area of the screen.



My services

Website Protection Enterprise

[redacted]

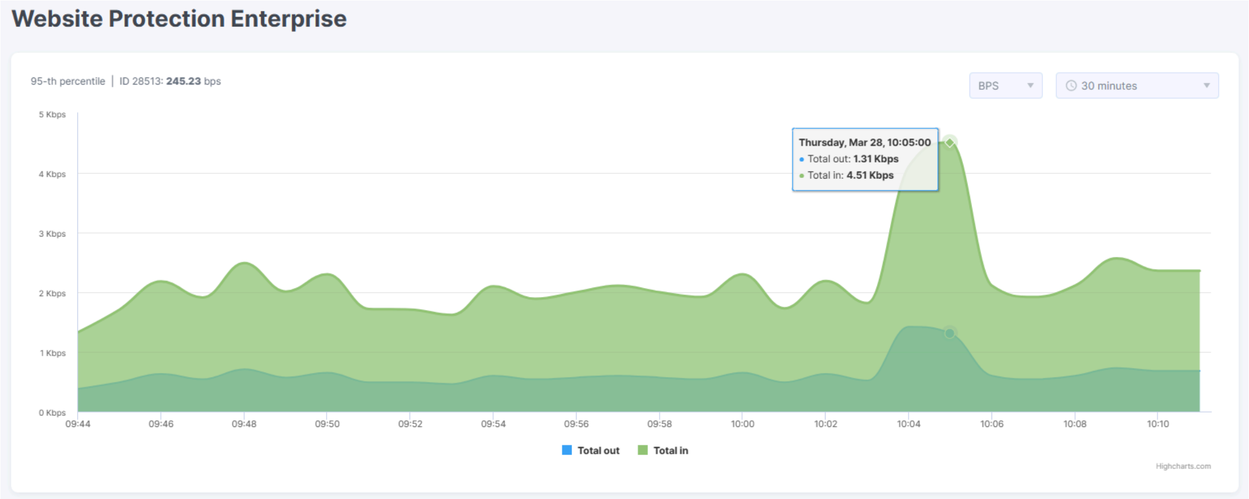


Website Protection Enterprise

[redacted]

To view details, click on the service field. The chart on the page that opens displays the volume of traffic before and after filtering.

To see numerical characteristics at a point in time, hover your mouse cursor over the chart.



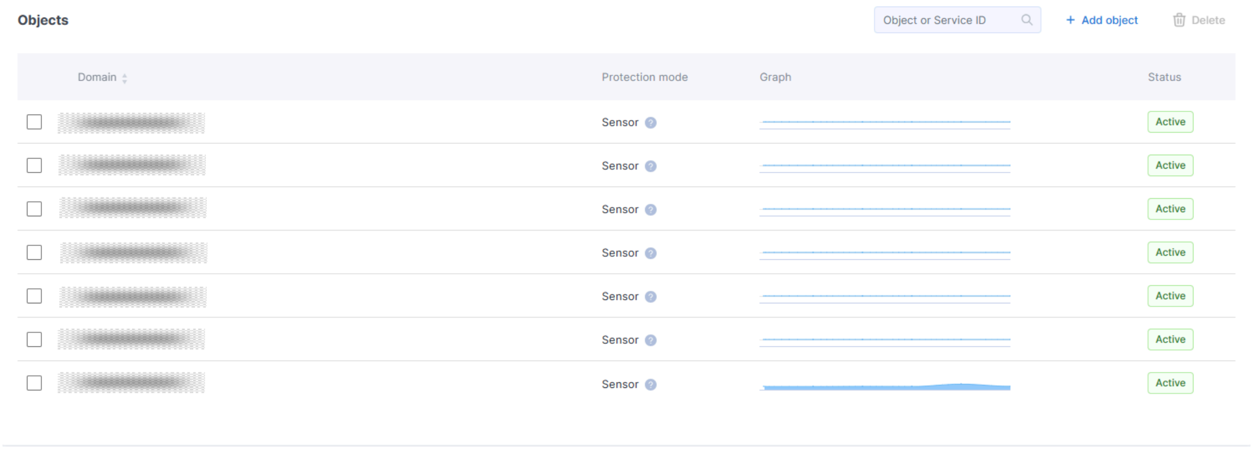
Website Protection Enterprise

95-th percentile | ID 28513: **245.23** bps

BPS: 30 minutes

Thursday, Mar 28, 10:05:00
- Total out: **1.31 Kbps**
- Total in: **4.51 Kbps**

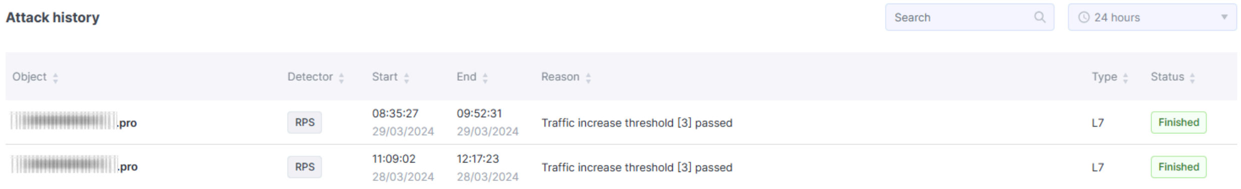
The list of objects is provided, for editing which you can use the **Add Object** and **Delete** buttons. Before deleting objects, select them by checking the boxes in the first column of the rows.



Objects

	Domain	Protection mode	Graph	Status
□	[redacted]	Sensor		Active
□	[redacted]	Sensor		Active
□	[redacted]	Sensor		Active
□	[redacted]	Sensor		Active
□	[redacted]	Sensor		Active
□	[redacted]	Sensor		Active
□	[redacted]	Sensor		Active

Below the list of objects, there is a history of attacks on them.

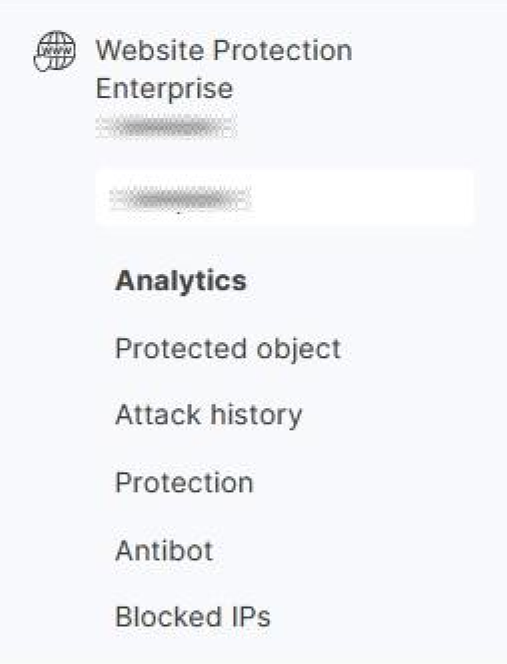


Attack history

Object	Detector	Start	End	Reason	Type	Status
[redacted].pro	RPS	08:35:27 29/03/2024	09:52:31 29/03/2024	Traffic increase threshold [3] passed	L7	Finished
[redacted].pro	RPS	11:09:02 28/03/2024	12:17:23 28/03/2024	Traffic increase threshold [3] passed	L7	Finished

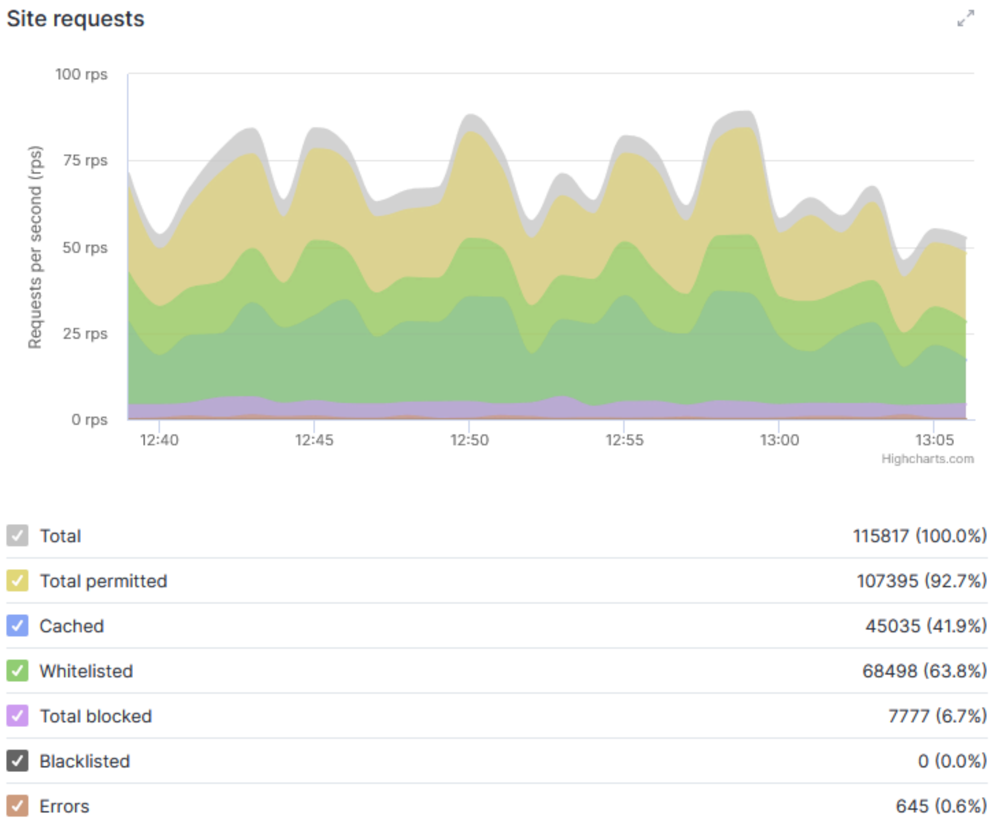
Analytics

Click on the chart thumbnail in the **Object** area to view analytical information. In doing so, a menu will open in the left area of the screen, where the current item selected is **Analytics**.



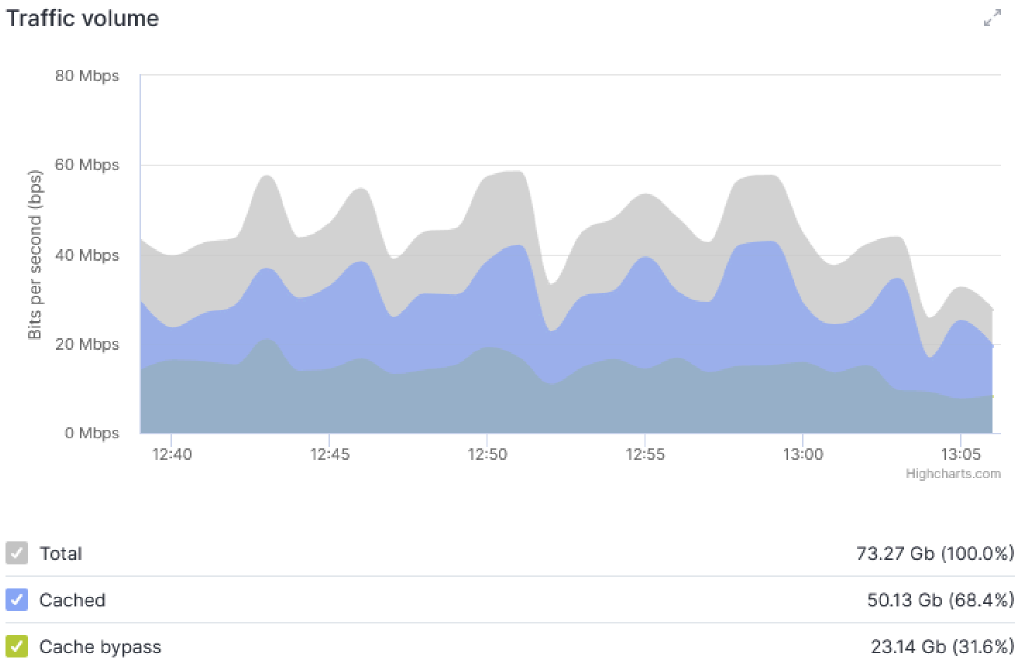
The page presents information.:

- Site requests - the number of requests coming to the site per second.



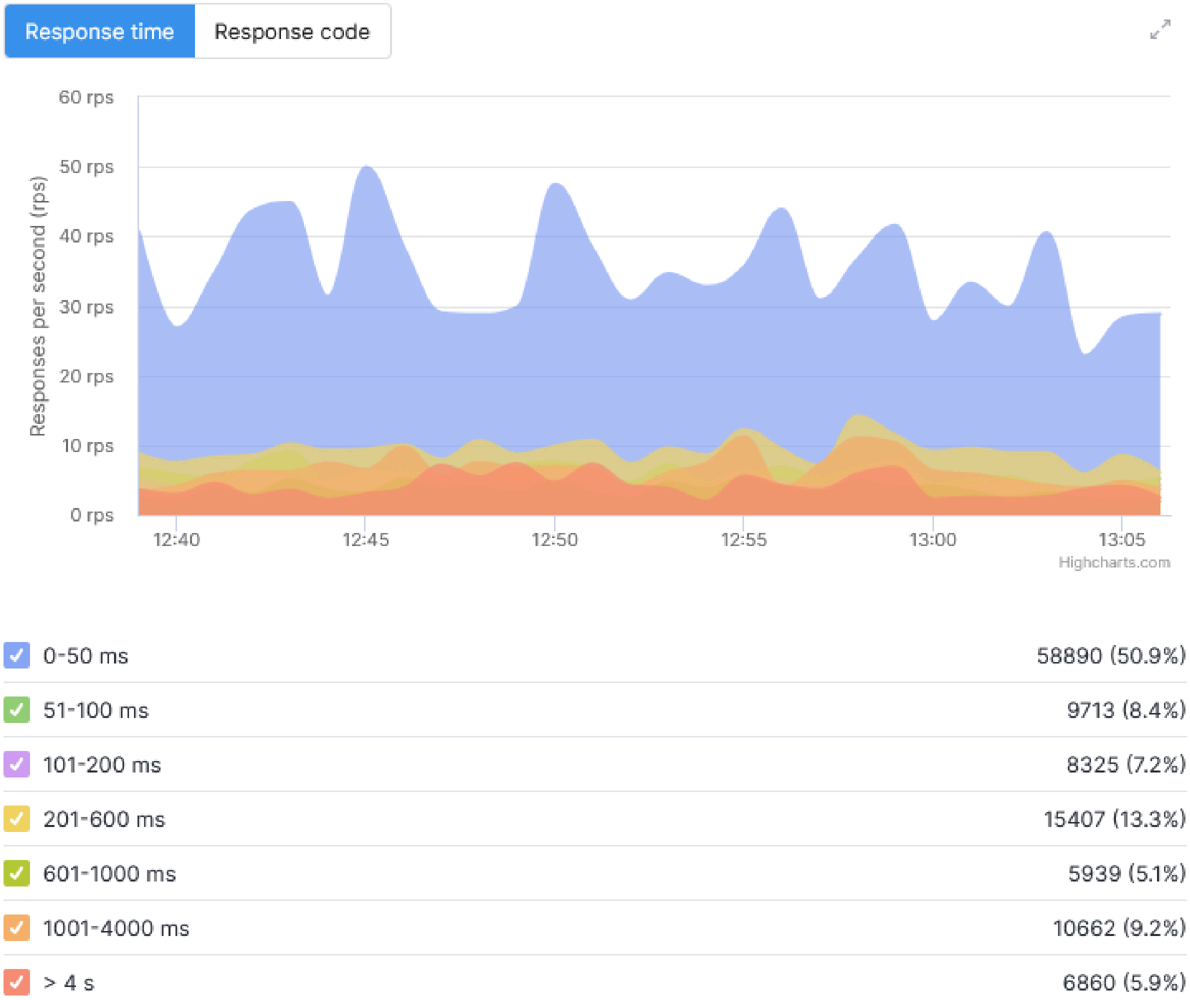
☑ Total	115817 (100.0%)
☑ Total permitted	107395 (92.7%)
☑ Cached	45035 (41.9%)
☑ Whitelisted	68498 (63.8%)
☑ Total blocked	7777 (6.7%)
☑ Blacklisted	0 (0.0%)
☑ Errors	645 (0.6%)

- Traffic volume (number of bits per second).

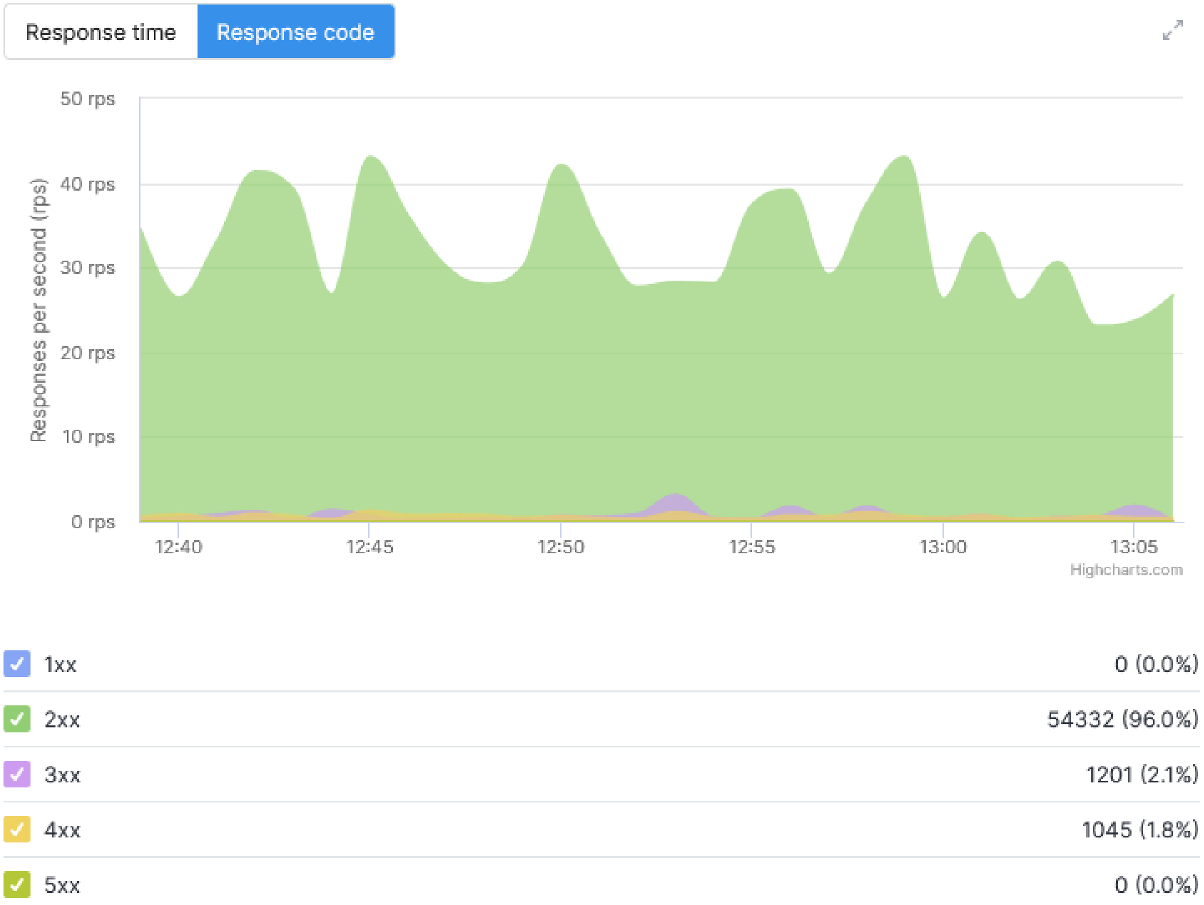


☑ Total	73.27 Gb (100.0%)
☑ Cached	50.13 Gb (68.4%)
☑ Cache bypass	23.14 Gb (31.6%)

- Response time (number of responses per second) / Response code.



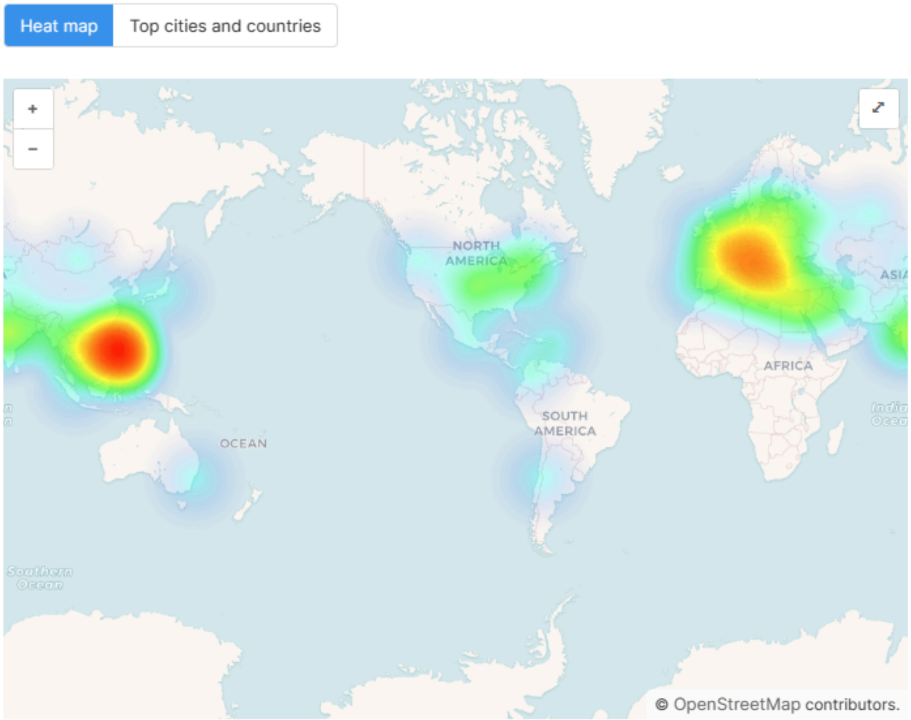
☑ 0-50 ms	58890 (50.9%)
☑ 51-100 ms	9713 (8.4%)
☑ 101-200 ms	8325 (7.2%)
☑ 201-600 ms	15407 (13.3%)
☑ 601-1000 ms	5939 (5.1%)
☑ 1001-4000 ms	10662 (9.2%)
☑ > 4 s	6860 (5.9%)



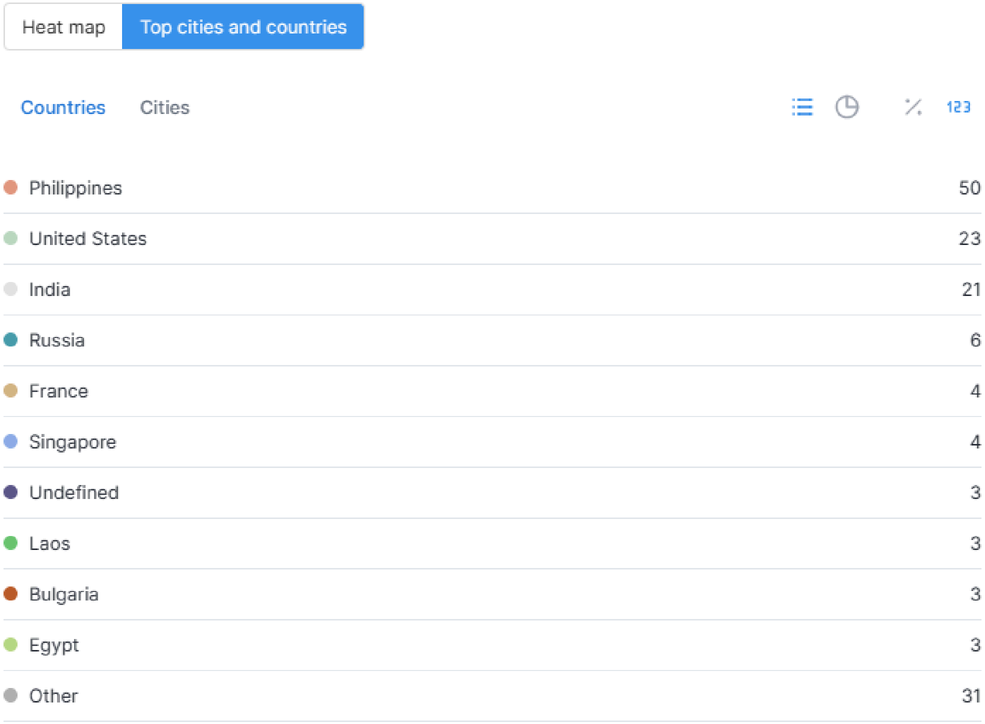
✓ 1xx	0 (0.0%)
✓ 2xx	54332 (96.0%)
✓ 3xx	1201 (2.1%)
✓ 4xx	1045 (1.8%)
✓ 5xx	0 (0.0%)

- Heatmap / Top cities and countries

  On the «Heatmap» tab, you can see the geographical distribution of requests to your resources. The maximum concentration of requests is shown in red. You can use this data to set up geo-based blocking or allowing rules. To expand the map, click on the «arrow» icon in the top right corner of the image.

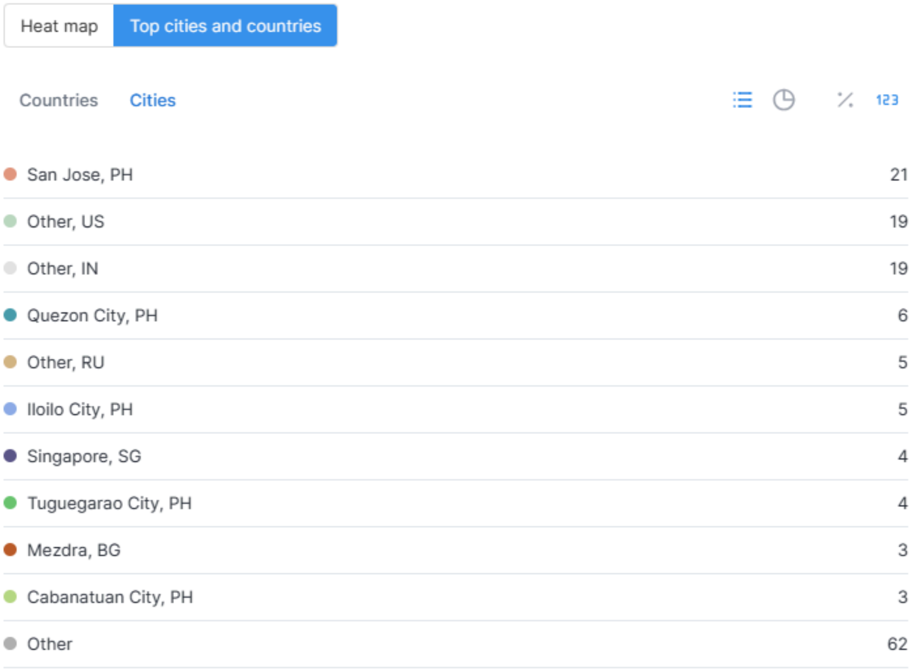


Open the **Top Cities and Countries** tab to view the list of the most active sources of attacks.



● Philippines	50
● United States	23
● India	21
● Russia	6
● France	4
● Singapore	4
● Undefined	3
● Laos	3
● Bulgaria	3
● Egypt	3
● Other	31

Navigate to the **Cities** tab to view them.

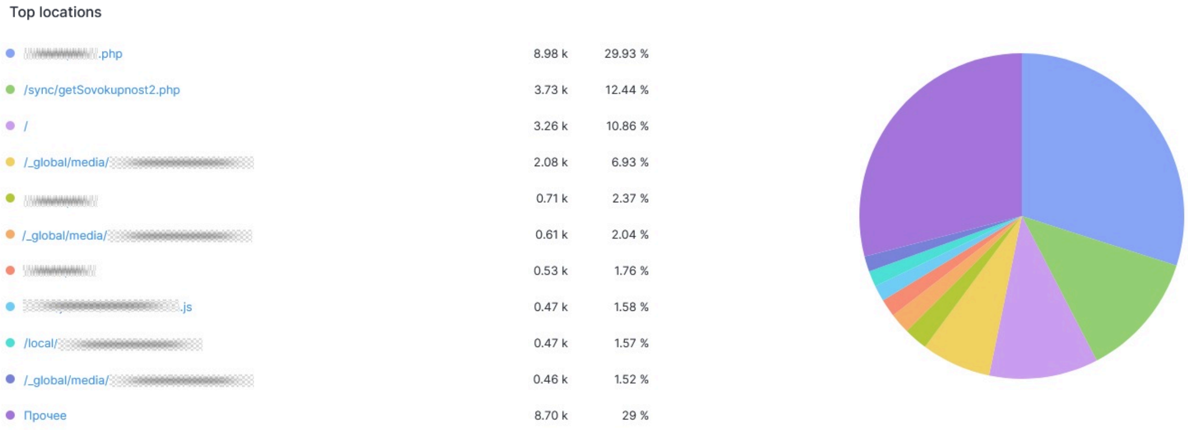


● San Jose, PH	21
● Other, US	19
● Other, IN	19
● Quezon City, PH	6
● Other, RU	5
● Iloilo City, PH	5
● Singapore, SG	4
● Tuguegarao City, PH	4
● Mezdra, BG	3
● Cabanatuan City, PH	3
● Other	62

Use the toolbar in the top right corner of the window to view the results in the form of charts.

- Top locations

  You can view information about which parts of your resource were visited more frequently by users or were subjected to attacks. For example, the main page of the site is often attacked.

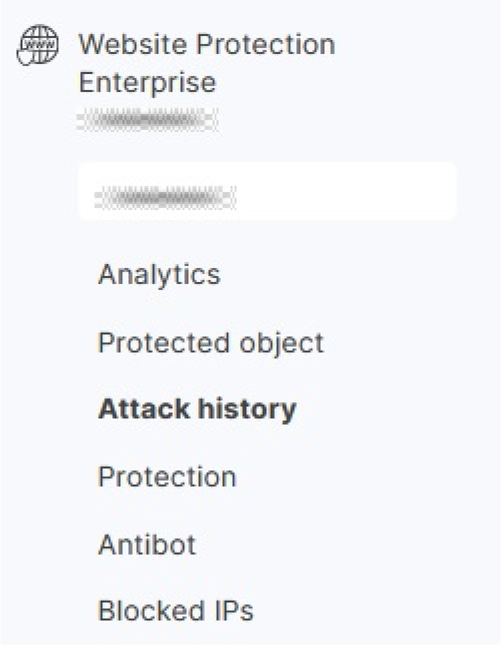


Top locations

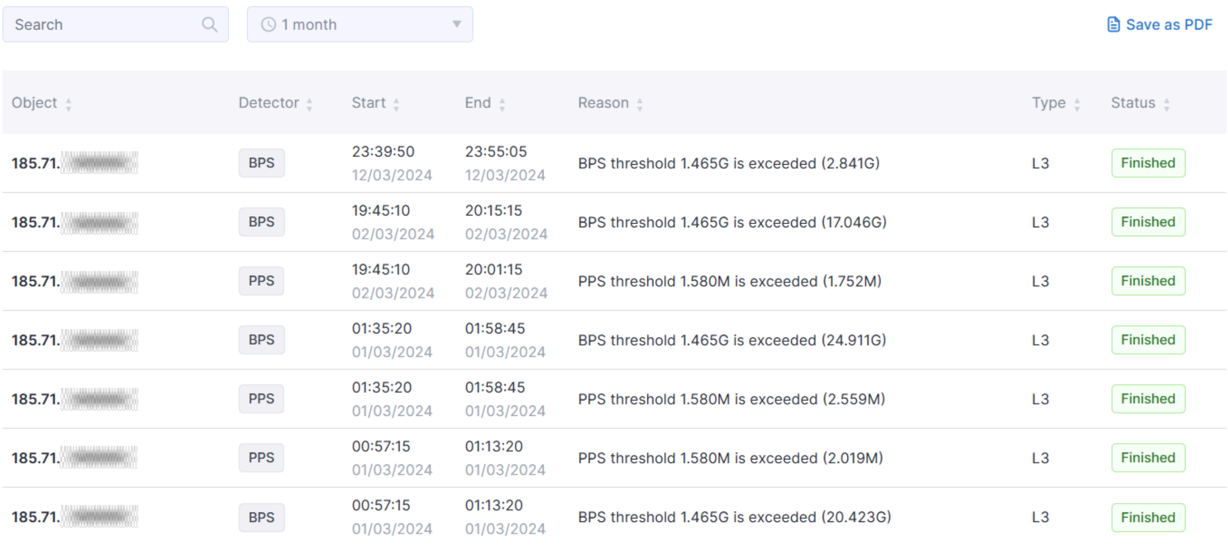
● [redacted].php	8.98 k	29.93 %
● /sync/getSovokupnost2.php	3.73 k	12.44 %
● /	3.26 k	10.86 %
● /_global/media/[redacted]	2.08 k	6.93 %
● [redacted]	0.71 k	2.37 %
● /_global/media/[redacted]	0.61 k	2.04 %
● [redacted]	0.53 k	1.76 %
● [redacted].js	0.47 k	1.58 %
● /local/[redacted]	0.47 k	1.57 %
● /_global/media/[redacted]	0.46 k	1.52 %
● Прочее	8.70 k	29 %

Attack History

In the left menu, select the **Attack history** item.



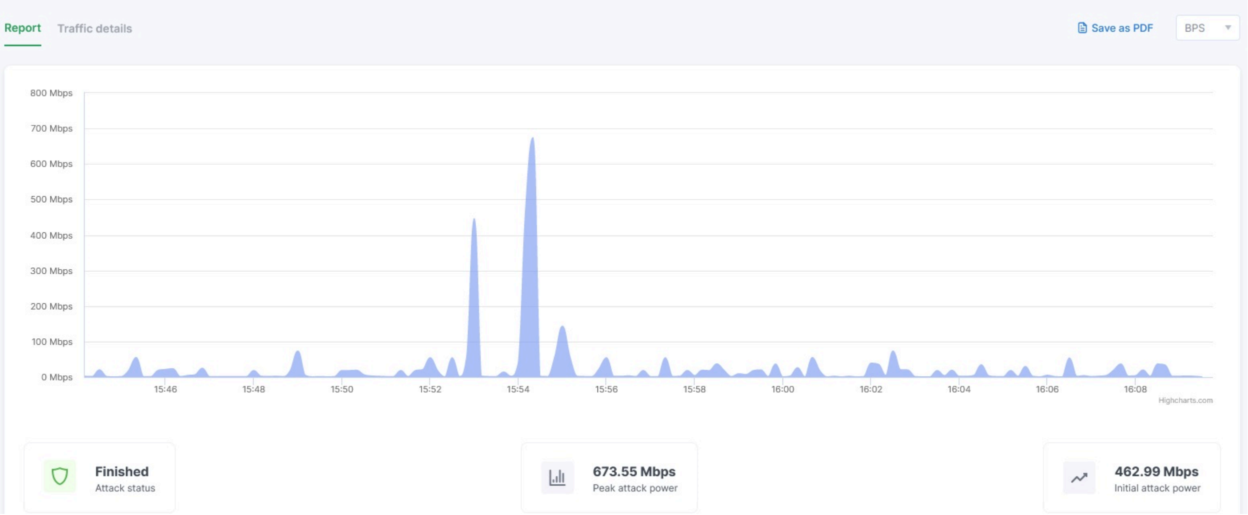
On the opened page, attacks are listed for a time interval that you can change.



Object	Detector	Start	End	Reason	Type	Status
185.71.[redacted]	BPS	23:39:50 12/03/2024	23:55:05 12/03/2024	BPS threshold 1.465G is exceeded (2.841G)	L3	Finished
185.71.[redacted]	BPS	19:45:10 02/03/2024	20:15:15 02/03/2024	BPS threshold 1.465G is exceeded (17.046G)	L3	Finished
185.71.[redacted]	PPS	19:45:10 02/03/2024	20:01:15 02/03/2024	PPS threshold 1.580M is exceeded (1.752M)	L3	Finished
185.71.[redacted]	BPS	01:35:20 01/03/2024	01:58:45 01/03/2024	BPS threshold 1.465G is exceeded (24.911G)	L3	Finished
185.71.[redacted]	PPS	01:35:20 01/03/2024	01:58:45 01/03/2024	PPS threshold 1.580M is exceeded (2.559M)	L3	Finished
185.71.[redacted]	PPS	00:57:15 01/03/2024	01:13:20 01/03/2024	PPS threshold 1.580M is exceeded (2.019M)	L3	Finished
185.71.[redacted]	BPS	00:57:15 01/03/2024	01:13:20 01/03/2024	BPS threshold 1.465G is exceeded (20.423G)	L3	Finished

Use the search and time filter for data selection. To download the attack history, click on the **Save as PDF** button.

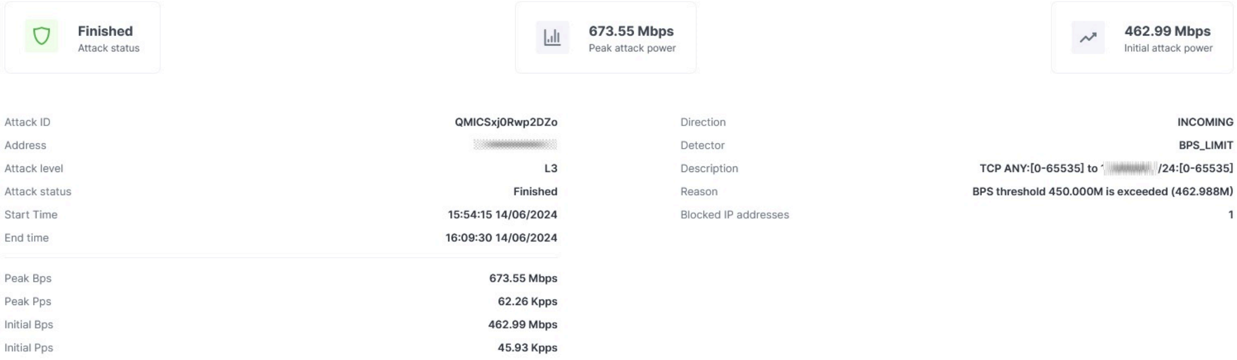
Click on the row of the attack you are interested in to view details about it.



Finished
Attack status

673.55 Mbps
Peak attack power

462.99 Mbps
Initial attack power



Finished
Attack status

673.55 Mbps
Peak attack power

462.99 Mbps
Initial attack power

Attack ID	QMICSxj0Rwp2DZo	Direction	INCOMING
Address	[redacted]	Detector	BPS_LIMIT
Attack level	L3	Description	TCP ANY:[0-65535] to [redacted]/24:[0-65535]
Attack status	Finished	Reason	BPS threshold 450.000M is exceeded (462.988M)
Start Time	15:54:15 14/06/2024	Blocked IP addresses	1
End time	16:09:30 14/06/2024		
Peak Bps	673.55 Mbps		
Peak Pps	62.26 Kpps		
Initial Bps	462.99 Mbps		
Initial Pps	45.93 Kpps		

Hover your mouse cursor over the chart to see numerical values. Detailed information about the attack is provided below the chart.

To view information about traffic, go to the **Traffic Details** tab. On this tab, you will find information about:

- Site requests;
- Traffic volume;
- Response time / response code;
- Heat map / top cities and countries;
- Top locations.

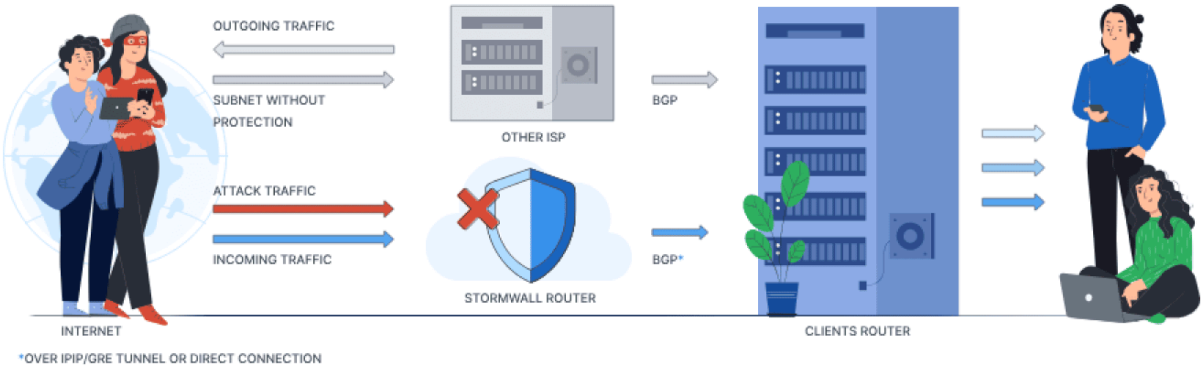
Network Protection

How the Service Works

The **«StormWall for Networks»** service is designed for internet service providers, data centers, hosting companies, and corporate clients with their own autonomous system. Our protection blocks and minimizes the consequences of even the most complex DDoS attacks on your network.

How the Service Works Algorithm of operation:

1. Connection setup;
2. Establishment of a BGP session, where you announce the necessary IP prefixes;
3. Reception of announcements, filtering, and redirection of cleaned traffic to you.



Connection Methods for Protection:

1. IPIP/GRE Tunnel
2. Internet Exchange (IX)
3. Physical Connection to the StormWall Network at one of our locations

Protection Options:

1. Enable Permanent Protection with all incoming traffic passing through our filters:

In this case, all of the client's networks will be under constant protection (DDoS attacks will never catch you off guard), but the flexibility in managing incoming traffic will be limited.

2. Manually connect protected networks - only the necessary client networks will be announced:

   Not all client networks will be announced, only those that require protection at a specific moment in time. For example, if you are expecting an attack or it has already begun, you can manually redirect network announcements to StormWall (removing them from other providers).

3. Automate the announcement of protected networks when an attack begins using a DDoS sensor:

   The sensor, installed on the client's side, automatically switches the attacked network to protection mode and removes it from unprotected providers immediately after detecting the beginning of an attack. After the attack is over, it returns the network back.

4. Deploy a DDoS sensor on the client's network:

   The sensor can receive traffic information via NetFlow, sFlow, or Mirror/SPAN and integrates with your edge router or router group using BGP, sending signals to activate protection using BGP Community. Deployment on a virtual machine is possible.

DDoS sensor operation scenarios:

[If the DDoS sensor is on the client's side]

1. The sensor detects the beginning of an attack on one or several IP addresses;
2. Then, the sensor initiates the announcement of the attacked network through StormWall;
3. After that, the sensor removes the attacked network from unprotected providers.

[Regardless of the presence of the sensor on the client's side]

4. The sensor on StormWall's side (FlowSense system) determines which IP addresses are being attacked and redirects the traffic going to these addresses for filtration;
5. The attack is cut off by StormWall's filters;
6. After the attack ends, the traffic stops being routed through the filters and goes directly.

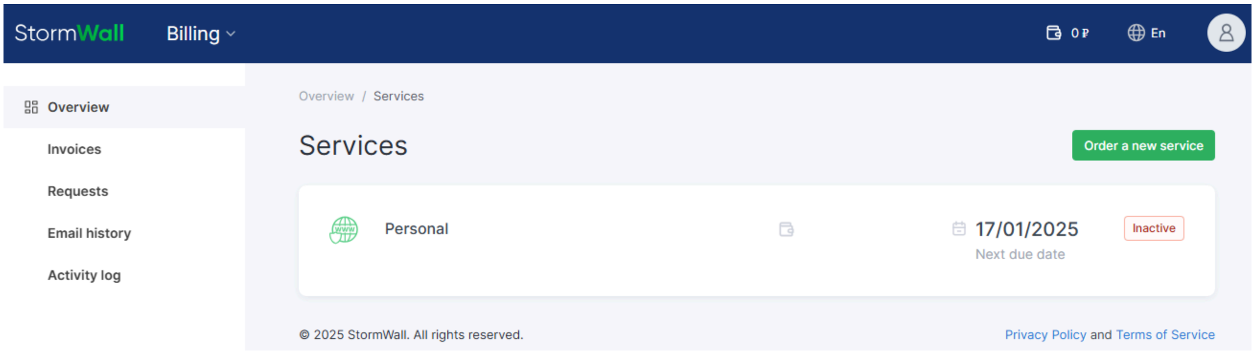
[If the sensor is on the client's side]

7. The network announcement is returned to its providers and removed from StormWall. Triple filtration (Triple Filter) is used for traffic filtering, FlowSence technology for anomaly detection and automatic attack type identification, and Global Session technology for protection against failures at StormWall network nodes.

Order

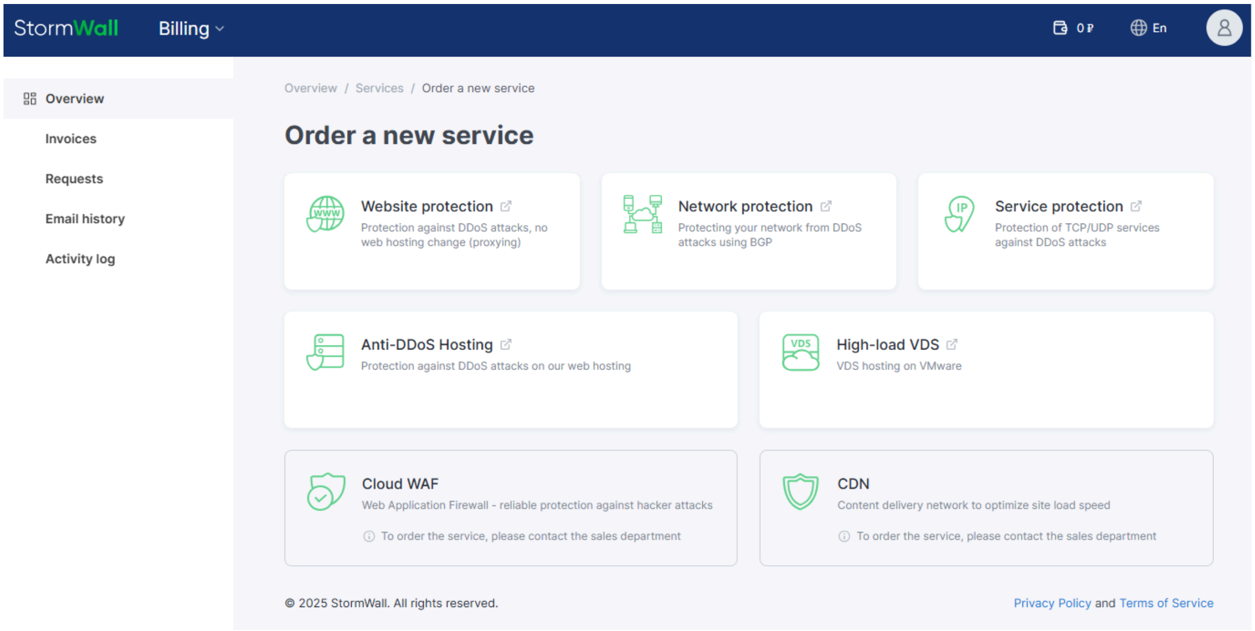
To set up DDoS protection for your network:

1. Log in to your Client Portal on the website;
2. On the top panel of the site, select the **Billing** tab;



Personal 17/01/2025 Next due date Inactive

3. In the tab that opens, select the **Network Protection** item;


StormWall Billing

0 ₽ En

Overview
Invoices
Requests
Email history
Activity log

Overview / Services / Order a new service

Order a new service

Website protection
Protection against DDoS attacks, no web hosting change (proxying)

Network protection
Protecting your network from DDoS attacks using BGP

Service protection
Protection of TCP/UDP services against DDoS attacks

Anti-DDoS Hosting
Protection against DDoS attacks on our web hosting

High-load VDS
VDS hosting on VMware

Cloud WAF
Web Application Firewall - reliable protection against hacker attacks
ⓘ To order the service, please contact the sales department

CDN
Content delivery network to optimize site load speed
ⓘ To order the service, please contact the sales department

© 2025 StormWall. All rights reserved.

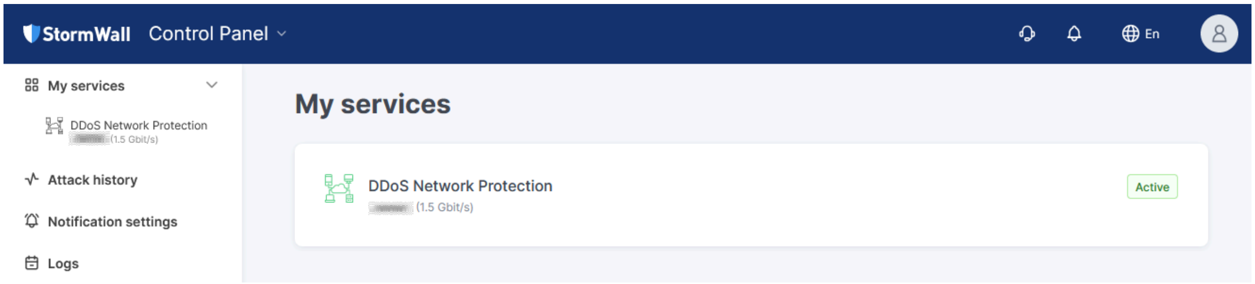
Privacy Policy and Terms of Service

4. You will be redirected to a website page with a detailed description of the service.
5. Review the information about the service and the pricing plans:
   - Personal;
   - Business;
   - Enterprise.

If none of the available pricing plans meet your requirements, please contact us — we will make a special offer for you.

Setting up security parameters

After connecting the service, it will be displayed on the main page of your **Client Portal** and in the **My Services** list.

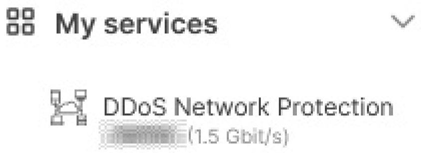

StormWall Control Panel

En

My services
DDoS Network Protection
[redacted] (1.5 Gbit/s)
Attack history
Notification settings
Logs

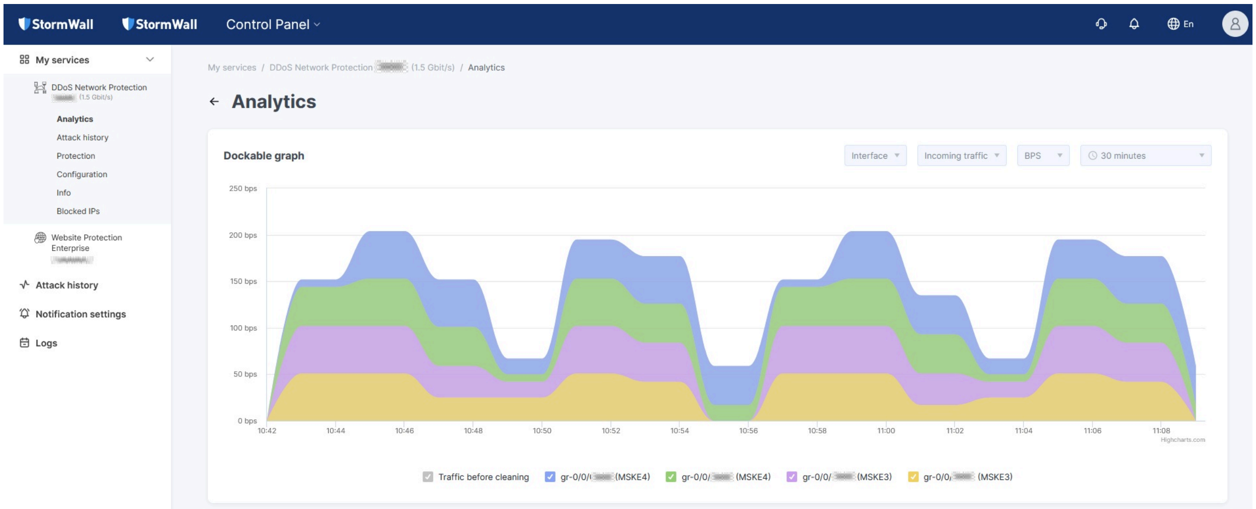
My services

DDoS Network Protection
[redacted] (1.5 Gbit/s)
Active

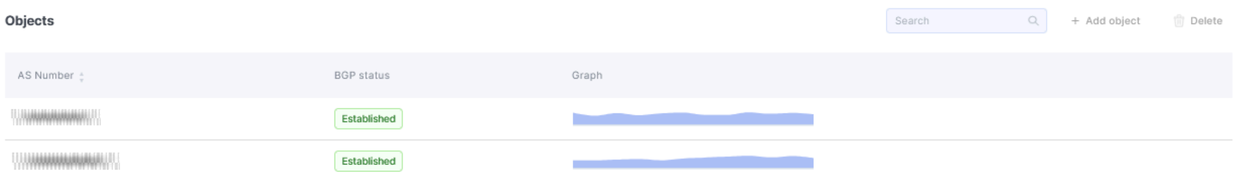


To view the details, click on the name of the service in the central area of the page or in the list on the left.

If there is only one object, a menu for working with it will open in the left area of the page.

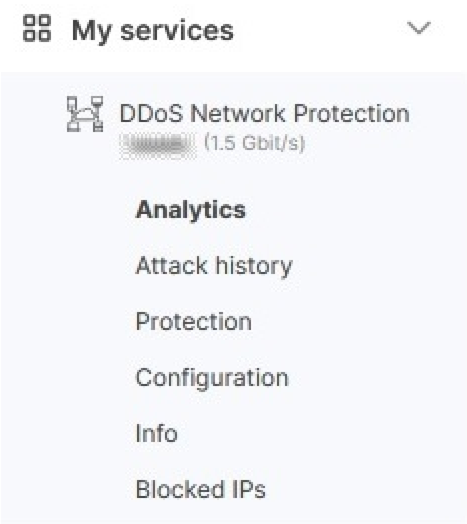


If there is only one object, a menu for working with it will open in the left area of the page.
If there are several objects, in the **Objects** area (below the graph), select the object you are interested in and click on its picture with miniature graphics.



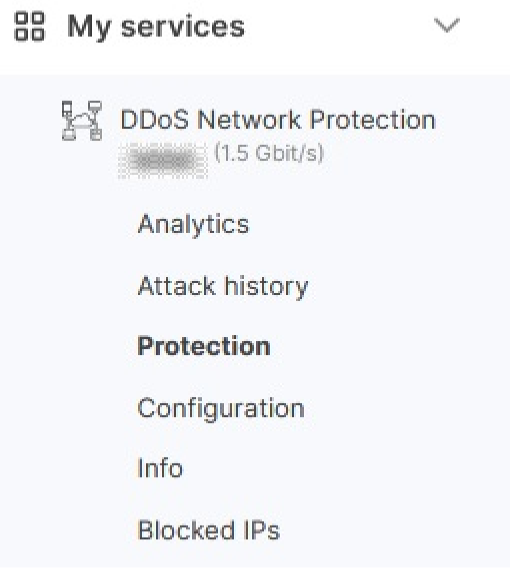
AS Number	BGP status	Graph
[redacted]	Established	
[redacted]	Established	

This will open a menu for working with the selected object in the left area of the page.



Protection

In the opened menu, select the **Protection** option.



A configuration area will open with the following fields:

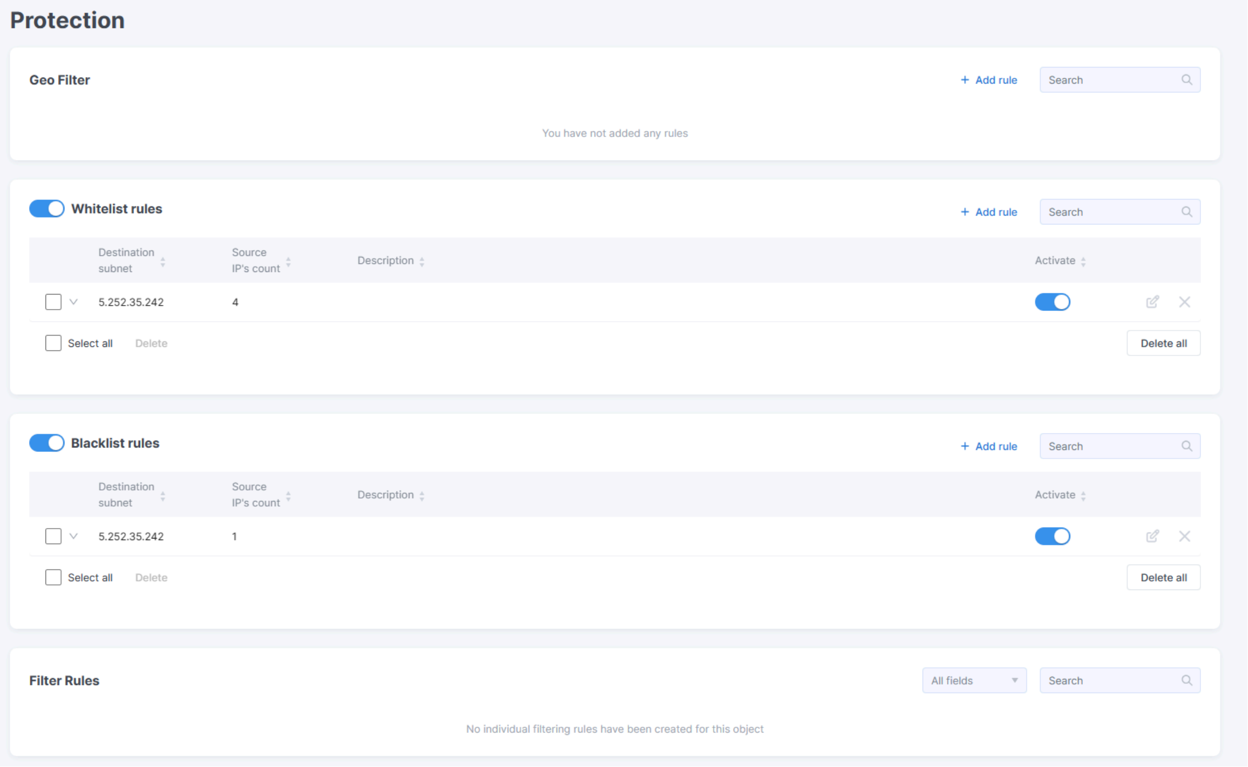
- Geo Filter
- Whitelist rules

  Requests from addresses listed here will be transmitted without filtering.

- Blacklist rules

  A user with an address from this list will not be able to send requests to your resource.

- Filter rules



Protection

Geo Filter

You have not added any rules

Whitelist rules

	Destination subnet	Source IP's count	Description	Activate
□	5.252.35.242	4		●

Blacklist rules

	Destination subnet	Source IP's count	Description	Activate
□	5.252.35.242	1		●

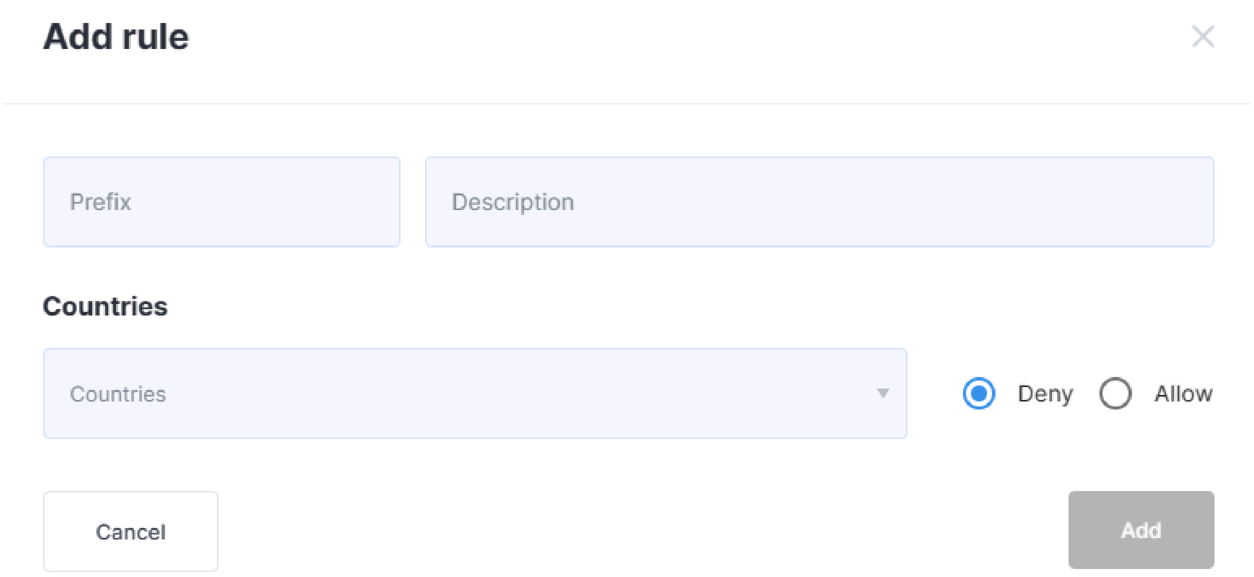
Filter Rules

No individual filtering rules have been created for this object

Click the **Add rule** button to create a restriction on the use of your resource.

To configure geo-blocking, you need to fill out the form:

- prefix (for which area of your network the rule will be applied);
- description (optional);
- countries (select from the dropdown list). Using the **Allow** and **Deny** toggles, you can set up both allowing and denying lists.

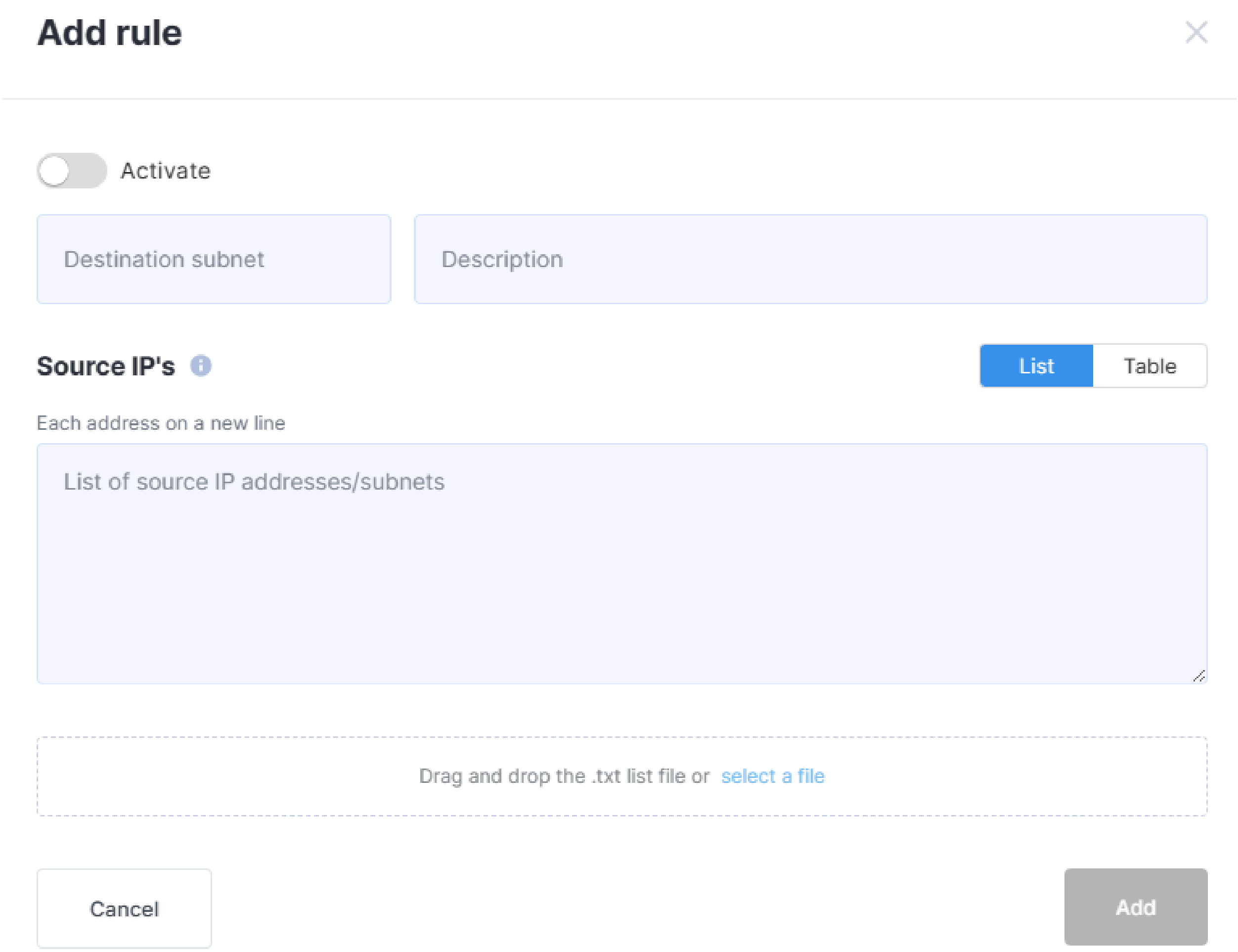


● Deny ○ Allow

To configure the rules by which users will be placed on black or white lists, fill out the form:

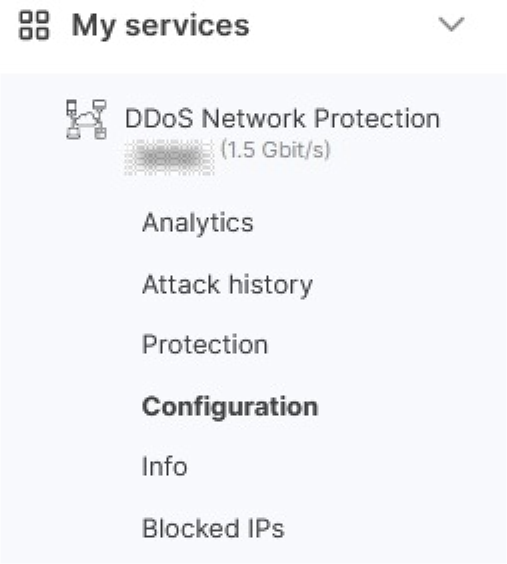
- Destination Subnet
- Description (optional)
- IP Sources

When adding IP addresses, each must be entered on a new line. You can also upload them as a “txt” file by clicking the **Select a File** button. To apply the rule, set the **Activate** toggle to the ON position.


Add rule
Activate
Destination subnet
Description
Source IP's
List
Table
Each address on a new line
List of source IP addresses/subnets
Drag and drop the .txt list file or select a file
Cancel
Add

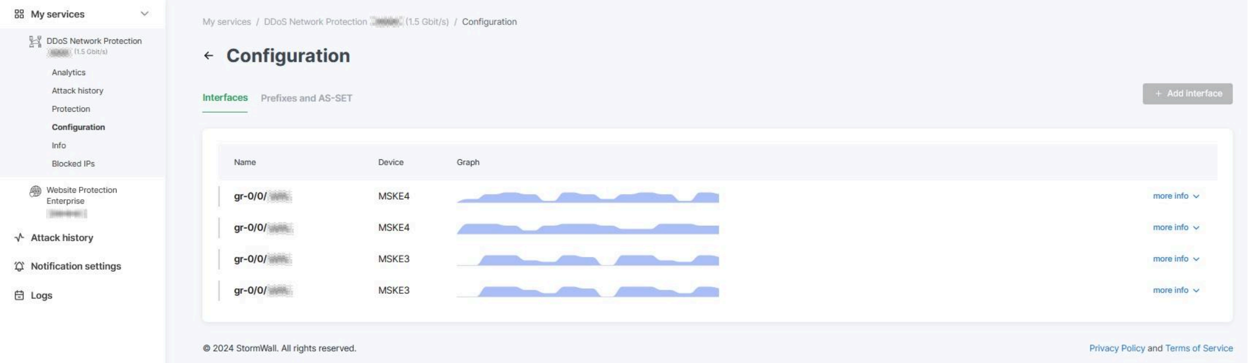
Configuration

In the left panel, select the **Configuration** option.



A page will open with two tabs:

- Interfaces
- Prefixes and AS-SET

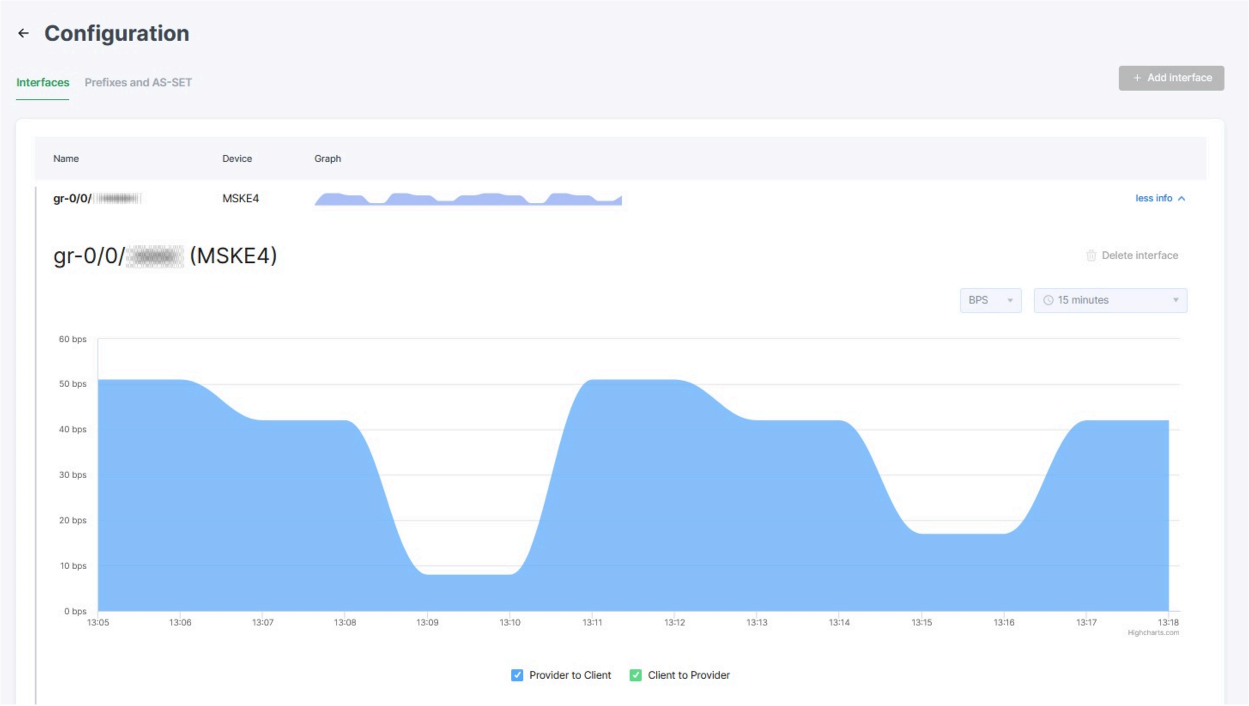


Name	Device	Graph	
gr-0/0/[redacted]	MSKE4		more info
gr-0/0/[redacted]	MSKE4		more info
gr-0/0/[redacted]	MSKE3		more info
gr-0/0/[redacted]	MSKE3		more info

© 2024 StormWall. All rights reserved.

Privacy Policy and Terms of Service

On the **Interfaces** tab, click the **Details** button in the interface row. A chart with traffic analysis will open.



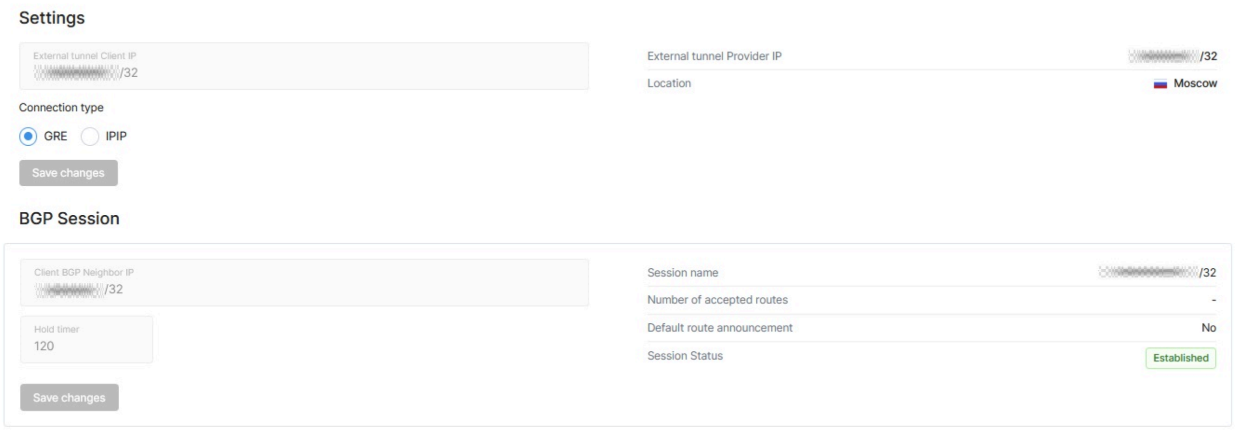
← Configuration

Name	Device	Graph
gr-0/0/[redacted]	MSKE4	less info ^

gr-0/0/[redacted] (MSKE4)

Place the mouse cursor over the time of interest on the chart - an information field with data for that moment in time will be displayed.

Below the chart, the **Settings** and **BGP Session** sections are located.



Settings

External tunnel Client IP: [redacted]/32

External tunnel Provider IP: [redacted]/32

Location: Moscow

Connection type

● GRE ○ IPIP

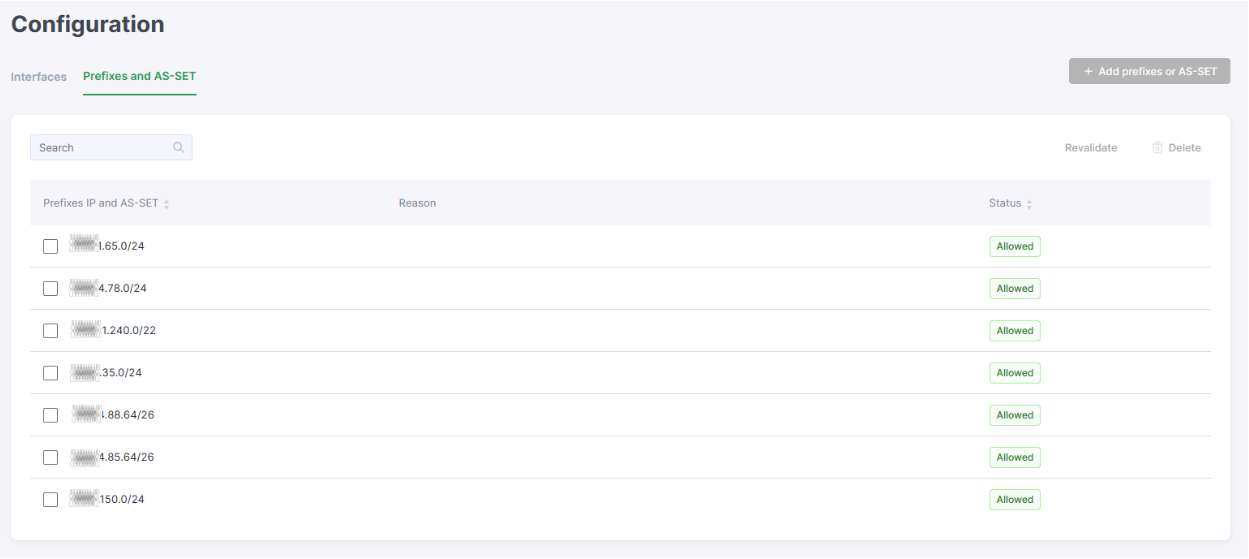
BGP Session

Client BGP Neighbor IP: [redacted]/32

Hold timer: 120

Session name	[redacted]/32
Number of accepted routes	-
Default route announcement	No
Session Status	Established

Open the **Prefixes and AS-SET** tab. An AS-SET object is a collection of Autonomous Systems (AS). Besides AS, AS-SET can include other AS-SET objects.



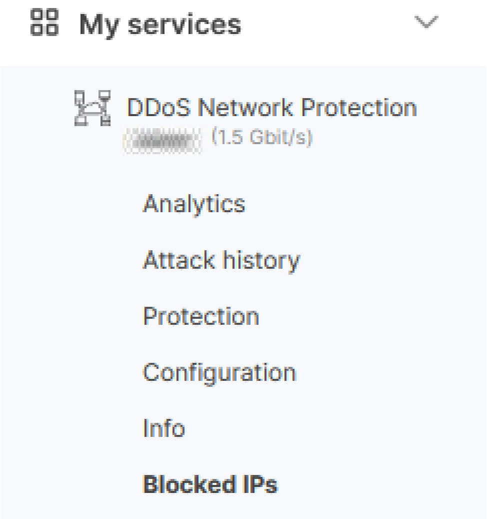
	Prefixes IP and AS-SET	Reason	Status
□	[redacted]1.65.0/24		Allowed
□	[redacted]4.78.0/24		Allowed
□	[redacted]1.240.0/22		Allowed
□	[redacted].35.0/24		Allowed
□	[redacted].88.64/26		Allowed
□	[redacted]4.85.64/26		Allowed
□	[redacted]150.0/24		Allowed

To add a new value, click the **Add Prefixes or AS-SET** button and fill out the form that opens. Select values by checking their boxes to use the **Revalidate** or **Delete** button.

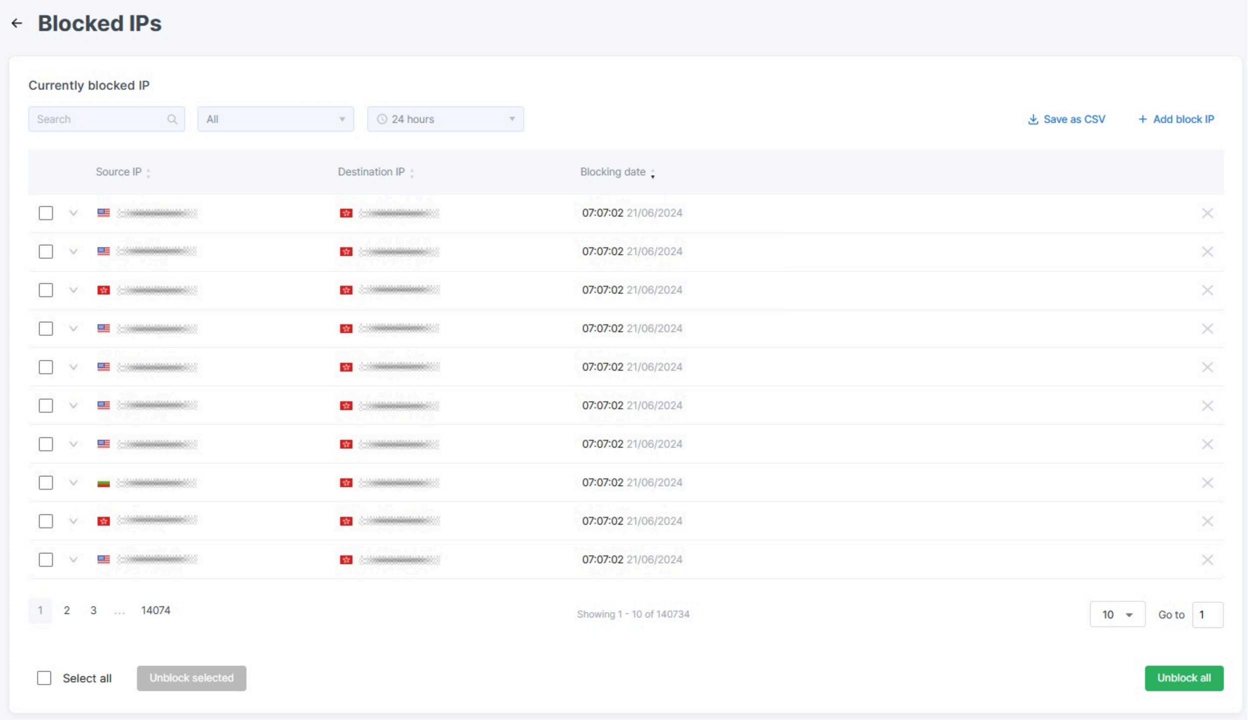
If buttons are inactive or if you have other questions, please contact technical support.

Blocked IP's

In the left menu, select the **Blocked IP's** item.



On the page that opens, there is a list of blocked IP addresses. Use the search area, the filter for test and real blocks, as well as time filtering. You can save the list of addresses by clicking the **Save as CSV** button.



← **Blocked IPs**

Currently blocked IP

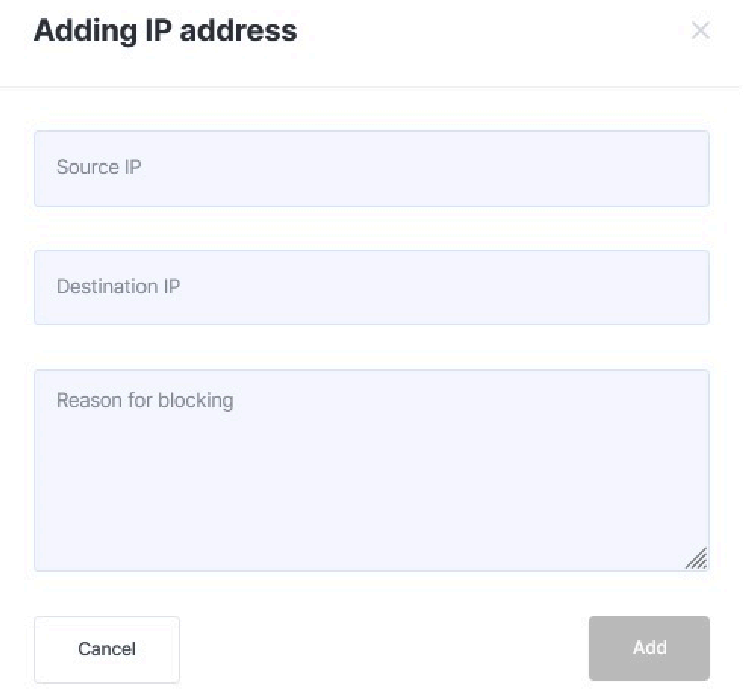
Search | All ▾ | 24 hours ▾ | Save as CSV | + Add block IP

		Source IP	Destination IP	Blocking date	
☐	⌄	🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×
☐	⌄	🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×
☐	⌄	🇭🇰 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×
☐	⌄	🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×
☐	⌄	🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×
☐	⌄	🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×
☐	⌄	🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×
☐	⌄	🇧🇬 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×
☐	⌄	🇭🇰 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×
☐	⌄	🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024	×

1 2 3 … 14074 Showing 1 - 10 of 140734 10 ▾ Go to 1

☐ Select all | Unblock selected | Unblock all

To block an IP address, click the **Add block IP** button. Fill out the form that opens and click the **Add** button.



Adding IP address ×

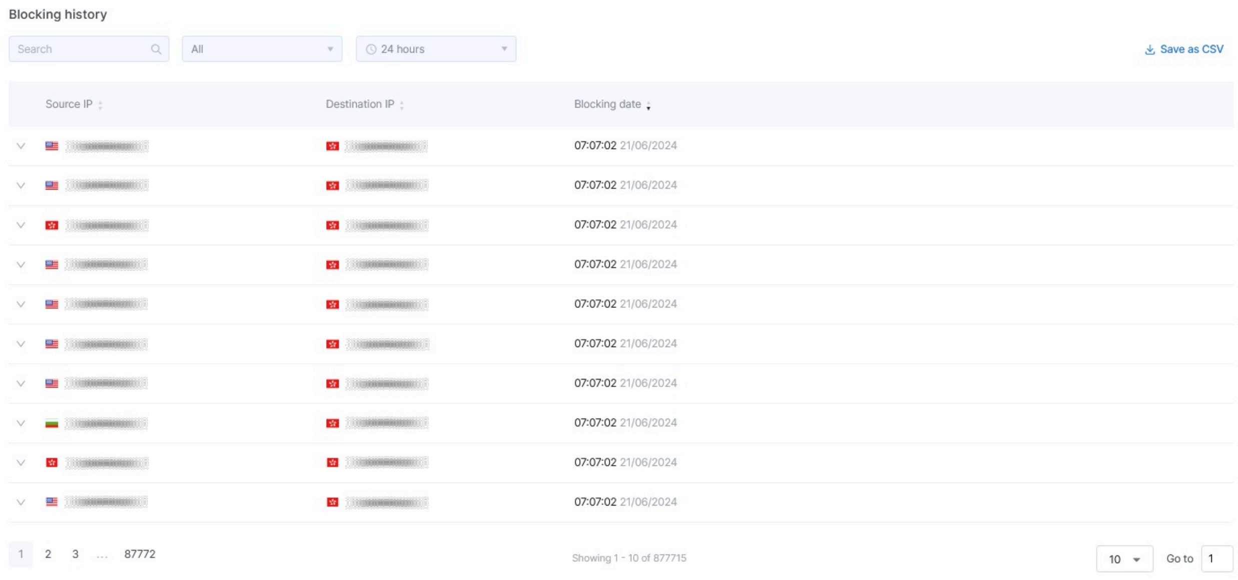
Source IP

Destination IP

Reason for blocking

Cancel | Add

Below the table of blocked IP addresses, there is a **Blocking history** table. It also offers search and filtering capabilities. You can save the list by clicking the **Save as CSV** button.



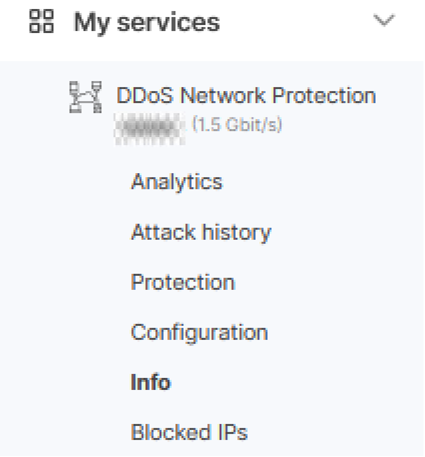
Blocking history

Source IP	Destination IP	Blocking date
🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024
🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024
🇭🇰 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024
🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024
🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024
🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024
🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024
🇧🇬 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024
🇭🇰 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024
🇺🇸 [redacted]	🇭🇰 [redacted]	07:07:02 21/06/2024

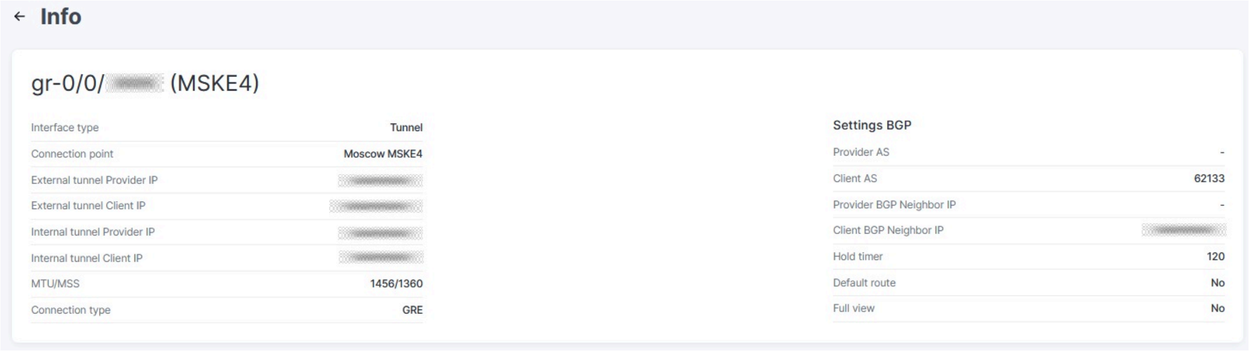
Showing 1 - 10 of 877715

Info

In the left menu, select the **Info** item.



The page that opens contains detailed information about each of the protected objects.



← Info

gr-0/0/[redacted] (MSKE4)

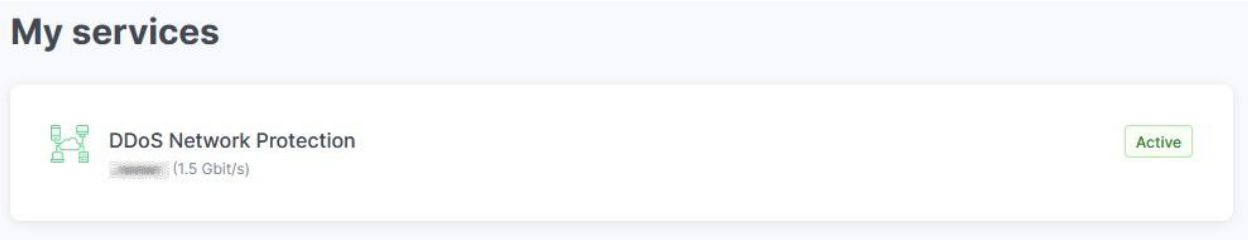
Interface type	Tunnel
Connection point	Moscow MSKE4
External tunnel Provider IP	[redacted]
External tunnel Client IP	[redacted]
Internal tunnel Provider IP	[redacted]
Internal tunnel Client IP	[redacted]
MTU/MSS	1456/1360
Connection type	GRE

Settings BGP

Provider AS	-
Client AS	62133
Provider BGP Neighbor IP	-
Client BGP Neighbor IP	[redacted]
Hold timer	120
Default route	No
Full view	No

Monitoring Tools

After connecting the service, it will be displayed on the main page of the account.

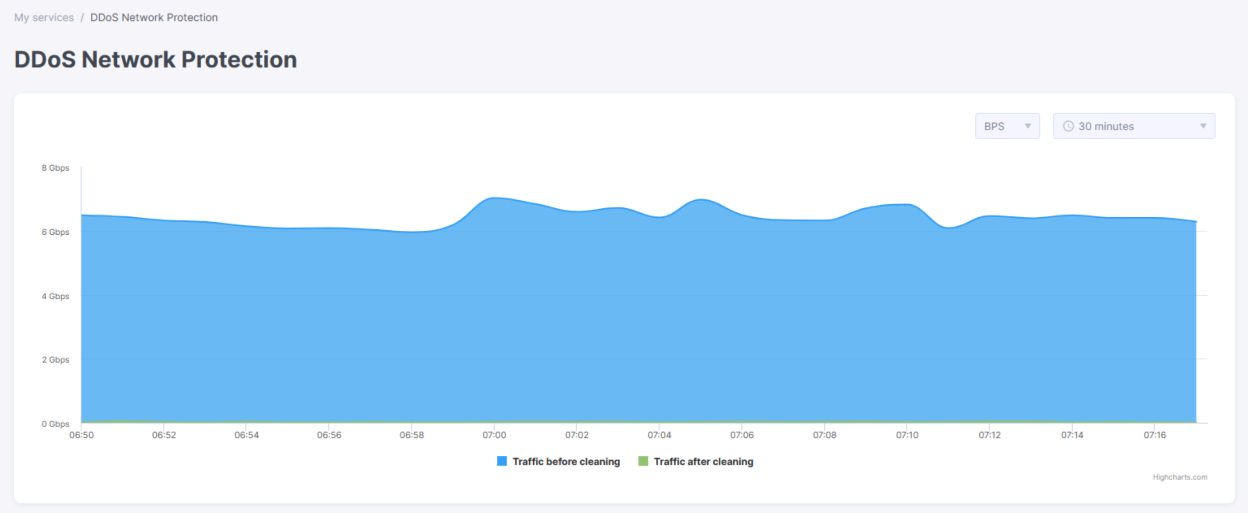


My services

DDoS Network Protection
[redacted] (1.5 Gbit/s)

To view the details, click on the service field. The chart on the opened page demonstrates the volume of traffic before and after filtration. Use the tools in the upper right corner of the chart:

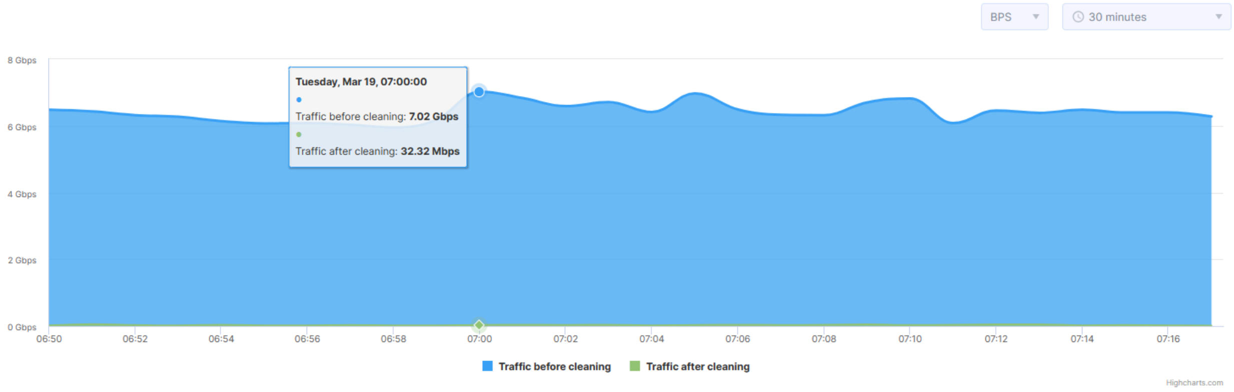
- BPS (bits per second) / PPS (packets per second);
- time filter.



My services / DDoS Network Protection

DDoS Network Protection

To see numerical characteristics at a specific moment in time, hover the mouse cursor over the chart.

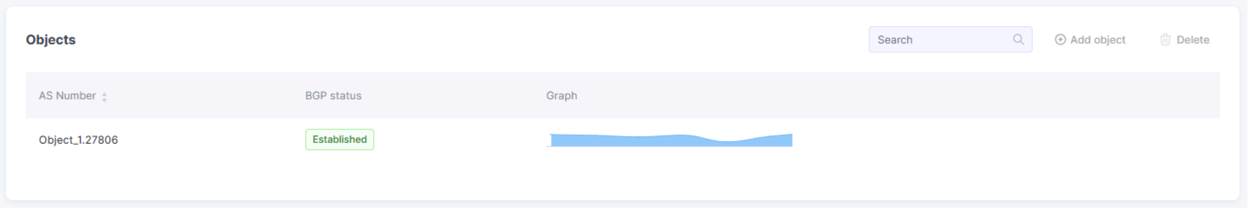


Tuesday, Mar 19, 07:00:00

● Traffic before cleaning: **7.02 Gbps**

● Traffic after cleaning: **32.32 Mbps**

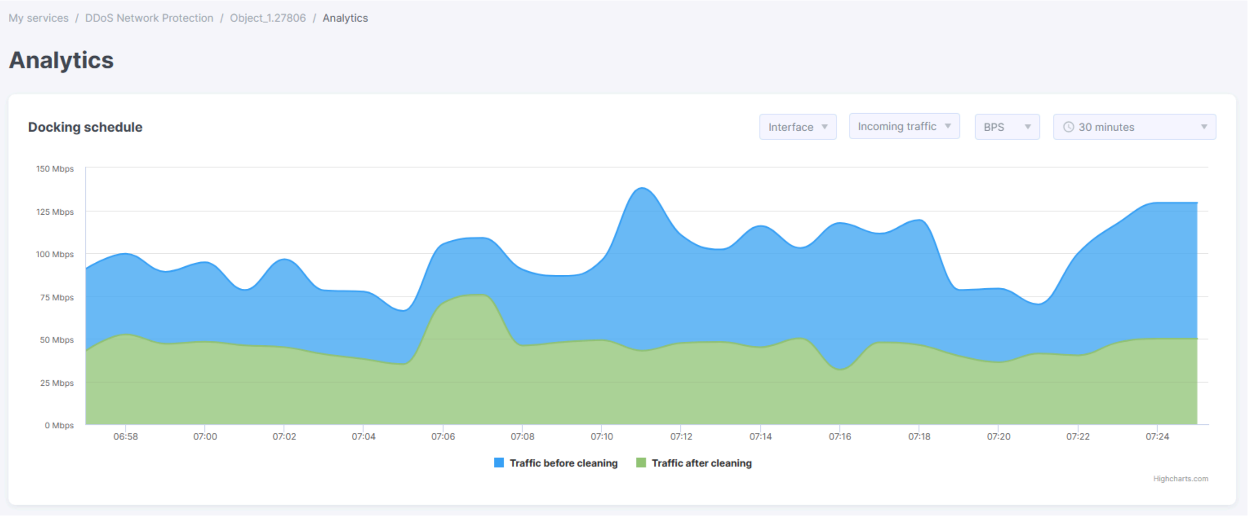
A list of objects is provided, which you can edit using the **Add Object** and **Delete** buttons.



Objects

AS Number	BGP status	Graph
Object_1.27806	Established	

Click on the chart thumbnail in the object row to view analytical information.



My services / DDoS Network Protection / Object_1.27806 / Analytics

Analytics

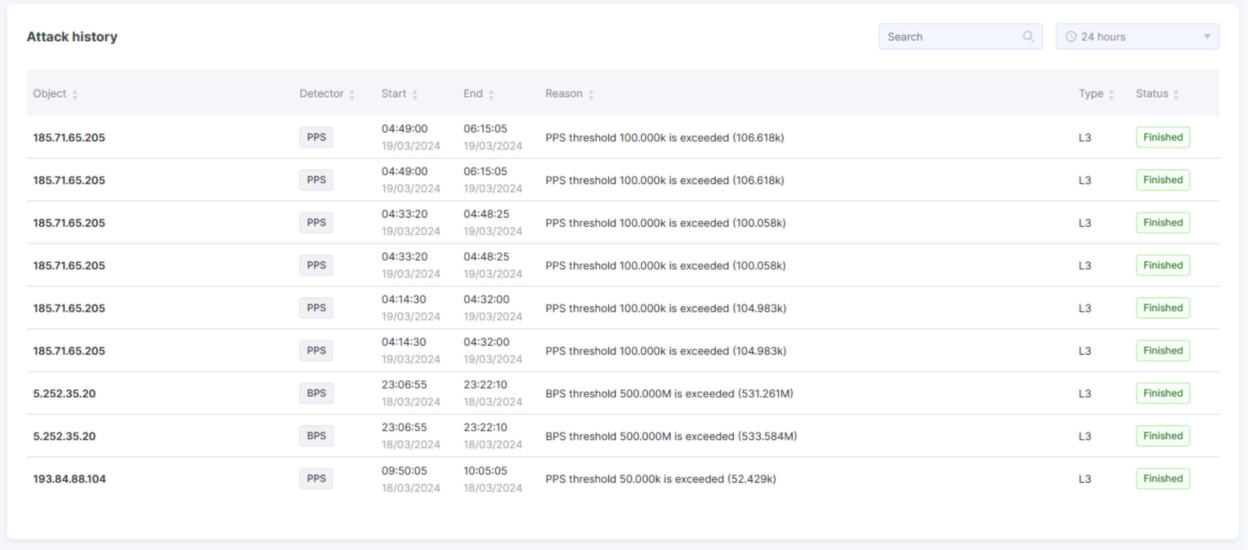
Docking schedule

Interface ▾ | Incoming traffic ▾ | BPS ▾ | 30 minutes ▾

Manage the dockable chart using the toolbar above it:

- Interface / Protocol;
- Outgoing Traffic / Incoming Traffic;
- BPS / PPS;
- Time Filter.

At the bottom of the page, there is a table of attack history. Use the **Search** tool and time filter to highlight information.

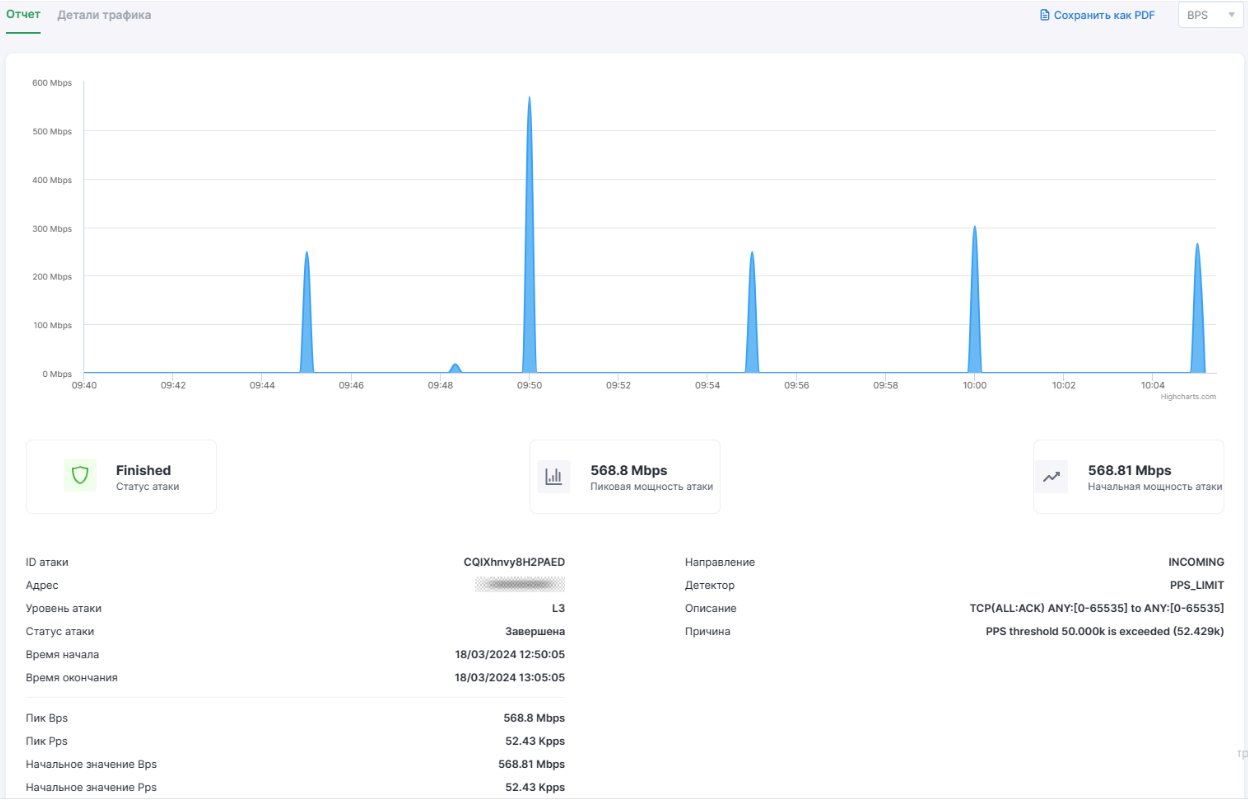


Attack history

Search | 24 hours ▾

Object	Detector	Start	End	Reason	Type	Status
185.71.65.205	PPS	04:49:00 19/03/2024	06:15:05 19/03/2024	PPS threshold 100.000k is exceeded (106.618k)	L3	Finished
185.71.65.205	PPS	04:49:00 19/03/2024	06:15:05 19/03/2024	PPS threshold 100.000k is exceeded (106.618k)	L3	Finished
185.71.65.205	PPS	04:33:20 19/03/2024	04:48:25 19/03/2024	PPS threshold 100.000k is exceeded (100.058k)	L3	Finished
185.71.65.205	PPS	04:33:20 19/03/2024	04:48:25 19/03/2024	PPS threshold 100.000k is exceeded (100.058k)	L3	Finished
185.71.65.205	PPS	04:14:30 19/03/2024	04:32:00 19/03/2024	PPS threshold 100.000k is exceeded (104.983k)	L3	Finished
185.71.65.205	PPS	04:14:30 19/03/2024	04:32:00 19/03/2024	PPS threshold 100.000k is exceeded (104.983k)	L3	Finished
5.252.35.20	BPS	23:06:55 18/03/2024	23:22:10 18/03/2024	BPS threshold 500.000M is exceeded (531.261M)	L3	Finished
5.252.35.20	BPS	23:06:55 18/03/2024	23:22:10 18/03/2024	BPS threshold 500.000M is exceeded (533.584M)	L3	Finished
193.84.88.104	PPS	09:50:05 18/03/2024	10:05:05 18/03/2024	PPS threshold 50.000k is exceeded (52.429k)	L3	Finished

To view information about an attack, click on the row with it. On the **Report** tab of the opened page, a chart of the attack and information about it will be provided. Click the **Save as PDF** button to download the report on the attack.



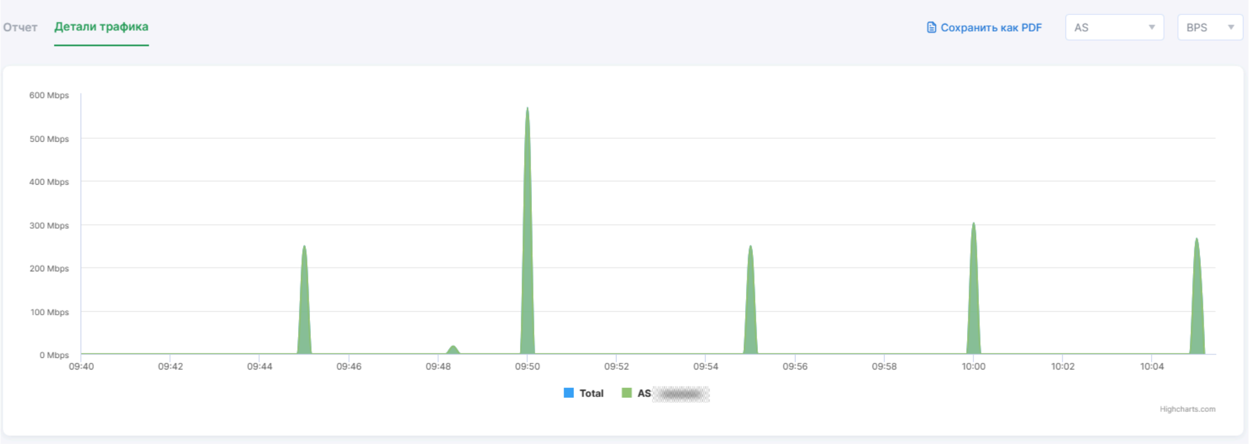
Finished
Статус атаки

568.8 Mbps
Пиковая мощность атаки

568.81 Mbps
Начальная мощность атаки

ID атаки	CQIXhnvy8H2PAED	Направление	INCOMING
Адрес	[redacted]	Детектор	PPS_LIMIT
Уровень атаки	L3	Описание	TCP(ALL:ACK) ANY:[0-65535] to ANY:[0-65535]
Статус атаки	Завершена	Причина	PPS threshold 50.000k is exceeded (52.429k)
Время начала	18/03/2024 12:50:05		
Время окончания	18/03/2024 13:05:05		
Пик Bps	568.8 Mbps		
Пик Pps	52.43 Kpps		
Начальное значение Bps	568.81 Mbps		
Начальное значение Pps	52.43 Kpps		

Familiarize yourself with the information on the **Traffic Details** tab - here, you can view charts for each Autonomous System (AS) separately.


Отчет
Детали трафика
Сохранить как PDF
AS
BPS
600 Mbps
500 Mbps
400 Mbps
300 Mbps
200 Mbps
100 Mbps
0 Mbps
09:40
09:42
09:44
09:46
09:48
09:50
09:52
09:54
09:56
09:58
10:00
10:02
10:04
Total
AS [redacted]
Highcharts.com

DDoS protection for TCP/UDP services

How the Service Works

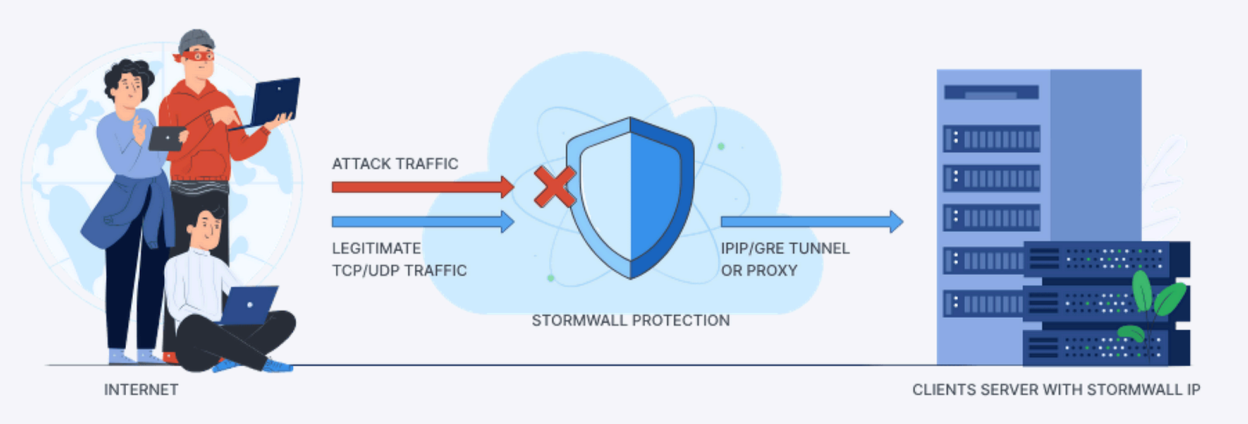
The **«StormWall for Servers»** service involves filtering any types of malicious traffic, connected via a tunnel based on the IPIP/GRE protocol, proxying, or directly on the platform. The service is aimed at both end customers (web services, gaming services, VoIP, web applications for business, etc.) and service providers (data centers, hosting and internet providers, telecom operators, etc.).

Implementation options:

- **Tunneling**
  We "teleport" an external protected Storm IP to your equipment, which clients connect to.
  You will know the IP addresses of your users.
  Suitable for Unix OS and specialized routers.
- **Proxying**
  All requests to the server will come from a single IP address.
  You will not know the IP addresses of your users.
  Suitable for Windows OS.

This service:

- provides reliable protection of TCP/UDP services from DDoS attacks;
- filters an unlimited volume of traffic;
- does not limit the number of ports on your server;
- provides filtering at OSI model levels 3-5.



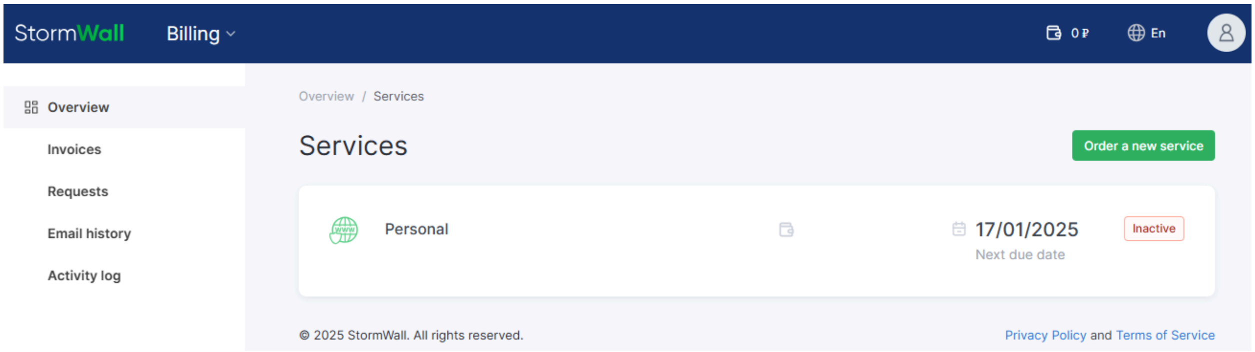
For traffic filtering, Triple Filter is used; for HTTP flood filtering, the BanHammer technology is applied; for protection against failures at StormWall network nodes, the Global Session technology is utilized; and for acceleration, the HyperCache technology is employed.

To reduce response time and minimize issues related to the use of NAT, StormWall implements the ZeroNAT Tunnels technology. As a result, the customer receives a real IP address directly on their server. Moreover, there are no restrictions on the number of ports used.

Order

To set up DDoS protection for TCP/UDP services for your network:

1. Log in to your Client Portal by authenticating on the website;
2. On the top panel of the site, select the **Billing** tab;



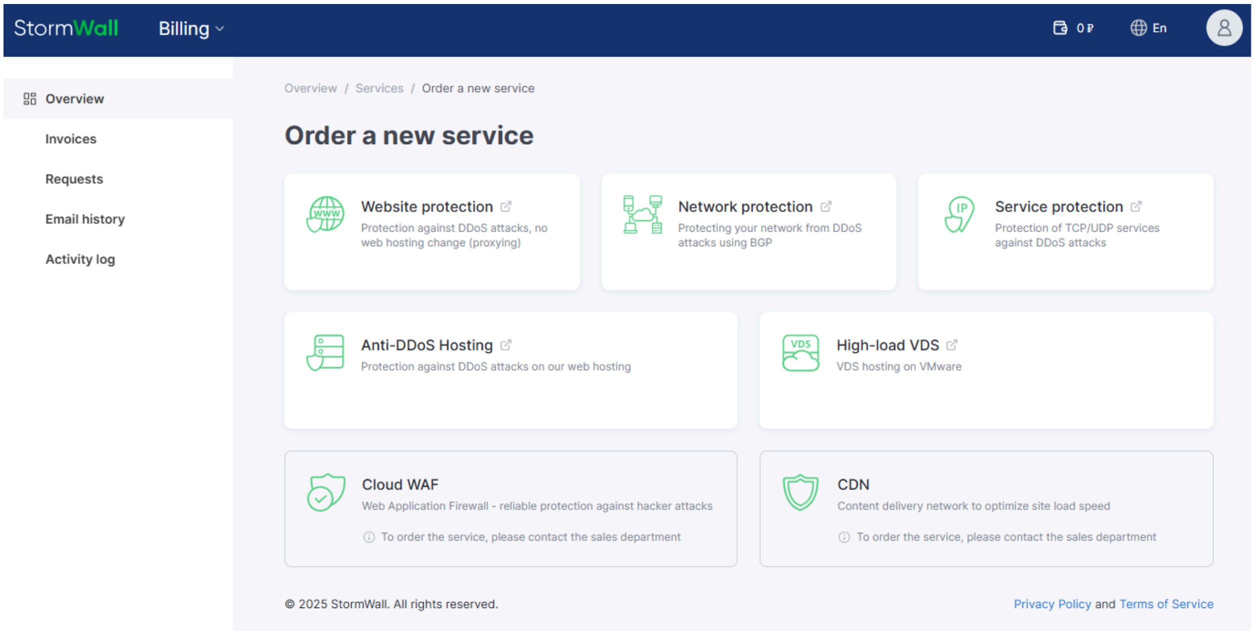
Services

Personal 17/01/2025 Next due date Inactive

© 2025 StormWall. All rights reserved.

Privacy Policy and Terms of Service

3. In the tab that opens, choose the **Protection of servers and networks** option.



Order a new service

Website protection
Protection against DDoS attacks, no web hosting change (proxying)

Network protection
Protecting your network from DDoS attacks using BGP

Service protection
Protection of TCP/UDP services against DDoS attacks

Anti-DDoS Hosting
Protection against DDoS attacks on our web hosting

High-load VDS
VDS hosting on VMware

Cloud WAF
Web Application Firewall - reliable protection against hacker attacks
To order the service, please contact the sales department

CDN
Content delivery network to optimize site load speed
To order the service, please contact the sales department

© 2025 StormWall. All rights reserved.

Privacy Policy and Terms of Service

4. You will be redirected to a [website page] with a detailed description of the service.
5. Familiarize yourself with the information about the service and pricing plans:
   - Personal
   - Business
   - Enterprise

If none of the presented plans meet your requirements, contact us - we will make you a special offer.

Activation

To connect protection on your server, you need to run the script we provided, **storm.sh**, with the command **«./storm.sh start»**.

First, make the file executable with the command: **«chmod +x storm.sh»**.

Add the following to your firewall exceptions:

185.121.240.0/22

193.84.78.0/24

103.134.155.0/24

188.0.150.0/24

193.104.120.0/24

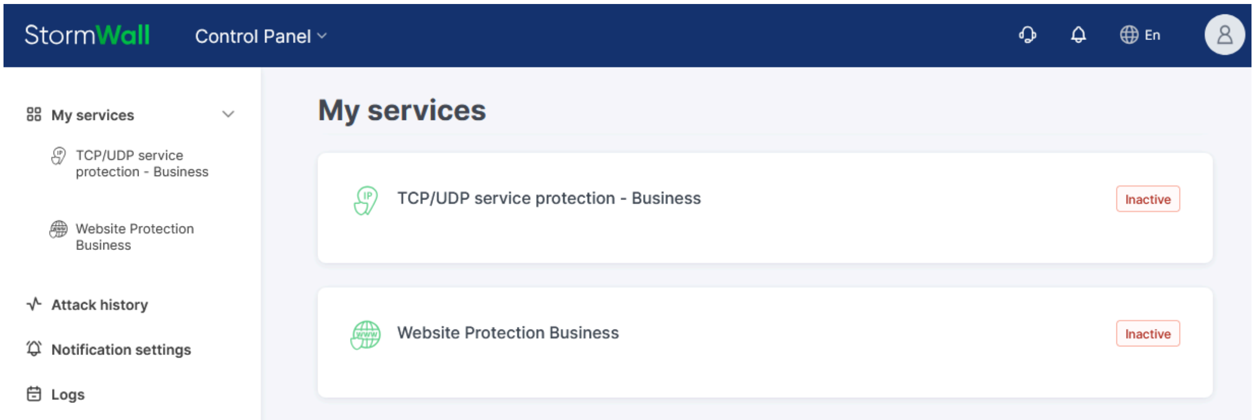
For example, you can use the following commands:

```
iptables -I INPUT -s 185.121.240.0/22 -j ACCEPT

iptables -I INPUT -s 193.84.78.0/24 -j ACCEPT

iptables -I INPUT -s 103.134.155.0/24 -j ACCEPT

iptables -I INPUT -s 188.0.150.0/24 -j ACCEPT

iptables -I INPUT -s 193.104.120.0/24 -j ACCEPT
```

We recommend adding this script to startup for automatic tunnel lifting after server reboot. If you have any questions or need assistance with setting up and configuring protection, please let us know through the chat on the website or the inquiry form in your personal account.

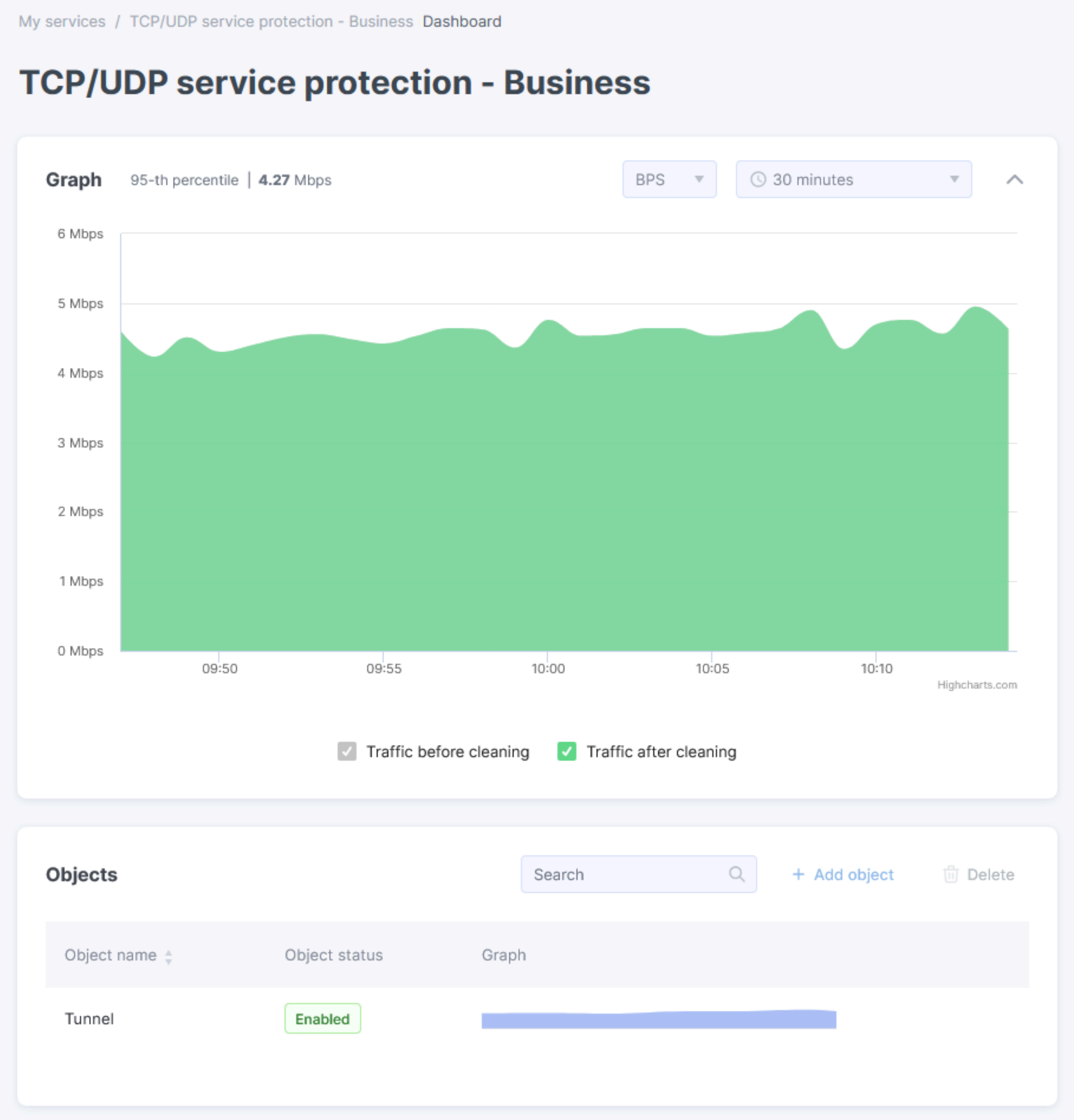
Configuration of security parameters

After the service is connected, it will appear on the main page of your **Client Portal** and in the **My Services** list.


StormWall
Control Panel
En
My services
TCP/UDP service protection - Business
Website Protection Business
Attack history
Notification settings
Logs
My services
TCP/UDP service protection - Business
Inactive
Website Protection Business
Inactive

To view the details, click on the name of the service in the central area of the page or in the list on the left.

If there is only one object, a menu for working with it will open in the left area of the page.



My services / TCP/UDP service protection - Business Dashboard

TCP/UDP service protection - Business

Graph 95-th percentile | **4.27** Mbps

BPS

30 minutes

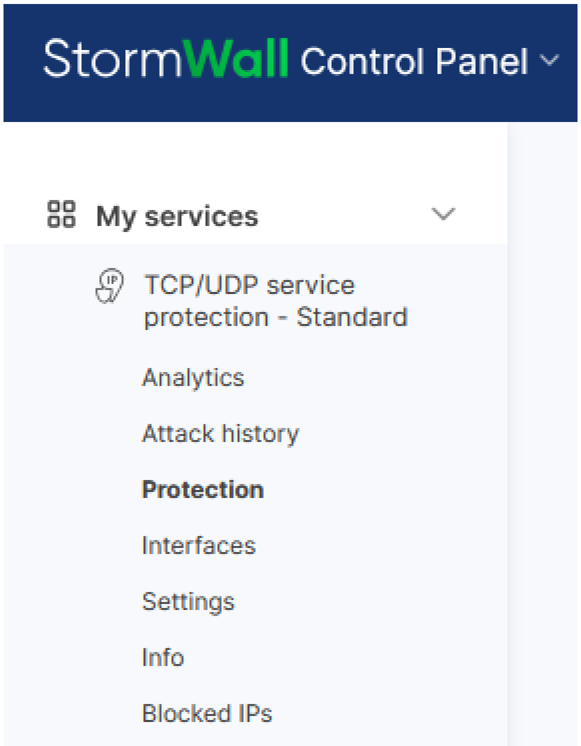
Objects

Object name	Object status	Graph
Tunnel	Enabled	

In the **Objects** section, select the object you are interested in and click on the chart thumbnail in its row. This action will open a menu for working with the selected object in the left area of the page.

Protection

In the opened menu, select the **Protection** option.



A configuration area will open with the following fields:

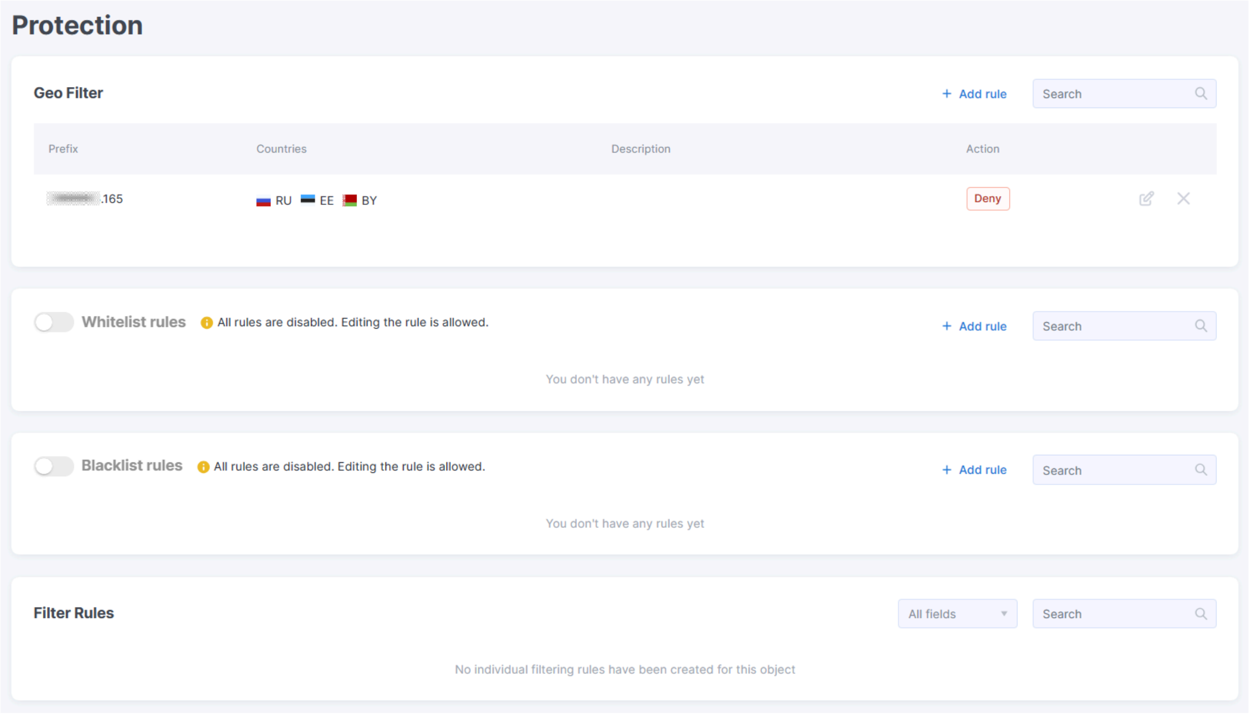
- Geolocation filter
- Whitelist rules

  Requests from addresses listed here will proceed without filtration.

- Blacklist rules

  A user with an address from this list will not be able to use your service.

- Filtering rules



Protection

Geo Filter

+ Add rule | Search

Prefix	Countries	Description	Action
[redacted].165	RU EE BY		Deny

Whitelist rules — All rules are disabled. Editing the rule is allowed.

+ Add rule | Search

You don't have any rules yet

Blacklist rules — All rules are disabled. Editing the rule is allowed.

+ Add rule | Search

You don't have any rules yet

Filter Rules

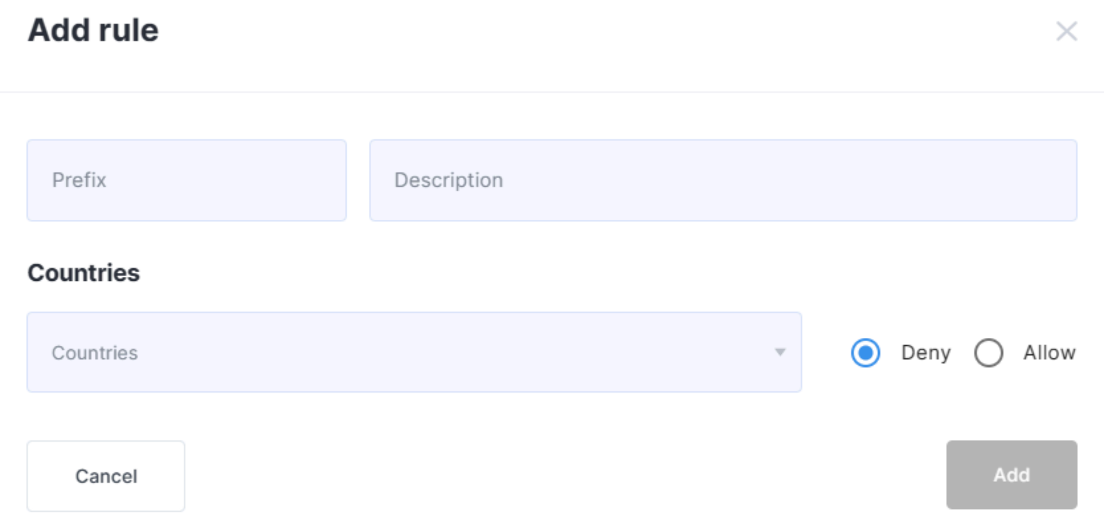
All fields | Search

No individual filtering rules have been created for this object

Click the **Add rule** button to create a restriction on the use of your resource.

To set up geo-blocking, you need to fill out the form:

- Prefix (for which area of your network the rule will be applied);
- Description (optional);
- Countries (select from the dropdown list). Using the **Allow** and **Deny** switches, you can configure both allowing and denying lists.



Add rule

Prefix

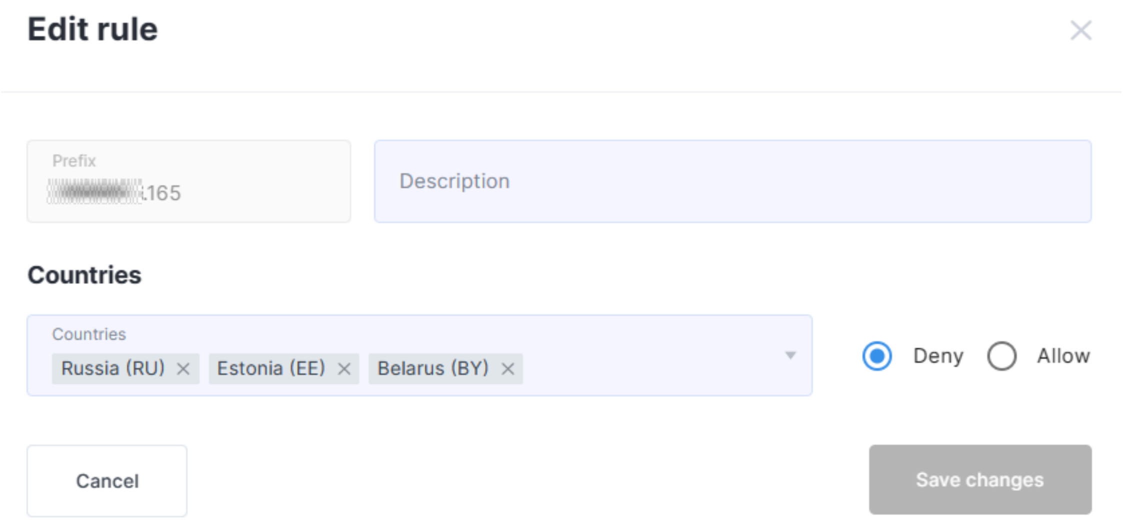
Description

Countries

Countries

● Deny ○ Allow

After filling out the form, click the **Add** button. By clicking the «pencil» icon in the field of the created rule, you can open the form to edit it.



Edit rule

Prefix
[redacted].165

Description

Countries

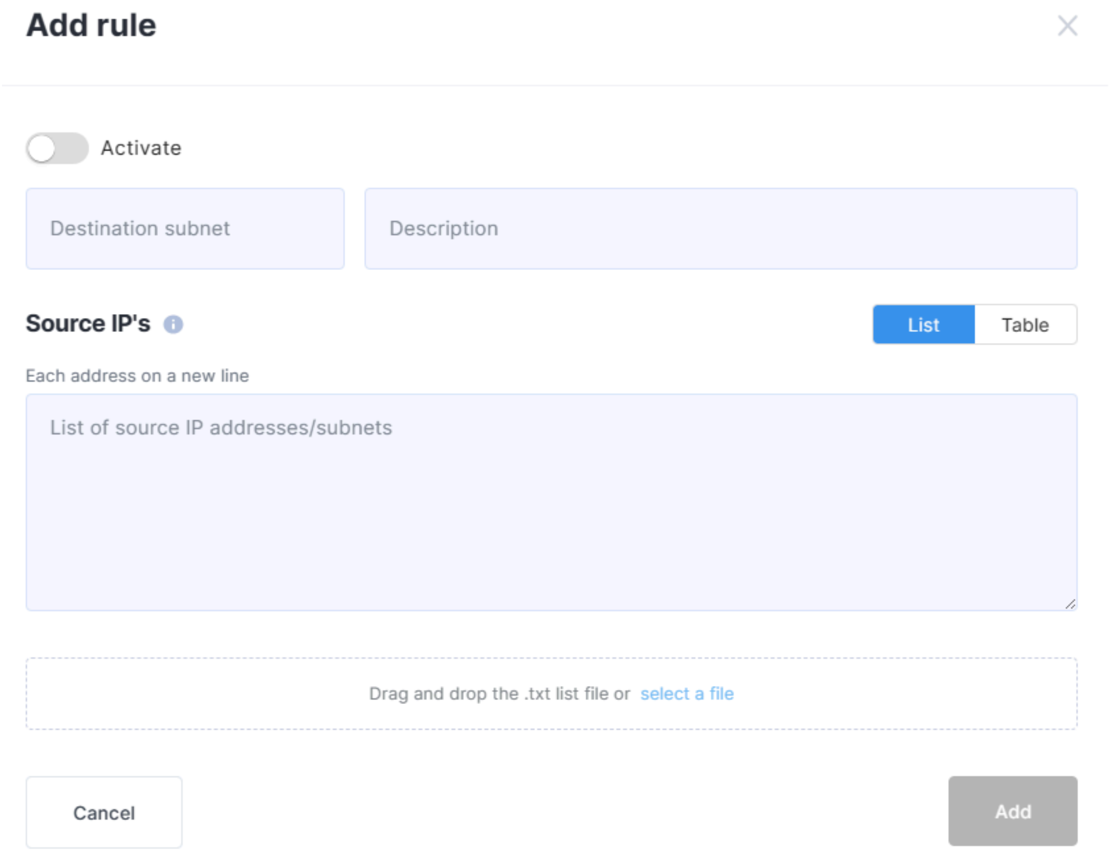
Countries
Russia (RU) × Estonia (EE) × Belarus (BY) ×

● Deny ○ Allow

After making changes, click the **Save** button. To configure the rules that will determine how users are added to black or white lists, fill out the form with the following information:

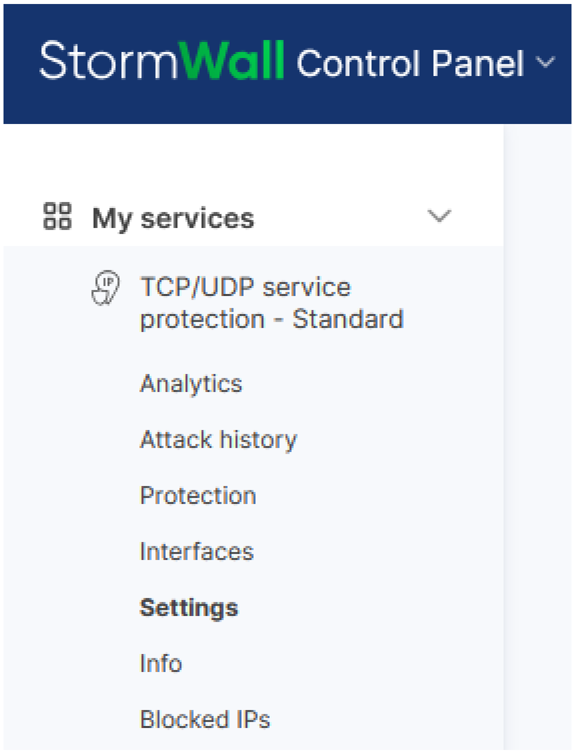
- Destination subnet;
- Description (optional);
- IP sources.

When adding IP addresses, each one must be entered on a new line. You can also upload them in a «txt» file format by clicking the **Select a file** button. To apply the rule, set the **Activate** toggle to the ON position.

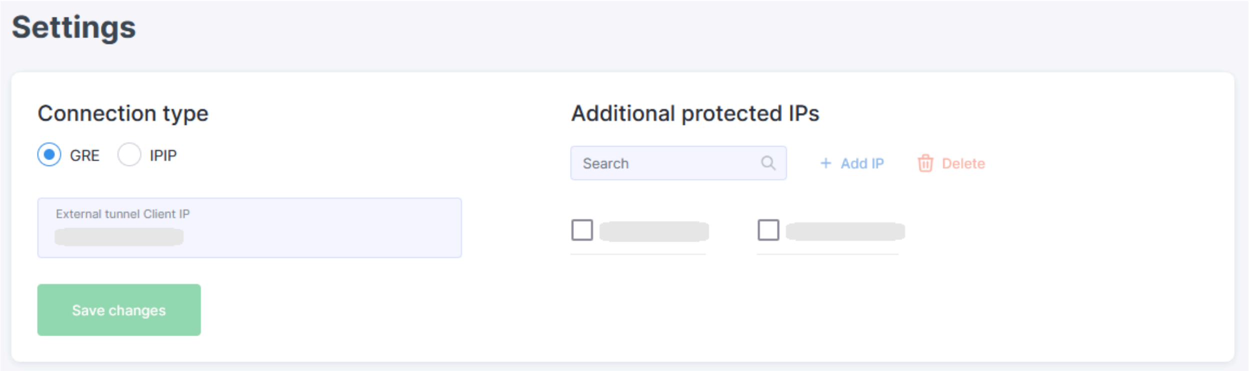

Add rule
Activate
Destination subnet
Description
Source IP's
List
Table
Each address on a new line
List of source IP addresses/subnets
Drag and drop the .txt list file or select a file
Cancel
Add

Settings

In the menu, select the **Settings** option.



The settings page will open.



Connection type

● GRE ○ IPIP

External tunnel Client IP: [redacted]

Additional protected IPs

□ [redacted] □ [redacted]

Select the type of connection:

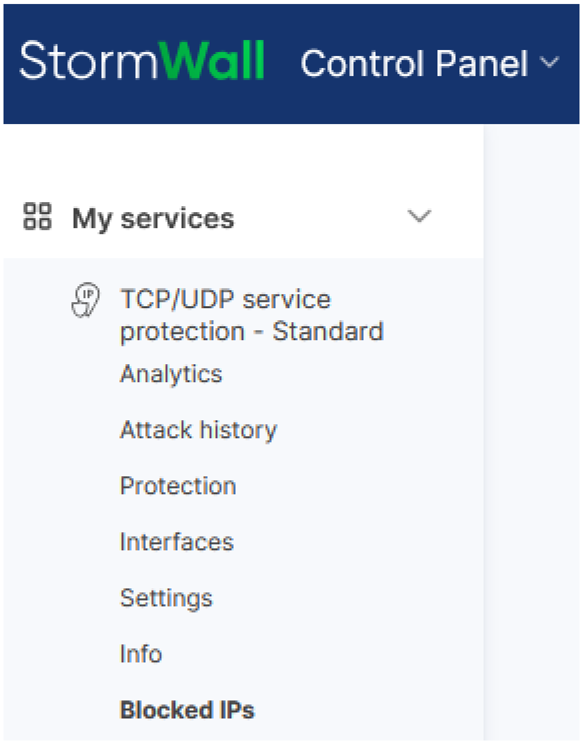
- **GRE**: GRE tunnel is one of the popular types of VPN. GRE tunnels are compatible with hardware security gateways, Mikrotik routers, Linux routers, and equipment that supports GRE (for example, Cisco, Juniper, etc.).

- **IPIP**: IPIP (IP over IP) is one of the simplest tunnels to set up (encapsulating only unicast IPv4 traffic). It can be configured on UNIX/Linux systems as well as various routers (for example, Cisco).

Fill in the «External IP address of the client tunnel». Use the **Add IP** button to add protected IP addresses. You can remove them at any time. After making changes, click the **Save** button.

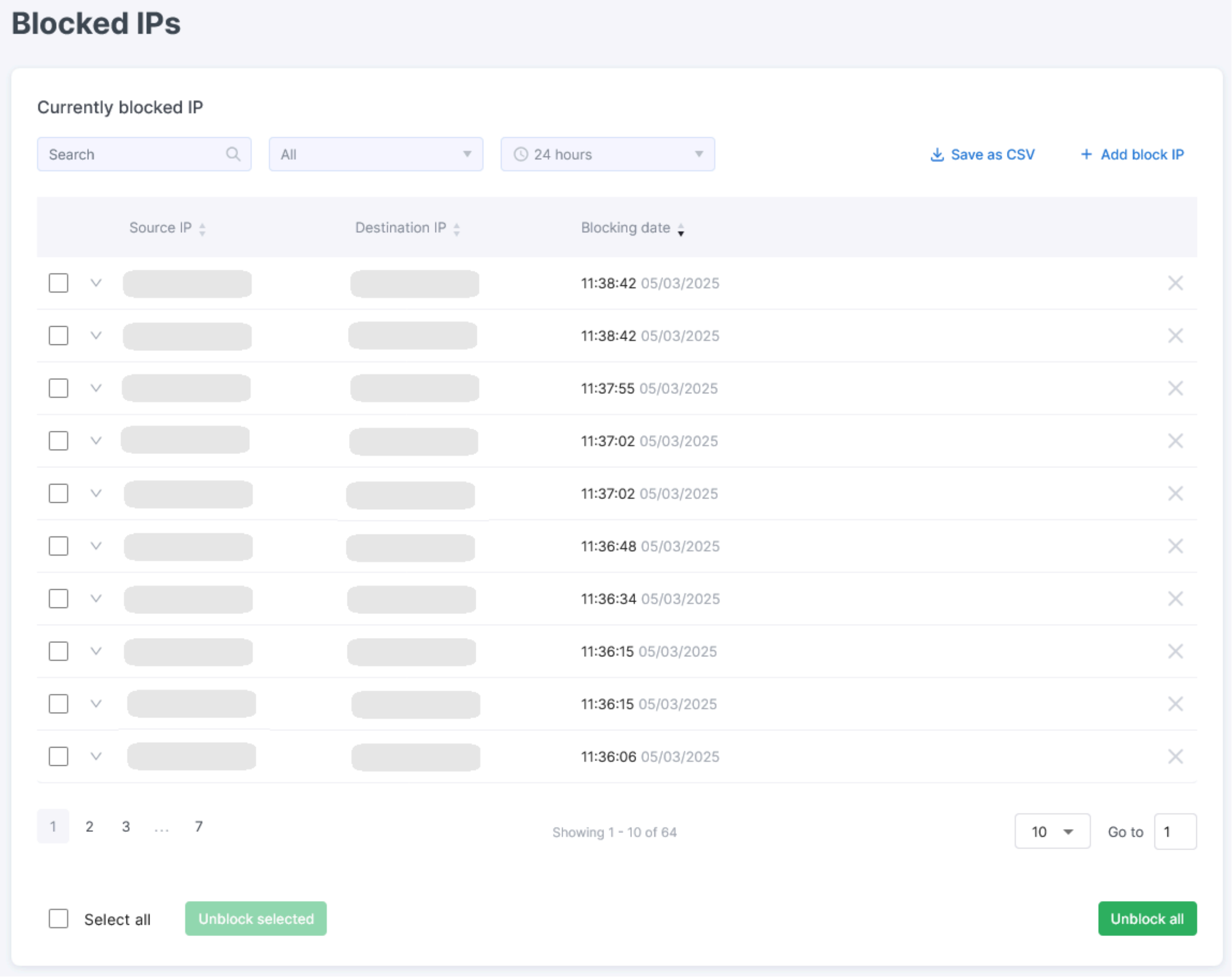
Blocked IPs

In the menu, select the **Blocked IPs** option.



The page that opens will display:

- Currently blocked IPs;
- Block history.



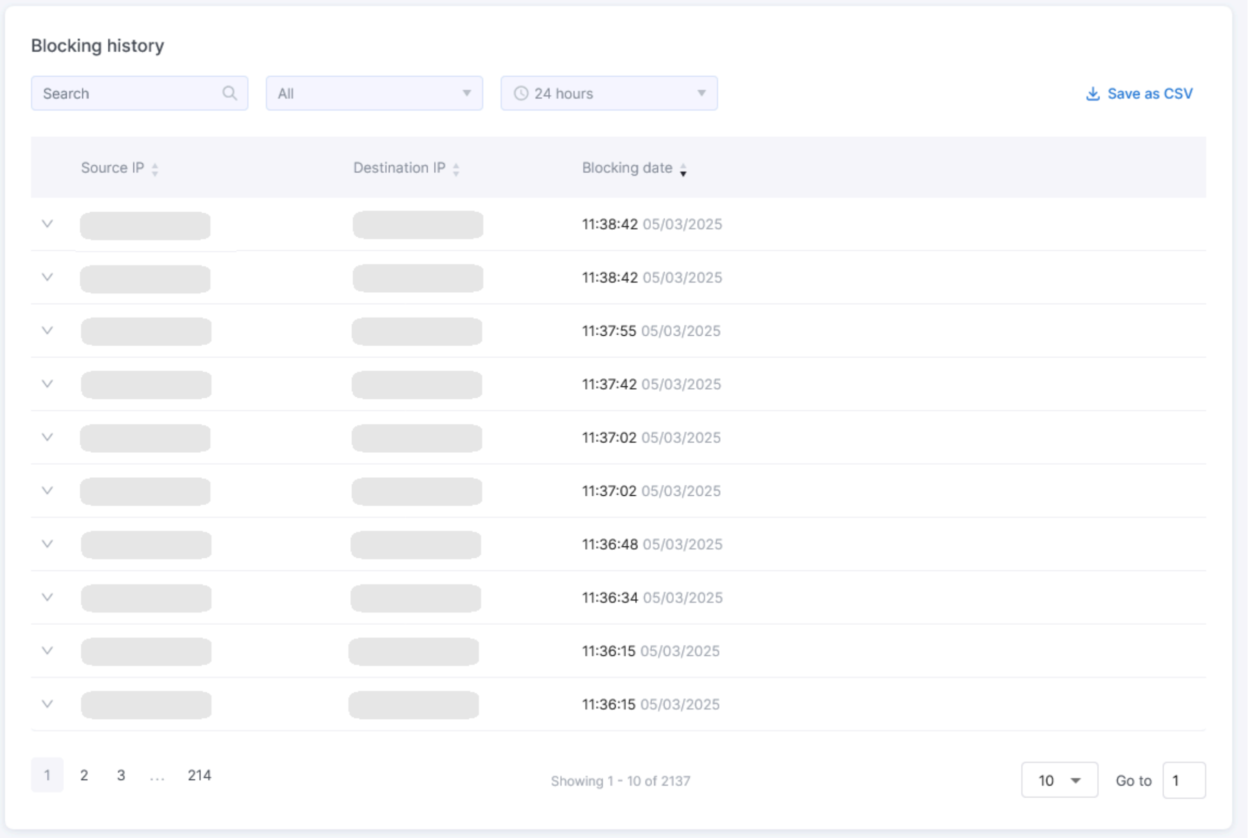
Blocked IPs

Currently blocked IP

		Source IP	Destination IP	Blocking date	
□	∨	[redacted]	[redacted]	11:38:42 05/03/2025	✕
□	∨	[redacted]	[redacted]	11:38:42 05/03/2025	✕
□	∨	[redacted]	[redacted]	11:37:55 05/03/2025	✕
□	∨	[redacted]	[redacted]	11:37:02 05/03/2025	✕
□	∨	[redacted]	[redacted]	11:37:02 05/03/2025	✕
□	∨	[redacted]	[redacted]	11:36:48 05/03/2025	✕
□	∨	[redacted]	[redacted]	11:36:34 05/03/2025	✕
□	∨	[redacted]	[redacted]	11:36:15 05/03/2025	✕
□	∨	[redacted]	[redacted]	11:36:15 05/03/2025	✕
□	∨	[redacted]	[redacted]	11:36:06 05/03/2025	✕

Showing 1 - 10 of 64

□ Select all



Blocking history

Search | All | 24 hours | Save as CSV

	Source IP	Destination IP	Blocking date
∨	[redacted]	[redacted]	11:38:42 05/03/2025
∨	[redacted]	[redacted]	11:38:42 05/03/2025
∨	[redacted]	[redacted]	11:37:55 05/03/2025
∨	[redacted]	[redacted]	11:37:42 05/03/2025
∨	[redacted]	[redacted]	11:37:02 05/03/2025
∨	[redacted]	[redacted]	11:37:02 05/03/2025
∨	[redacted]	[redacted]	11:36:48 05/03/2025
∨	[redacted]	[redacted]	11:36:34 05/03/2025
∨	[redacted]	[redacted]	11:36:15 05/03/2025
∨	[redacted]	[redacted]	11:36:15 05/03/2025

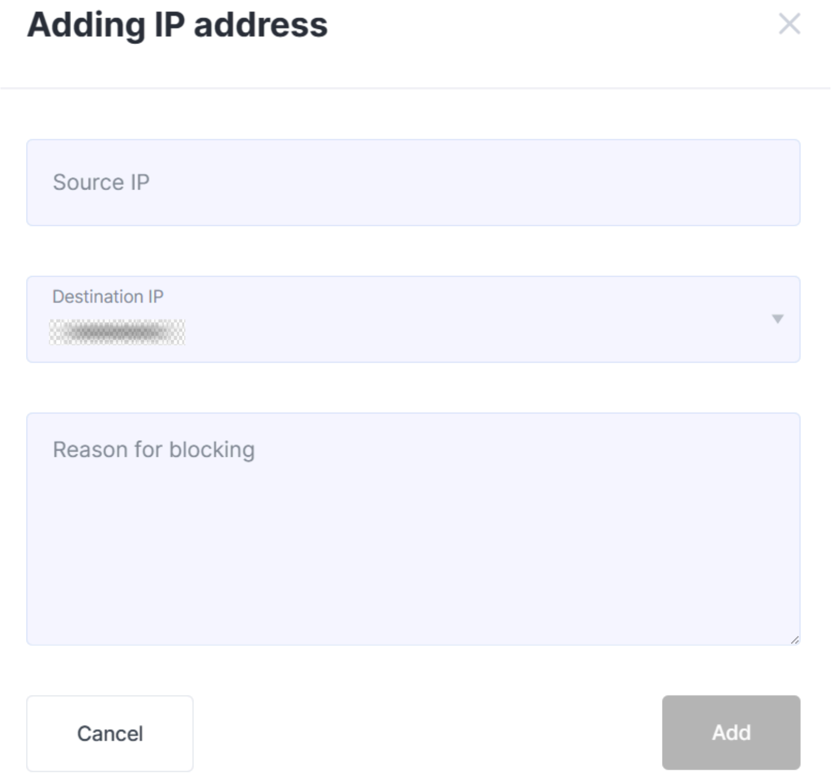
Showing 1 - 10 of 2137

You can remove some IP addresses from the block list by checking their boxes and clicking the **Unblock Selected** button. You can also completely clear the list using the **Unblock All** button.

Use the search and filters by time and data type to refine your list of addresses. You can save the records to a file by clicking the **Save as CSV** button.

You can block an IP address by clicking the **Add block IP** button. Fill out the form that opens:

- Source IP address - the one that needs to be blocked;
- Destination IP address - your address that needs protection;
- Reason for blocking - this field is optional.



Adding IP address

Source IP

Destination IP
[redacted]

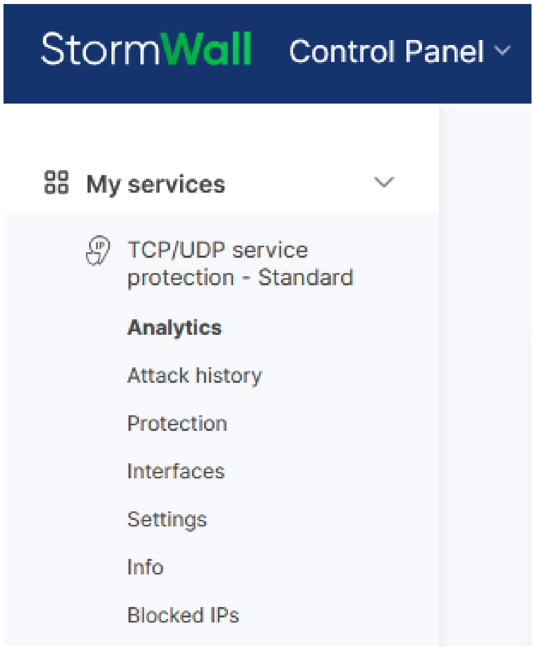
Reason for blocking

After filling out the form, click the **Add** button.

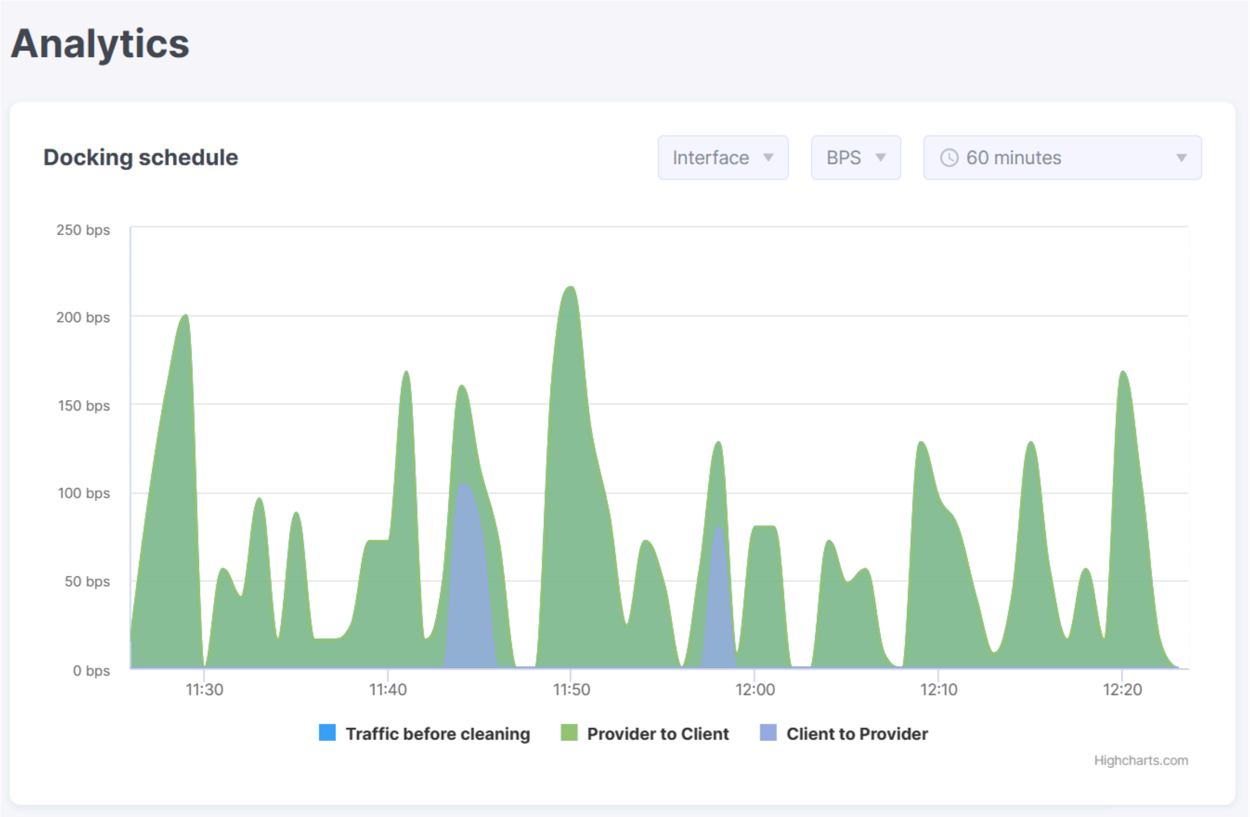
Monitoring Tools

Analytics

In the menu, select the **Analytics** option.



On the page, a docking chart and prefix statistics are displayed. Familiarize yourself with the docking chart - when you hover your mouse cursor over it, data for the specified moment in time is shown.

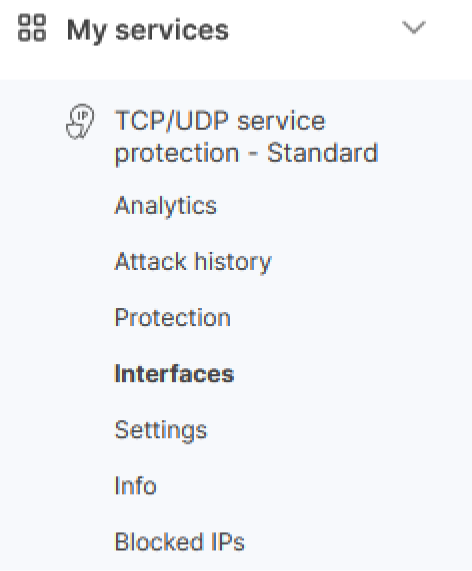


Use the tools in the upper right corner of the chart:

- Interface / Protocol;
- BPS (bits per second) / PPS (packets per second);
- Time filter.

Interfaces

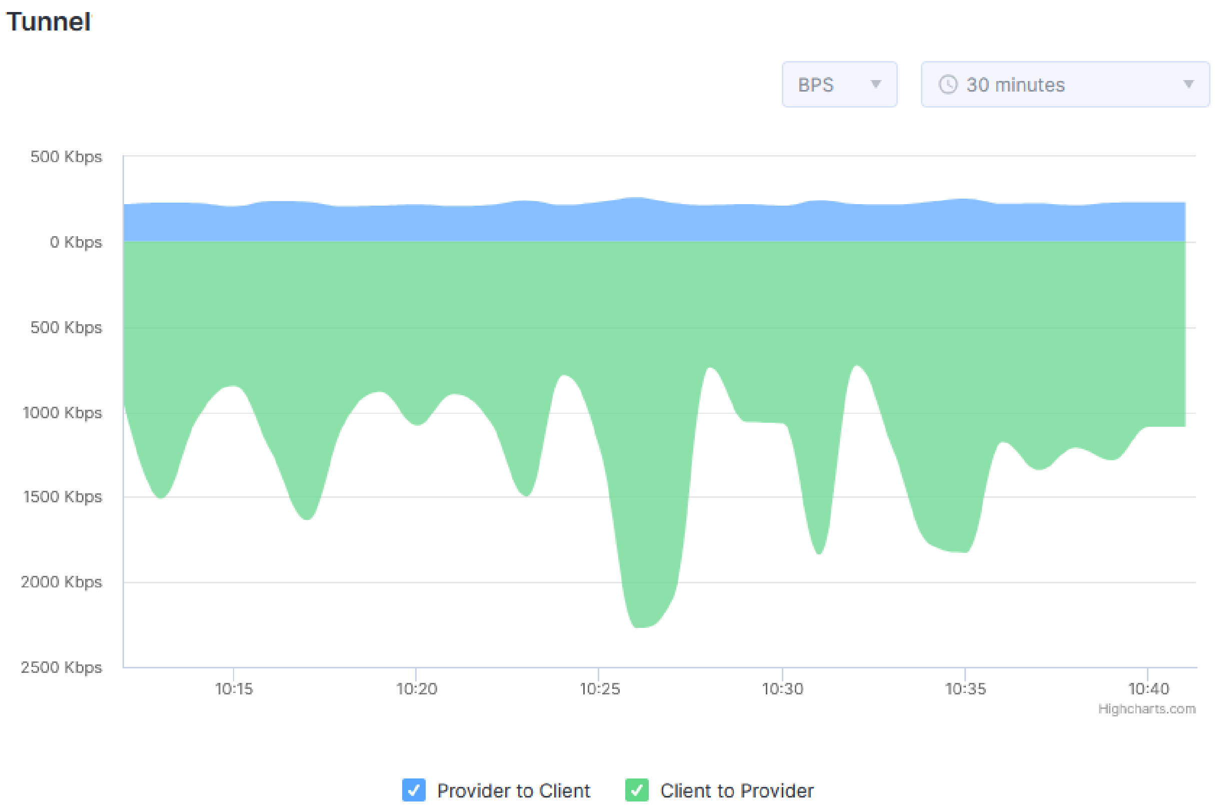
In the menu, select the **Interfaces** option.



In the central part of the page, information about each interface is displayed. Scroll down the page to view all the charts.

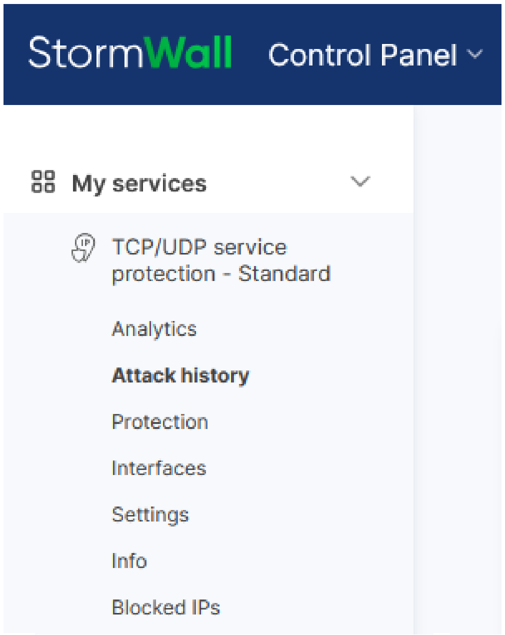
Use the tools in the upper right corner of the chart:

- BPS (bits per second) / PPS (packets per second);
- Time filter.

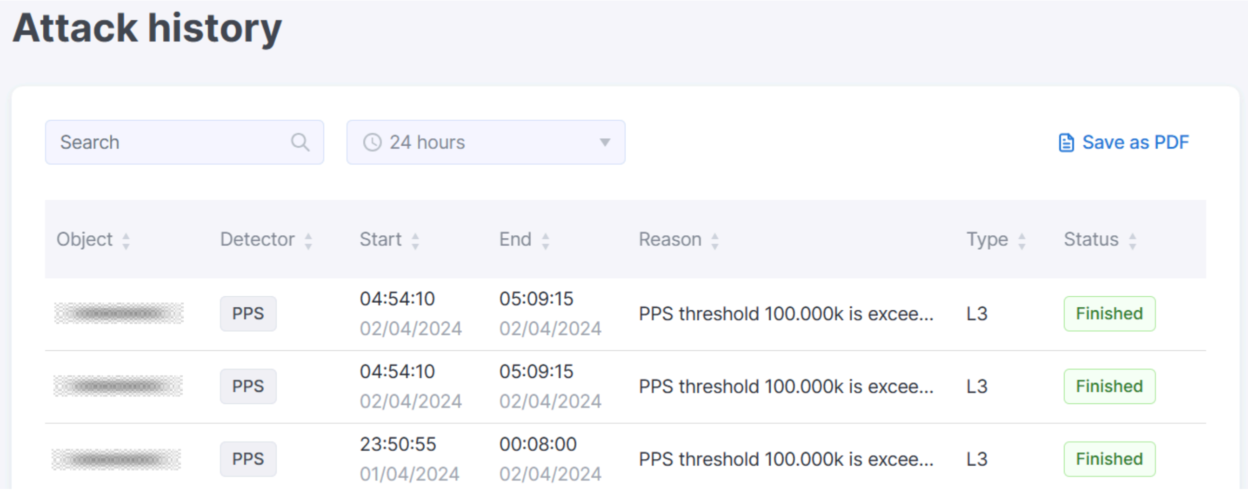


Attack History

In the menu, select the **Attack history** option.



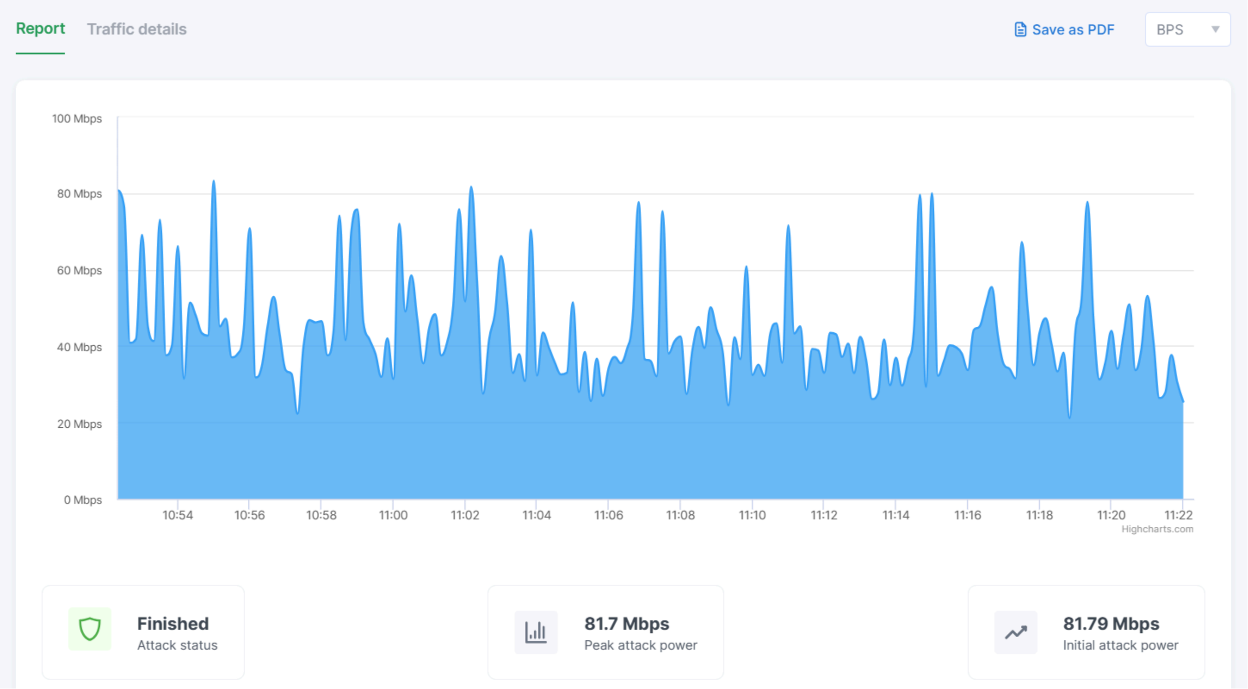
In the central part of the page, information about each attack is displayed. You can use the search and time filter to narrow down the list of attacks. To save the selection, click the **Save as PDF** button.



Attack history

Object	Detector	Start	End	Reason	Type	Status
[redacted]	PPS	04:54:10 02/04/2024	05:09:15 02/04/2024	PPS threshold 100.000k is excee...	L3	Finished
[redacted]	PPS	04:54:10 02/04/2024	05:09:15 02/04/2024	PPS threshold 100.000k is excee...	L3	Finished
[redacted]	PPS	23:50:55 01/04/2024	00:08:00 02/04/2024	PPS threshold 100.000k is excee...	L3	Finished

Click on the attack row to view all information about it. On the **Report** tab that opens, a chart will be displayed.

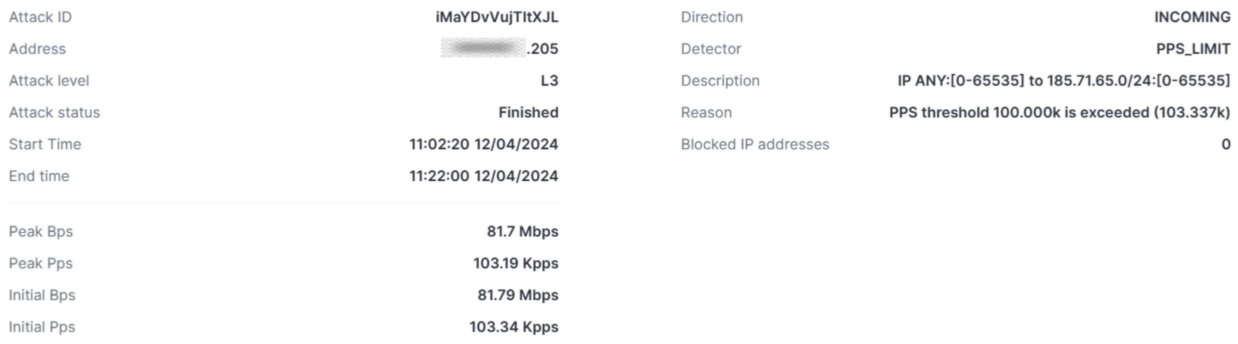


Finished
Attack status

81.7 Mbps
Peak attack power

81.79 Mbps
Initial attack power

Detailed information is provided below the chart.



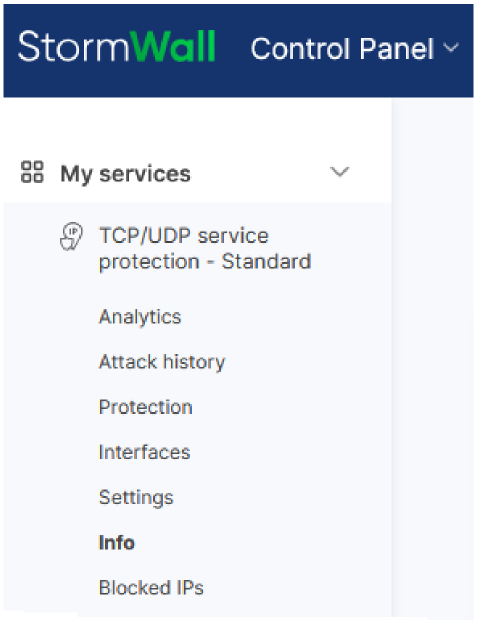
Attack ID	iMaYDvVujTItXJL	Direction	INCOMING
Address	[redacted].205	Detector	PPS_LIMIT
Attack level	L3	Description	IP ANY:[0-65535] to 185.71.65.0/24:[0-65535]
Attack status	Finished	Reason	PPS threshold 100.000k is exceeded (103.337k)
Start Time	11:02:20 12/04/2024	Blocked IP addresses	0
End time	11:22:00 12/04/2024		

Peak Bps	81.7 Mbps
Peak Pps	103.19 Kpps
Initial Bps	81.79 Mbps
Initial Pps	103.34 Kpps

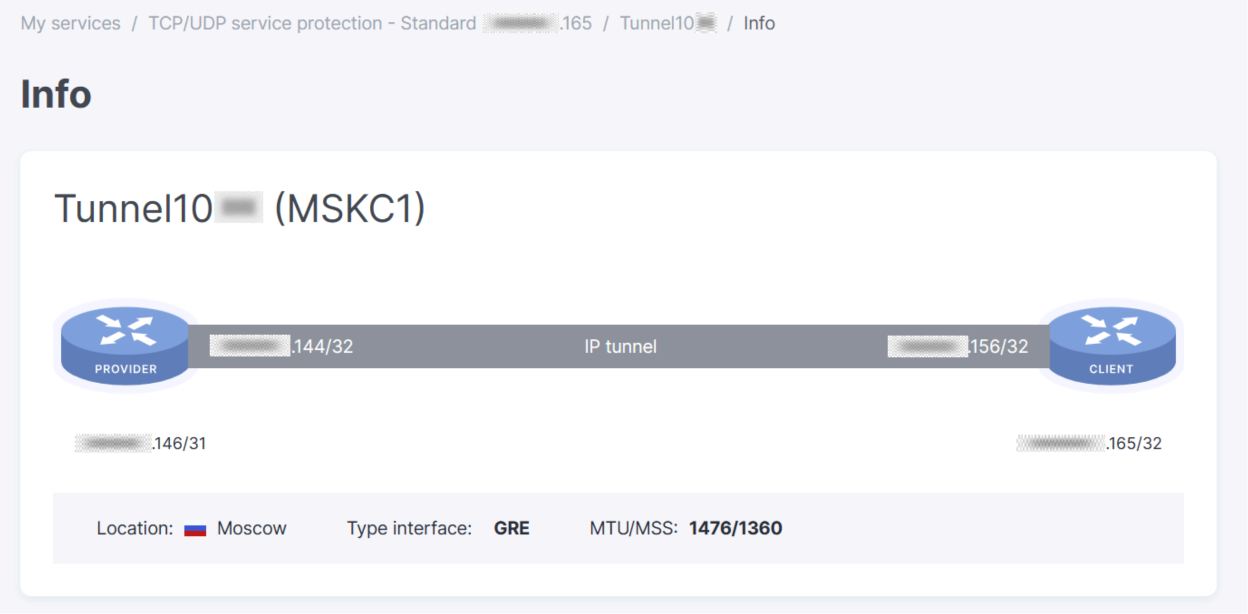
Navigate to the **Traffic Details** tab. On this page, information about the ports, protocols, and locations recorded during the attack will be displayed.

Information

In the menu, select the **Info** option.



The page displays all connected services along with a brief description of each.



My services / TCP/UDP service protection - Standard [redacted].165 / Tunnel10[redacted] / Info

Info

Tunnel10[redacted] (MSKC1)

Location: Moscow Type interface: GRE MTU/MSS: 1476/1360

WAF

How the Service Works

«Web Application Firewall (WAF)» - is a cloud service for protecting web applications. The service is designed to filter traffic with the aim of ensuring the security and stability of web resources during attacks.

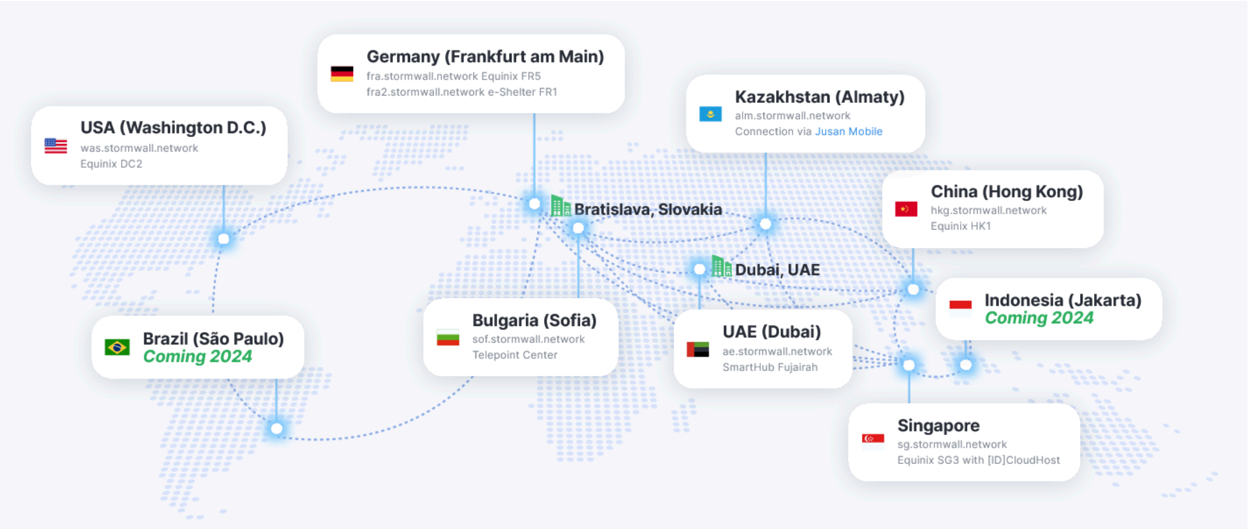
By using the cloud-based WAF service, you will receive a level of protection comparable to that provided by integrated tools.

Key features of the cloud-based WAF service:

- **Integration with DDoS protection:** WAF is typically provided along with DDoS attack protection, which enhances the defense of your web application against mass attacks.
- **No need for separate infrastructure:** Using cloud-based WAF does not require the installation of additional equipment or software, which reduces costs and simplifies deployment.

- **Application of models and anomaly detection methods:** The cloud-based WAF utilizes detailed models of the protected application combined with signature and semantic methods to detect and prevent anomalies. This includes protection against both common and more complex and specific attacks.
- **Machine learning algorithms:** The use of machine learning algorithms enhances the accuracy of threat detection, reduces the number of false positives, and automates the process of creating application working models.
- **Early false positive suppression mechanism:** Effective data processing and filtering mechanisms minimize the risk of false positives, contributing to the stable operation of web applications even in the face of active attacks.

Using cloud-based WAF can significantly strengthen the overall security of your web project, reduce risks, and improve performance, while also reducing operational costs and the complexity of security management.

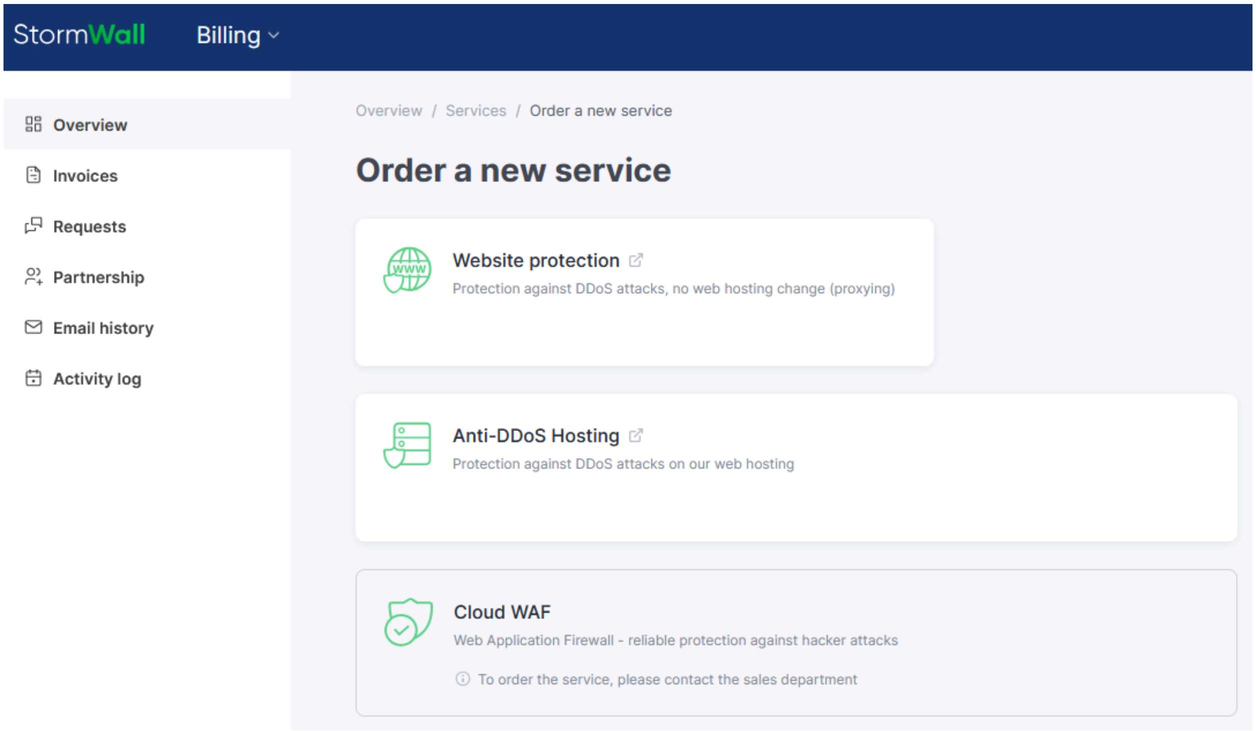


Integration with DDoS protection allows for easy defense of applications from all vectors of hacker attacks.

Order and Service Management

To connect the service:

1. Log into your personal account by authenticating on the website.
2. On the top panel of the website, select the **Billing** tab, following the instructions provided in the «How to connect service» section.
3. In the tab that opens, choose the **Cloud WAF** option.



Order a new service

Website protection
Protection against DDoS attacks, no web hosting change (proxying)

Anti-DDoS Hosting
Protection against DDoS attacks on our web hosting

Cloud WAF
Web Application Firewall - reliable protection against hacker attacks
To order the service, please contact the sales department

Please note that activating the service independently is not provided. When selecting the WAF service, you must fill out an application form, which will be sent to our specialists.

You can contact technical support with any questions about WAF, or submit requests to connect or disconnect the service.

After connecting the service, you will gain access to a special personal Client Portal. There, you can independently obtain information about the service operation, utilize analytical tools, and adjust settings. The appearance of the personal Client Portal depends on the solution selected at the time of connection.

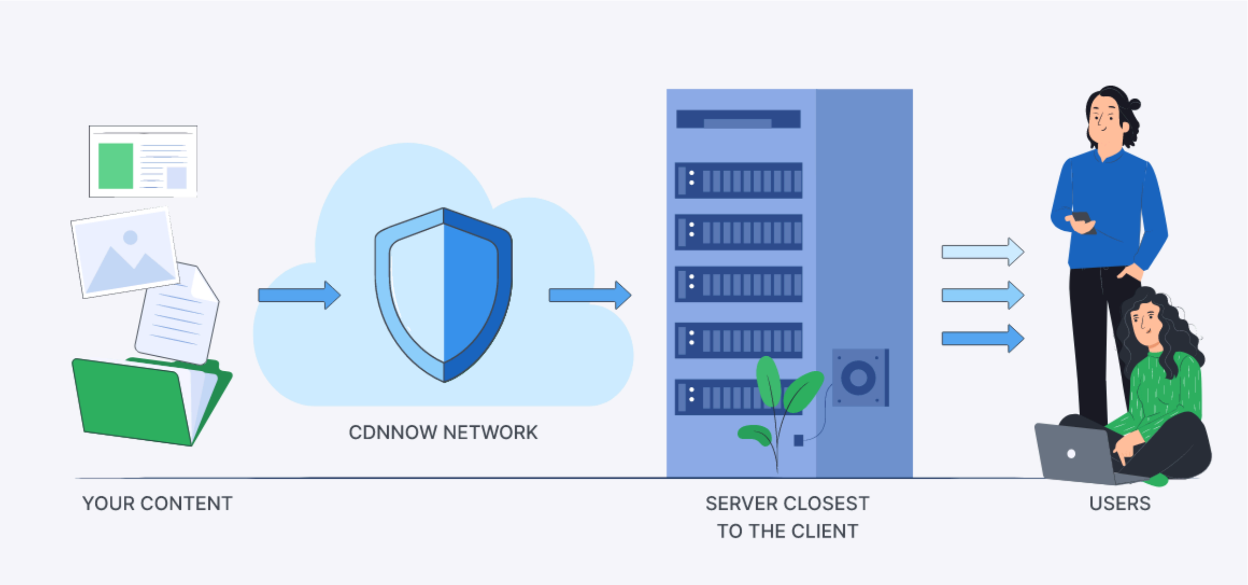
CDN

How the Service Works

A **«Content Delivery Network (CDN)»** is a service for accelerating content loading, storage, and the rapid distribution of large volumes of data. Statistics show that if a page takes more than three seconds to load, half of the users will leave the site without waiting for the content to load fully.

The CDN service addresses this issue in the following way:

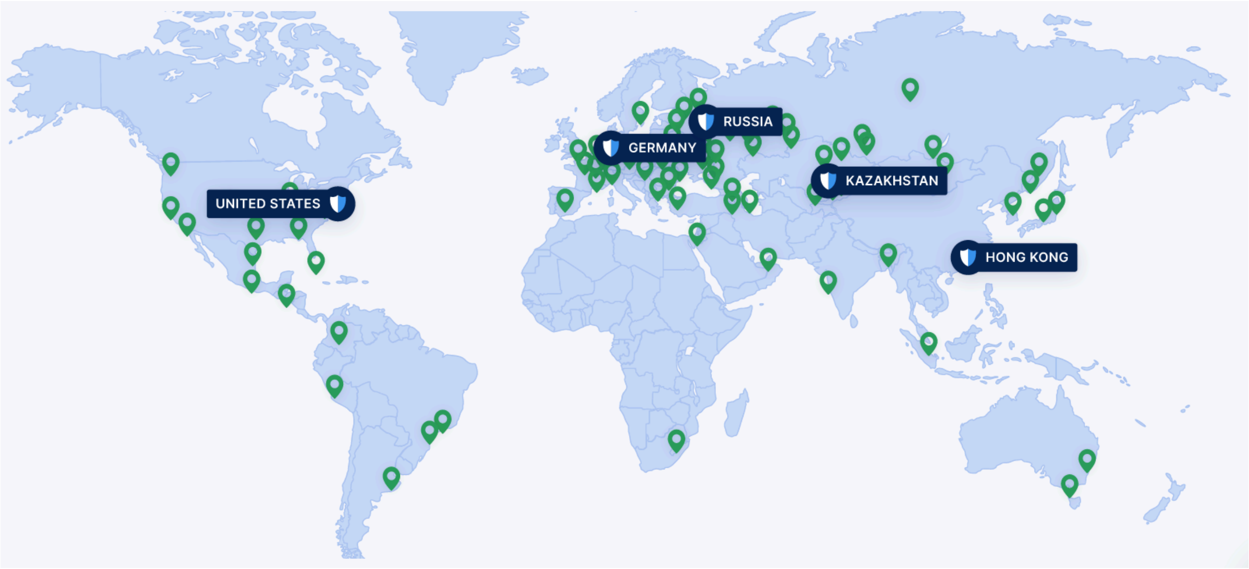
- Your content is uploaded to the cdnnow network.
- The uploaded content is distributed across network servers.
- The resource user receives data from the server closest to them in the cdnnow network.



The «Content Delivery Network (CDN)» service is designed to transmit content at the highest possible speed to an unlimited number of users worldwide, irrespective of the location of both the content source and its consumer. Clients of the service are not required to bear the costs associated with deploying and operating their own infrastructure, software, and high-performance communication channels for storing and rapidly providing large volumes of content, especially as the cost of technical support for such infrastructures steadily increases with age.

Data travels from the content owner to the consumer via the shortest (and therefore fastest) route. As a result, every user around the world receives content from the CDN server closest to them.

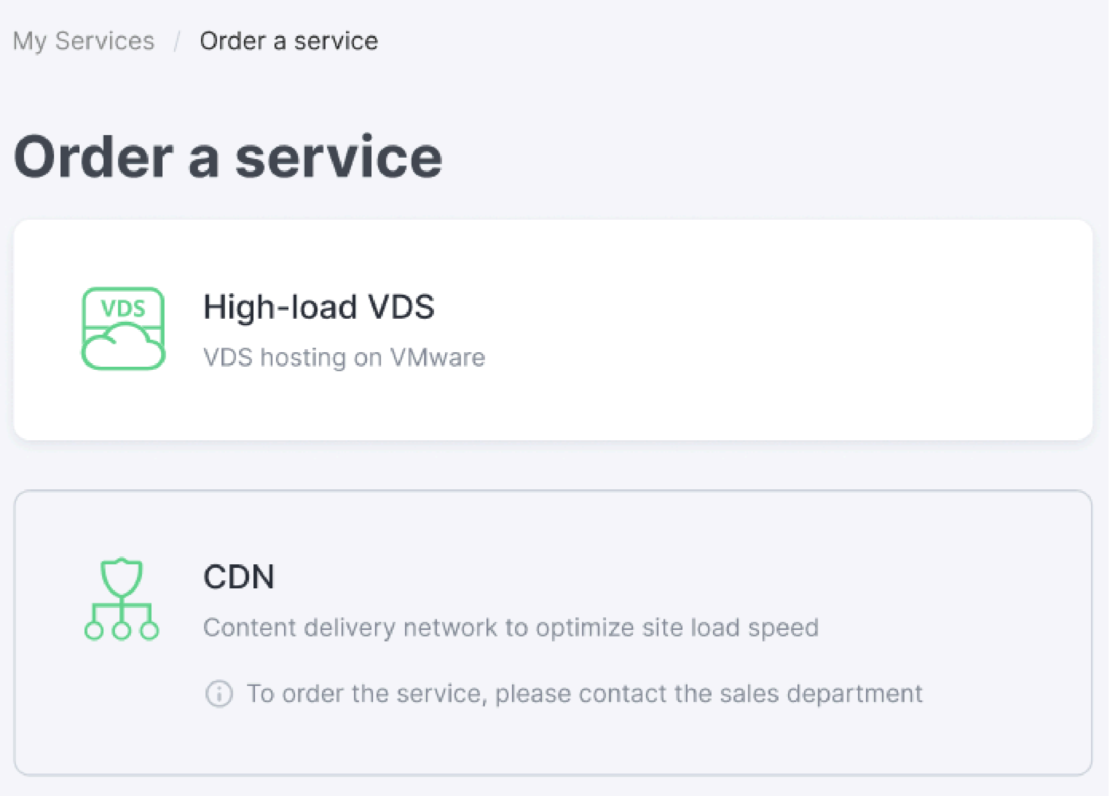
The total network capacity of the CDN is 500 Gbps. CDN data centers are located in more than 40 cities worldwide.



Order and Service Management

To connect the service:

1. Log into your personal account by authenticating on the website.
2. On the top panel of the website, select the **Billing** tab, following the instructions provided in the «How to connect your service» section.
3. In the tab that opens, choose the **CDN** option.



My Services / Order a service

Order a service

High-load VDS

VDS hosting on VMware

CDN

Content delivery network to optimize site load speed

ⓘ To order the service, please contact the sales department

Please note that activating the service independently is not an option. When selecting the CDN service, you must fill out an application that will be sent to our specialists.

To manage the service, please contact technical support. In your personal account, you can submit requests for connecting or disconnecting the service.

Anti-DDoS Hosting

How the Service Works

Unlike the «StormWall for Website» service, which keeps your website on its current hosting, this service provides you with a new secure hosting.

For the implementation of the «Anti-DDoS Hosting» service, the following are used:

- Border routers to cut off inter-zone traffic

- Hardware filters to block TCP/UDP flooding
- Stateful filters for filtering other types of attacks

When you order this service, you will receive the following benefits:

- Hosting and DDoS protection from a single provider;
- Effective filtering of any DDoS attacks;
- Accelerated performance of your websites;
- An optimal pricing plan with monthly payment;
- No additional costs for equipment, software, and DDoS protection;
- The ability to connect the necessary number of domains and subdomains within the plan;
- Mail server, databases, DNS server, dedicated IP addresses, and disk space on solid-state drives (SSD);
- Simple and quick migration of your internet resources to our facilities, including with the help of StormWall specialists;
- Daily data backup.

Features of the service

The client's web server is located within StormWall's secure network. Incoming web traffic arrives with a delay of less than 1 millisecond to the filtering system.

High-quality service is ensured through triple traffic filtration (Triple Filter):

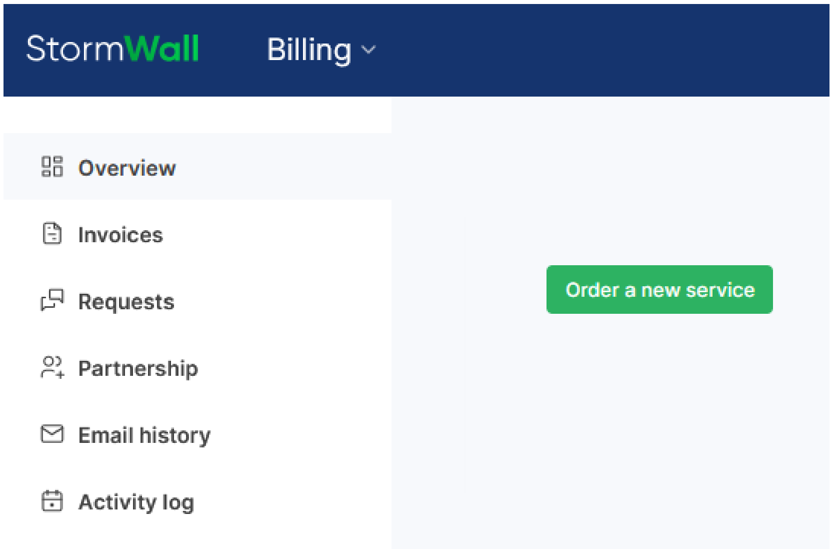
- **Border Routers**: Located globally, these cut off inter-zone traffic.
- **Hardware Filters**: Block the main part of TCP/UDP flooding.
- **Stateful Filters**: Provide a level of fine filtration that blocks the most sophisticated attacks, including bot attacks.

If it concerns website protection, the next level is HTTP filtration with the BanHammer cleaning system. The BanHammer HTTP flood filtration system utilizes intelligent methods and algorithms "trained" on tens of thousands of attacks on client sites of StormWall. The FlowSense system continuously monitors all data streams going to the server, tracks anomalies, and automatically identifies the type of attack that has begun, dynamically adjusting the protection parameters accordingly.

High website performance within the Hosting with Protection service is guaranteed by the HyperCache technology. It caches large files in the server's RAM, so users receive them almost instantly. When StormWall protection is connected, traffic from the nearest filtration point to the client to the server is routed via StormWall's own leased communication channels between data centers, which ensure minimal ping, minimal latency fluctuation, and have no shaping. Protection against global failures at StormWall network nodes is provided by Global Session technology. StormWall's filtering nodes around the world "know" that a client has connected to your server, and if one of the nodes becomes unavailable, traffic is automatically directed to another, nearest to the client, node.

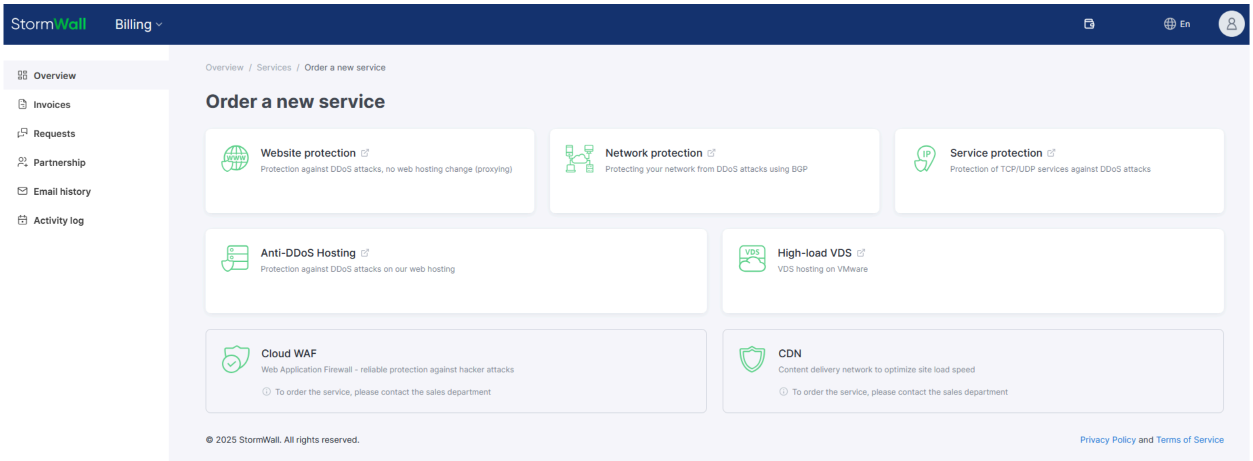
Order

Log in to your personal account on the website. On the top panel of the website, select the **Billing** tab.



Click the **Order a new service** button.

In the opened tab, select **Anti-DDoS Hosting**.



Overview / Services / Order a new service

Order a new service

Website protection
Protection against DDoS attacks, no web hosting change (proxying)

Network protection
Protecting your network from DDoS attacks using BGP

Service protection
Protection of TCP/UDP services against DDoS attacks

Anti-DDoS Hosting
Protection against DDoS attacks on our web hosting

High-load VDS
VDS hosting on VMware

Cloud WAF
Web Application Firewall - reliable protection against hacker attacks
ⓘ To order the service, please contact the sales department

CDN
Content delivery network to optimize site load speed
ⓘ To order the service, please contact the sales department

© 2025 StormWall. All rights reserved.

Privacy Policy and Terms of Service

You will be redirected to a website page with a detailed description of the service.

Review the service details and pricing plans:

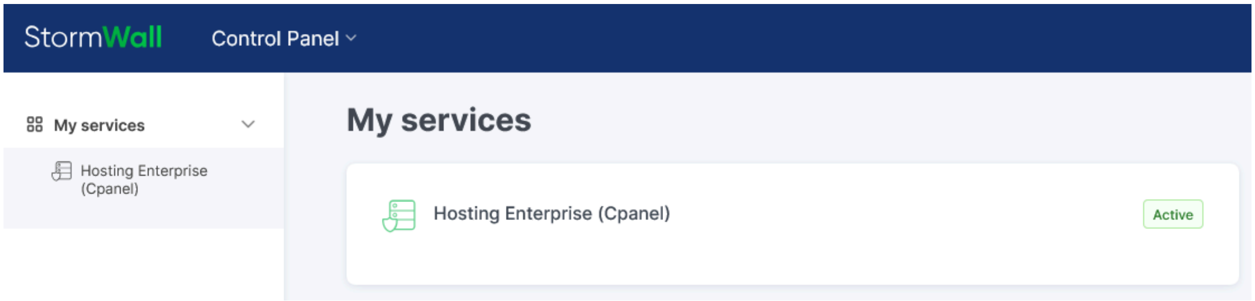
- **Personal**
- **Business One**
- **Enterprise One**

After selecting a plan, click **Order** or **Submit a request**, then fill out the form on the website.

If none of the available plans meet your requirements, contact us—we will offer you a custom solution.

Managing Your Service

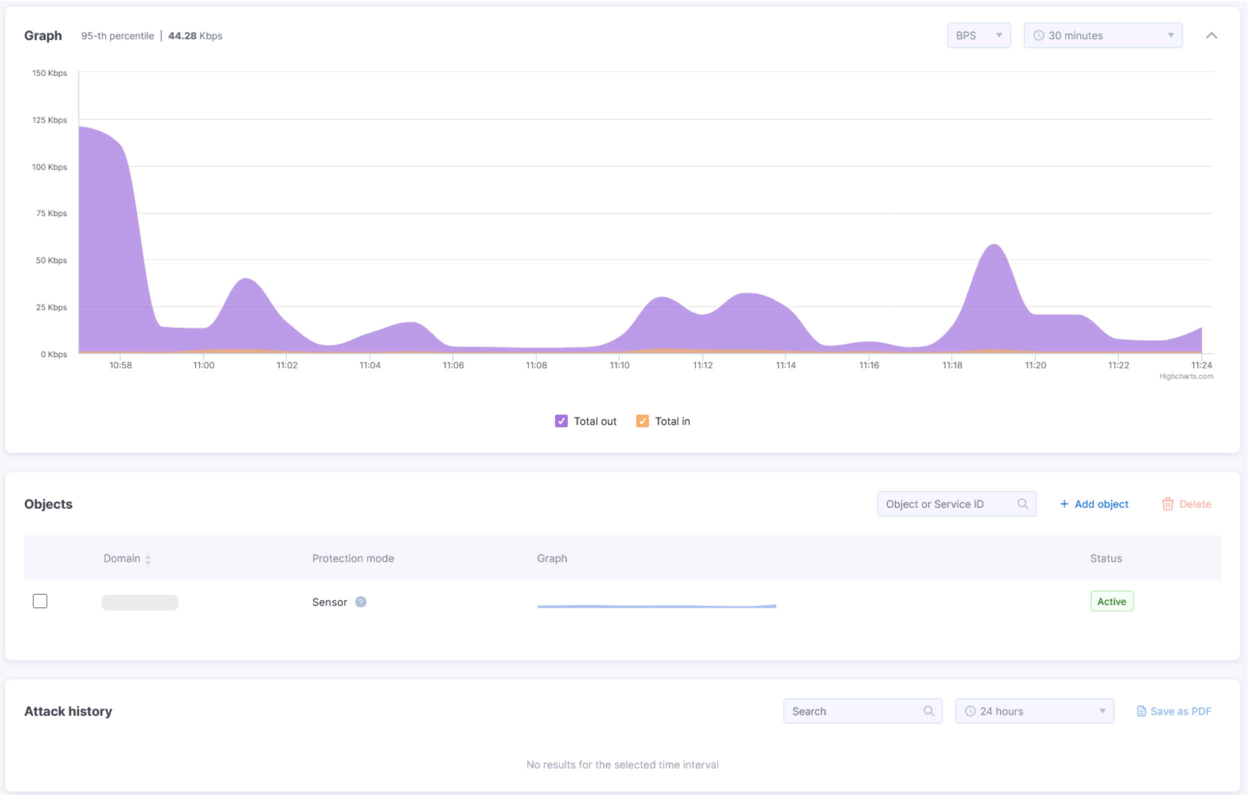
Once activated, your service will appear on the main page of your account and in the **My Services** list.



My services

Hosting Enterprise (Cpanel) Active

To view details, click the service name in the central area of the page or from the left-side list.



Objects

Object or Service ID | + Add object | Delete

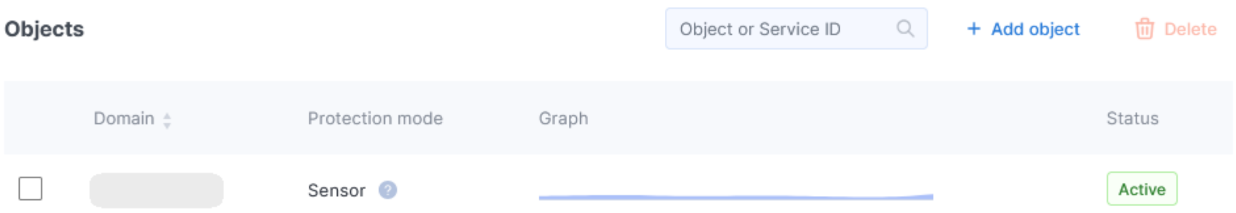
	Domain	Protection mode	Graph	Status
□		Sensor		Active

Attack history

Search | 24 hours | Save as PDF

No results for the selected time interval

- If you have one object, the left-side menu will open for management.
- If you have multiple objects, go to the **Objects** section (below the graph), select the desired object, and click on its row with the graph thumbnail.



Objects

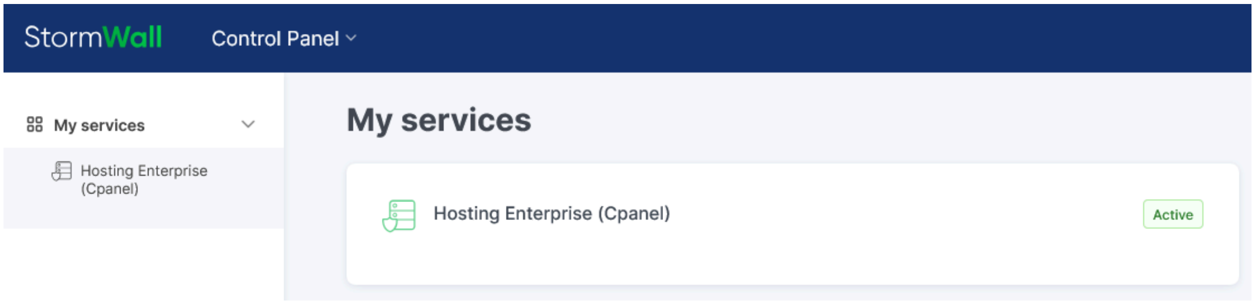
Object or Service ID | + Add object | Delete

	Domain	Protection mode	Graph	Status
□		Sensor		Active

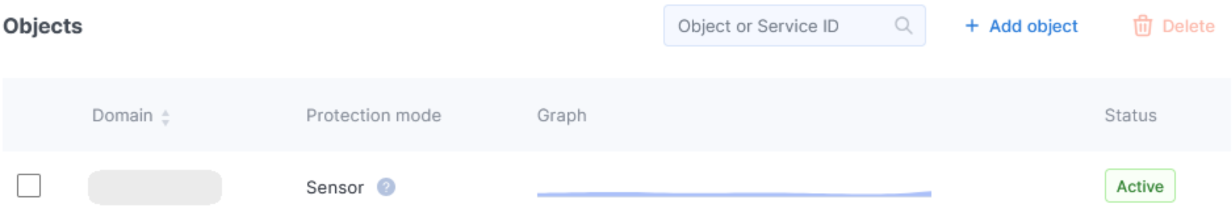
The left-side menu will then open for managing the selected object.

Protection Settings

Open the **Control Panel** tab by clicking on the service name in the central area or the left menu.



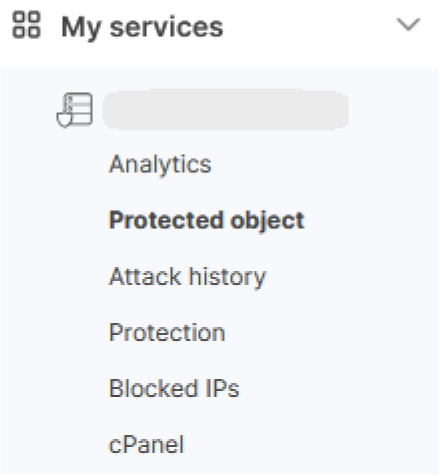
If you have multiple protected objects, select the required one in the **Objects** section.



	Domain	Protection mode	Graph	Status
□	[redacted]	Sensor		Active

Protected Object

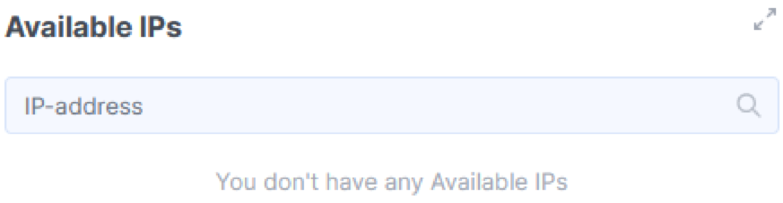
In the left menu, select **Protected Object**.



In the left menu, select **Protected Object**. The opened page will display the configurable parameters.

Available IPs

We provide multiple **IP addresses** that you can assign to your domains, either manually or with our assistance.



You don't have any Available IPs

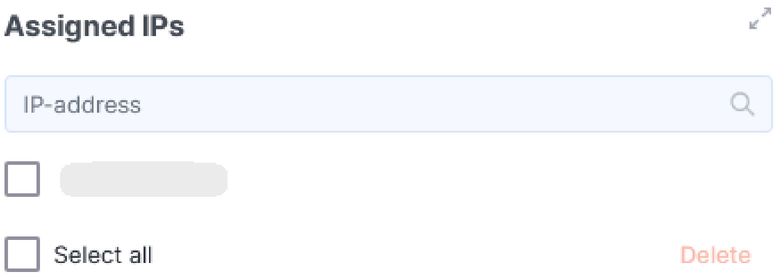
To assign an IP from the provided list:

- Select it by checking the box at the beginning of the row.
- Click **Assign**.

To obtain available addresses, contact technical support.

Assigned Domain

This section displays the currently selected IP addresses.



To remove an IP address:

- Select one or more unnecessary addresses by checking the boxes.
- Click **Delete**.

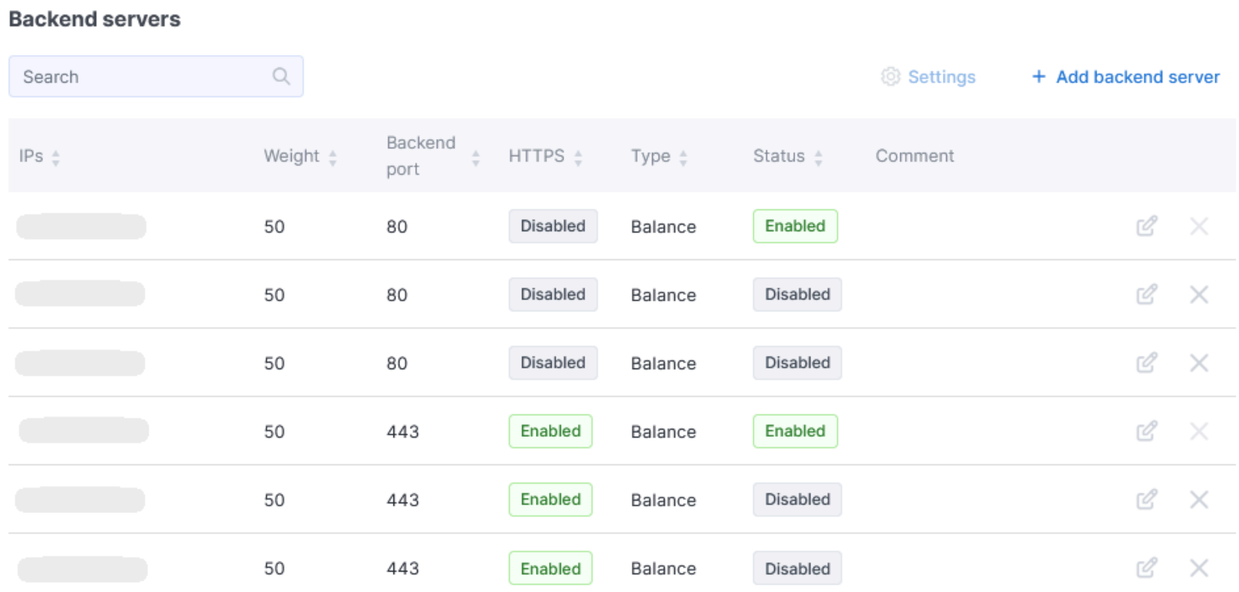
Backend Servers

The service provides traffic balancing by default.

Each backend server must be assigned a weight and a status—either «Active» or «Reserve».

Active servers handle traffic, while Reserve servers take over if an Active server fails.

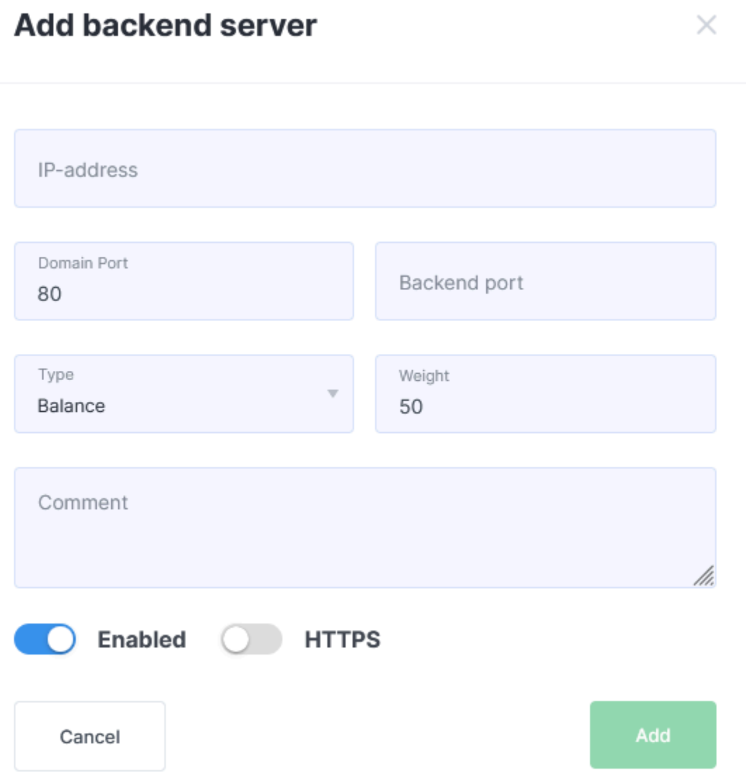
Supported protocols: HTTP (port 80) and HTTPS (port 443).



Backend servers

IPs	Weight	Backend port	HTTPS	Type	Status	Comment
[redacted]	50	80	Disabled	Balance	Enabled	
[redacted]	50	80	Disabled	Balance	Disabled	
[redacted]	50	80	Disabled	Balance	Disabled	
[redacted]	50	443	Enabled	Balance	Enabled	
[redacted]	50	443	Enabled	Balance	Disabled	
[redacted]	50	443	Enabled	Balance	Disabled	

To add a new backend server click **+ Add backend** and fill out the form.



Add backend server

IP-address

Domain Port: 80

Backend port

Type: Balance

Weight: 50

Comment

● Enabled ○ HTTPS

To edit a backend server, click the «edit» icon in the right column.

To delete a backend server, click the **X** icon in the right column.

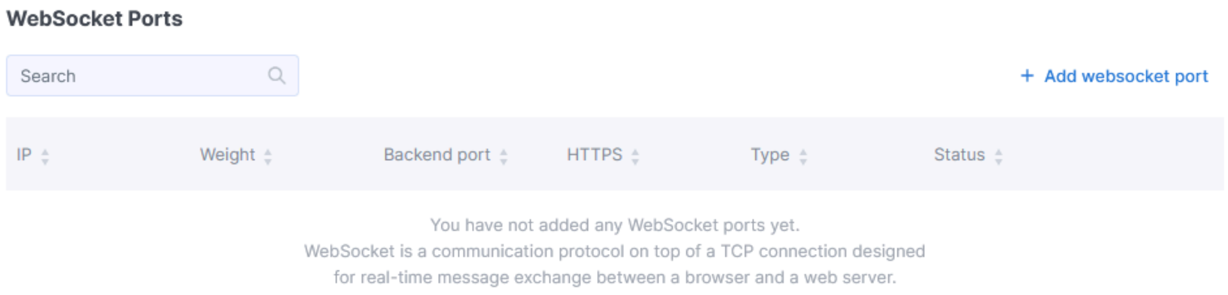
- If the backend is active, a warning message will appear.
- If you are sure, disable the server first by clicking **Disable backend server** in the warning message.

WebSocket Ports

Configure WebSocket DDoS protection.

Standard Setting: Ports **80 and 443** are used automatically.

Custom Ports: If using custom ports, you need to specify them.



WebSocket Ports

Search

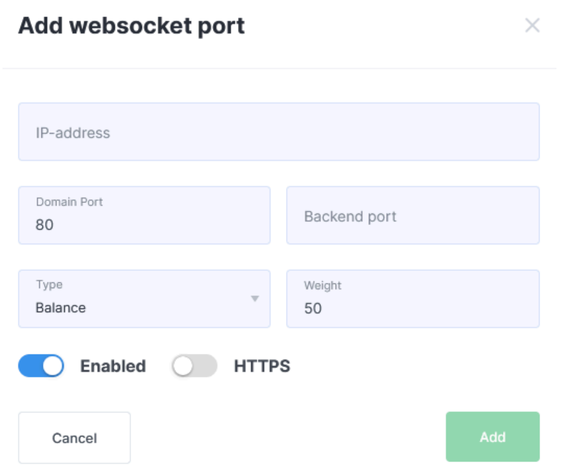
+ Add websocket port

IP	Weight	Backend port	HTTPS	Type	Status

You have not added any WebSocket ports yet.
WebSocket is a communication protocol on top of a TCP connection designed
for real-time message exchange between a browser and a web server.

To add a WebSocket port:

- Click **Add WebSocket Port**.
- Fill out the form and click **Add**.
- If the button is inactive, the maximum number of ports has been reached.



Add websocket port

IP-address

Domain Port: 80

Backend port

Type: Balance

Weight: 50

● Enabled ○ HTTPS

Cancel

Add

SSL Certificate

You can choose one of two options:

- Obtain a **free SSL certificate** from **Let's Encrypt**
- Upload **your own certificate**

Additionally, there is an option to **enable or disable automatic redirection** from HTTP to HTTPS (or vice versa), which helps reduce the load on the target server.

Using Your Own Certificate

If you decide to use your own certificate, you will need to provide:

- The public certificate and private key for SSL traffic validation (they are displayed in a shortened form to prevent copying).
- The root and, if applicable, intermediate CA certificates.

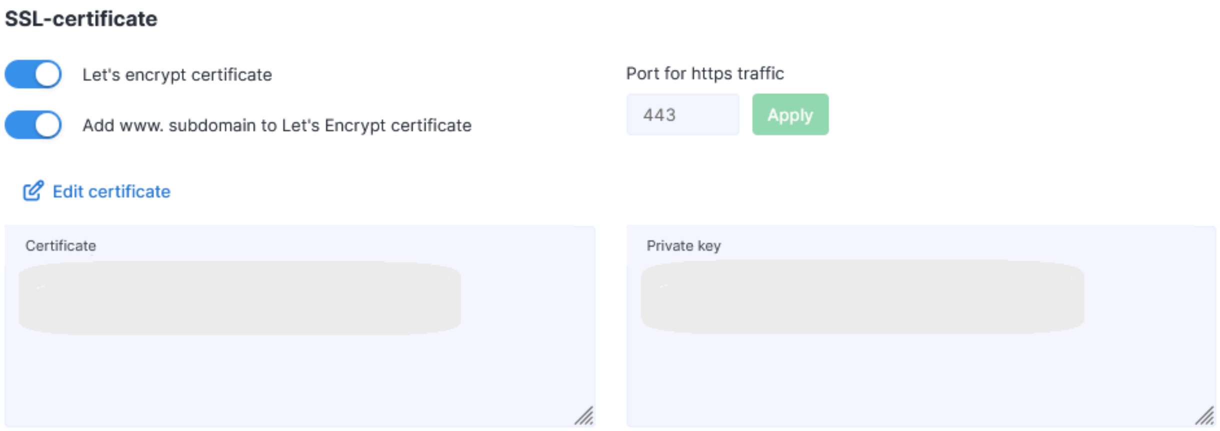
Keep in mind that if you use your own certificate, you are responsible for renewing it before it expires.

Each certificate must:

- Start with **«BEGIN CERTIFICATE»**
- End with **«END CERTIFICATE»**
- The private key must start with **«BEGIN RSA PRIVATE KEY»**

Before inserting the certificate, **turn off Let’s Encrypt sertificate** in the settings.
If a validation error occurs:

- Check the correctness of the **Common Name**, **SANs**, and **Validity** fields.
- Use `openssl` to compare certificate and key hashes.
- Ensure the certificate chain is complete.



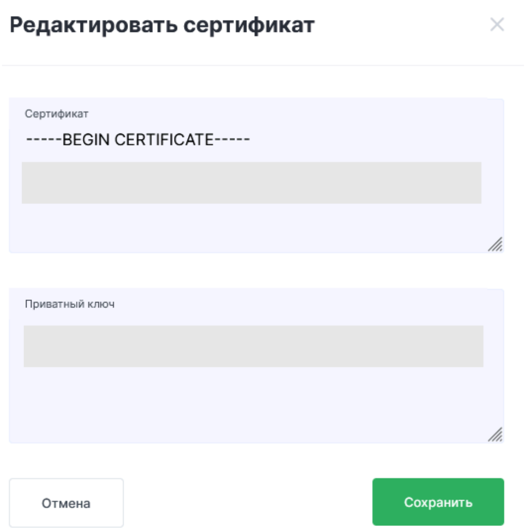
SSL-certificate

● Let's encrypt certificate

● Add www. subdomain to Let's Encrypt certificate

Port for https traffic: 443

To edit the certificate, click **Edit Certificate**.



Сертификат

-----BEGIN CERTIFICATE-----

[redacted]

Приватный ключ

[redacted]

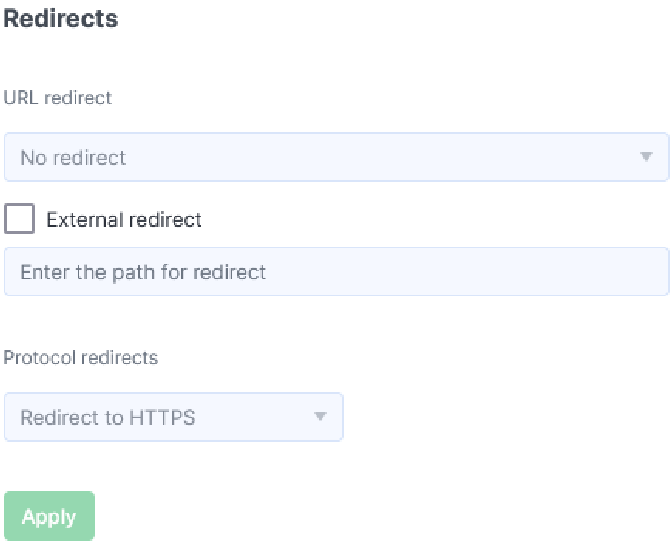
Cache

Enabling caching will provide your site with additional reliability and significantly improve speed.

- Static files will be cached in the StormWall memory servers.
- This reduces load on the main server.

To activate caching:

1. Select the cache lifetime and file types.


Redrects

URL redirect

No redirect ▾

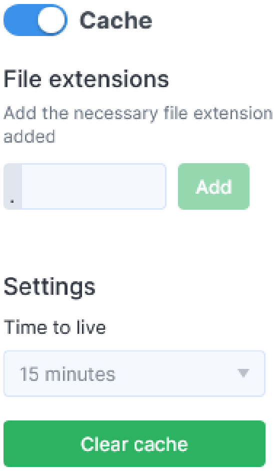
□ External redirect

Enter the path for redirect

Protocol redirects

Redirect to HTTPS ▾

2. Toggle the **Cache** switch to **ON**.


Cache

File extensions

Add the necessary file extensions for caching, or remove those already added

Settings

Time to live

15 minutes ▾

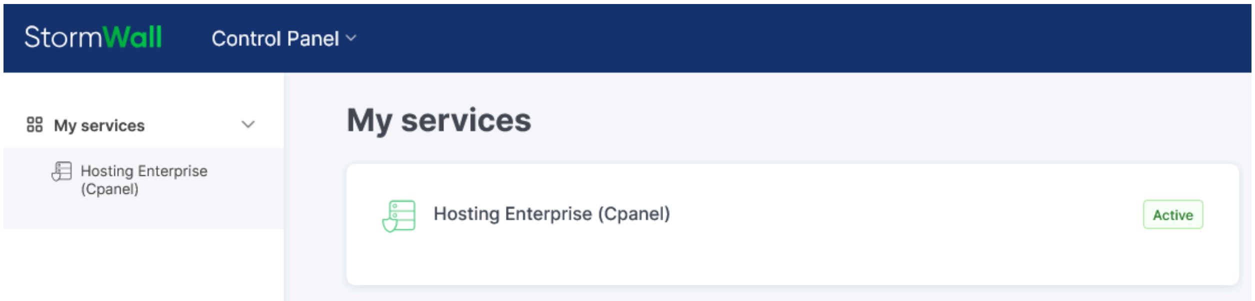
To reload all data from resources, click **Clear Cache**.

Redirects

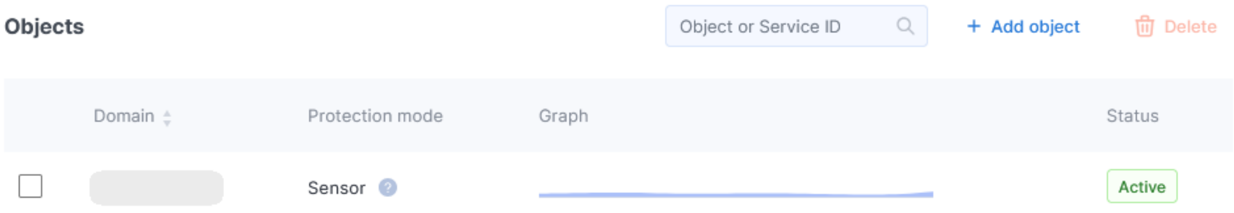
In the **Redirects** section, you can set up rules for redirections, such as redirecting from **HTTP to HTTPS**.

Protection

Open the **Control Panel** tab by clicking on the service name in the central area or the left menu.

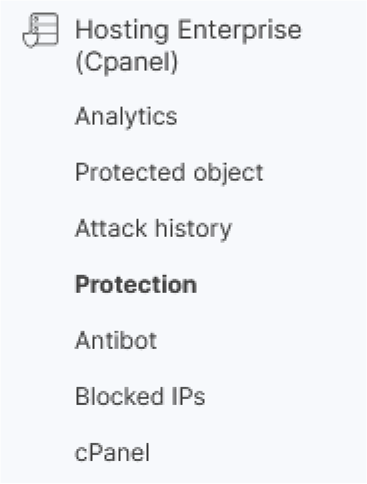


If you have multiple protected objects, select the required one in the **Objects** section.



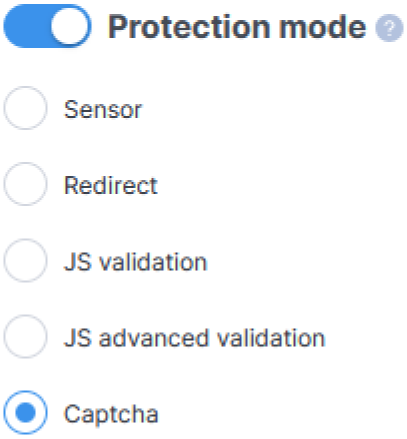
	Domain	Protection mode	Graph	Status
□		Sensor		Active

In the left menu, select **Protected Object**.



Protection Modes

- **Sensor** – Monitors the number of requests, spikes in activity, and errors. Filters operate in passive mode but switch to active mode when an attack is detected.
- **Redirect** – Uses additional redirection for visitor requests.
- **JS Validation** – JavaScript validation is applied to requests from regular IPs.
- **JS Advanced Validation** – Advanced JavaScript validation is used.
- **Captcha** – In some cases, users must complete a Captcha for validation.



Protection mode ?

○ Sensor

○ Redirect

○ JS validation

○ JS advanced validation

● Captcha

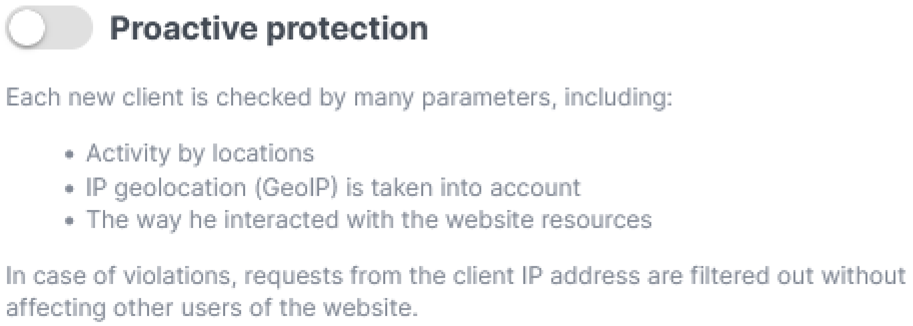
Proactive Protection

Protection is carried out based on a positive usage model of the resource.
Users whose behavior goes beyond this model may be blocked or subjected to additional checks, depending on the configured settings.

When proactive protection is enabled in sensor mode, not all requests are filtered. However, each new visitor is checked based on the following parameters:

- Visited pages and locations
- Use of keepalive connections
- Presence of attacks on other sites
- Exceeding request limits
- Types of User-Agent used
- Other potential violation indicators

If violations are detected, user behavior monitoring is activated.
Selective validation allows the system to avoid switching entirely into active mode.



Proactive protection

Each new client is checked by many parameters, including:

- Activity by locations
- IP geolocation (GeoIP) is taken into account
- The way he interacted with the website resources

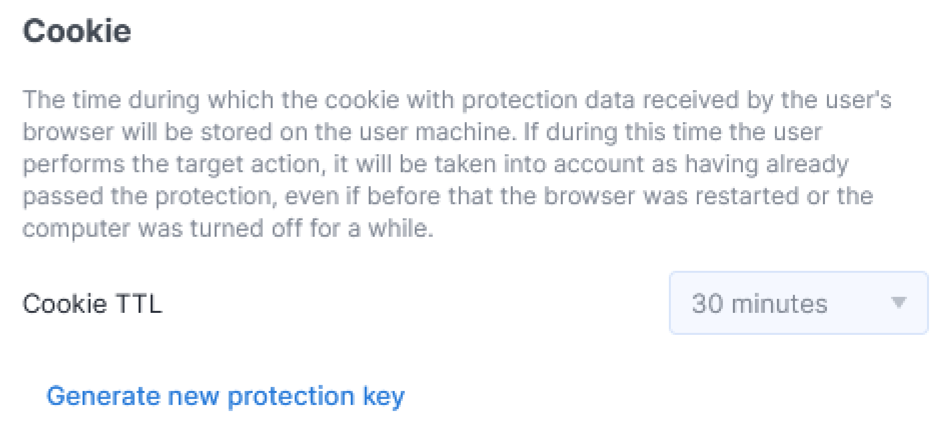
In case of violations, requests from the client IP address are filtered out without affecting other users of the website.

Cookie
You can set the session duration interval for visitors. Once this period expires, the system will revalidate the user.

- By default, the session time is 30 minutes, which is important for resources like online stores.
- However, if a customer stays too long on one page and the session expires, AJAX requests may fail.
- For most websites, this parameter is not critical.

Additionally, when clicking the **Generate new key** button, all active users will be forced to undergo revalidation.

Note! The validity period of cookies used by the protection system does not affect the session duration on the website, as the original cookies remain unchanged.



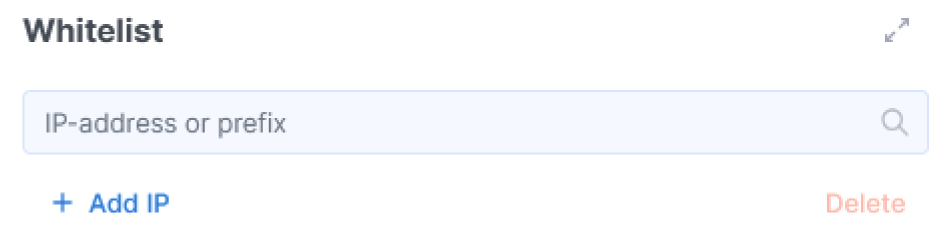
Cookie

The time during which the cookie with protection data received by the user's browser will be stored on the user machine. If during this time the user performs the target action, it will be taken into account as having already passed the protection, even if before that the browser was restarted or the computer was turned off for a while.

Cookie TTL: 30 minutes

Whitelist

Requests from the **specified addresses** will be processed **without filtering**.



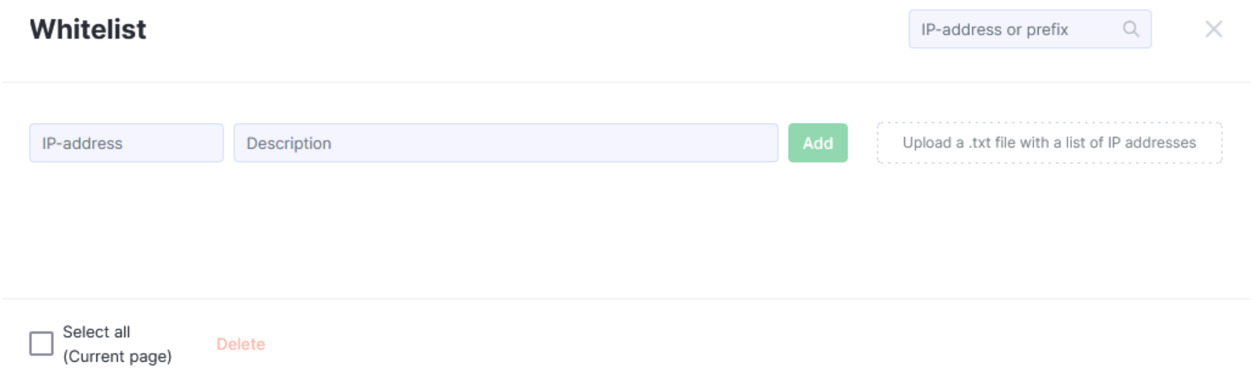
Whitelist

To add an IP address to the whitelist:

1. Click the **+ Add IP** button.
2. Fill out the form that appears.
3. You can upload a list of IP addresses as a file.
    - Ensure that each IP address in the file starts on a new line.

You can add:

- Single IP addresses (e.g., `8.8.8.8`).
- A network with a subnet mask (e.g., `8.8.8.0/24`).



To remove one or multiple IP addresses from the whitelist:

1. Select the unnecessary addresses by checking the boxes next to them.
2. Click the **Delete** button.

Blacklist

A user whose address is added to this list will receive an «HTTP 403 Forbidden» error when attempting to access your resource.

To add a new address to the blacklist, follow the same procedure as for the «whitelist»:

1. Click the **+ Add IP** button.
2. Fill out the **form** that appears.
3. You can **upload a list of IP addresses** as a file.
   - Ensure that **each IP address** in the file **starts on a new line**.

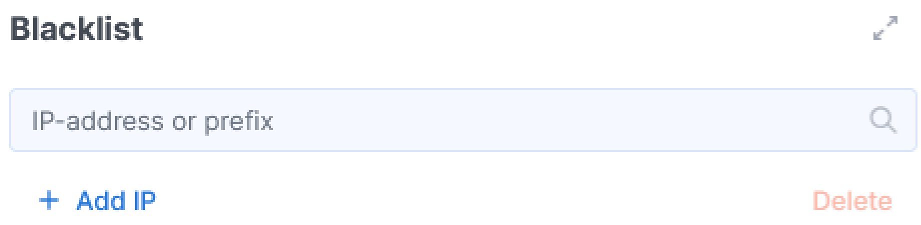
You can add:

- Individual IP addresses (e.g., `8.8.8.8`).

- A subnet using a mask (e.g., `8.8.8.0/24`).

To remove an IP address from the blacklist:

1. Select the addresses to remove by checking the boxes next to them.
2. Click the **Delete** button.



Greylist

You can assign a custom protection method for specific IP addresses or subnets, different from the general protection settings.

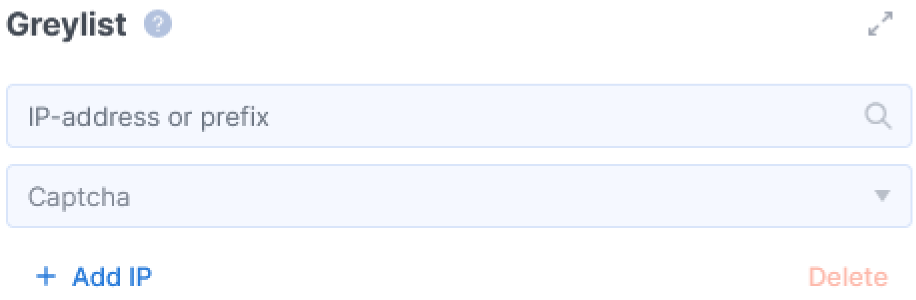
To add an IP address or subnet to the **Greylist**:

1. Click **+ Add IP**.
2. Fill out the form that appears.
3. Select the protection method to apply for these addresses.

You can add:

- Individual IP addresses (e.g., `8.8.8.8`).
- A subnet using a mask (e.g., `8.8.8.0/24`).

This feature allows fine-tuning of security rules, customizing protection levels for specific IPs or networks based on their behavior or level of trust.

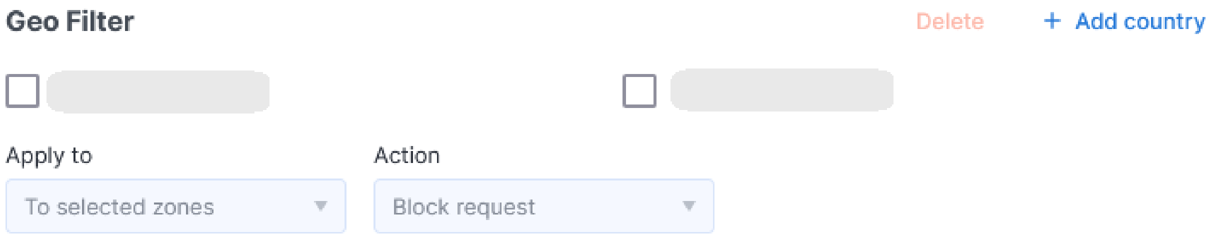


Captcha

Geo Filter

You can restrict access to your resource based on the visitor's country.

- If you notice unusually high activity from regions where you do not have a target audience, you can configure rules to limit or block access from those areas.
- If your service is intended for users from specific regions, you can set rules to allow access only from those areas, blocking all others.

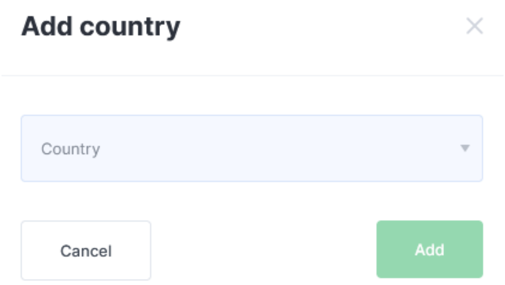


Apply to: To selected zones

Action: Block request

To **add a country restriction**:

1. Click **+ Add country**.
2. Select countries from the drop-down list.



Restrictions:

- When using L3 and L7 filtering without SSL decryption, you can add up to 15 countries per rule.
- When using L7 filtering with SSL decryption, there are no limits on the number of countries.

Location Exceptions

For certain requests, interactive validation checks can be disabled.

For example, if a specific server resource is accessed only by bots or mobile applications, validation checks may cause service failures for clients. In such cases, specify these local resources in the Location Exceptions section.

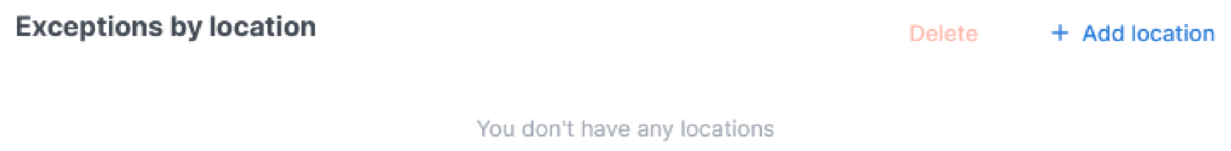
A request will be whitelisted if its path (to your resource) contains a part specified in this setting.

For example, if you add the path **«/location»** to the whitelist, the following requests will be processed without additional checks:

- `site.com/location`
- `site.com/location/`
- `site.com/location.php`
- `site.com/location.php?id=123`
- `site.com/admin/location`

At the same time, the following requests will still be processed under general rules:

- `site.com/some-other-location`
- `site.com/en_location.php`

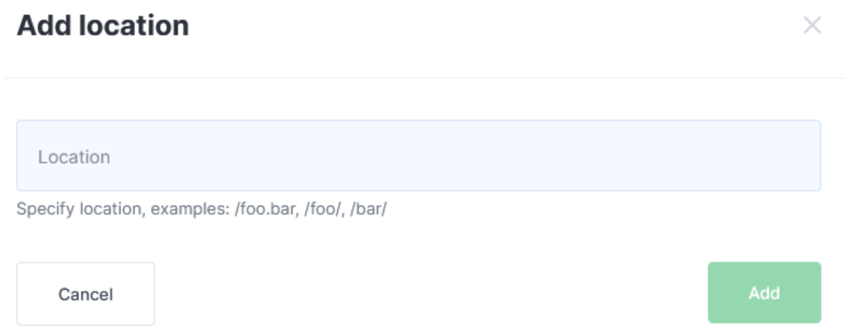


Exceptions by location

You don't have any locations

To add a location exception:

1. Click **+ Add Location**.
2. Fill out the form.



Add location

Location

Specify location, examples: /foo.bar, /foo/, /bar/

Header Filter

This section provides detailed filtering settings for HTTP headers, which is especially useful for advanced users.

You can create both:

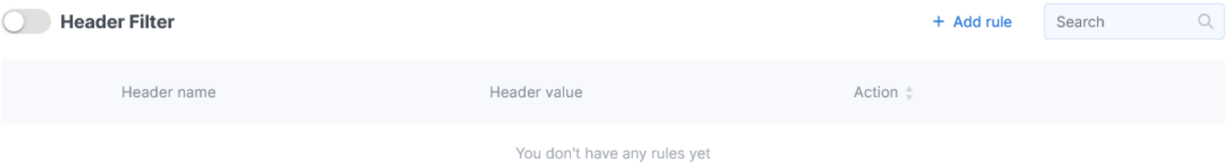
- **Blocking rules** – to filter out specific headers.
- **Allowing rules** – to permit certain headers.

For consultation or assistance in creating custom rules, please contact technical support.

This feature is particularly relevant for API-based websites, where requests are made by separate applications.

You can configure filtering for:

- Specific headers
- Combinations of headers, allowing for more precise control over incoming requests.



Header Filter

+ Add rule

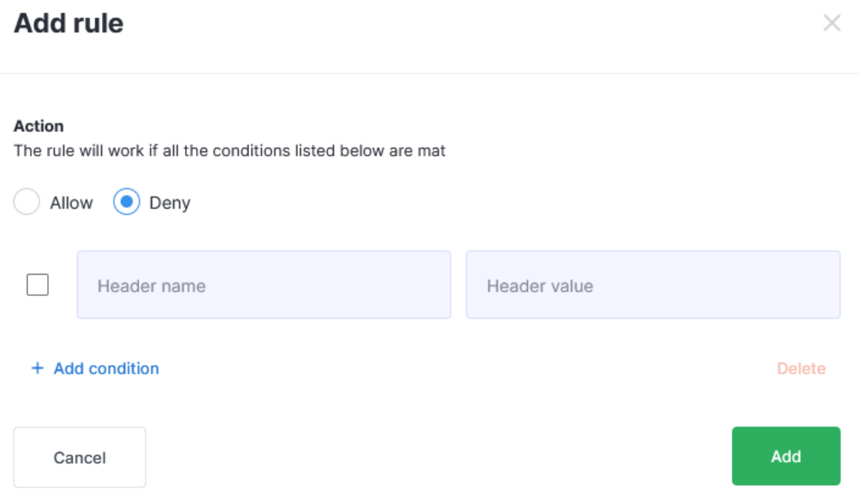
Search

Header name	Header value	Action

You don't have any rules yet

To add a new rule:

1. Click **+ Add Rule**.
2. Fill out the form.



Add rule

Action

The rule will work if all the conditions listed below are mat

○ Allow ● Deny

□ Header name | Header value

+ Add condition

Delete

Cancel

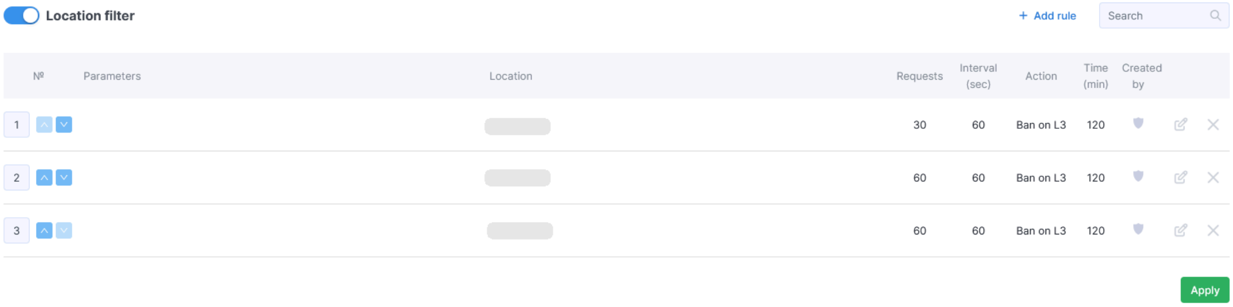
Add

Once the rules are added, they will appear in the table, where you can:

- Edit them;
- Delete them.

Location Filter

You can set filtering rules for different locations within your resource.



Location filter

+ Add rule

Search

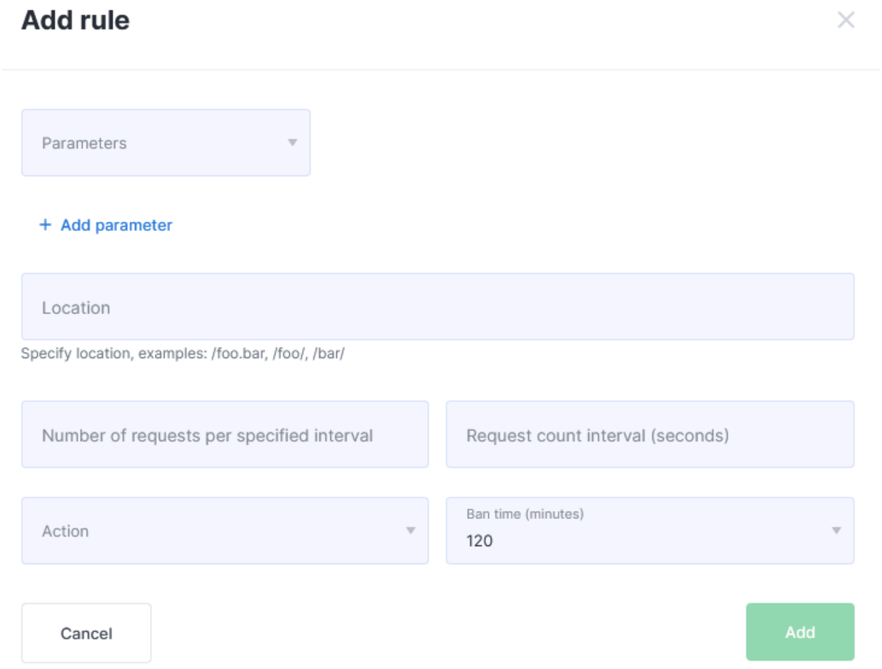
№	Parameters	Location	Requests	Interval (sec)	Action	Time (min)	Created by
1			30	60	Ban on L3	120	
2			60	60	Ban on L3	120	
3			60	60	Ban on L3	120	

Apply

To add a new rule:

1. Click **+ Add Rule**.
2. Fill out the form following the provided instructions.

Once added, the rule will be applied to the specified location, ensuring customized filtering based on your security needs.



Add rule

Parameters

+ Add parameter

Location

Specify location, examples: /foo.bar, /foo/, /bar/

Number of requests per specified interval

Request count interval (seconds)

Action

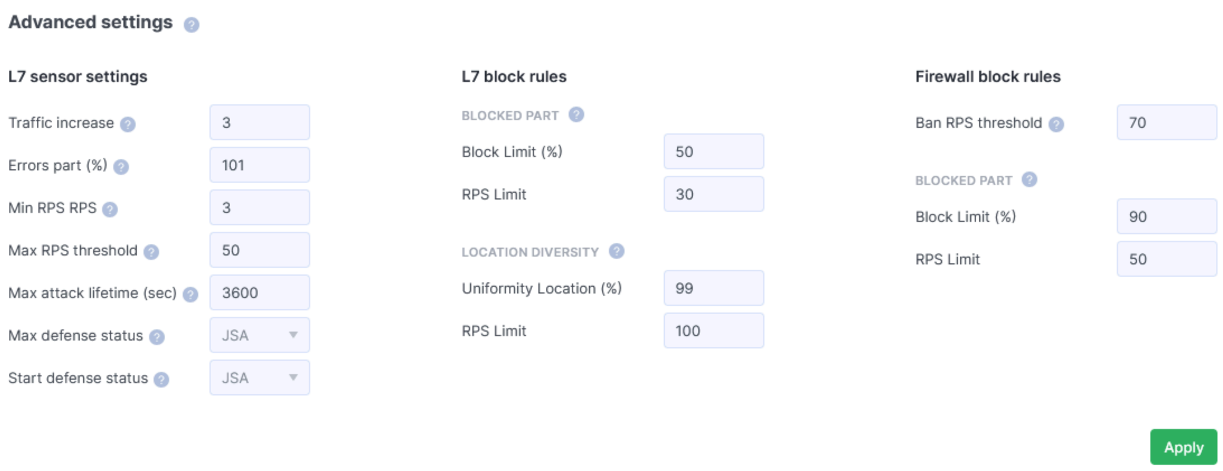
Ban time (minutes)
120

Cancel

Add

Advanced Rules

You can configure various sensor parameters yourself after reviewing the information about them.



Advanced settings

L7 sensor settings

Traffic increase: 3

Errors part (%): 101

Min RPS RPS: 3

Max RPS threshold: 50

Max attack lifetime (sec): 3600

Max defense status: JSA

Start defense status: JSA

L7 block rules

BLOCKED PART

Block Limit (%): 50

RPS Limit: 30

LOCATION DIVERSITY

Uniformity Location (%): 99

RPS Limit: 100

Firewall block rules

Ban RPS threshold: 70

BLOCKED PART

Block Limit (%): 90

RPS Limit: 50

This section allows you to set up application-level (L7) filtering and firewall rules to ensure effective protection of your resource.

L7 Sensor Settings

Traffic Increase

Determines how many times the number of requests must increase within a short period to activate protection.

- For example, if the value is «3», the system will switch to active protection mode if the number of requests triples within the last 15 minutes.

Errors Part

Sets the percentage of erroneous requests at which filters activate.

- For example, if set to 30%, once 30% or more of requests return 500-series errors, protection measures will be enabled.

Set Min RPS (Minimum Requests Per Second)

Defines the minimum threshold below which checks for traffic increase and error rates are not performed.

Max RPS Threshold

The maximum number of requests per second at which protection activation triggers.

Max Attack Lifetime (Seconds)

The maximum duration of an attack in seconds.

- After this period, the filter attempts to return to sensor mode.
- This is useful for mitigating intermittent attacks.

Max Defence Status

Defines the maximum level of protection when triggers activate automatically.

Start Defence Status

The initial protection level set when switching from sensor mode to active mode.

L7 Blocking Rules

These settings help **detect suspicious bot activity**:

Blocked Part

If an IP address exceeds the RPS Limit (Requests Per Second) and the percentage of blocked requests exceeds the Block Limit, the IP is added to the Greylist.

Block Limit (%)

Defines the percentage threshold beyond which an IP address is blocked.

RPS Limit

The maximum number of requests per second from a single IP before blocking starts.

Location Diversity

If a single IP accesses too many different sections of the website, it may indicate automated activity.

Uniformity Location (%)

Sets the percentage threshold determining the uniformity of access to specific locations.

Firewall Blocking Rules

These settings allow **blocking traffic at the network level (L3/L4)**:

Ban RPS Threshold

If the number of requests from an IP address exceeds this value, the address is blocked immediately without additional checks.

Blocked Part L3 (%)

If an IP address exceeds the RPS Limit, and the percentage of blocked requests exceeds the Block Limit, the address is blocked.

Block Limit (%)

Defines the percentage threshold beyond which an IP address is blocked.

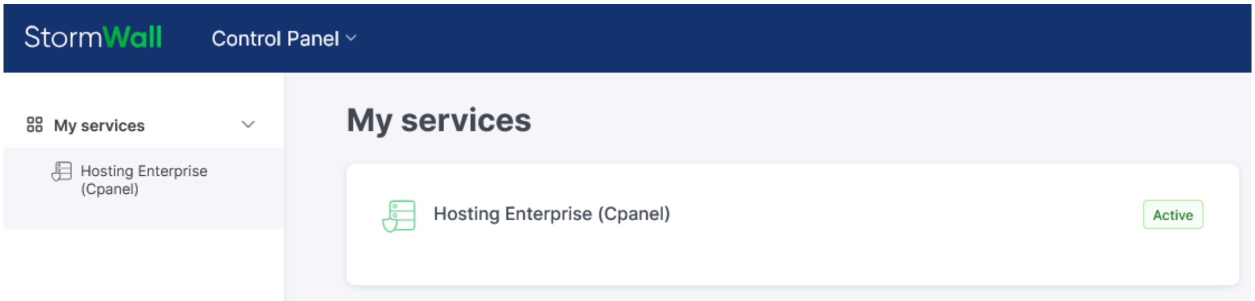
RPS Limit

The maximum number of requests per second from a single IP before blocking starts.

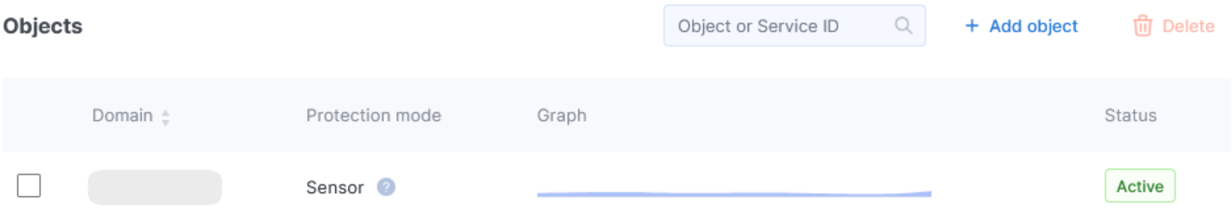
Proper configuration of these parameters allows you to effectively protect your resource from various types of attacks, ensuring stable and secure operation.

Blocked IPs

Open the **Control Panel** and click on the service name **Hosting Protection**.

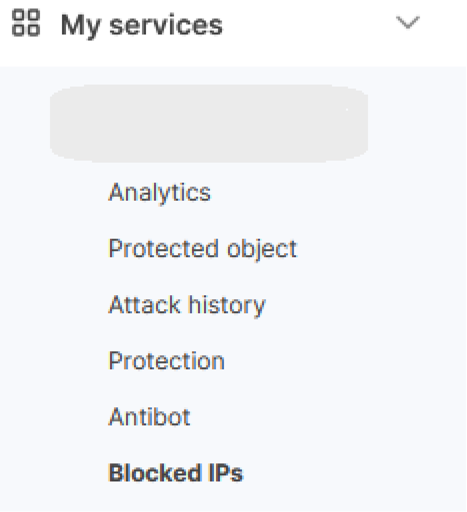


If you have multiple protected objects, select the necessary one in the **Objects** field on the opened page.



	Domain	Protection mode	Graph	Status
□	[redacted]	Sensor		Active

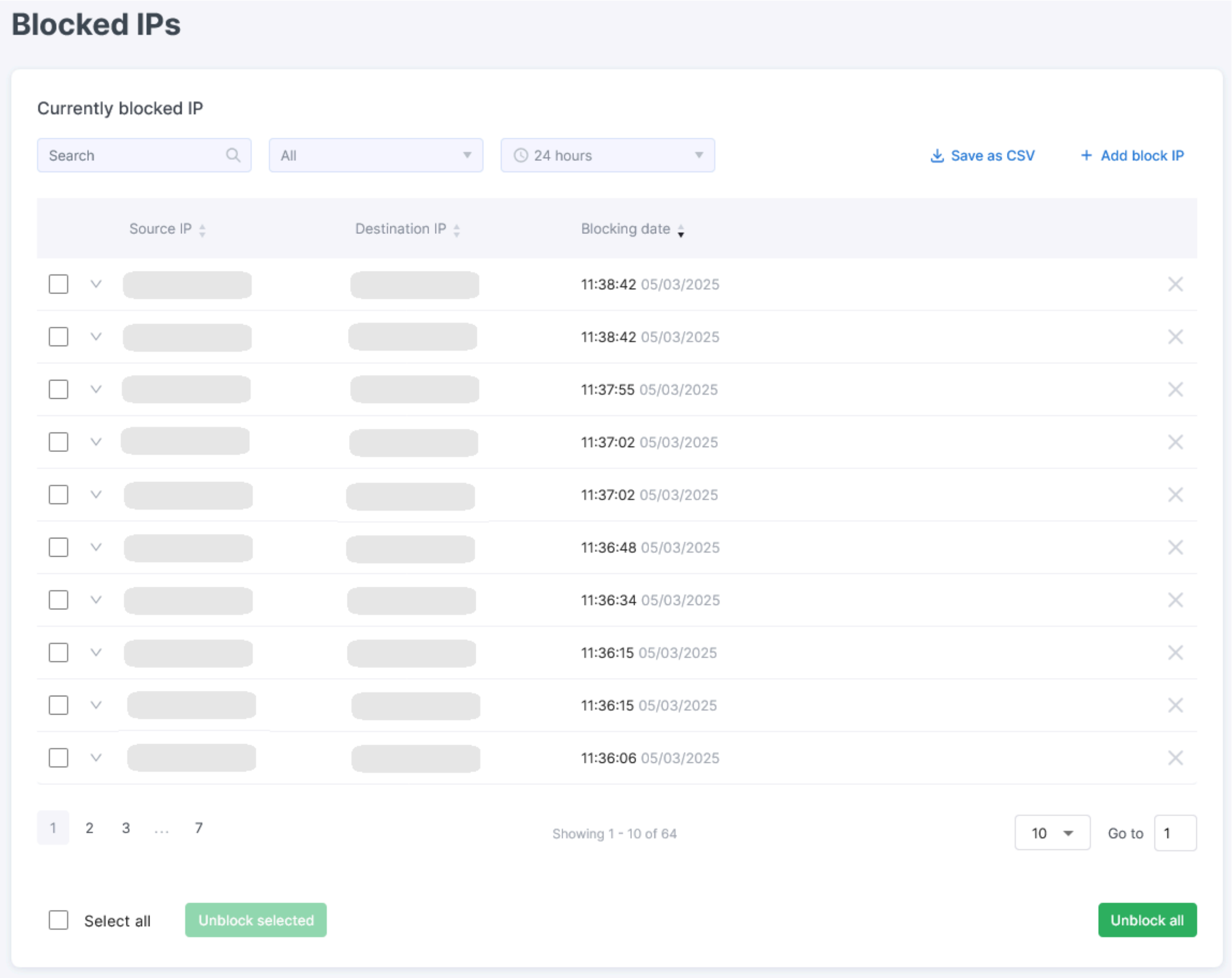
In the left menu, select **Blocked IPs**.



On the current page, the IP addresses that are currently blocked are displayed, and below is the block history. You can manage these lists by removing specific IP addresses from the block by checking the boxes next to them and clicking the **Unblock**

Selected button. To completely clear the list of blocked addresses, use the **Unblock All** button.

Please note that removing an IP address from the blocklist may be necessary if you are sure of its safety and want to restore access for the corresponding user or device. It is recommended to regularly review and update blocklists to maintain the optimal security level of your resource.



Blocked IPs

Currently blocked IP

		Source IP	Destination IP	Blocking date	
□	⌄	[redacted]	[redacted]	11:38:42 05/03/2025	✕
□	⌄	[redacted]	[redacted]	11:38:42 05/03/2025	✕
□	⌄	[redacted]	[redacted]	11:37:55 05/03/2025	✕
□	⌄	[redacted]	[redacted]	11:37:02 05/03/2025	✕
□	⌄	[redacted]	[redacted]	11:37:02 05/03/2025	✕
□	⌄	[redacted]	[redacted]	11:36:48 05/03/2025	✕
□	⌄	[redacted]	[redacted]	11:36:34 05/03/2025	✕
□	⌄	[redacted]	[redacted]	11:36:15 05/03/2025	✕
□	⌄	[redacted]	[redacted]	11:36:15 05/03/2025	✕
□	⌄	[redacted]	[redacted]	11:36:06 05/03/2025	✕

For efficient IP address management on your platform, it is recommended to use the built-in search and filtering tools.

This will allow you to quickly find and process the necessary data.

IP Address Search and Filtering

Use the search function and configure filters by time and data type to obtain a selection of the IP addresses you are interested in. This is especially useful for analyzing activity and identifying potential threats.

After applying filters, you can save the retrieved records to a file by clicking the **Save as CSV** button. This will allow you to maintain an event log and, if necessary, share information with colleagues or use it for further analysis.

Time Filtering Features

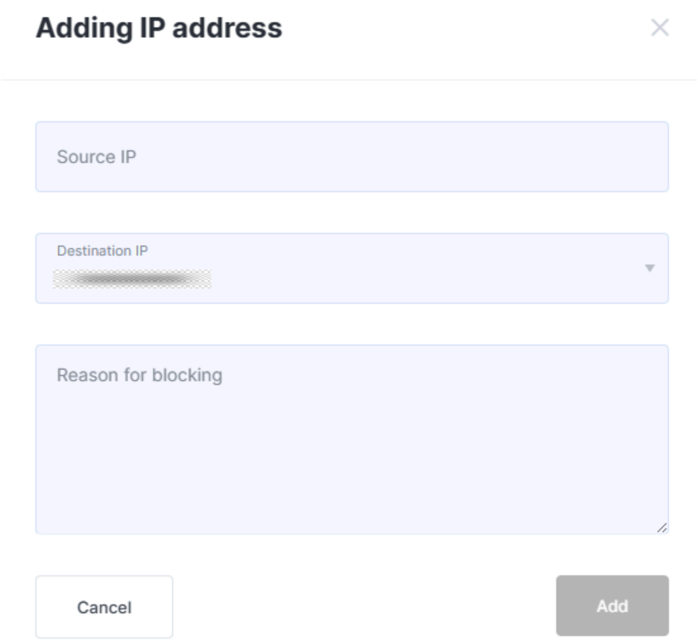
When setting time ranges using the **«from ... to ...»** parameters, please note that the data in the table does not update automatically. To refresh the information, you need to manually reset the filter or select predefined time intervals such as **«5 min», «24h»,** and others.

When selecting predefined time intervals, data updates automatically every **minute**. This ensures the relevance of the displayed information without the need for manual updates.

Blocking IP Addresses

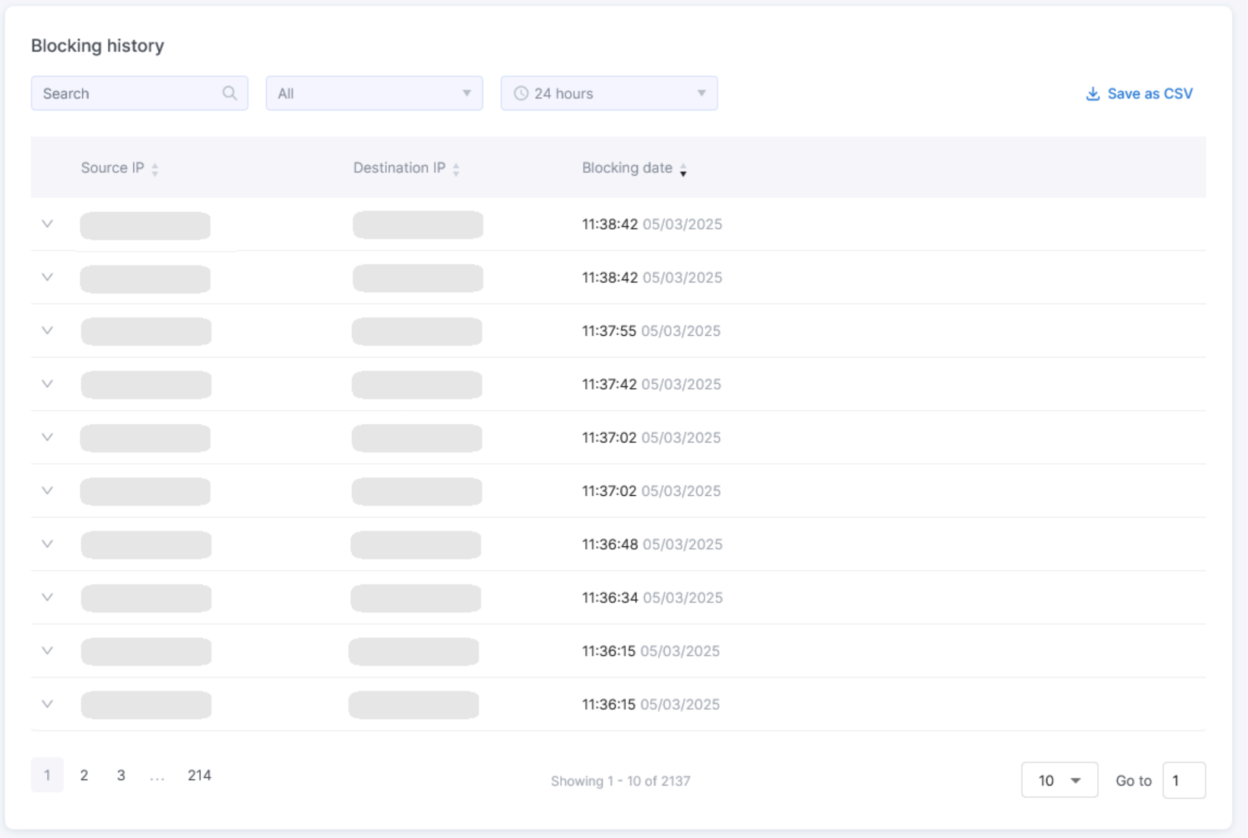
To block a specific IP address, click the **Block IP** button. In the opened form, specify:

- **Source IP address:** the address you want to block.
- **Destination IP address:** your address that needs protection.
- **Block reason:** an optional field where you can specify the reason for the decision.



After adding an IP address to the blocklist, you can manage this list by deleting or adding addresses as needed. This allows you to maintain the security of your network and prevent unwanted activity.

The **Blocking history** is presented in a table with similar filtering and data-saving capabilities.



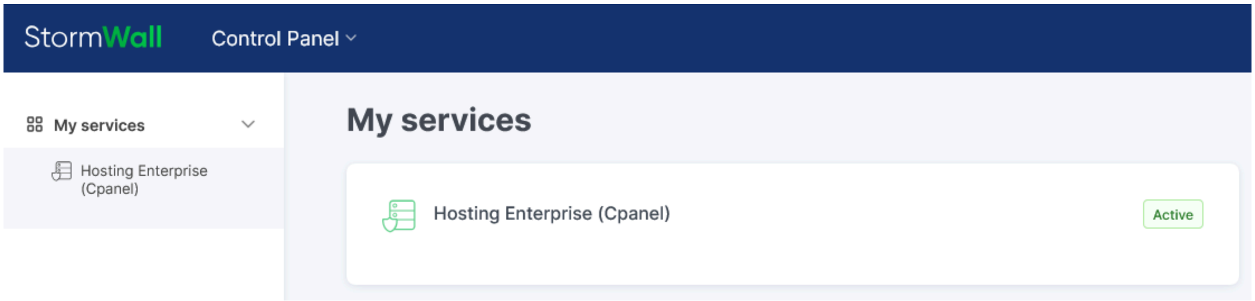
Blocking history

Source IP	Destination IP	Blocking date
[redacted]	[redacted]	11:38:42 05/03/2025
[redacted]	[redacted]	11:38:42 05/03/2025
[redacted]	[redacted]	11:37:55 05/03/2025
[redacted]	[redacted]	11:37:42 05/03/2025
[redacted]	[redacted]	11:37:02 05/03/2025
[redacted]	[redacted]	11:37:02 05/03/2025
[redacted]	[redacted]	11:36:48 05/03/2025
[redacted]	[redacted]	11:36:34 05/03/2025
[redacted]	[redacted]	11:36:15 05/03/2025
[redacted]	[redacted]	11:36:15 05/03/2025

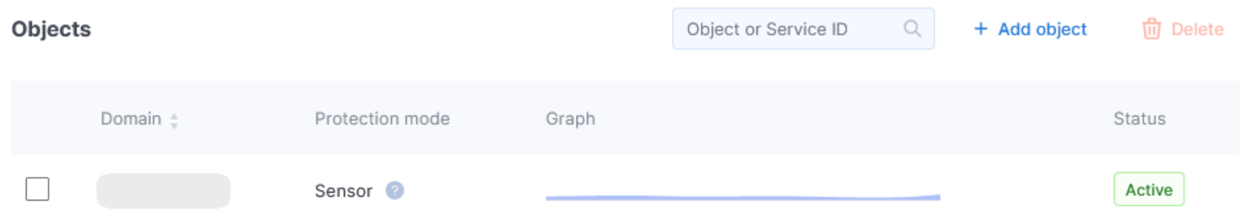
Using these tools will help you effectively control access to your resource and ensure its security.

cPanel

Log into the **Control Panel** and select the required service by clicking on its name in the center of the page or in the left menu.



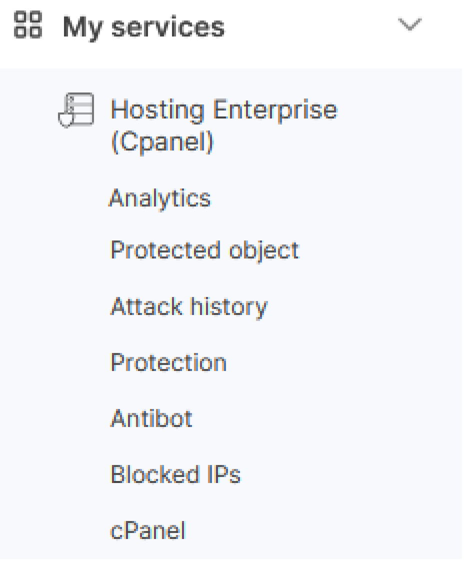
If you have multiple protected objects, select the necessary one in the **Objects** section on the opened page.



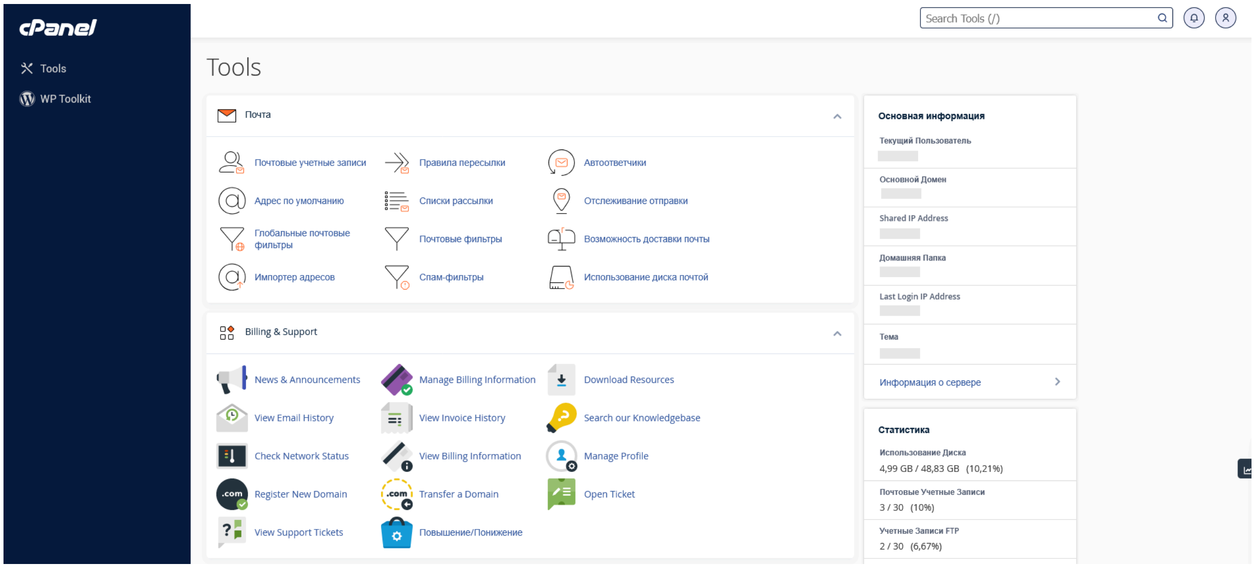
Objects

	Domain	Protection mode	Graph	Status
□		Sensor		Active

In the opened menu, select **cPanel**.



The **cPanel** interface will open.



cPanel

Tools

WP Toolkit

Search Tools (/)

Tools

Почта

Почтовые учетные записи | Правила пересылки | Автоответчики

Адрес по умолчанию | Списки рассылки | Отслеживание отправки

Глобальные почтовые фильтры | Почтовые фильтры | Возможность доставки почты

Импортер адресов | Спам-фильтры | Использование диска почтой

Billing & Support

News & Announcements | Manage Billing Information | Download Resources

View Email History | View Invoice History | Search our Knowledgebase

Check Network Status | View Billing Information | Manage Profile

Register New Domain | Transfer a Domain | Open Ticket

View Support Tickets | Повышение/Понижение

Основная информация

Текущий Пользователь
[redacted]

Основной Домен
[redacted]

Shared IP Address
[redacted]

Домашняя Папка
[redacted]

Last Login IP Address
[redacted]

Тема
[redacted]

Информация о сервере

Статистика

Использование Диска
4,99 GB / 48,83 GB (10,21%)

Почтовые Учетные Записи
3 / 30 (10%)

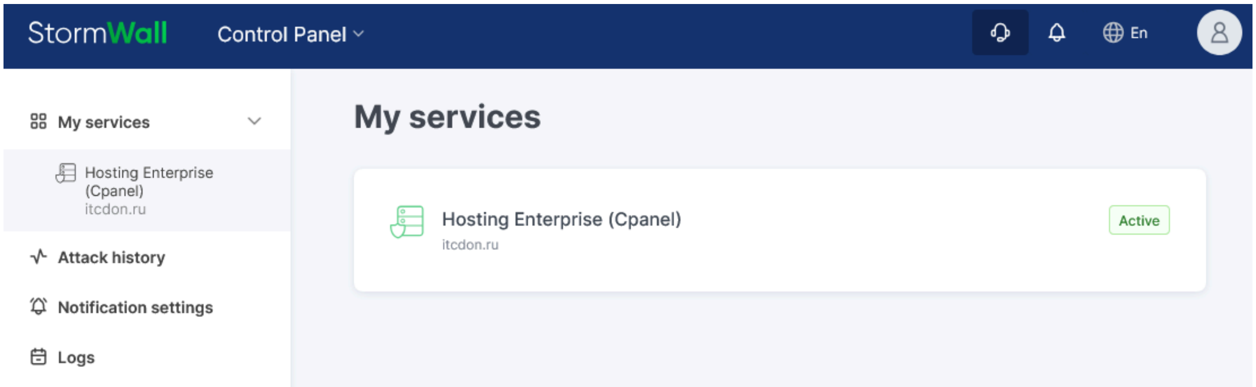
Учетные Записи FTP
2 / 30 (6,67%)

Review the **instructions** on how to work with the tools in the panel.

Monitoring Tools

Analytics

Log into the **Control Panel** and select the required service by clicking on its name in the central area of the page or in the left menu.



StormWall

Control Panel

En

My services

Hosting Enterprise (Cpanel)
itcdon.ru

Attack history

Notification settings

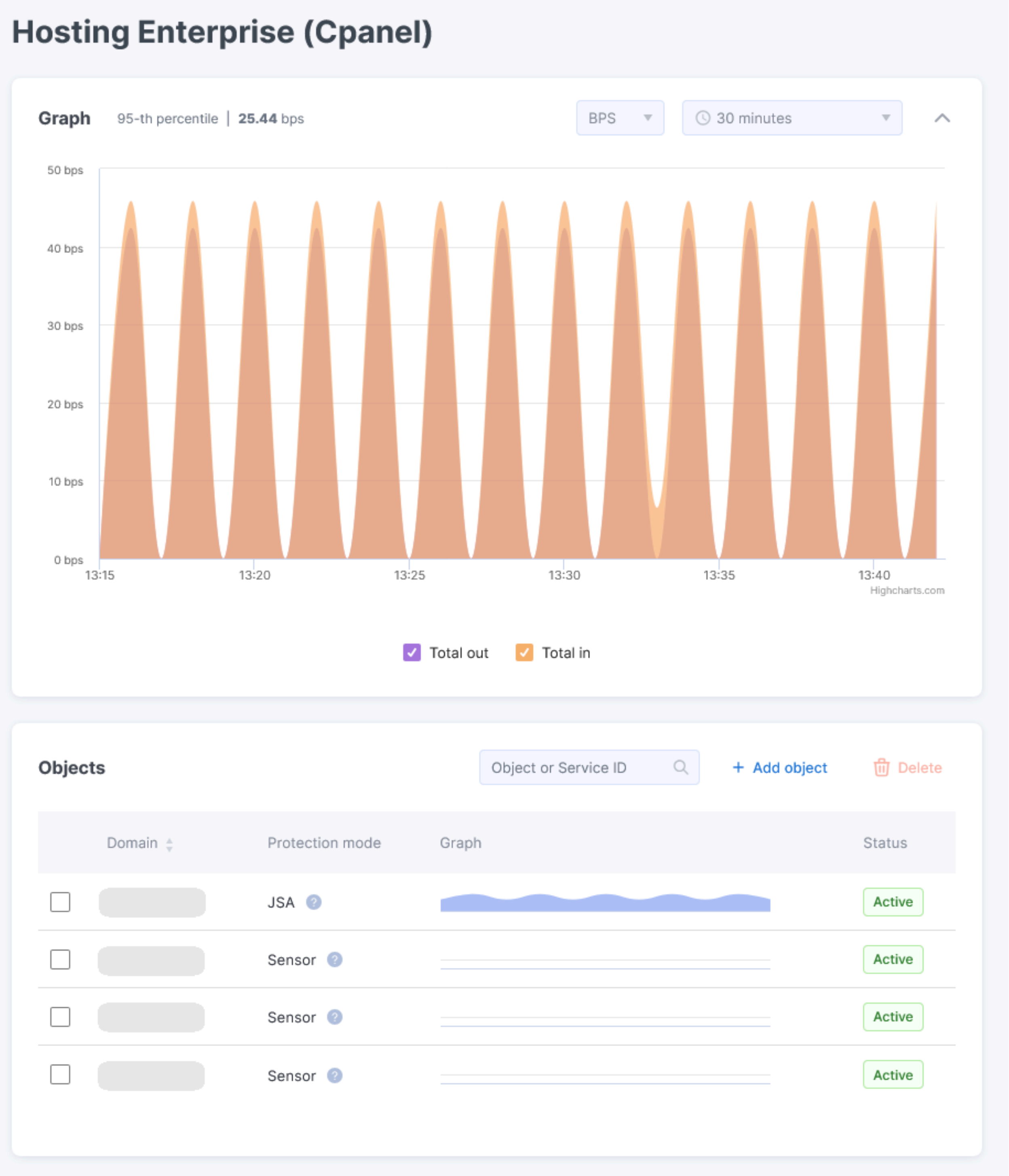
Logs

My services

Hosting Enterprise (Cpanel)
itcdon.ru

Active

If you have multiple protected objects, select the necessary one in the **Objects** section on the newly opened page.



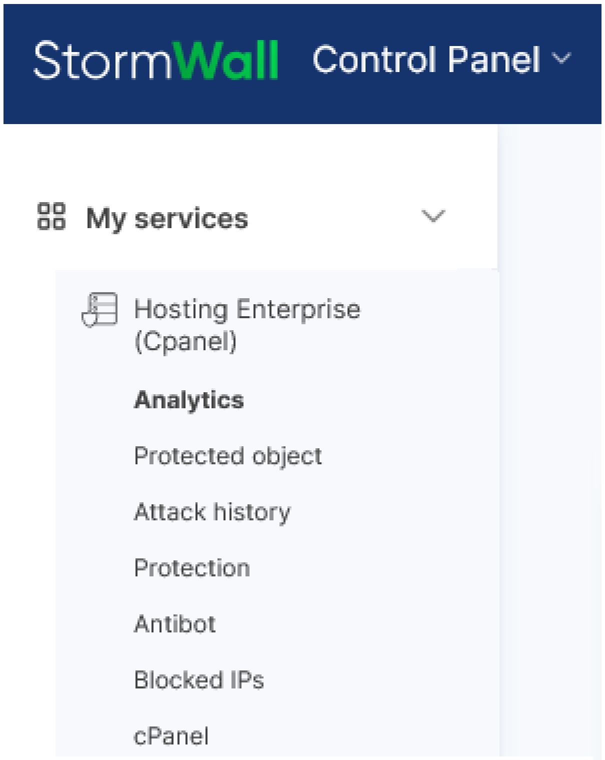
Hosting Enterprise (Cpanel)

Graph 95-th percentile | **25.44** bps

Objects

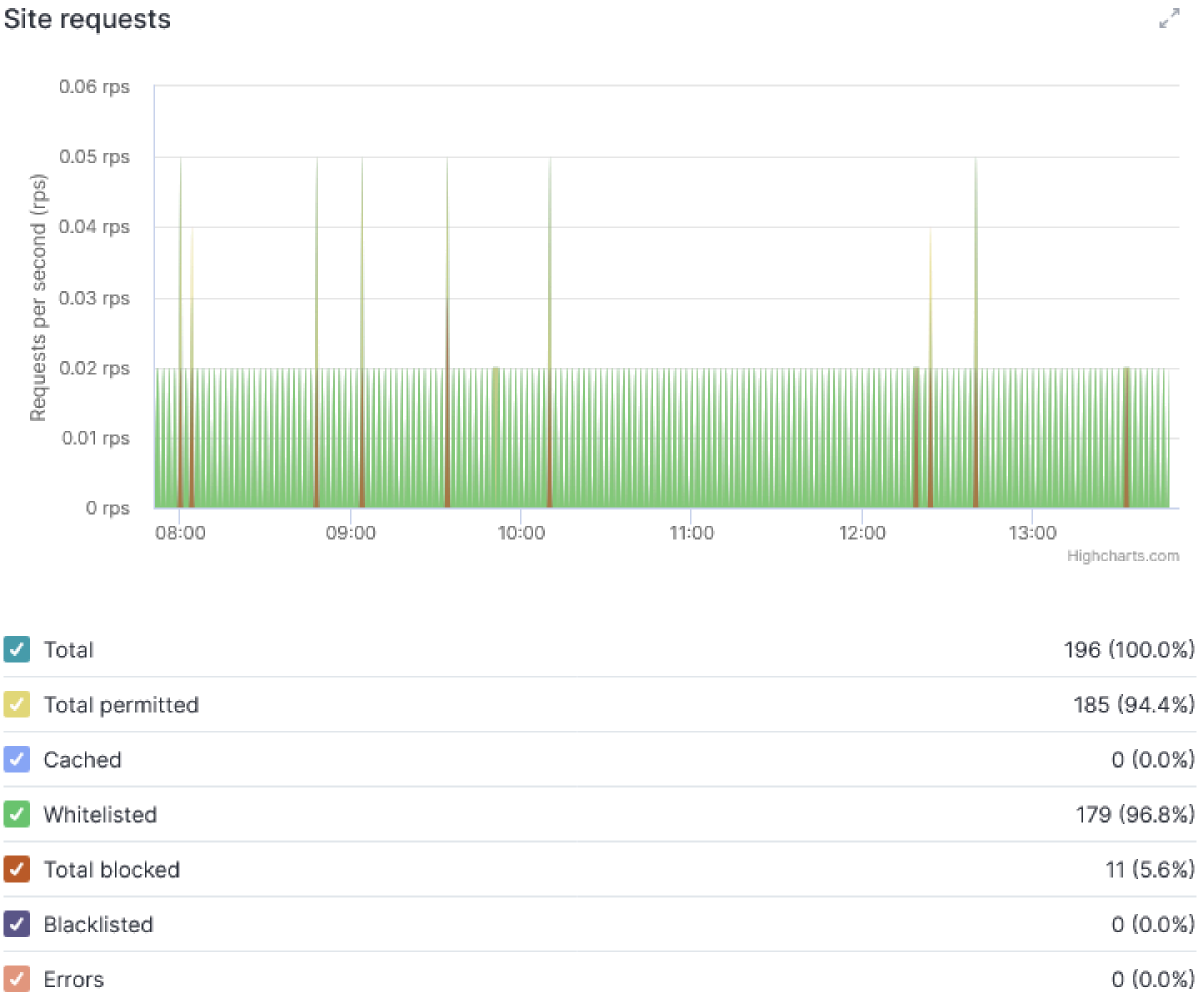
	Domain	Protection mode	Graph	Status
□		JSA		Active
□		Sensor		Active
□		Sensor		Active
□		Sensor		Active

In the opened menu, select **Analytics**.



The page provides the following information:

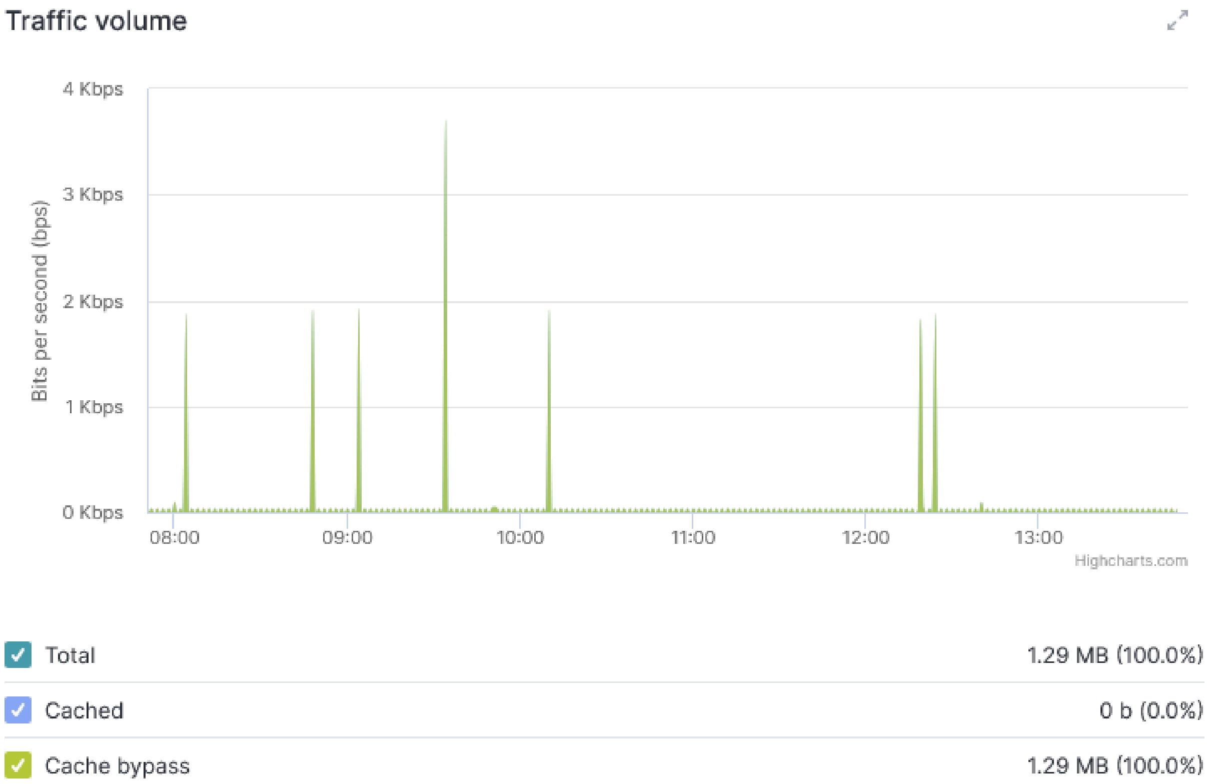
- **Website Requests** (number of requests per second received by the website)



Site requests

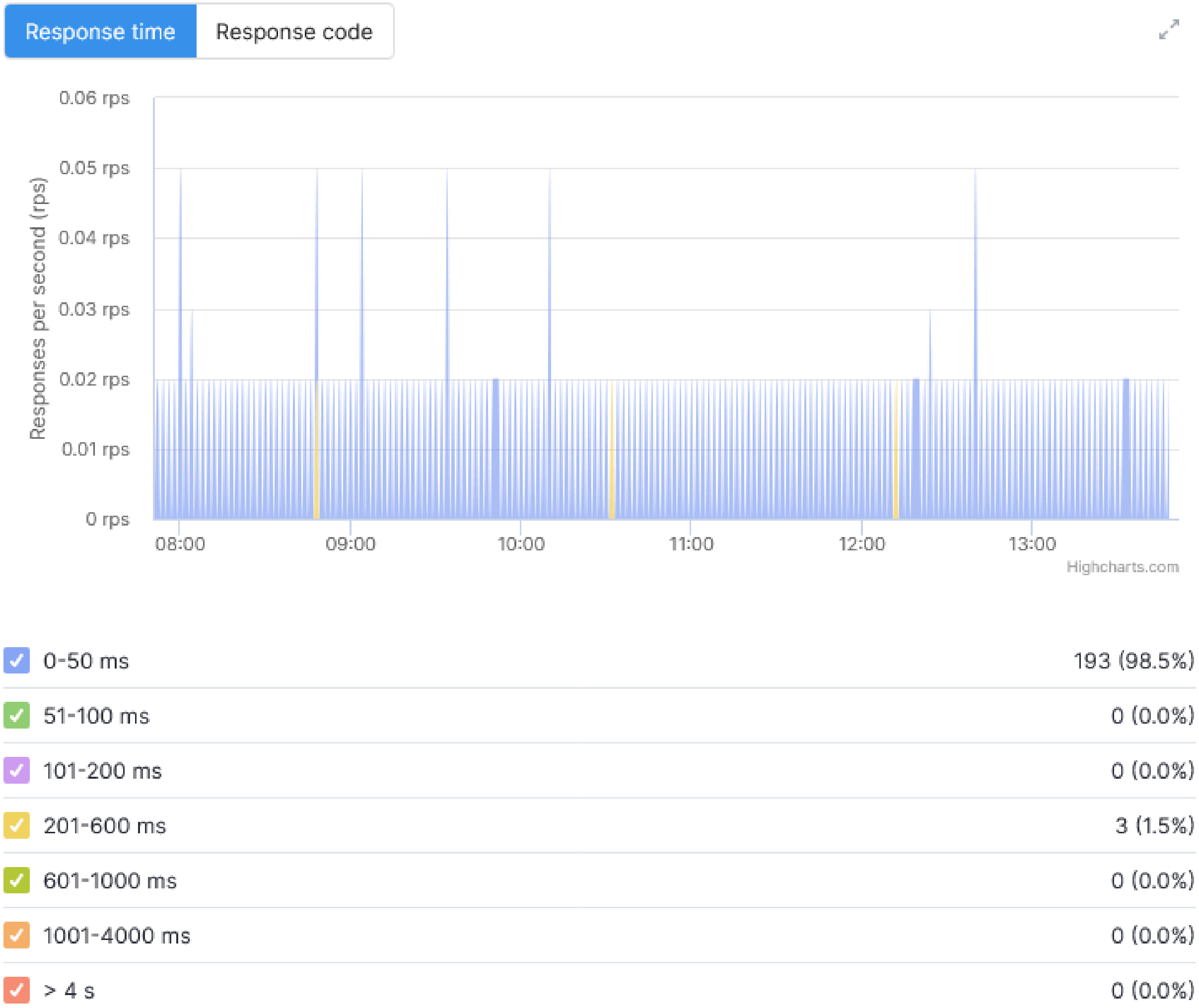
☑ Total	196 (100.0%)
☑ Total permitted	185 (94.4%)
☑ Cached	0 (0.0%)
☑ Whitelisted	179 (96.8%)
☑ Total blocked	11 (5.6%)
☑ Blacklisted	0 (0.0%)
☑ Errors	0 (0.0%)

- **Traffic Volume** (number of bits per second)



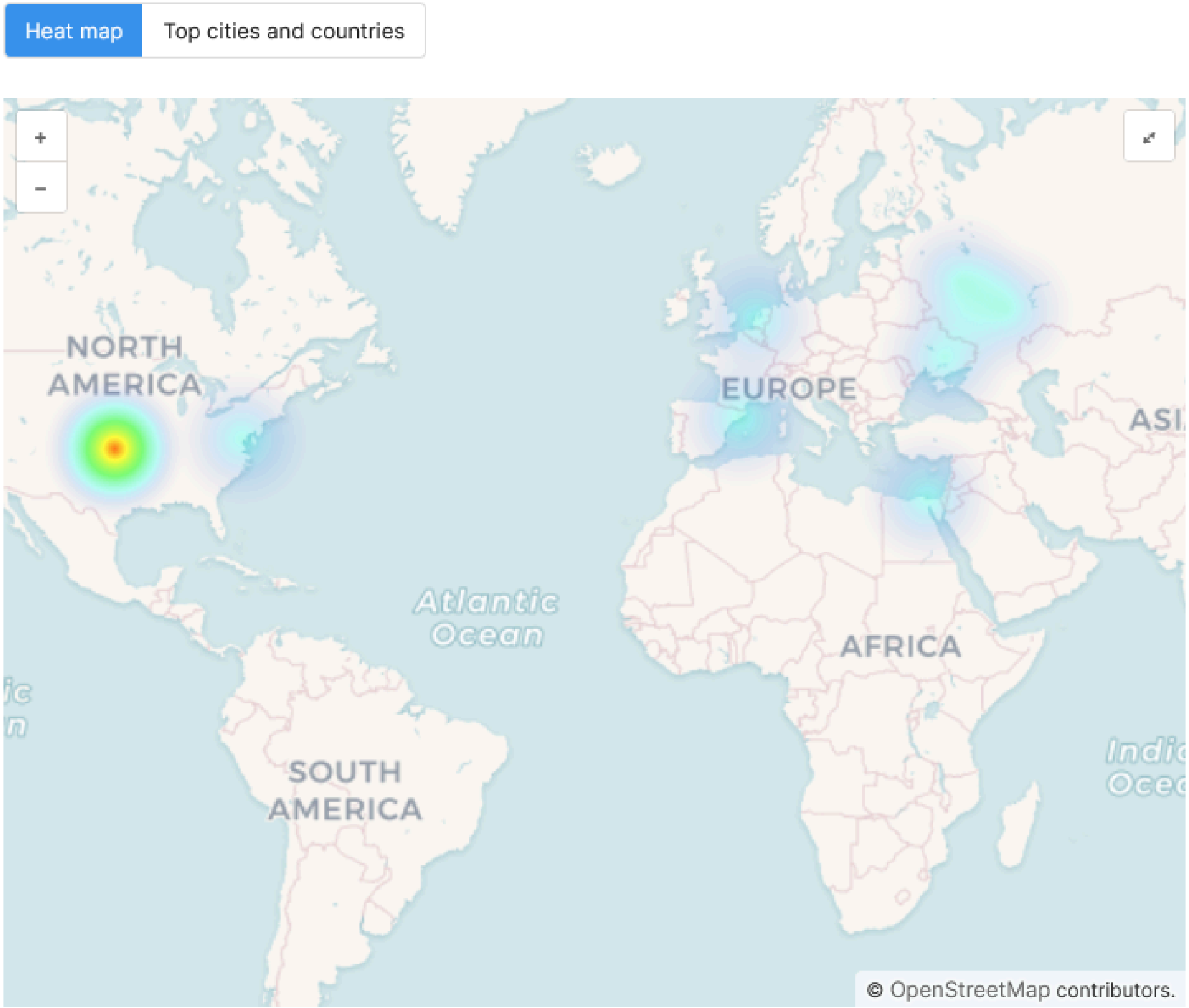
☑ Total	1.29 MB (100.0%)
☑ Cached	0 b (0.0%)
☑ Cache bypass	1.29 MB (100.0%)

- **Response Time** (number of responses per second) / **Response Code**



☑ 0-50 ms	193 (98.5%)
☑ 51-100 ms	0 (0.0%)
☑ 101-200 ms	0 (0.0%)
☑ 201-600 ms	3 (1.5%)
☑ 601-1000 ms	0 (0.0%)
☑ 1001-4000 ms	0 (0.0%)
☑ > 4 s	0 (0.0%)

- **Heat map / Top Cities and Countries**

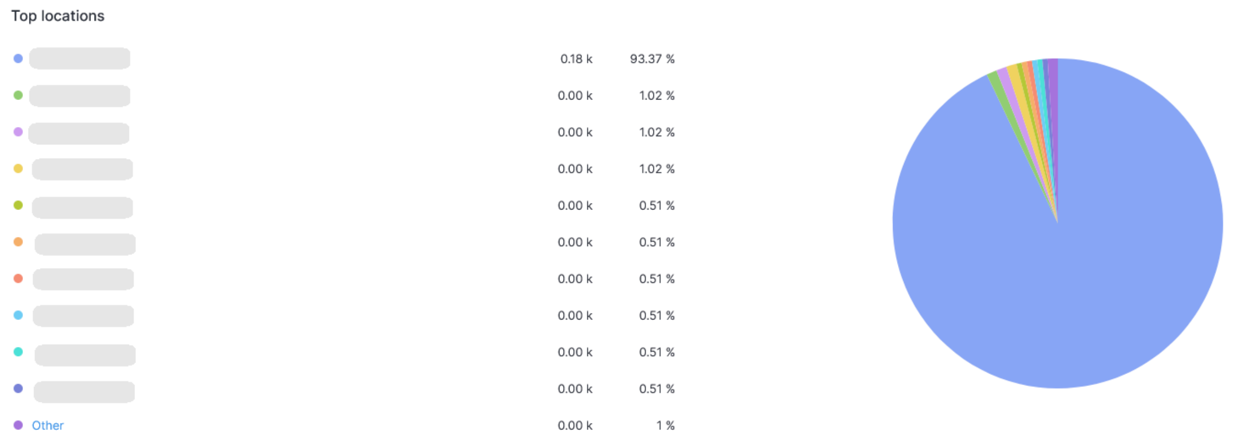


On the **Heat map** tab, you can observe the geographical distribution of requests to your resources. Areas with the highest concentration of requests are highlighted in red. This data is useful for configuring access rules based on the users' geographic locations using the **GEO filter** tool.

To view a more detailed map, click the arrow icon in the top-right corner of the image.

To see a list of the most active attack sources, open the **Top Cities and Countries** tab.

- Top Locations



Top locations

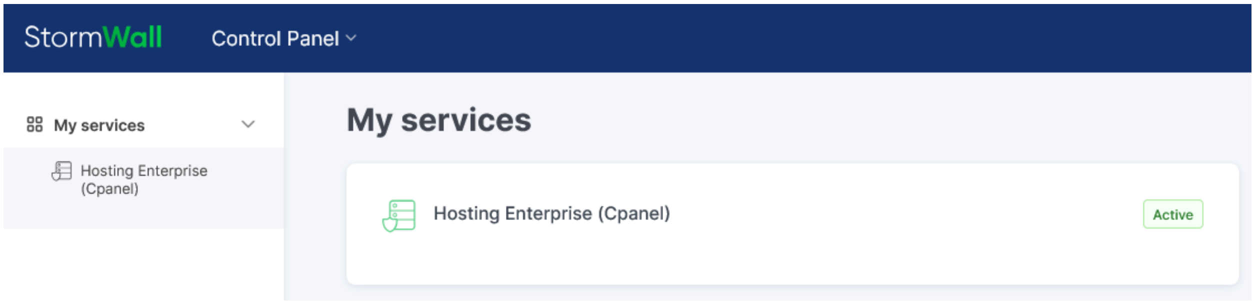
●	[redacted]	0.18 k	93.37 %
●	[redacted]	0.00 k	1.02 %
●	[redacted]	0.00 k	1.02 %
●	[redacted]	0.00 k	1.02 %
●	[redacted]	0.00 k	0.51 %
●	[redacted]	0.00 k	0.51 %
●	[redacted]	0.00 k	0.51 %
●	[redacted]	0.00 k	0.51 %
●	[redacted]	0.00 k	0.51 %
●	[redacted]	0.00 k	0.51 %
●	Other	0.00 k	1 %

You can view information about which parts of your resource were frequently visited by users or targeted by attacks.

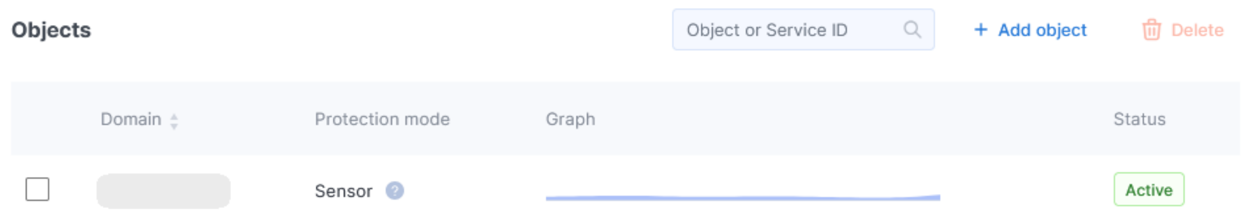
For example, the homepage of the website is often attacked.

Attack History

Open the **Control Panel** and click on the name of the required service located in the center of the page or in the left sidebar menu.

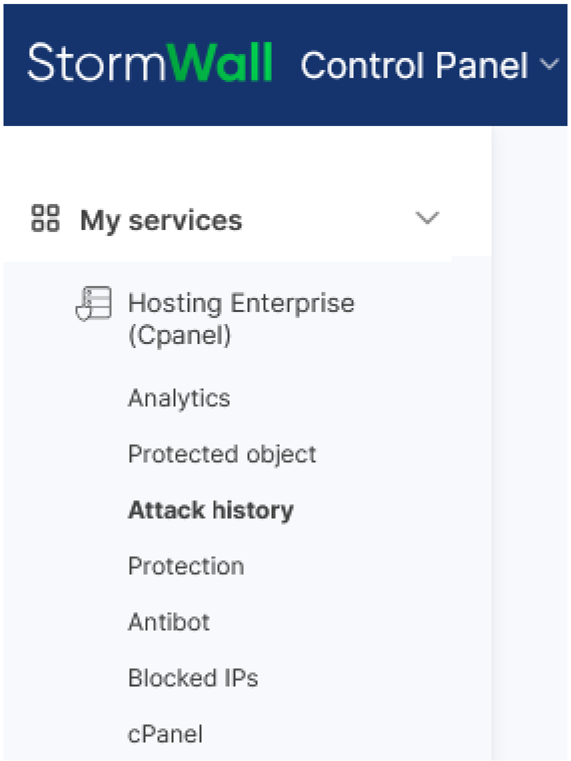


If you have multiple protected objects, select the required one in the **Objects** section on the opened page.

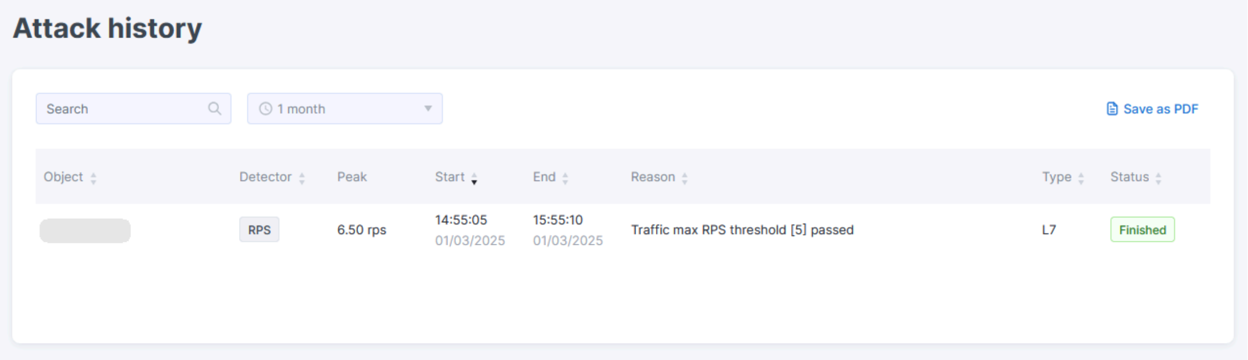


	Domain	Protection mode	Graph	Status
□		Sensor ?		Active

In the opened menu, select **Attack History**.



The displayed page shows attacks over a selected time period, which you can customize.



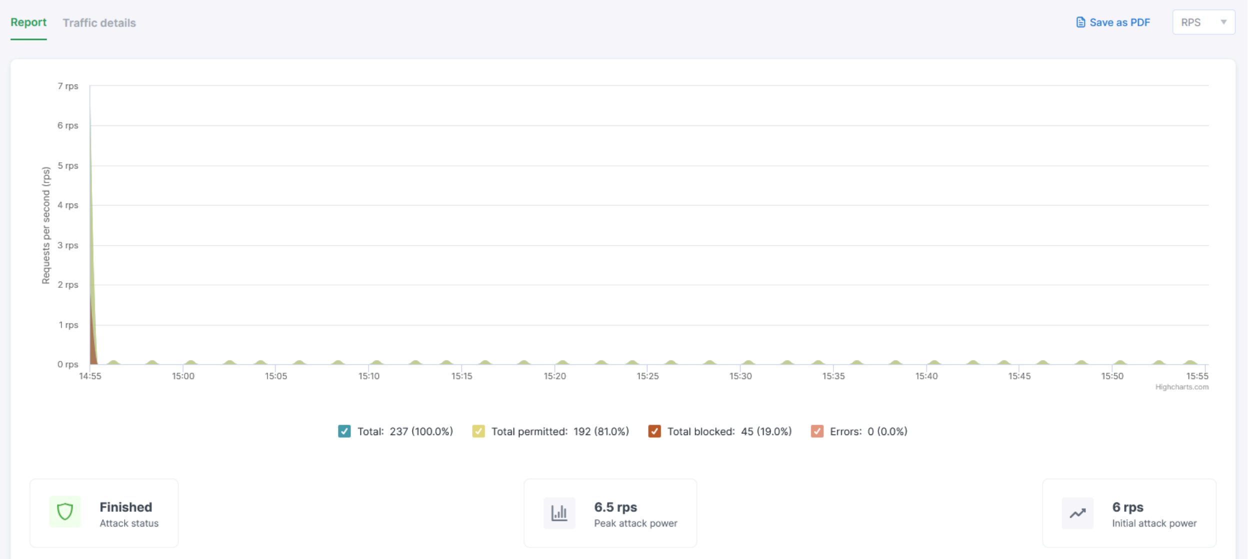
Attack history

Object	Detector	Peak	Start	End	Reason	Type	Status
[redacted]	RPS	6.50 rps	14:55:05 01/03/2025	15:55:10 01/03/2025	Traffic max RPS threshold [5] passed	L7	Finished

Use the search and time filter to retrieve specific data.

To download the attack history, click the **Save as PDF** button.

To view detailed information about an attack, click on the row of the attack you are interested in.



☑ Total: 237 (100.0%) ☑ Total permitted: 192 (81.0%) ☑ Total blocked: 45 (19.0%) ☑ Errors: 0 (0.0%)

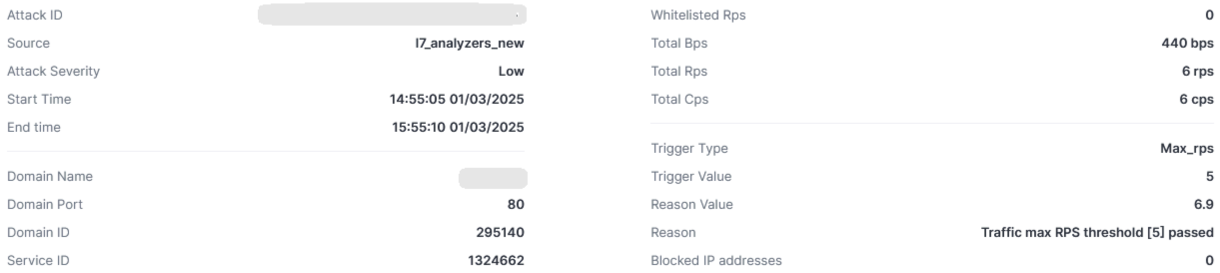
Finished
Attack status

6.5 rps
Peak attack power

6 rps
Initial attack power

Hover your mouse cursor over the graph to see numerical values.

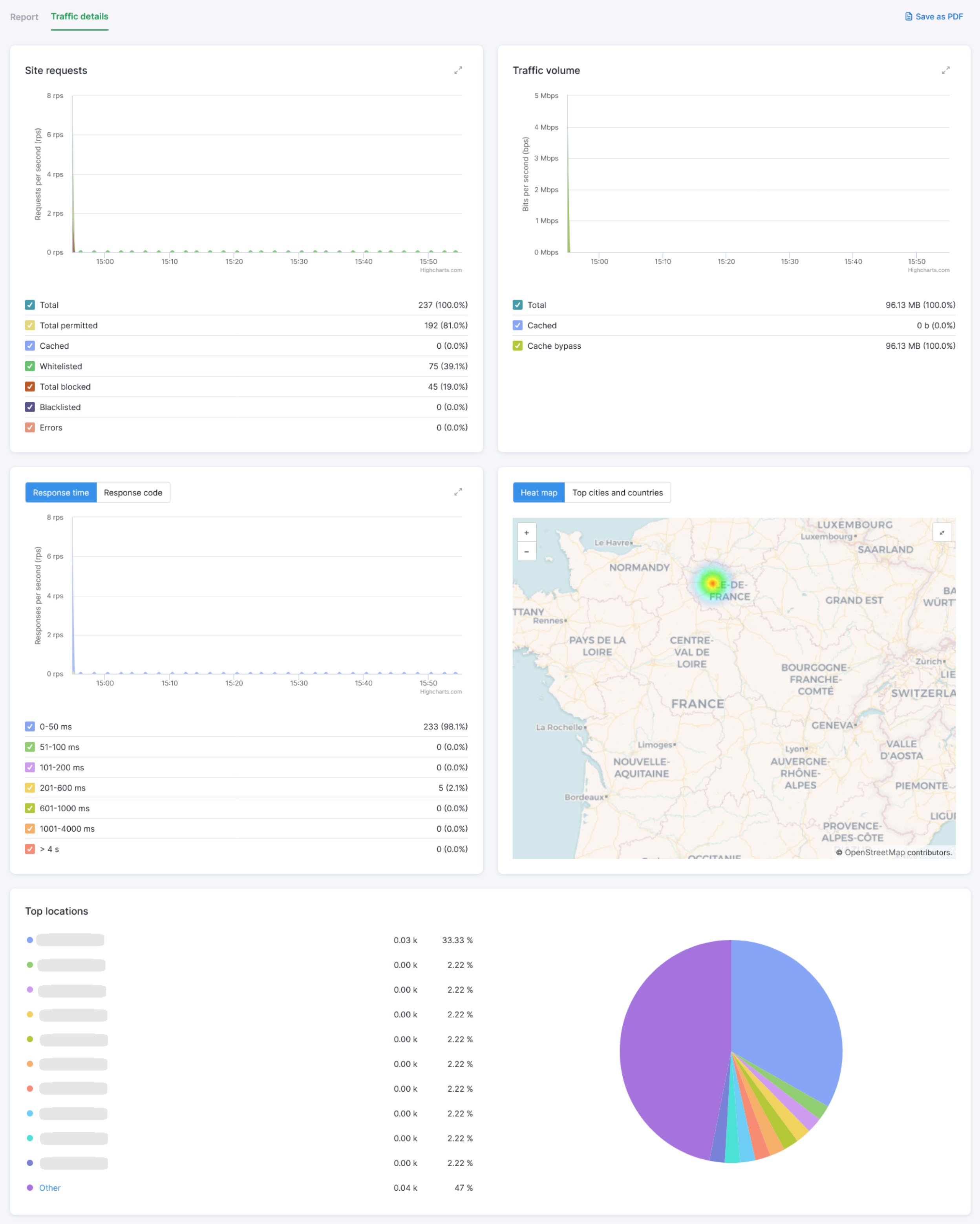
Detailed attack information is displayed below the graph.



Attack ID	[redacted]
Source	l7_analyzers_new
Attack Severity	Low
Start Time	14:55:05 01/03/2025
End time	15:55:10 01/03/2025
Domain Name	[redacted]
Domain Port	80
Domain ID	295140
Service ID	1324662

Whitelisted Rps	0
Total Bps	440 bps
Total Rps	6 rps
Total Cps	6 cps
Trigger Type	Max_rps
Trigger Value	5
Reason Value	6.9
Reason	Traffic max RPS threshold [5] passed
Blocked IP addresses	0

On the **Traffic details** tab you can see the graphs.



Site requests

☑ Total	237 (100.0%)
☑ Total permitted	192 (81.0%)
☑ Cached	0 (0.0%)
☑ Whitelisted	75 (39.1%)
☑ Total blocked	45 (19.0%)
☑ Blacklisted	0 (0.0%)
☑ Errors	0 (0.0%)

Traffic volume

☑ Total	96.13 MB (100.0%)
☑ Cached	0 b (0.0%)
☑ Cache bypass	96.13 MB (100.0%)

☑ 0-50 ms	233 (98.1%)
☑ 51-100 ms	0 (0.0%)
☑ 101-200 ms	0 (0.0%)
☑ 201-600 ms	5 (2.1%)
☑ 601-1000 ms	0 (0.0%)
☑ 1001-4000 ms	0 (0.0%)
☑ > 4 s	0 (0.0%)

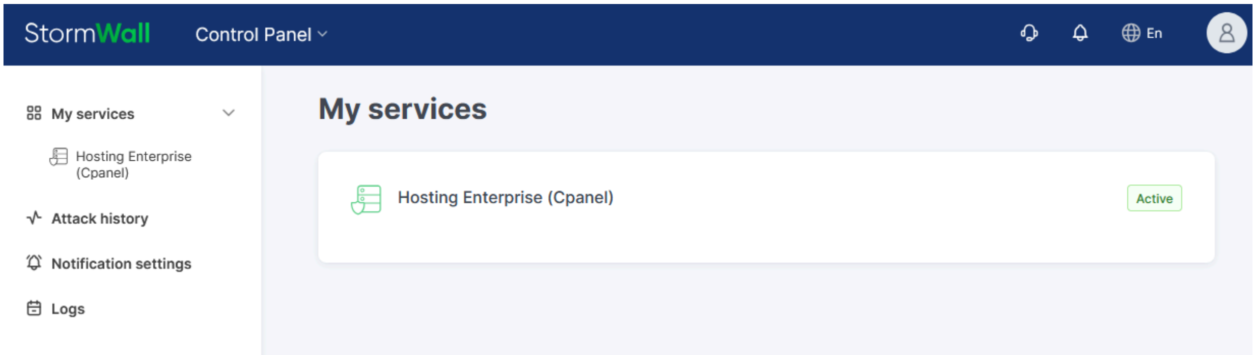
© OpenStreetMap contributors.

Top locations

● [redacted]	0.03 k	33.33 %
● [redacted]	0.00 k	2.22 %
● [redacted]	0.00 k	2.22 %
● [redacted]	0.00 k	2.22 %
● [redacted]	0.00 k	2.22 %
● [redacted]	0.00 k	2.22 %
● [redacted]	0.00 k	2.22 %
● [redacted]	0.00 k	2.22 %
● [redacted]	0.00 k	2.22 %
● [redacted]	0.00 k	2.22 %
● Other	0.04 k	47 %

How to Link a Domain to Hosting

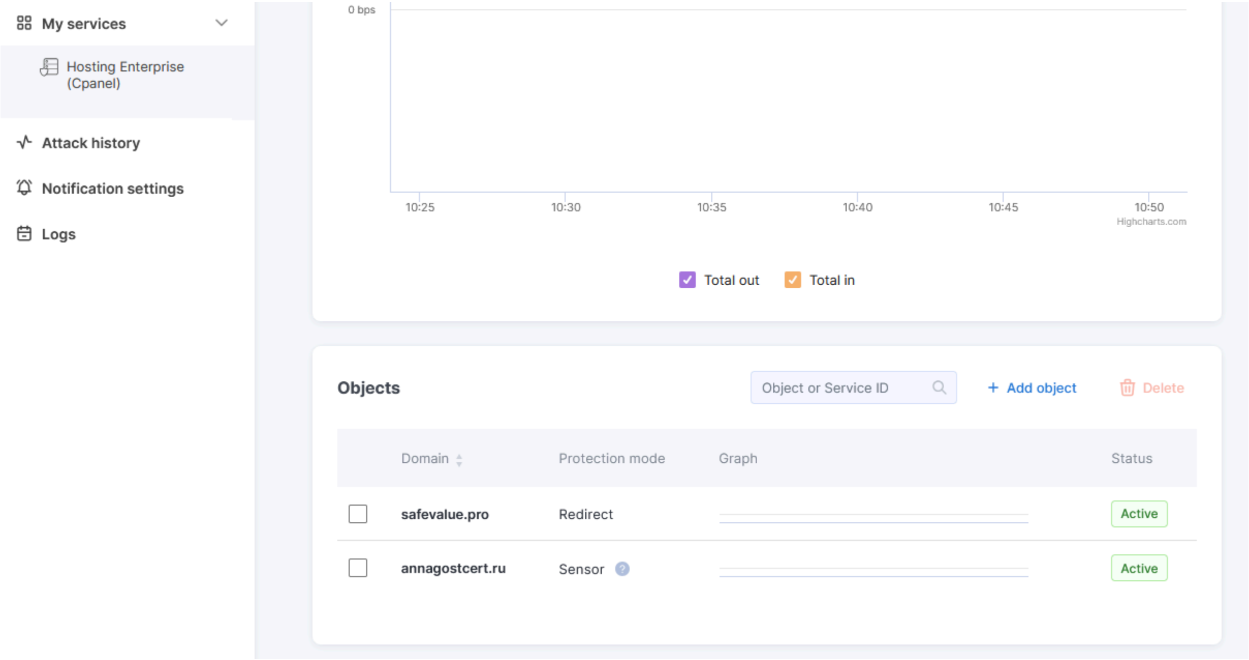
Go to the **Control Panel** tab in your **Client Portal**.



My services

Hosting Enterprise (Cpanel) Active

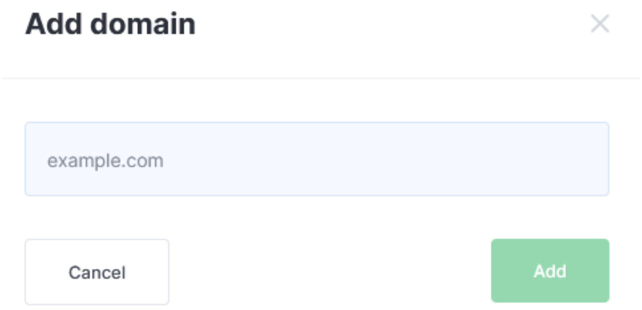
Select the service to view its details as shown in the screenshot.



Objects

	Domain	Protection mode	Graph	Status
□	safevalue.pro	Redirect		Active
□	annagostcert.ru	Sensor ?		Active

In the **Objects** section, click **+ Add Object**. A form for adding a new domain will open.


Add domain

example.com

Enter the **domain name** and click **Add**. After this, you can proceed with the configuration for the new **protected object**.

Website Migration to Hosting

Migrating your website to a **DDoS-protected hosting** is handled by our **technical support specialists**. To ensure a **successful migration**, the following information is required:

- **Access to the current hosting or server**: login credentials for connection.
- **Access to the control panel**: e.g., **cPanel, ISPmanager**, and others.
- **Access to the CMS admin panel**: for managing website content.
- **List of domains for migration**: all domain names that need to be transferred.
- **Contact phone number**: for urgent communication in case of any issues.

In some cases, additional information may be required:

- **Paths to CMS configuration files**: if they differ from standard locations.
- **Database access**: if these credentials are known.
- **Access to the DNS records control panel**: if our engineers will manage your DNS settings.
- **List of specific software**: if your website uses custom software solutions.
- **List of tests for functionality verification**: if you wish to run specific tests after migration to confirm that your website works correctly.

If any of the required information is missing, please inform our **technical support team**, and we will find a solution.

Important: Domains **not listed** in the initial request will require a **separate migration request**.

If you plan to update **DNS records manually**, it is recommended to **wait for confirmation** from our team before making changes.

VDS/VPS

How the Service Works

The **«Virtual Dedicated Servers (VDS/VPS)»** involves renting a virtual dedicated server with administrative rights. Websites and applications hosted on such a server are protected immediately upon launch.

Service Workflow: Protected VDS/VPS servers are deployed on a fail-safe cluster. A traffic filtration system is in operation—traffic directed to the VDS/VPS is processed by the StormWall system at OSI model layers 3-4, protecting your resources from attacks aimed at overwhelming communication channels and overloading computing capacities. If you are using VDS/VPS for hosting websites, it is advisable to connect protection for incoming HTTP/HTTPS traffic, including the analysis of requests to your server, optimization, and delivery of cleansed traffic.

Technologies Used: VMWare platform is used for creating virtual servers. Triple Filter technology is used for traffic filtration. BanHammer technology is used for filtering HTTP flood. FlowSense technology is used for anomaly detection and automatic attack type determination.

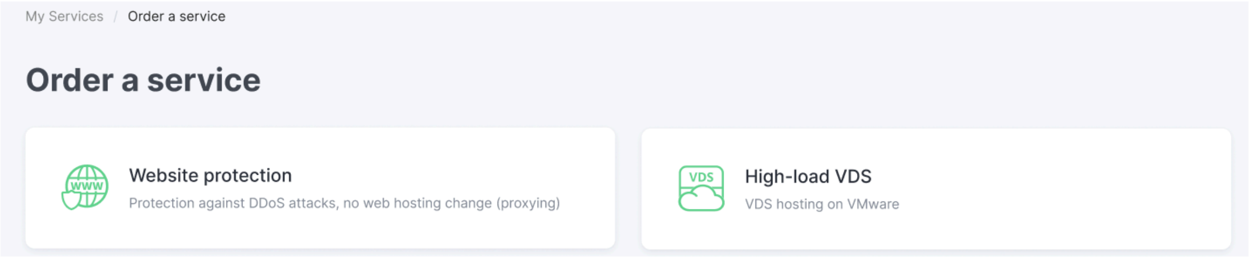
When ordering the service, you can configure:

- The hardware configuration of the dedicated virtual server (number of CPU cores, amount of RAM, SSD storage volume, number of IP addresses);
- Level of protection (basic (no domain), protection up to 3 domains, protection for games and applications);
- Geographical location of the StormWall company's site;
- Whether to enable or disable server administration by StormWall company employees (for an additional fee).

Order

To connect the service:

1. Log into your personal account by authenticating on the website.
2. On the top panel of the website, select the **Billing** tab, following the instructions provided in the «How to connect service» section.
3. In the tab that opens, choose the **High-load VDS** option.



My Services / Order a service

Order a service

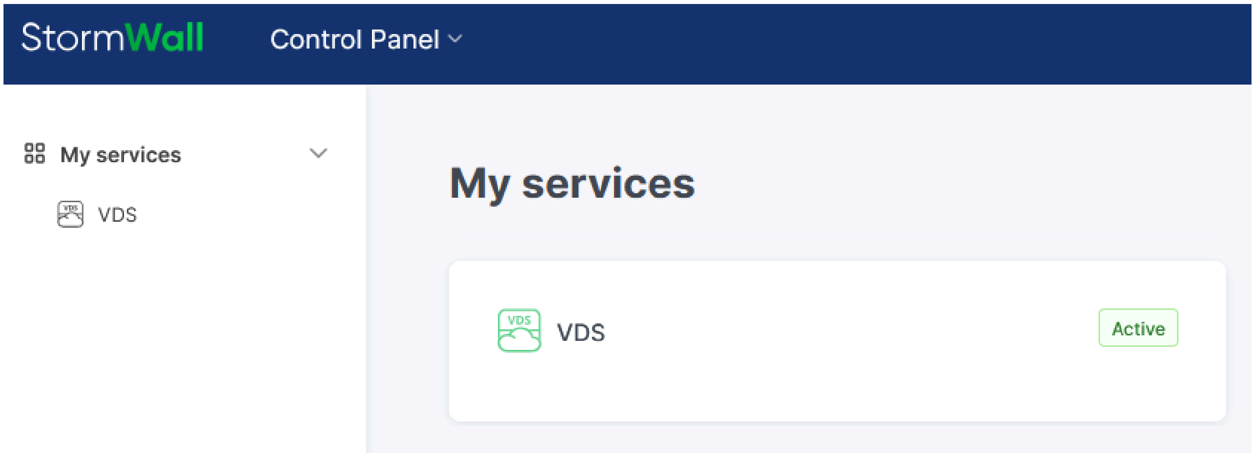
Website protection
Protection against DDoS attacks, no web hosting change (proxying)

High-load VDS
VDS hosting on VMware

4. You will be redirected to a [website page]() with a detailed description of the service.
5. Review the information and submit an application to connect the service on the website.

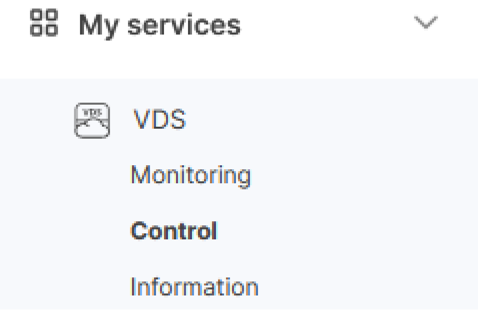
Service Management

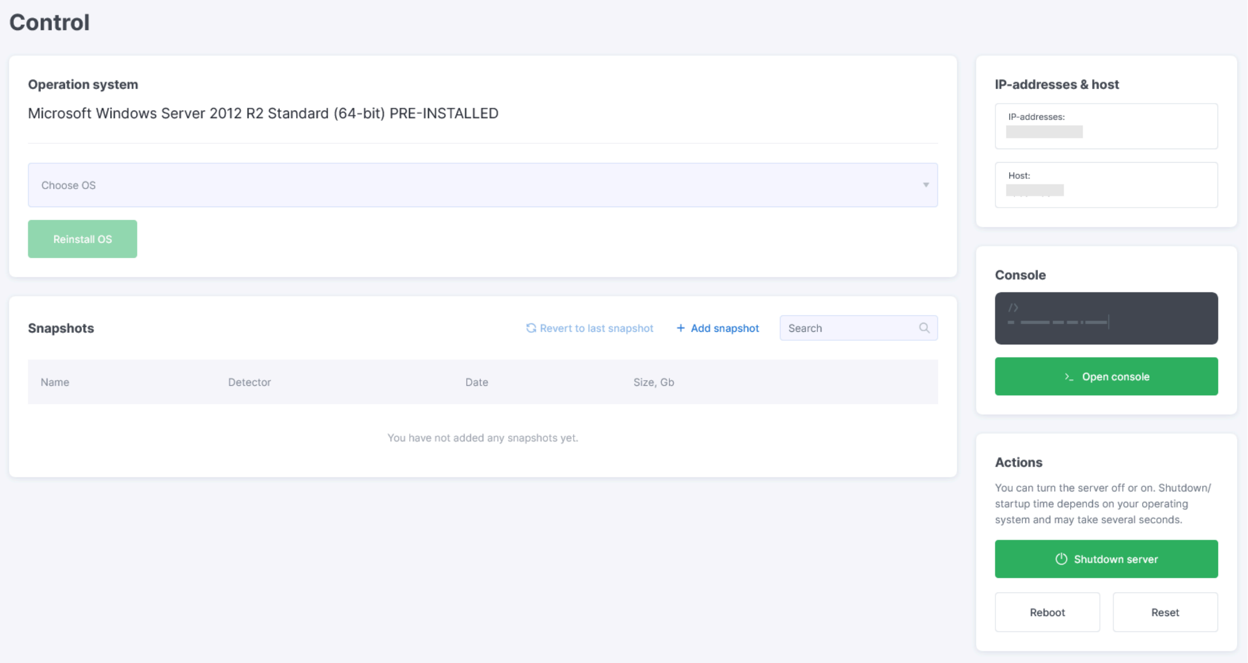
After the service is connected, it will appear on your account's main page and in the **My Services**.



To view details, click on the service name in the center of the page or in the list on the left.

In the opened menu, select **Control**.





Control

Operation system

Microsoft Windows Server 2012 R2 Standard (64-bit) PRE-INSTALLED

IP-addresses & host

IP-addresses: [redacted]

Host: [redacted]

Snapshots

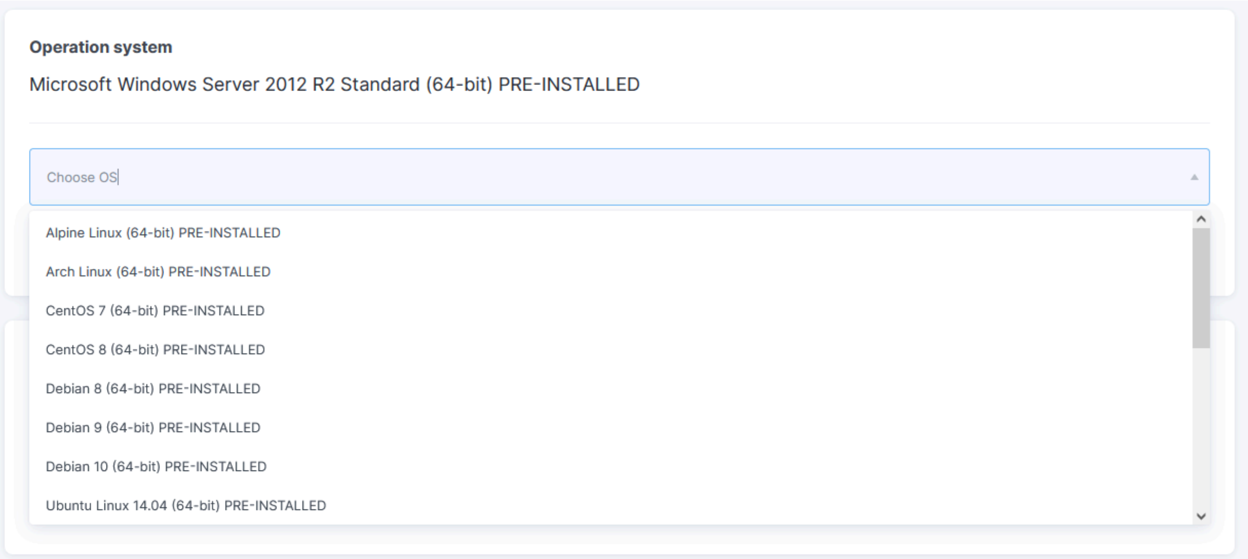
Name	Detector	Date	Size, Gb

You have not added any snapshots yet.

Actions

You can turn the server off or on. Shutdown/startup time depends on your operating system and may take several seconds.

To reinstall the operating system, choose the desired one from the drop-down list and click the **Reinstall OS** button.



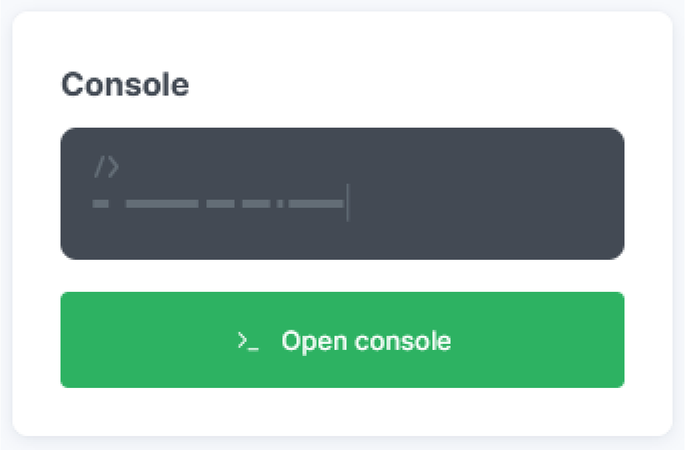
Operation system

Microsoft Windows Server 2012 R2 Standard (64-bit) PRE-INSTALLED

Choose OS

- Alpine Linux (64-bit) PRE-INSTALLED
- Arch Linux (64-bit) PRE-INSTALLED
- CentOS 7 (64-bit) PRE-INSTALLED
- CentOS 8 (64-bit) PRE-INSTALLED
- Debian 8 (64-bit) PRE-INSTALLED
- Debian 9 (64-bit) PRE-INSTALLED
- Debian 10 (64-bit) PRE-INSTALLED
- Ubuntu Linux 14.04 (64-bit) PRE-INSTALLED

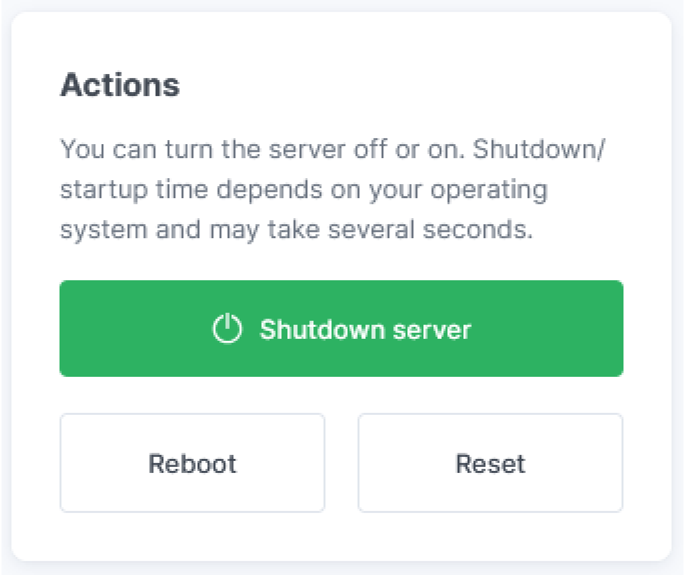
To manage the server, use the console by clicking the **Open console** button. The console will open in a new browser tab.



If the connection is lost, an error message «The console has been disconnected» will be displayed.

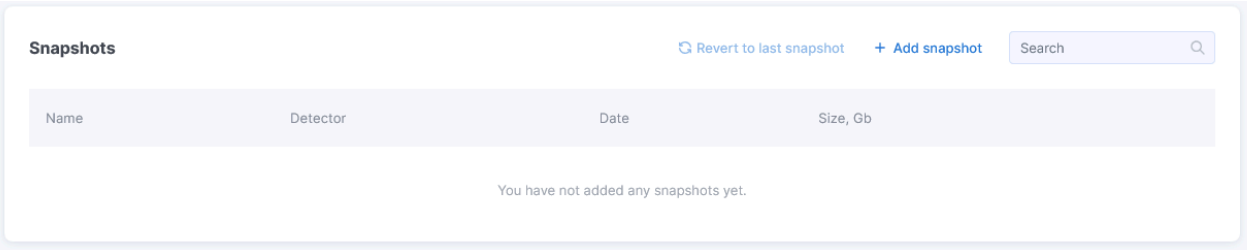
You can also use the RDP protocol to connect to a virtual server with Windows installed, or the SSH protocol to connect to a virtual server with Linux installed. You will receive your login credentials (username and password) by email when this service is activated.

Using the corresponding buttons, you can turn the server on or off, reboot it, or reset it to its default settings.



You can turn the server off or on. Shutdown/ startup time depends on your operating system and may take several seconds.

The **Add Snapshot** button allows you to quickly capture the current state of the system, so that you can restore it from that snapshot if necessary. The number of snapshots you can take depends on your subscription plan.



Name	Detector	Date	Size, Gb

You have not added any snapshots yet.

To view performance charts of your server, select **Monitoring** from the left menu.

You can set the time range for which the information will be displayed.

To view your server’s specifications, select Information from the left menu.

In the opened area, you can monitor all parameters of your server.

API

How to Use the API?

What is an API?

An API (Application Programming Interface) is an interface that allows two applications to interact with each other using predefined sets of commands.

The API enables the management of objects within ordered services—such as adding and removing domains, updating configuration parameters, retrieving attack history, and more. Through this interaction, you can also retrieve or add information to your personal account, automatically extract service lists, manage "black" and "white" user lists, and much more.

Detailed descriptions of commands and data models for requests and responses can be found at the following addresses:

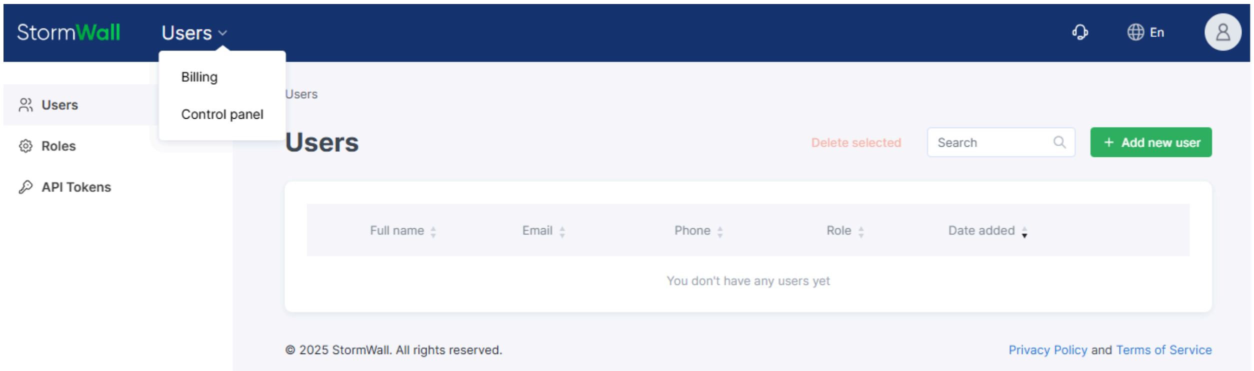
- **StormWall API v1** — https://api.stormwall.pro/documentation
- **StormWall API v2** — https://apiv2.stormwall.pro/swagger-public

How to Create a Token?

To ensure secure access to information from your personal account, authentication is implemented based on tokens.

When requesting information from your device, it will be authenticated using an authentication token, just as you would use a login and password to access your personal account.

1. Go to the new control panel using any of the options available in your personal account.
2. Tokens created in the new personal account are valid indefinitely!
3. Open the **Users** tab in the top-left section of the screen. This will reveal the menu options: **Users**, **Roles**, and **API Tokens**.



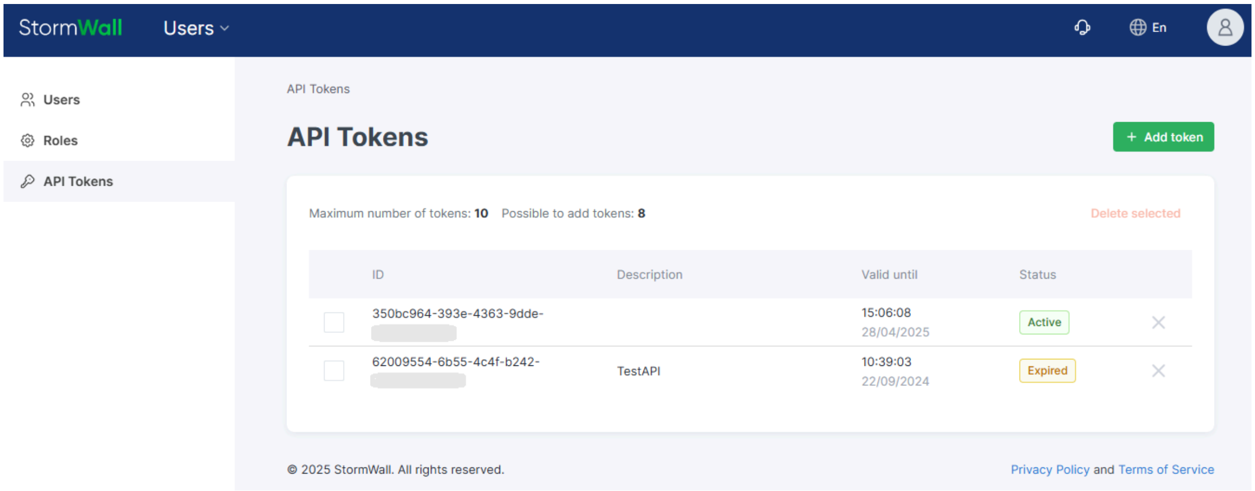
Users

Full name	Email	Phone	Role	Date added

You don't have any users yet

© 2025 StormWall. All rights reserved.

4. Click on **API Tokens**.



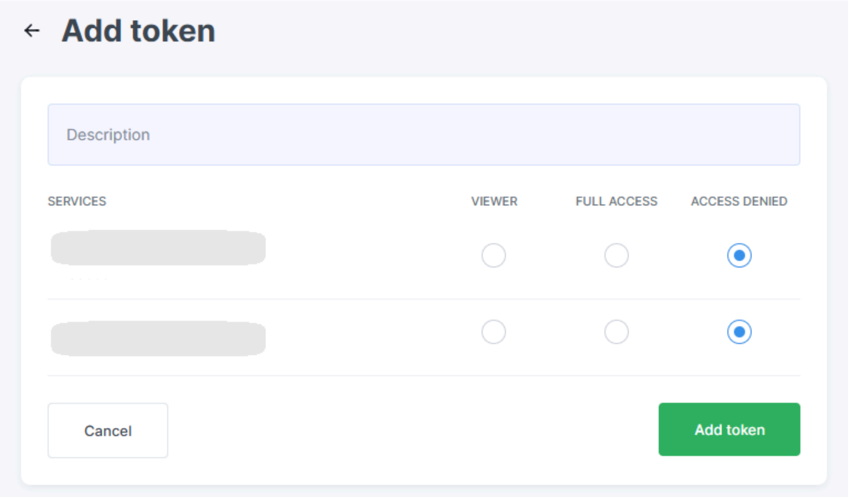
API Tokens

Maximum number of tokens: **10** Possible to add tokens: **8**

	ID	Description	Valid until	Status	
□	350bc964-393e-4363-9dde- [redacted]		15:06:08 28/04/2025	Active	✕
□	62009554-6b55-4c4f-b242- [redacted]	TestAPI	10:39:03 22/09/2024	Expired	✕

© 2025 StormWall. All rights reserved. Privacy Policy and Terms of Service

5. On the newly opened page, you can add or delete tokens.
6. To add a new token, click **+ Add Token**.

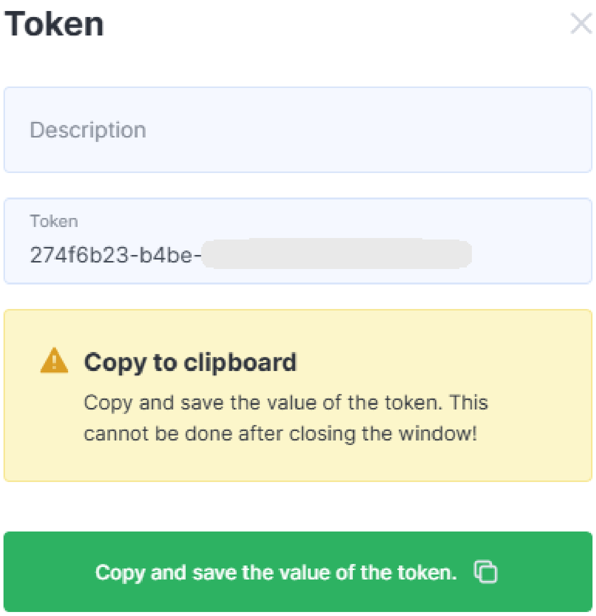


Add token

Description

SERVICES	VIEWER	FULL ACCESS	ACCESS DENIED
[redacted]	○	○	●
[redacted]	○	○	●

7. Select access permissions for the token. You can add a description in the **Description** field or leave it blank.
8. Click **Add Token**.



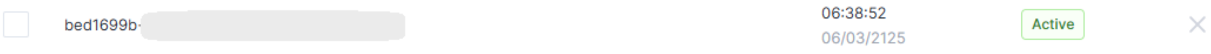
Token

Description

Token
274f6b23-b4be-[redacted]

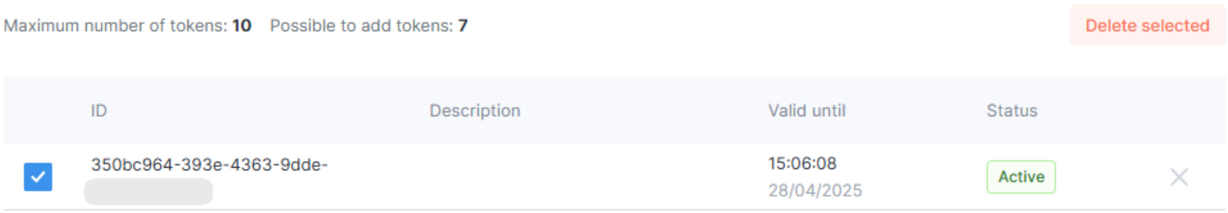
Copy to clipboard
Copy and save the value of the token. This cannot be done after closing the window!

9. Be sure to copy the generated token — click **Copy to Clipboard and Close**.
10. A new row with the status «Active» will appear in the token table.



□	bed1699b-[redacted]	06:38:52 06/03/2125	Active	×

11. You can delete expired tokens by selecting them and clicking **Delete Selected**.



Maximum number of tokens: **10**   Possible to add tokens: **7**

	ID	Description	Valid until	Status	
☑	350bc964-393e-4363-9dde- [redacted]		15:06:08 28/04/2025	Active	×

Each token has a unique **ID**, which can be used to identify actions performed with that token (e.g., creation, deletion) in the request log.

API Interface Description

The API uses a **REST** interface and only built-in HTTP functions, which are understood by any standard HTTP client.

- For ease of proxying and monitoring, object identification data is always passed as part of the URL path.
  - Example: `GET /user/service/1/domain/2`, where `1` is the service ID, and `2` is the domain ID.
- For lists in read commands, request parameters with a repeating key are used.
  - Example: `GET /user/service/1/domain/stats?domain_id=3&domain_id=6`.
- All other data for modifying commands is sent in the request body in JSON format.
- Responses are always returned in JSON format, including error messages, except for conversion commands.

Request Size Limits:

- **Maximum request body size:** 1 MB
- **Maximum header size:** 8 KB

Error Handling in the API

There are **two levels** of error indication in the system:

1. HTTP status code
2. Error code list in the response

- An HTTP status other than **«200»** indicates a **critical** error from either the user or the system.
- If the HTTP status is **«200»**, the error list contains only **non-critical** errors (warnings).

If the API returns a **critical** error, no actions have been taken on the objects, and the request can be retried, possibly with corrected data.

- Example: If a command requires a **domain name**, but an invalid string (e.g., with spaces) is submitted, the API will return **«400»** («Bad Request»).

If at least one non-critical error appears in the list, it means that some operations have already been performed, possibly on physical hardware. These errors do not cause object malfunctions but may require additional actions.

- Example: If an SSL certificate installation returns a **non-critical** error, it means that while the certificate format is correct, the system refuses to install it for the given domain because the domain name does not match the certificate records.

HTTP Methods and Their Actions

HTTP Method	Action
POST	Create a new object
GET	Retrieve object information
PUT	Update object information
DELETE	Delete an object

HTTP Response Status Codes

Status Code	Description
200	Request successfully executed
400	Invalid command input data
403	Command or input data is not allowed for the specified token
404	Command not defined in the system
405	Method not applicable to this command

501	This command is under development
503	System functionality is currently unavailable or request limit exceeded
500+	Internal system errors

Fields in "Critical" Error Responses

Field Name	**Type**	**Description**
statusCode	Number	Numeric HTTP status representation
error	String	String representation of the HTTP status
message	String	Description of the error reason

Example Response:

json

```
{
  "statusCode": 400,
  "error": "Bad Request",
  "message": "Invalid request params input"
}
```

Fields in "Non-Critical" Error List (`error_list`)

Field Name	Type	Description
type	Number	Error category
code	String	Error code

Example Response:

json

```
{
          "error_list": [{ "type": "SSL", "code":
"INVALID_CERT_KEY_PAIR" }]
}
```

API Authentication and Token Usage

Most commands require authentication via an **API token**. The token is passed using the **Cookie** header with the name `api_access_token`.

Getting Started with API Token Authentication

1. **Generate a token** (as explained earlier).
2. **Test API requests in Swagger documentation**:
    - Open an endpoint in the API documentation.

Enter your active token in the **cookie** field:

```
ini
api_access_token=eyJhb…
```

- Fill in the other endpoint parameters.
- Click **Try it out**—this will generate a **cURL request string**.

Using cURL Requests on Different Systems

- The generated cURL request works on **Linux**.
- On **Windows**, replace **single quotes (' ')** with **double quotes (" ")** or use a Linux-like terminal such as **Git Bash**.

API Documentation & Support

For each command in the API documentation, you can view **data models** for responses and complex parameters by switching to the **Model** tab. The models specify field types and provide short descriptions.

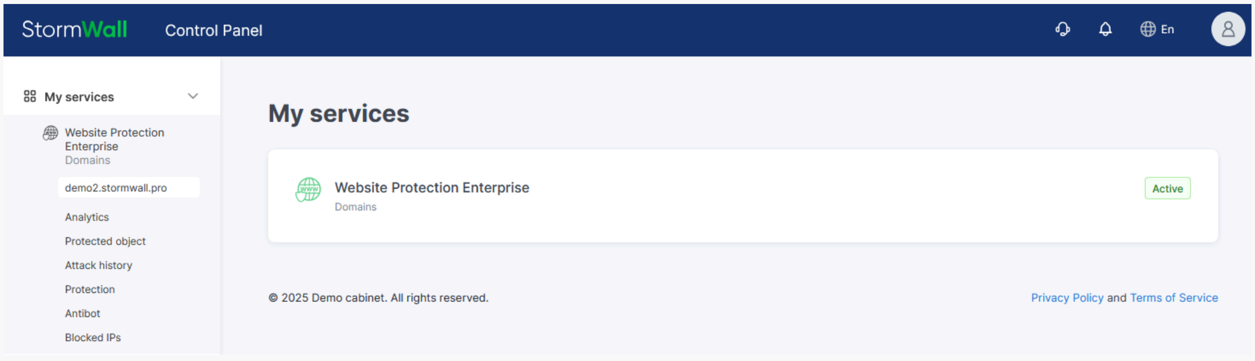
If you have any difficulties using the API, please contact **support** via:

- **Live chat on the website**
- **Support request form in your personal account**

FAQ

How to find out if an IP address is blocked? How to block and unblock an IP address?

Find the service for which you need to view information in the client panel, for example, **Website Protection**.



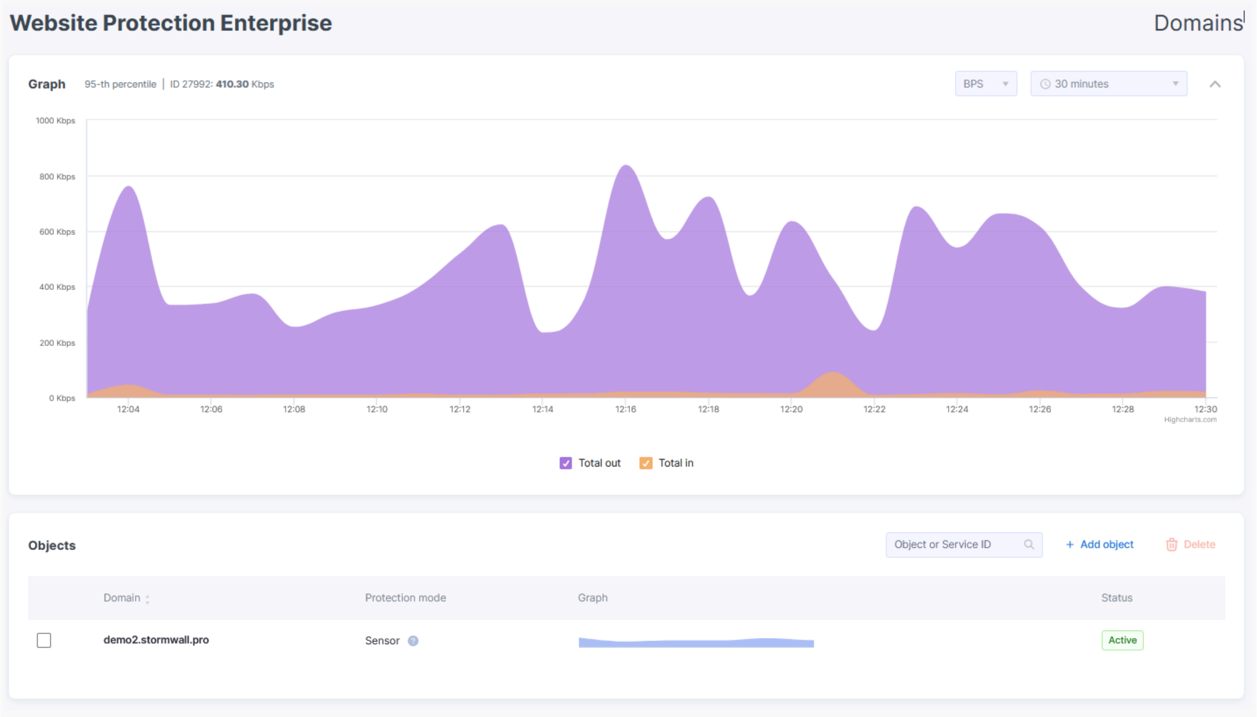
My services

Website Protection Enterprise
Domains
Active

© 2025 Demo cabinet. All rights reserved.

Privacy Policy and Terms of Service

Click on the line with the **Website Protection** service. A page with information about the service will open. Below the graph, a list of protected objects will be displayed.



Website Protection Enterprise

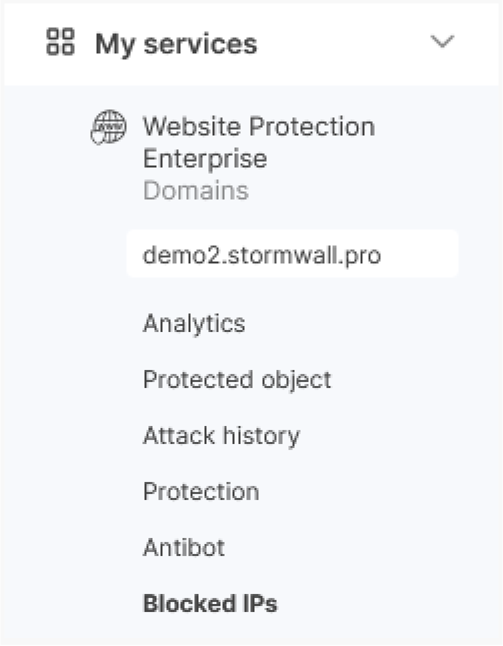
Domains

Graph 95-th percentile | ID 27992: **410.30** Kbps

Objects

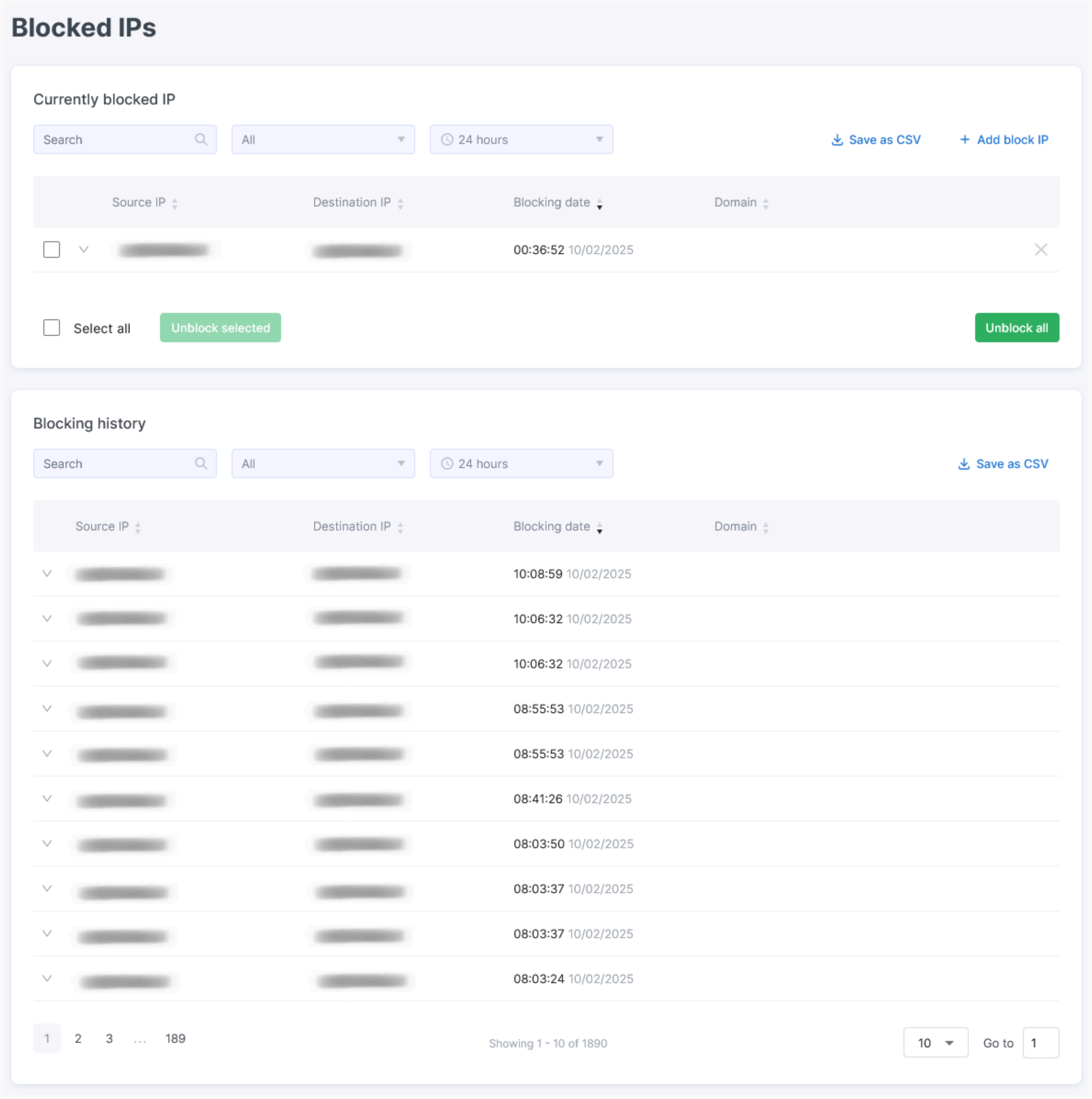
	Domain	Protection mode	Graph	Status
□	demo2.stormwall.pro	Sensor		Active

Click on the object you are interested in. A menu will appear on the left side of the page.



Choose the **Blocked IPs** menu item. A page will open with two sections: currently blocked IPs and a block history.

You can view the blocked IP addresses in the upper section of the page. There, you can use a time filter and a search box.



Blocked IPs

Currently blocked IP

	Source IP	Destination IP	Blocking date	Domain	
□	[redacted]	[redacted]	00:36:52 10/02/2025		✕

Blocking history

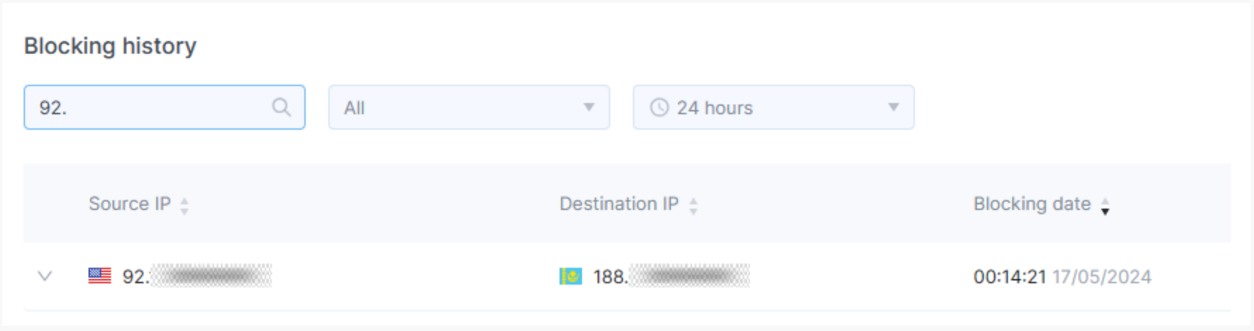
Source IP	Destination IP	Blocking date	Domain
[redacted]	[redacted]	10:08:59 10/02/2025	
[redacted]	[redacted]	10:06:32 10/02/2025	
[redacted]	[redacted]	10:06:32 10/02/2025	
[redacted]	[redacted]	08:55:53 10/02/2025	
[redacted]	[redacted]	08:55:53 10/02/2025	
[redacted]	[redacted]	08:41:26 10/02/2025	
[redacted]	[redacted]	08:03:50 10/02/2025	
[redacted]	[redacted]	08:03:37 10/02/2025	
[redacted]	[redacted]	08:03:37 10/02/2025	
[redacted]	[redacted]	08:03:24 10/02/2025	

Showing 1 - 10 of 1890

If there are currently blocked IP addresses, they will appear in the upper section of the page. Select them by ticking the boxes next to each address individually or select **Select all**. When the IP addresses are selected, press the **Unblock selected** button.

To unblock all IP addresses, press the **Unblock All** button.

To find out if a specific IP address has been blocked in the past, you can search for it in the **Blocking history** table using the search field.

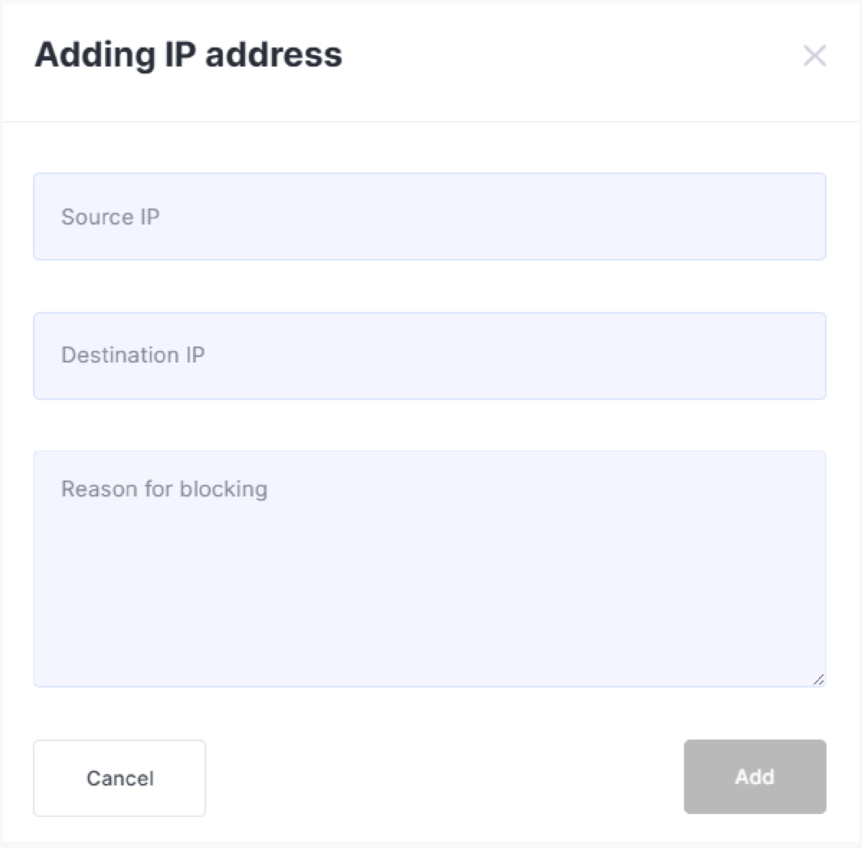


Blocking history

92.

Source IP	Destination IP	Blocking date
92.[redacted]	188.[redacted]	00:14:21 17/05/2024

To block an IP address, press the **Add block IP** button at the top of the page.



Fill in the form that opens and press the **Add** button.

Done! The IP address is blocked for 2 hours. To block an IP address for a different period, contact support.

How to configure equipment for the L7 protection option?

After selecting a protected IP address, you will receive instructions describing the necessary settings and commands to execute them.

With these instructions, you will need to perform the following:

- Add our serving networks to the exceptions of your firewall;
- Configure the detection of the real IP address of site visitors;

- Block direct connections to your server from external sources.

According to the instructions, you will:

- Change the A-record of your domain in DNS to the protected IP address;
- Add our outgoing addresses to the trusted list, removing restrictions;
- Close access to ports 80 and 443 for all networks except local connections and connections from our serving networks;
- Restart the web server;
- Configure Nginx by modifying the configuration file;
- Configure Apache by modifying the configuration file.

For IIS, you will need to follow the actions in the instructions.

If you have any questions while setting up, please contact support.