STORMWALL SERVICES

User Manual

Version 0.1

Contents

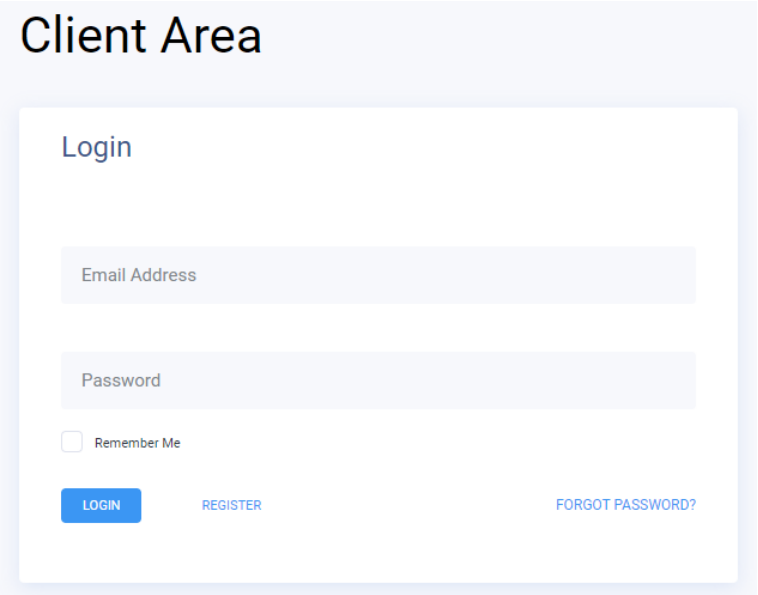
Registration 3
Client Area 5
User information 6
Balance 9
Billing 10
Active products/services 10
Recent Requests 11
Announcements 13
StormWall's top menu 14
My services 15
Invoices 15
Partnership 15
Support 15
Cart 16
Account 16
Switching language 19
StormWall Services 19
DDoS Protection 19
How a DDOS attack happens 19
How protection works 20
Webite protection 20
How the service works 20
Ordering a service 21
Service management 24
Advanced sensor settings 28
View attack history 30
Traffic details 31
Sample 32
Anti-DDoS Hosting 32
How the service works 33
Ordering a service 33
Service management 34
DDoS protection for TCP/UDP services 36
How the service works 37
Ordering a service 37
Service management 38

View attack history 39
Traffic details 40
Protecting the network from DDoS attacks using BGP 40
How the service works 40
Ordering a service 42
Service management 42
IP-transit 42
How the service works 43
Ordering a service 44
Service management 44
Servers & VPS 44
VDS/VPS DDoS servers 44
How the service works 44
Ordering a service 44
Service management 46
Dedicated servers 48
How the service works 48
Ordering a service 48
Service management 48
Colocation 48
How the service works 49
Ordering a service 49
Service management 49
CDN&WAF 49
Content delivery network (CDN) 49
How the service works 49
Ordering a service 50
Service management 50
Cloud WAF 50
How the service works 50
Ordering a service 50
Service management 51
API for clients 51
How the service works 51
Glossary 51

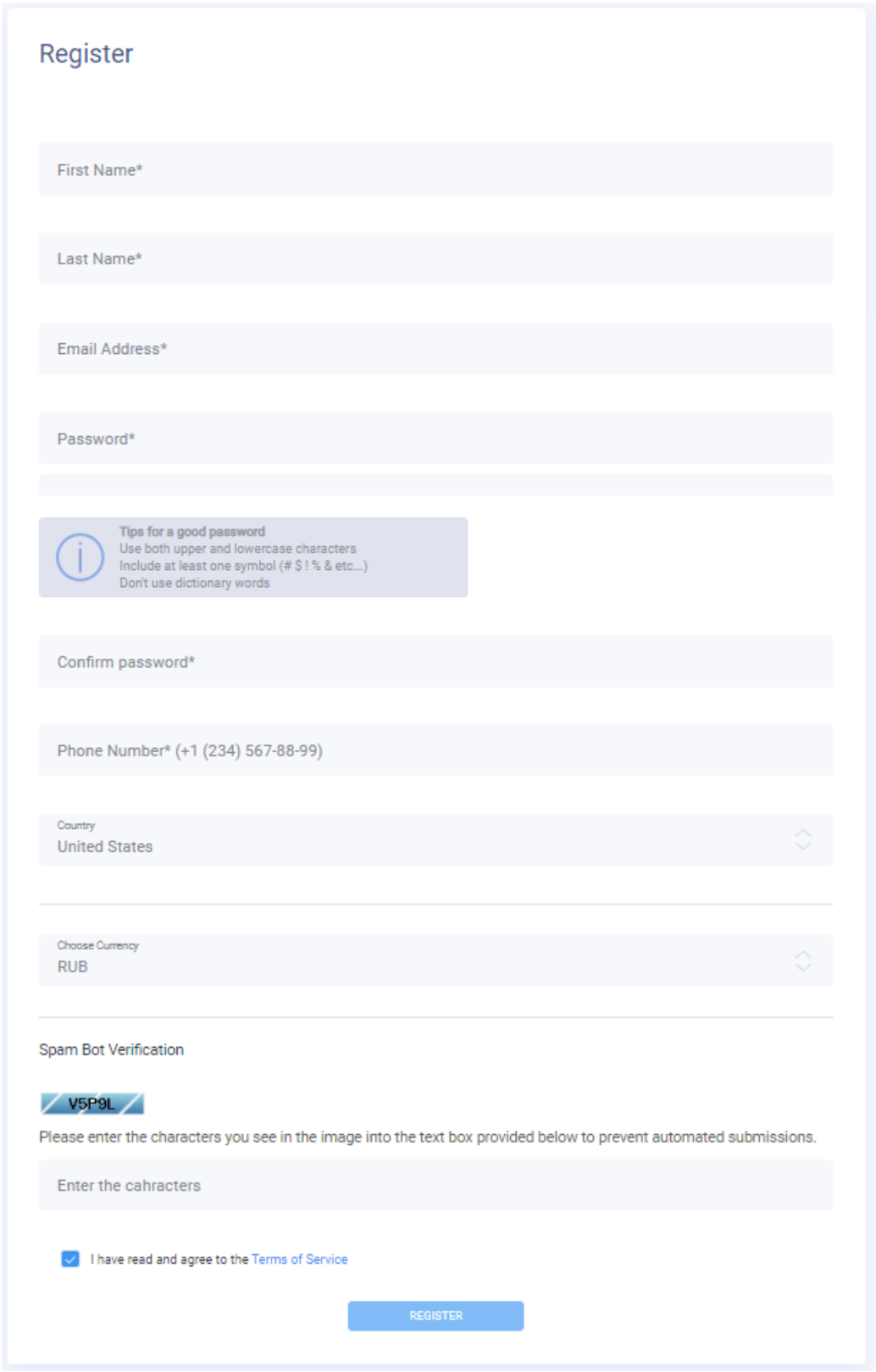
Registration

In order to start using StormWall's services, you need to register as a new user. To do this, follow these steps:

- Type this address in the search bar https://stormwall.pro;
- On the top menu press Registration | Enter;
- **Client Area** login window will open;



- Select **Register**;
- Fill in the new user registration form:
  - Fields **First Name**, **Last Name**, **Email Address**, **Password** (with confirmation) and **Phone Number** are required. Other fields are optional. Please enter valid data. In case of loss of access, the specified information will be used to restore it.
  - Entering a password, you can use **Tips for a good password**.
  - To protect against spambots, enter a code, generated in a special field.
  - Do not forget to check the **I have read and agree to the Terms of Service** box.



- Press **Register**;
- Registration is complete. To the Email address specified during registration you will receive a letter with confirmation, password and other entered information.

Client Area

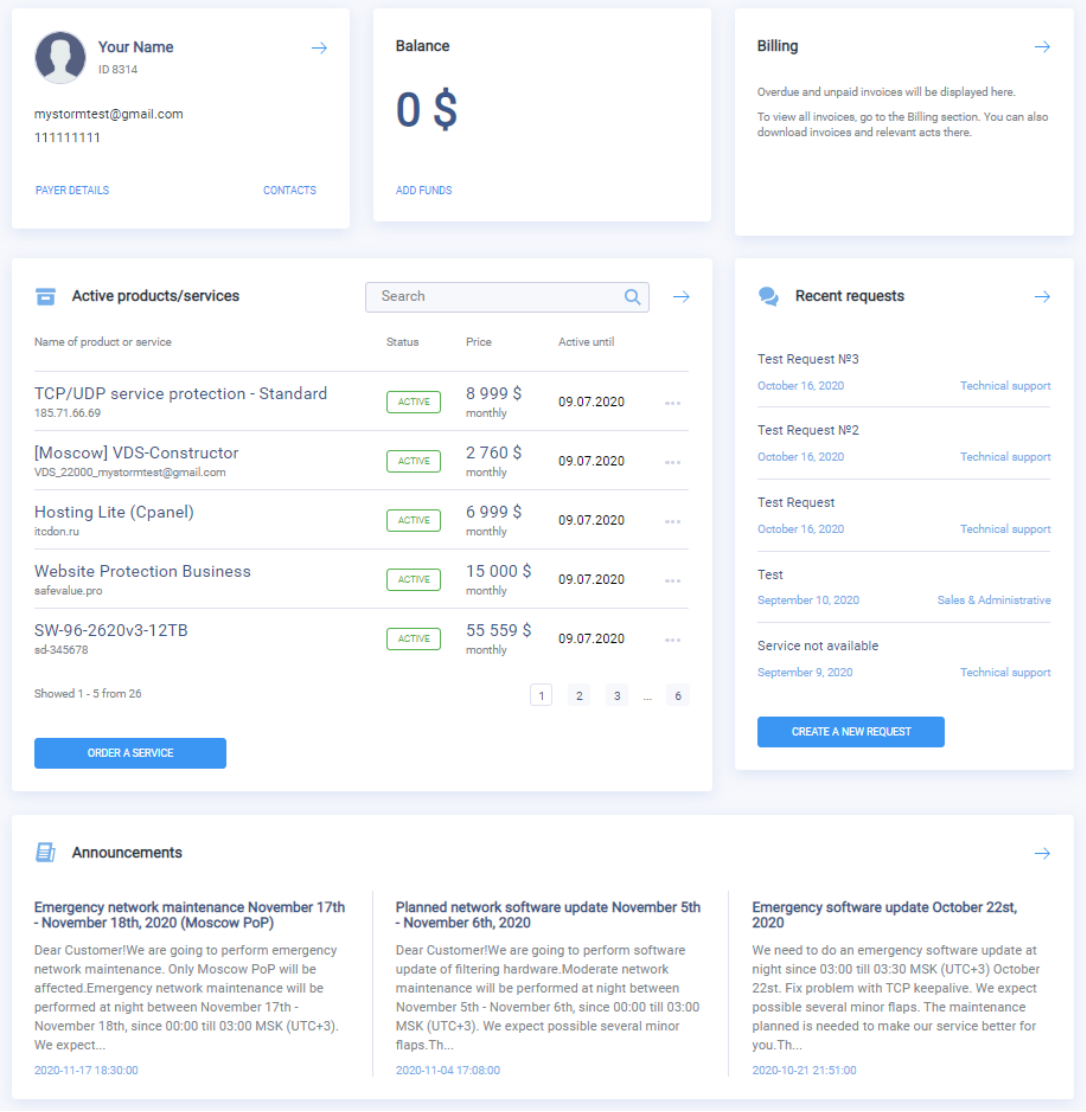
To enter the **Client Area**, you must be registered on the StormWall Portal as a service user. To enter the **Client Area**, follow these steps:

- Type this address in the search bar https://stormwall.pro;
- On the top menu press: Registration | Enter;
- Enter your Email address and password to the **Client Area** window;
- To avoid having to enter your Email address and password again, check the box **Remember Me**;
- Press **Login**.

If you forgot your password press **Forgot Password?.** Password recovery window will open. Enter your Email address and follow the further instructions.

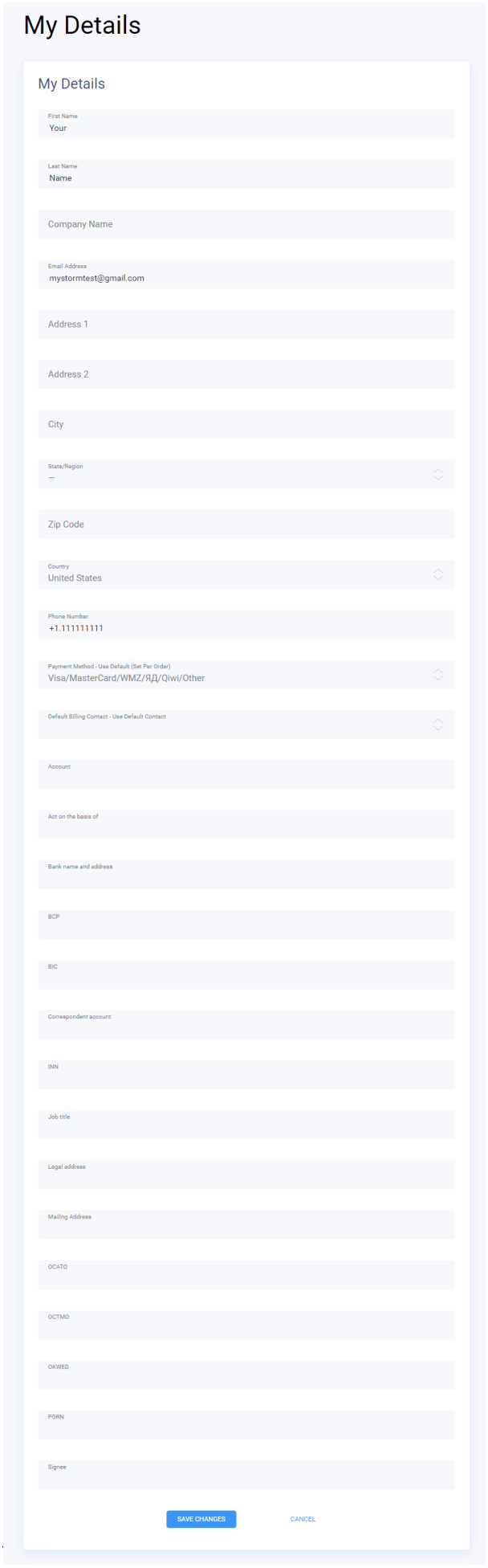
Client Area includes six blocks:

- User information;
- **Balance**;
- **Billing**;
- **Active products/services**;
- **Recent requests**;
- **Announcements**.



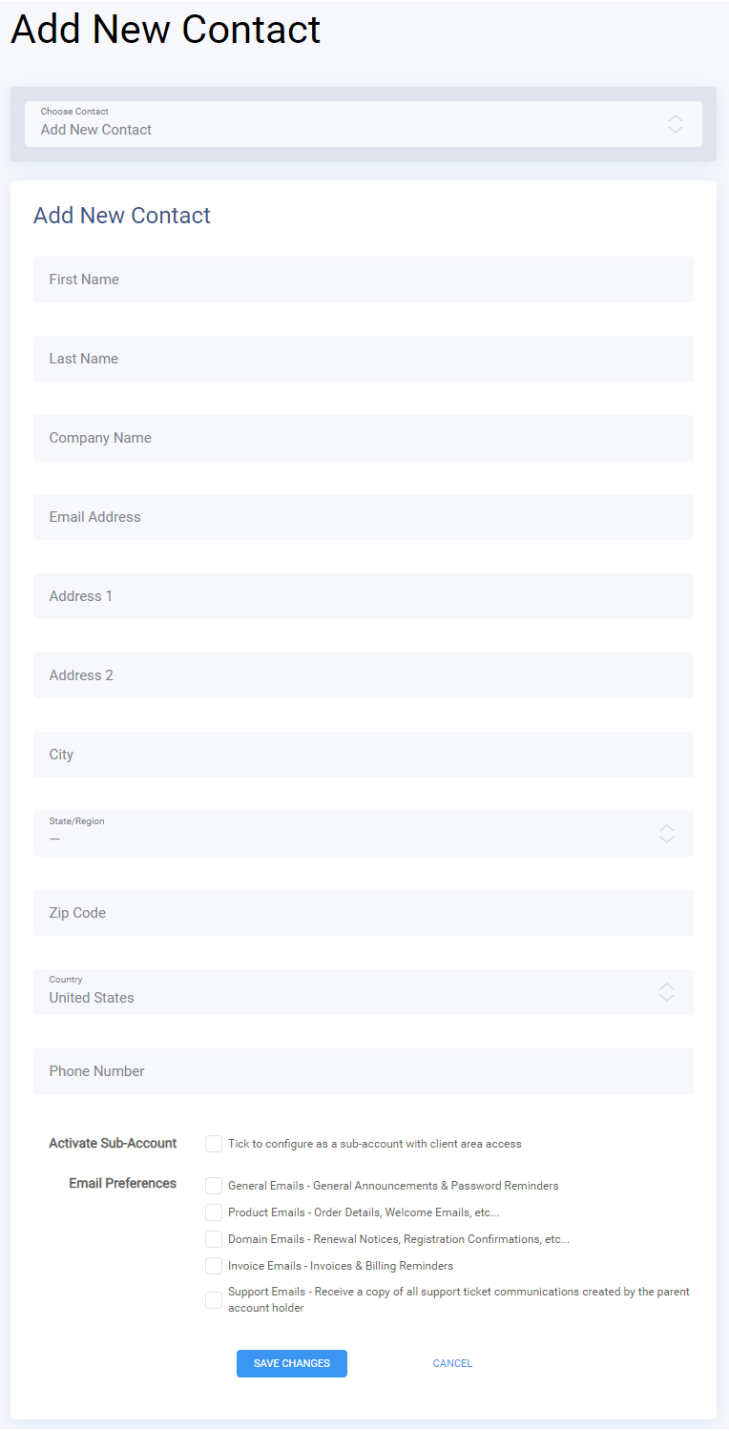
User information

The block includes the data entered during the registration process: your **First Name, Last Name, Email address, Phone number** and **ID**, assigned by the system. To enter additional data (physical address, company name, payment information, etc.), click on the button →. In the opened form, enter the information you need and click **Save Changes**.

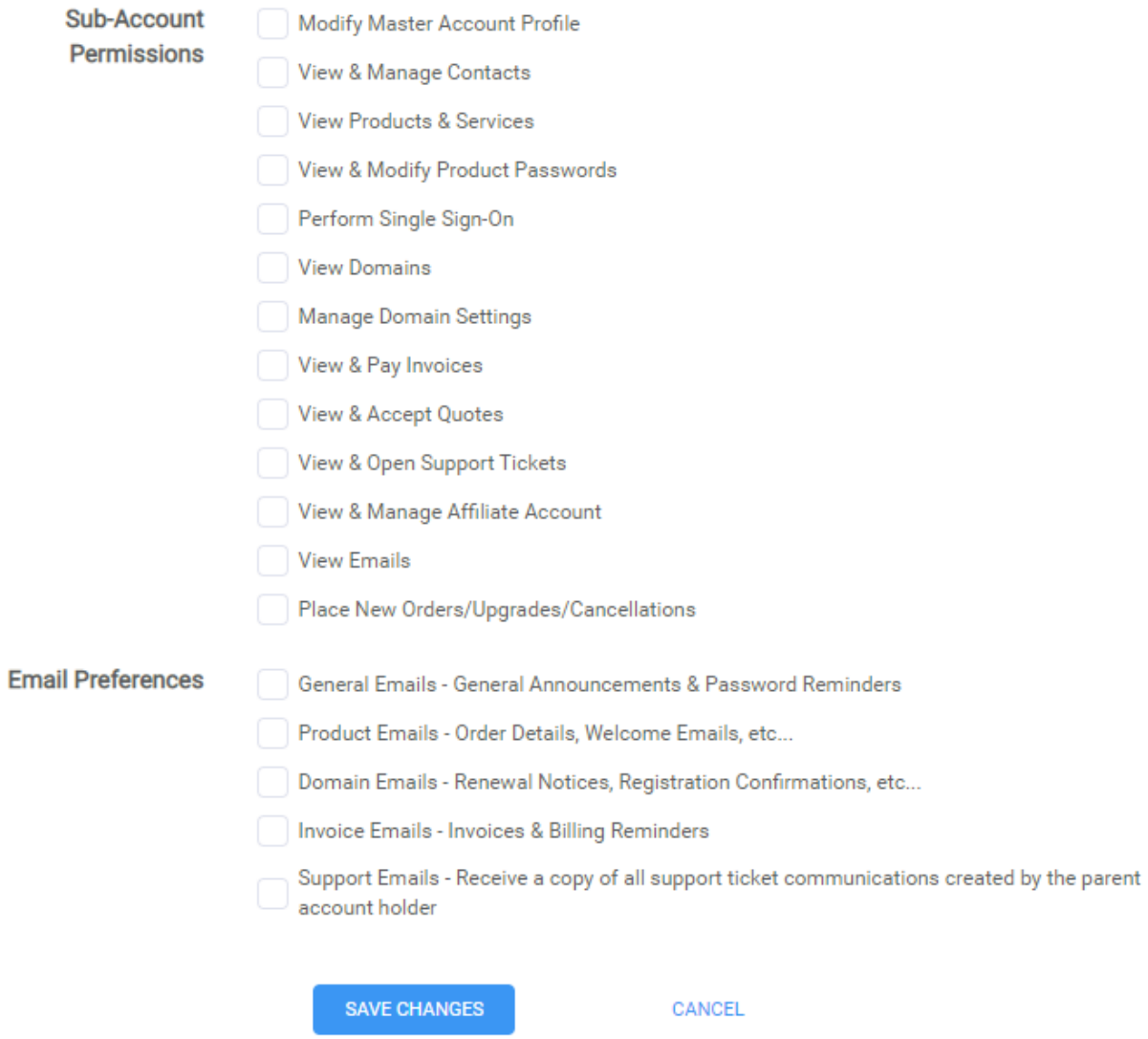

My Details
My Details
First Name
Your
Last Name
Name
Company Name
Email Address
mystormtest@gmail.com
Address 1
Address 2
City
State/Region
—
Zip Code
Country
United States
Phone Number
+1.111111111
Payment Method - Use Default (Set Per Order)
Visa/MasterCard/WMZ/ЯД/Qiwi/Other
Default Billing Contact - Use Default Contact
Account
Act on the basis of
Bank name and address
BCP
BIC
Correspondent account
INN
Job title
Legal address
Mailing Address
OCATO
OCTMO
OKWED
PGRN
Signee
SAVE CHANGES
CANCEL

To enter the data on the payer click on the button **Payer details**. In the **Payer details** window fill in all the necessary fields and click **Done**.

To add new contacts associated with your account, click **Contacts**. On a new page, fill in the **Add New Contact** form. Enter information about a new user.



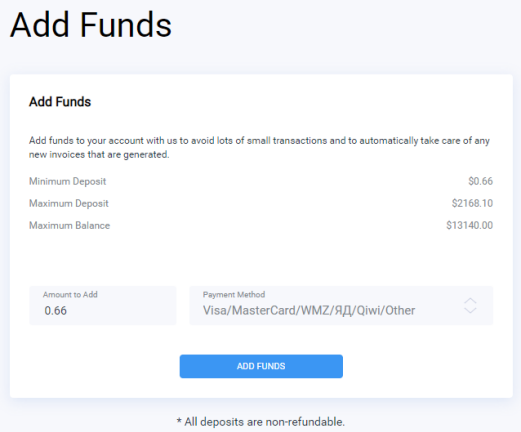
If you want a new user to have access to your **Client Area,** tick **Activate Sub-Account.** In the open form, enter login (Email address) and password for the new user, and tick the rights that you would like to give to a new user in the **Client Area**.



In the **Email Preferences** menu, tick those types of emails that a new user should receive. When you've finished adding a new user, click **Save Changes**.

Balance

The **Balance** block shows the state of your account's credit balance. The amount is in the currency that was chosen at the registration. To top up your balance, click **Add Funds**. In a new window, specify the amount you top up and choose a payment method.

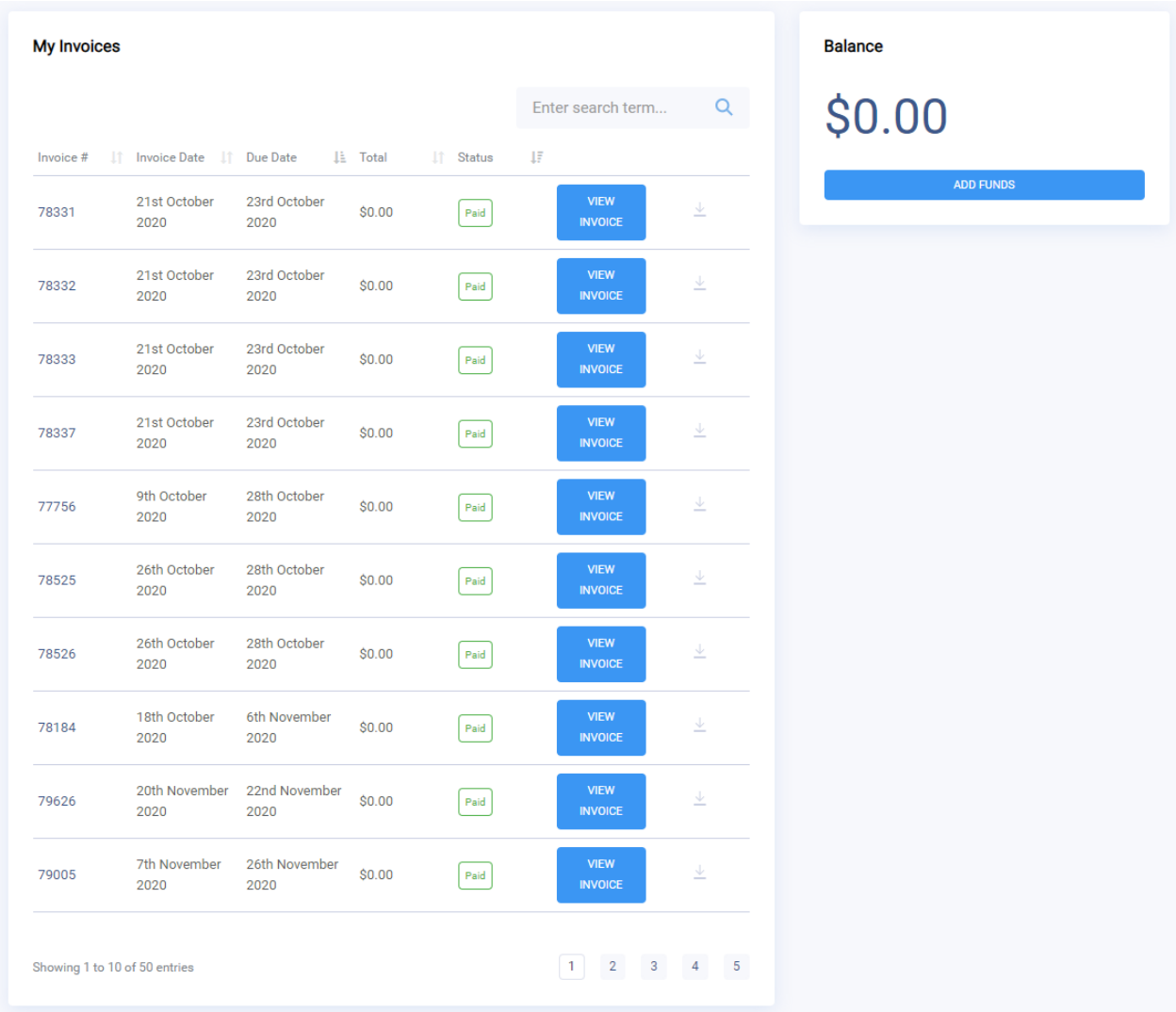


Click **Add Funds**. Depending on the payment method you choose, the system will divert you to a secure payment gateway where you can safely make a payment. We recommend replenishing the balance for the required amount. In this case, the billing may be made from the user's credit balance.

Billing

Block **Billing** displays a list of user accounts: paid, unpaid, overdue. For a detailed view of each bill category, click **X Unpaid Bills, X Paid Bills,** or **X Overdue Accounts**. To see the full account information, click →.

My invoices page shows all StormWall user bills. For each invoice, the status is: **Paid** or **unpaid**. You can read about each invoice by clicking **View invoice** or downloading it to your computer in PDF format, to do so, click ↓. All invoices you will also be able to receive by email, specified at registration.

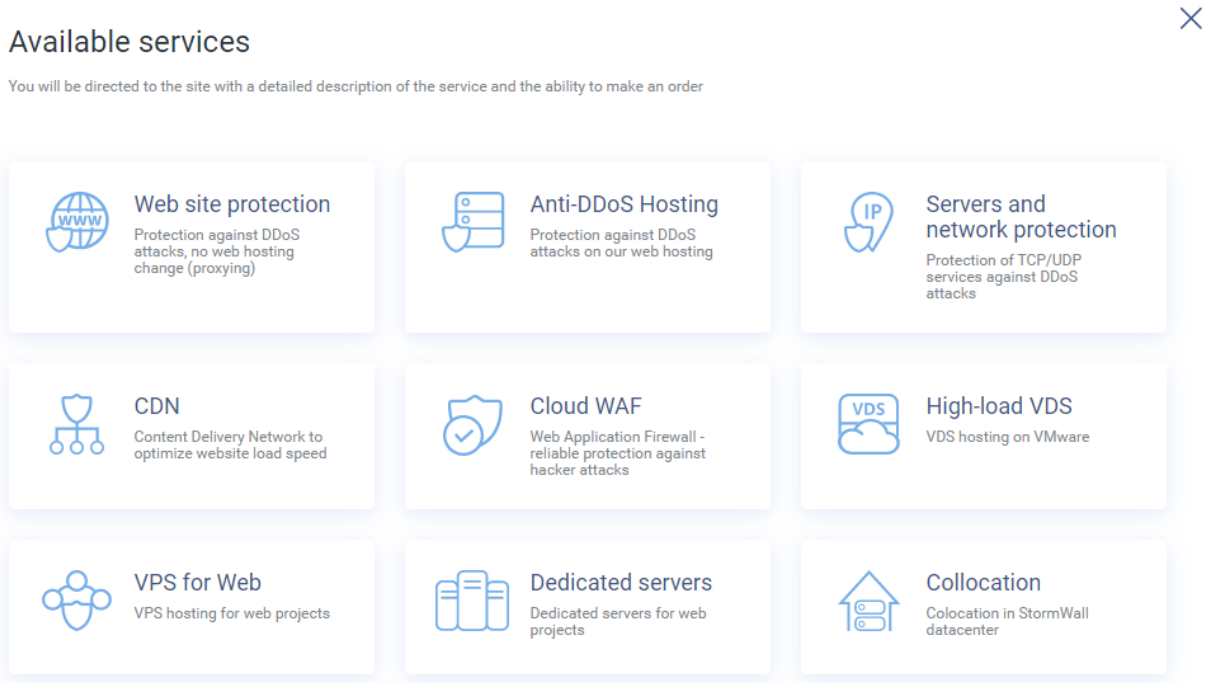


To the right of **my account** menu is **the Balance** menu, with which you can top up your user account credit balance (see Balance).

Active products/services

The **Active products/services** unit is designed to connect the products and services that StormWall offers its customers. Initially, the block contains an inscription **You don't have any active services**.

To go to StormWall's product and services directory, click **Order a service**. On the Available services page, choose the product or service you want to connect. For more information on how to connect each product or service, see the section on this product or service.



When you click →, located in the top right corner of the **Active products/services** block, a page opens that contains a list of already connected products and services. If you haven't connected any product or service yet, you'll see the inscription **You don’t have any active services**. Underneath it is a button **Order a service**, clicking on which you also end up in the directory **Available services**.

Recent Requests

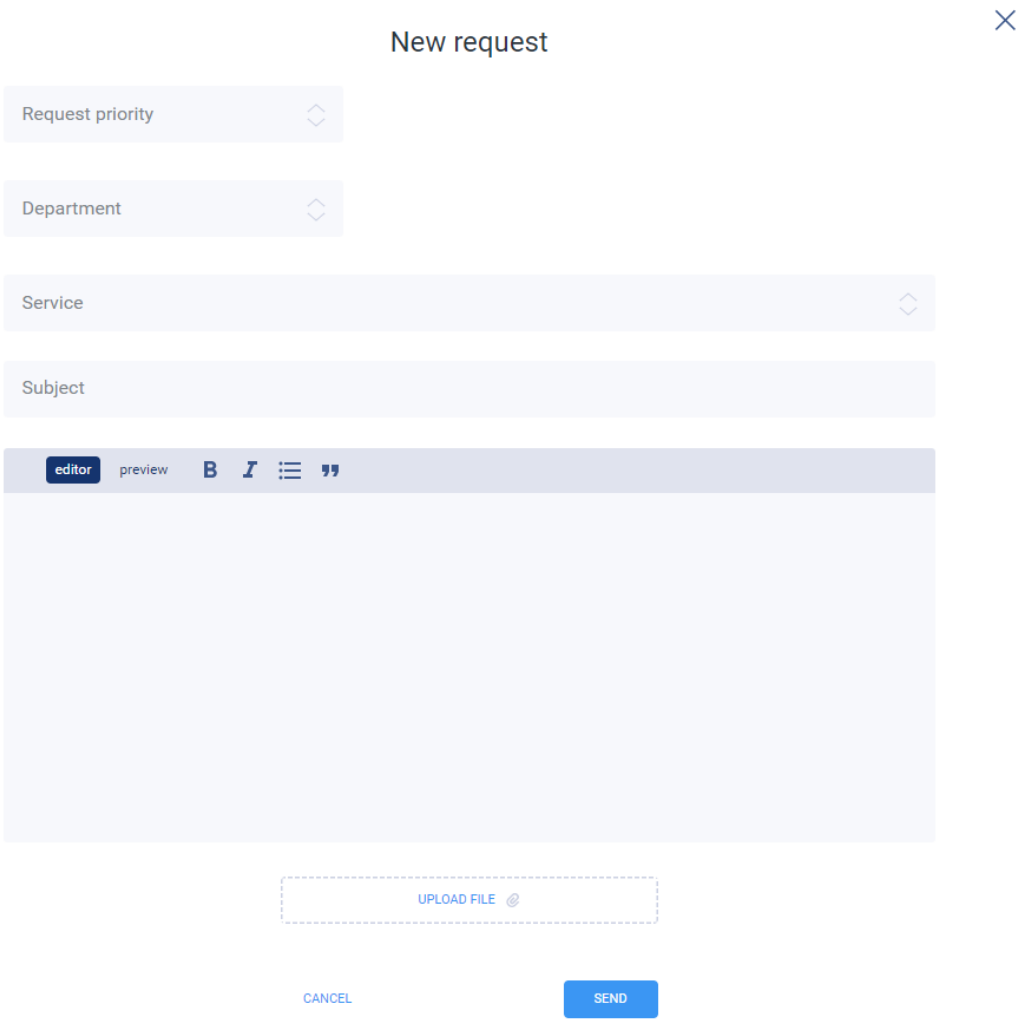
The **Recent Requests** block groups messages to StormWall's technical support team.

To submit a new request, click **Create a new request**. **New Request** form opens. Fill its fields:

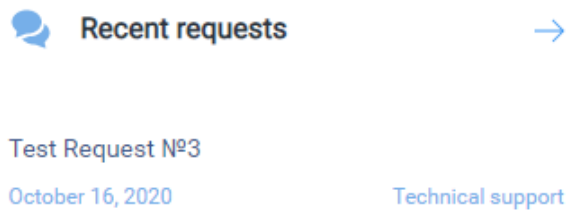
- **Request priority** (choose **High**, **Medium**, **Low**). The priority depends on the criticality of the problem. The response time and fix of the problem depends on the plan and ranges from 15 minutes to 60 minutes. For low-priority issues, the time of the decision may not be regulated. The nature of the problems is divided into priorities as follows:
    - **High** – Inefficiency of sites or basic services, or parts of sites and services; Complete inoperability of protection at the time of attack; a security failure that critically impacts services. This category also includes situations where you need to get information from StormWall "here and now." For example, when working on a client's servers.
    1. **Medium** – Any problems that directly affect the stability of the system as a whole; the need to adjust the current uptime (continuous operation) of the system. For example, the service is under attack, the defense works, but the nature of the attack changes, respectively, need to reconfigure the defense.
    - **Low** – any other problems and issues.
- **Department** - Select from the list:
    - **Technical support;**
    - **Sales & Administrative;**
    - **Other issues.**
- **Service** – Select from a list of connected services.
- **Subject** – briefly specify the topic of the request.

1. In an editing form, describe the problem in detail. If necessary, attach a screenshot or other file by clicking Upload file.

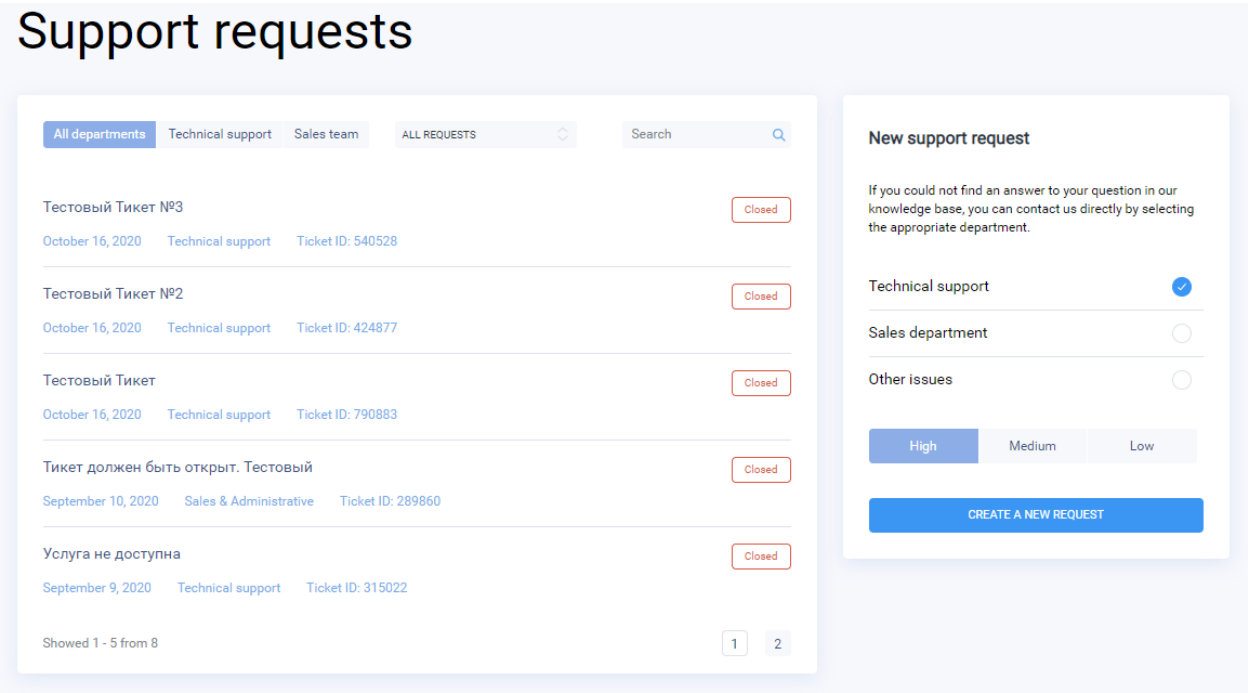
- Click **Send**.



After you have submitted your request, it will be available in the **Recent Requests** in **Client Area**.



When you press the button → **Support requests** page will open. On it you can see the full list of cases with the department to which it is addressed, as well as status and ID. Чтобы найти в списке нужное обращение, воспользуйтесь формой поиска. You can open a previously sent request and supplement it or delete it. When you receive an answer to your request, you can assess how much the answer helped solve your problem or question.

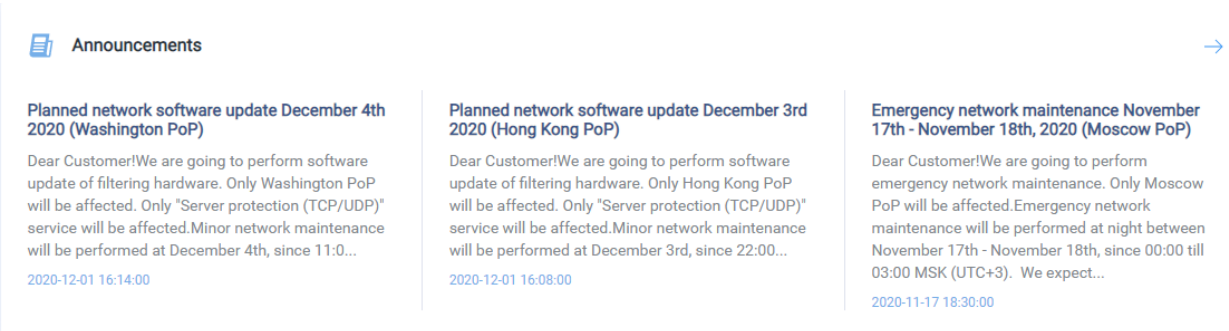


You can also create a new request from **Support request**. To do this, use the form **New support request**.

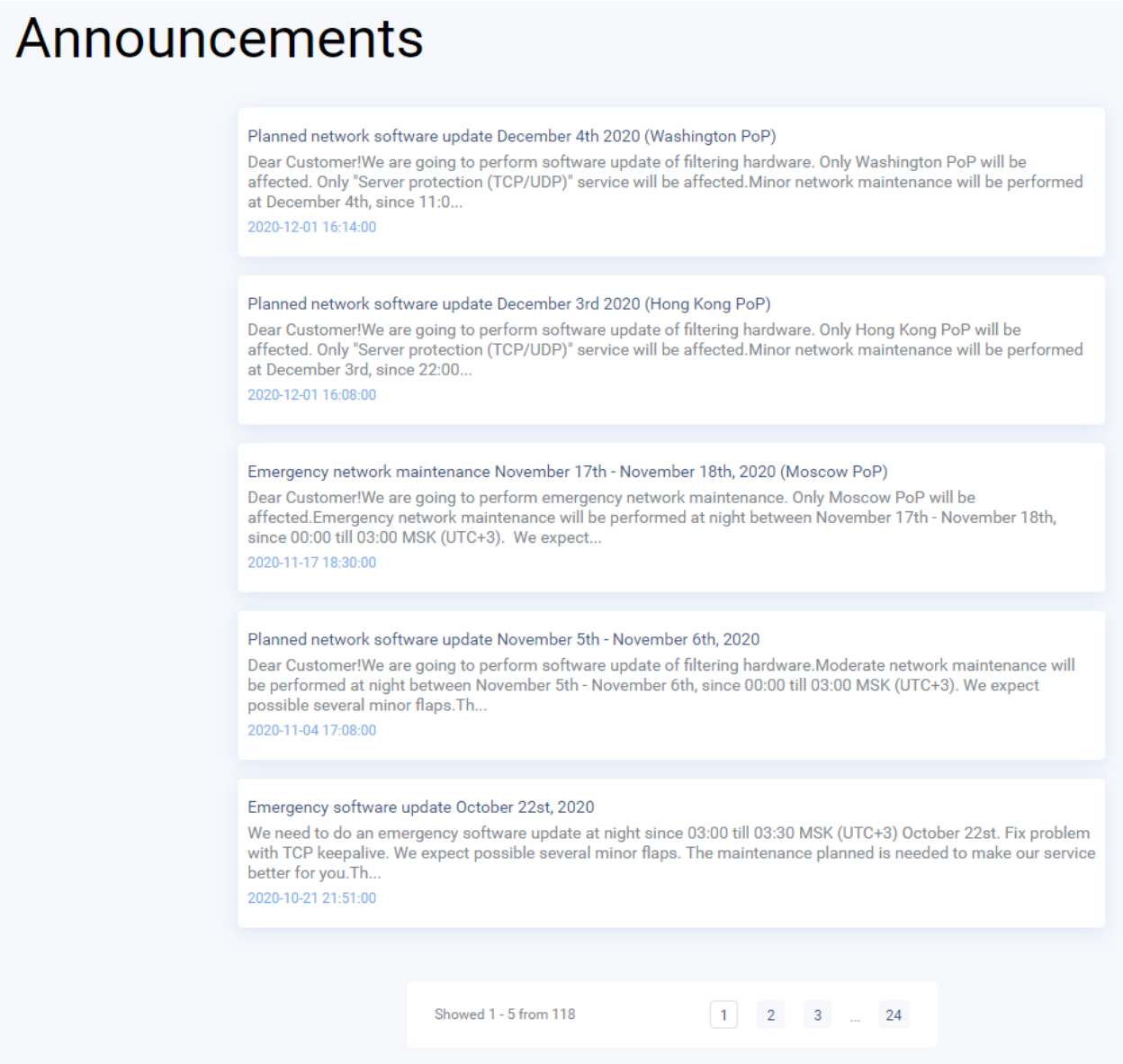
All Responses from StormWall employees to user requests are also sent via email.

Announcements

The **Announcements** contains announcements and user alerts from StromWall. On the **Client Area** homepage there are three most recent announcements.



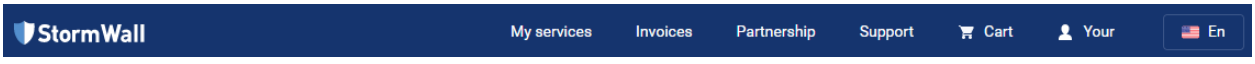
When you click, → you open the **Announcements** page with a full archive of ads and alerts sorted by date.



StormWall's top menu

The Stormwall.pro portal has a top menu, which consists of six items:

- **My services;**
- **Invoices**;
- **Partnership**;
- **Support**;
- **Cart**;
- **Account**;
- Language.



My services

My Services opens a page with connected products and user services, similar to the block **Active products/services** on the **Client Area**.

Invoices

Billing opens the **My Invoices** page, which is also available from block **billing** on **Client Area**.

Partnership

The partnership allows the user to participate in StormWall's partner program, receiving a financial reward for new customers attracted by a unique affiliate link issued to the user. New users who come through the affiliate link are tracked via cookies. To activate the participation in the affiliate program, click **Activate Partnership**.

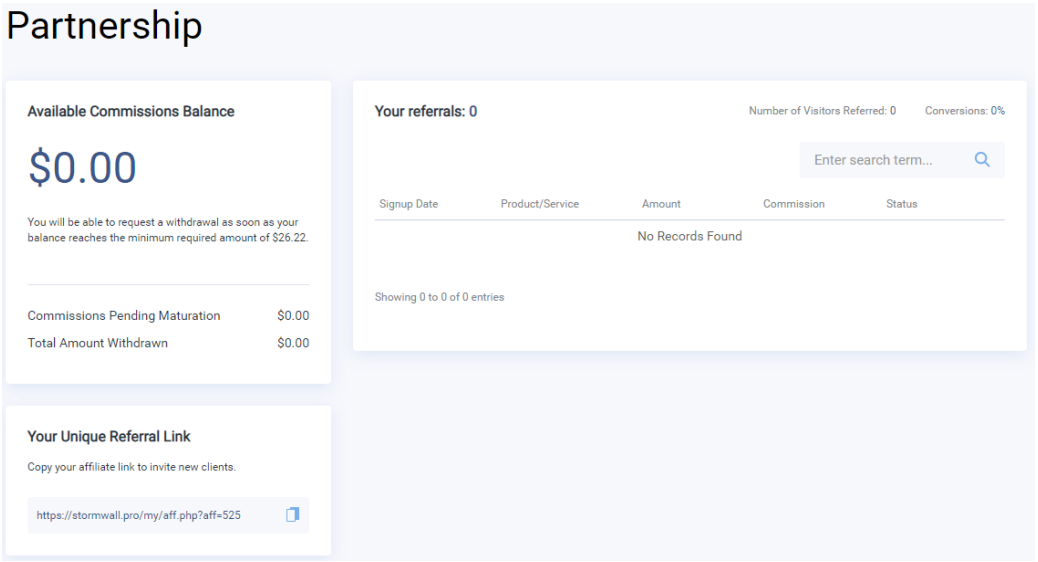
When you click **Activate Partnership**, you'll see a **Partnership** page that includes three information blocks:

- **Available Commissions Balance**;
- **Your referrals**;
- **Your Unique Referral Link**.

Available Commissions Balance displays the user's money earned in the affiliate program. If a certain amount is reached, these funds can be withdrawn.

Your referrals displays the number of customers involved in the user's affiliate program.

Your Unique Referral Link contains a unique link that can be copied and pasted to the user's website or other resource. StormWall's new customers who sign up for this link become members of this user's partner program.



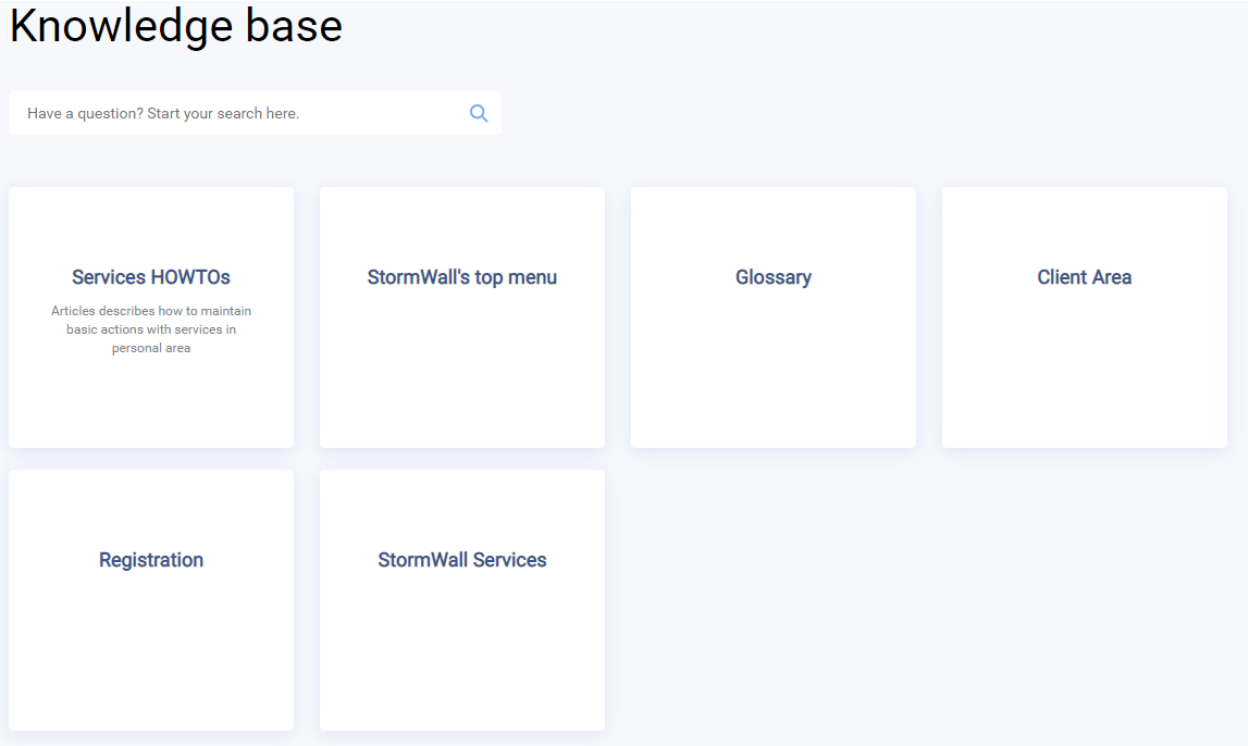
Support

Support includes three sub-points available on the drop-down menu:

- **Support requests;**
- **Knowledge base**;
- **Announcements**.

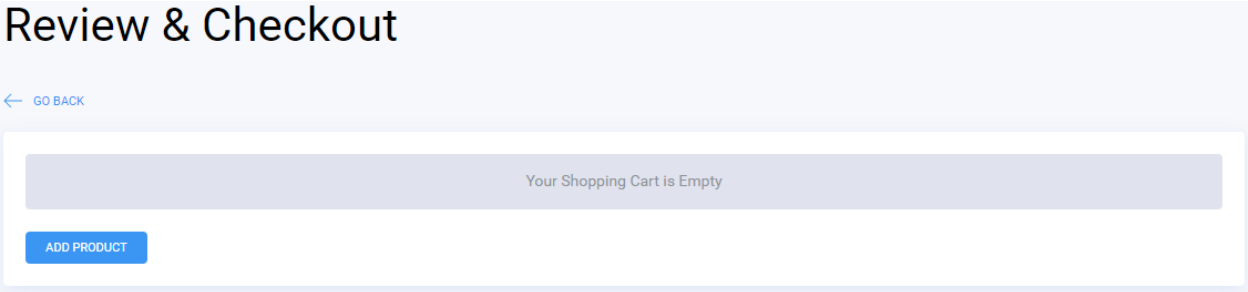
Support requests opens the **Support requests** page, which is also available from **Recent Requests** on **Clients Area**.

The knowledge base contains background information for users (instructions, frequently asked questions, articles). The information is grouped by category and equipped with a search form.



Cart

Cart opens **Review & Checkout**. Here you can see the list of connected services, as well as connect a new service. To do so click **Add product**.



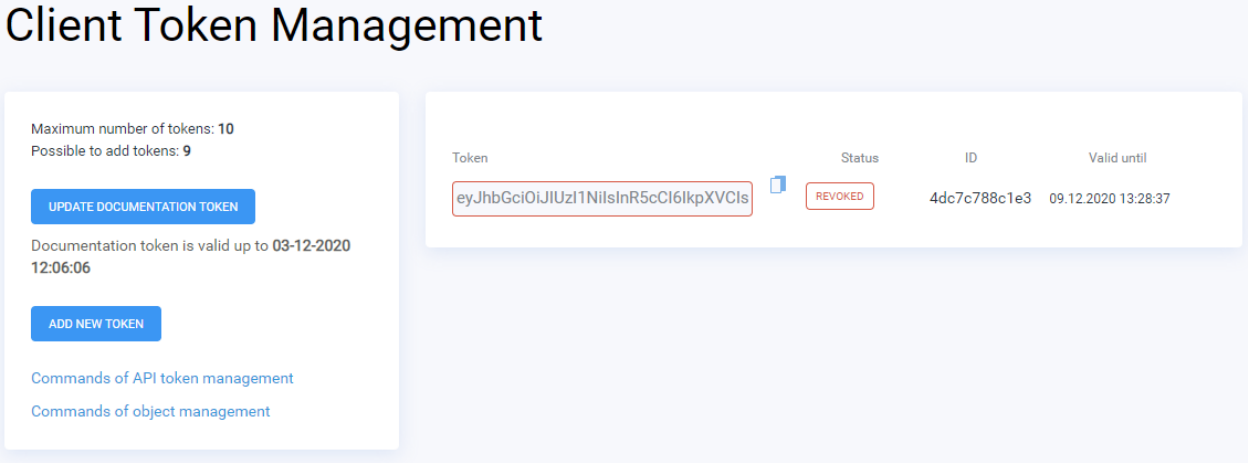
Account

This sub-point is indicated by the username listed at the registration. If a user has not logged into their account, instead of the name, this sub-point is called **Account**. When you click on your name, you open a drop-down menu that includes the following sub-points:

- **API;**
- **Personal data**;
- **Subaccounts**;
- **Change password**;
- **Security Settings**;
- **E-mail History**;
- **Logout**.

API includes everything you need to use StormWall's services and services using third-party apps. StormWall.pro supports API (Application Programming Interface). API allows you to automate services and services, and directly make requests for various operations. APIs can be integrated into any user's programs and online resources. With API, customers can automate StormWall's connected products and services management process. The list of API-supported queries is available at https://api.stormwall.pro/documentation. Each request is accompanied by a description and an example of how to use. **Tokens** are required for authorization of API queries. When you go to the **API** sub-point**,** you'll see the **client token management** page. Here you can create or update your current documentation token. To do this, you need to click **Update documentation token**. The documentation token is designed for customer test requests, which are carried out on a special documentation page. You can also generate one or more tokens on **client tokens management** page to authorize API queries. To do this, you need to click **Add new token**. Once a new token has been created, it is granted **Active** status by default. The list of generated tokens (there may be no more than 10 in **Active** status) is on the same page. You can copy the token to the clipboard or recall (delete).

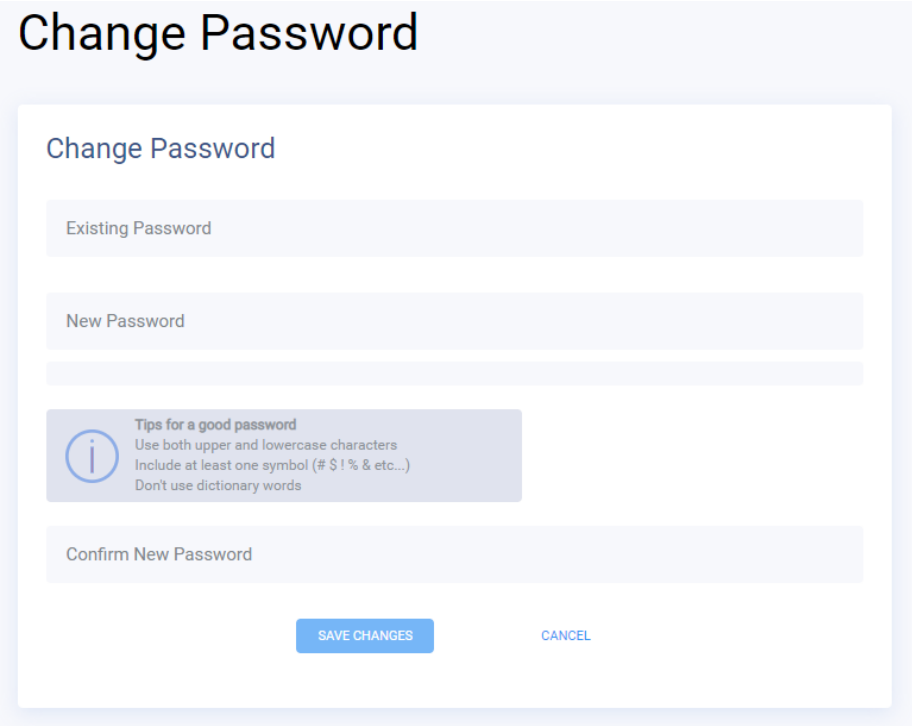
On the same page, there are links to Swagger-supported API lists and descriptions for token management and object management.



Personal Data opens **Personal Data** page from **User Information** block on **Client Area**.

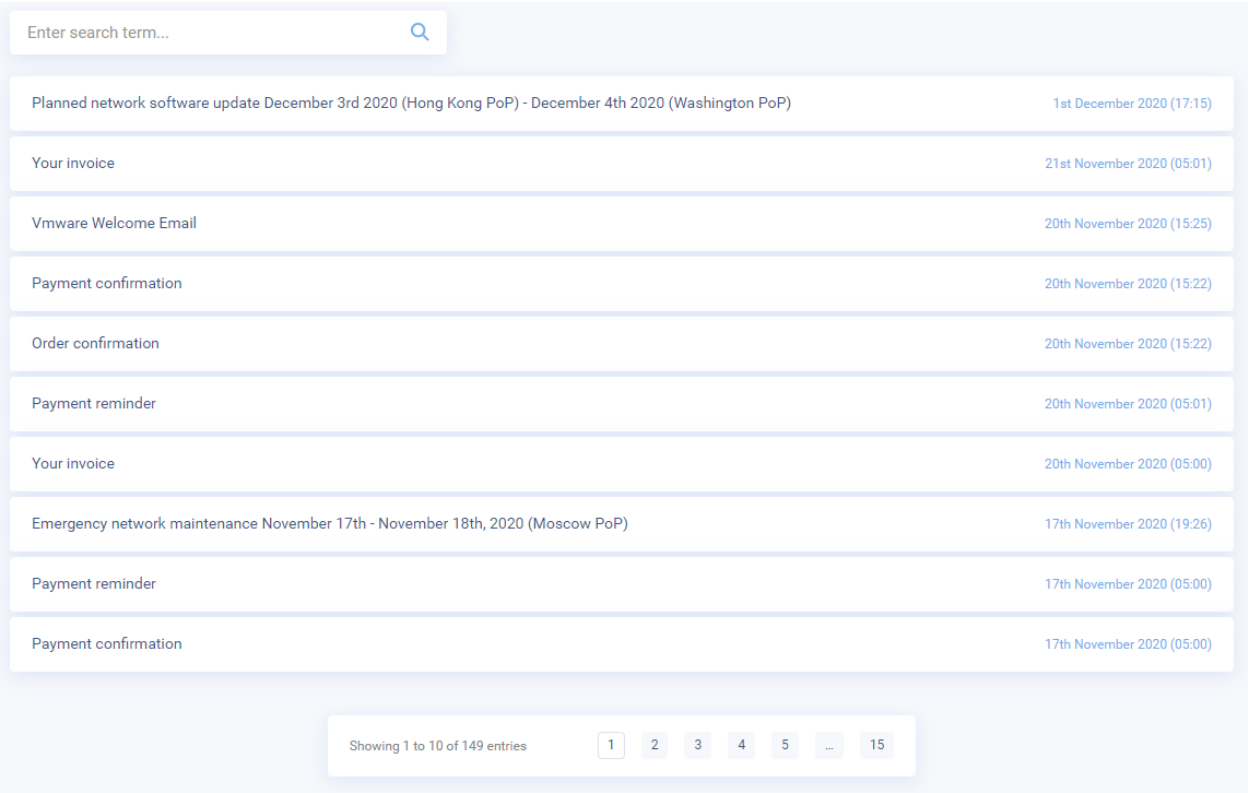
Subaccounts opens **Subaccounts** page from **User information** on **Client Area**.

Change password opens form to change password. To do so, enter the current password, then a new one, followed by a new one again to confirm. To save changes, click **Save changes**.



Security settings allows you to choose how to authorize a user on the portal. There are two options available: **Single entry** (by login and password) and **two-step authentication,** which includes an additional layer of protection, such as entering a special key in addition to login and password.

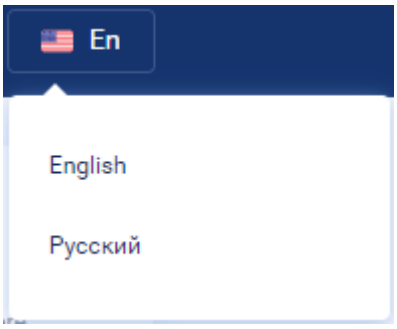
E-mail history opens **E-mail History** page, which contains the entire history of user correspondence with StormWall. For convenience, it is equipped with a search form.



When choosing a **Logout** sub-point, the user exits his account and appears on the https://stormwall.pro/my/. To re-enter, you need to log in to the **Account** - **Login** menu.

Switching language

Two interface languages are available on the Stormwall.pro portal: Russian and English. To switch between them, click with a flag.



StormWall Services

To view and order services, log in to the StormWall.pro portal and log in to the **Client Area**. Next, use one of two options:

- Go to The **Active products/services** block and click **Order a service**.
- In the top menu of the portal, choose **My services**. On a new page, click **Order new service**.

StormWall's **Available Services** catalog opens, where you can choose the service you need, read the information about it, and connect it.

DDoS Protection

How a DDOS attack happens

Any network resource, including a web server, has certain limits on the number of requests it can serve at the same time. There are also restrictions on the bandwidth of the network channel. Once these restrictions exceed the acceptable level, the resource slows down and then it may not be available to queries at all. This is how distributed network attacks occur, related to denial of request service (Distributed Denial-of-Service, DDoS).

Such attacks are quite complex in terms of technical implementation. It is almost impossible to carry out a powerful and long-term DDoS attack from a single computer; for this purpose, networks of computers infected with malware are used, the so-called "botnets", which are controlled by a coordinating server controlled by the attacker. Not only PCs, but also any devices with Internet access can participate in the attack. Often, users of such infected devices do not even suspect that their PC, smartphone or tablet is infected with malware and is currently taking part in an attack on one or another network resource that the attacker who built the botnet has chosen as a victim.

A DDoS attack can target both the network infrastructure (protocol-level attacks) and software components (application-level attacks). The purpose of the attack on the network infrastructure: to exceed the possible bandwidth of the network channel (traffic volume, number of simultaneous connections). The purpose of the application attack is to generate and send the number of requests, the processing of which is capable of exceeding the server's processing capabilities (processor power, RAM, etc.).

How protection works

Protection against distributed network attacks must be taken care of in advance. The client's protected network resource connects to StormWall servers, where multilevel filtering is performed.

- The first layer is provided by border routers located around the world. These routers act as gateways for inter-area traffic. This layer blocks TCP and UDP amplification attacks.
- The second level is hardware filters. They block most of the TCP/UDP flood. Filtering network, built in such a way as to evenly distribute the load across several hardware filters.
- The third layer is stateful filters or "packet inspectors". The most sophisticated attacks are blocked at this level, including attacks by bots...

When it comes to protecting sites, the next level is HTTP filtering with BanHammer cleaning system. It uses behavioral and signature analysis. Thus, all malicious, parasitic and suspicious traffic is eliminated, and the client, in turn, receives only "clean" and verified requests, while the IP addresses of visitors are stored in the HTTP request header.

“Smart” filtering of incoming traffic is also provided by the FlowSense system. It monitors incoming traffic, analyzes anomalies, and, based on this analysis, identifies the type of attack. Further, the protection parameters are dynamically adjusted for this type of attack using BGP FlowSpec (RFC 5575) and the StormWall API. Thanks to artificial intelligence algorithms, not only the detection of abnormal traffic is carried out, but also the prediction of the attack, as well as the identification of its possible scenario.

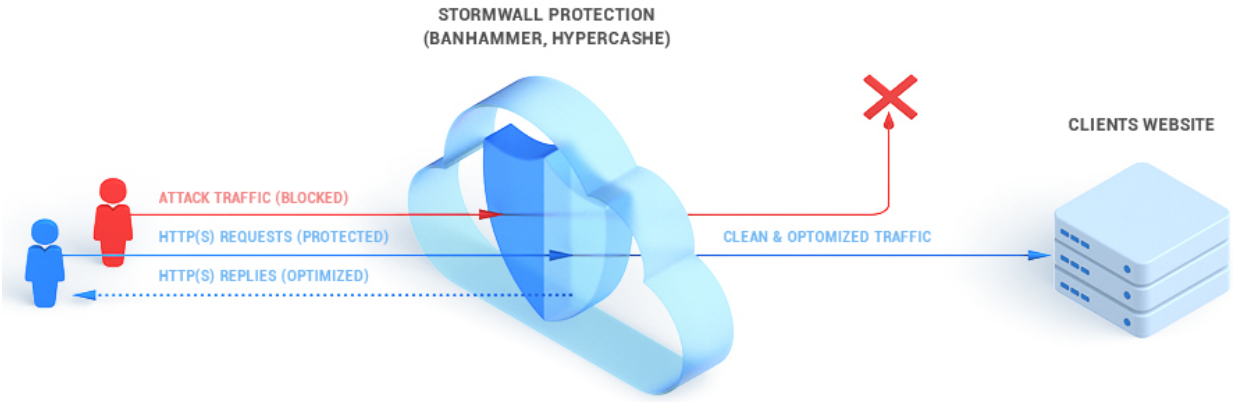
CDN (Content Delivery Network) technology can be used as an additional measure to protect against DDoS attacks. It provides the user with content from the site that is located next to him. On the one hand, this helps to increase the connection speed, and on the other hand, it increases the degree of resistance to attacks. After all, if one of the nodes of the CDN network is overloaded as a result of an attack, the others work normally.

Website protection

The StormWall service for protecting sites from DDoS attacks will ensure the stability of the work of all customer's Internet resources. The service filters all external traffic at the L7 level using proxying technology, while the availability of the site is guaranteed under the "Guaranteed availability, no less" rule. By caching static elements, your site will not only work more reliably, but also faster - the response time to requests from users will noticeably decrease. In this case, no additional costs will be required - only a subscription to the service!

How the service works

1. You get a secure address in the StormWall cloud;
2. You redirect the site's DNS record to it (by yourself, contacting your hosting provider, or with the help of StormWall specialists. You need to edit the A-record for the domain, which indicates the protected IP address);
3. Traffic coming from your website visitors is checked and filtered. Attack traffic is blocked;
4. Only "cleaned" traffic is sent to your server, with the real IP addresses of visitors stored in the HTTP header.



For more information about the service, please visit https://stormwall.pro/website-protection.

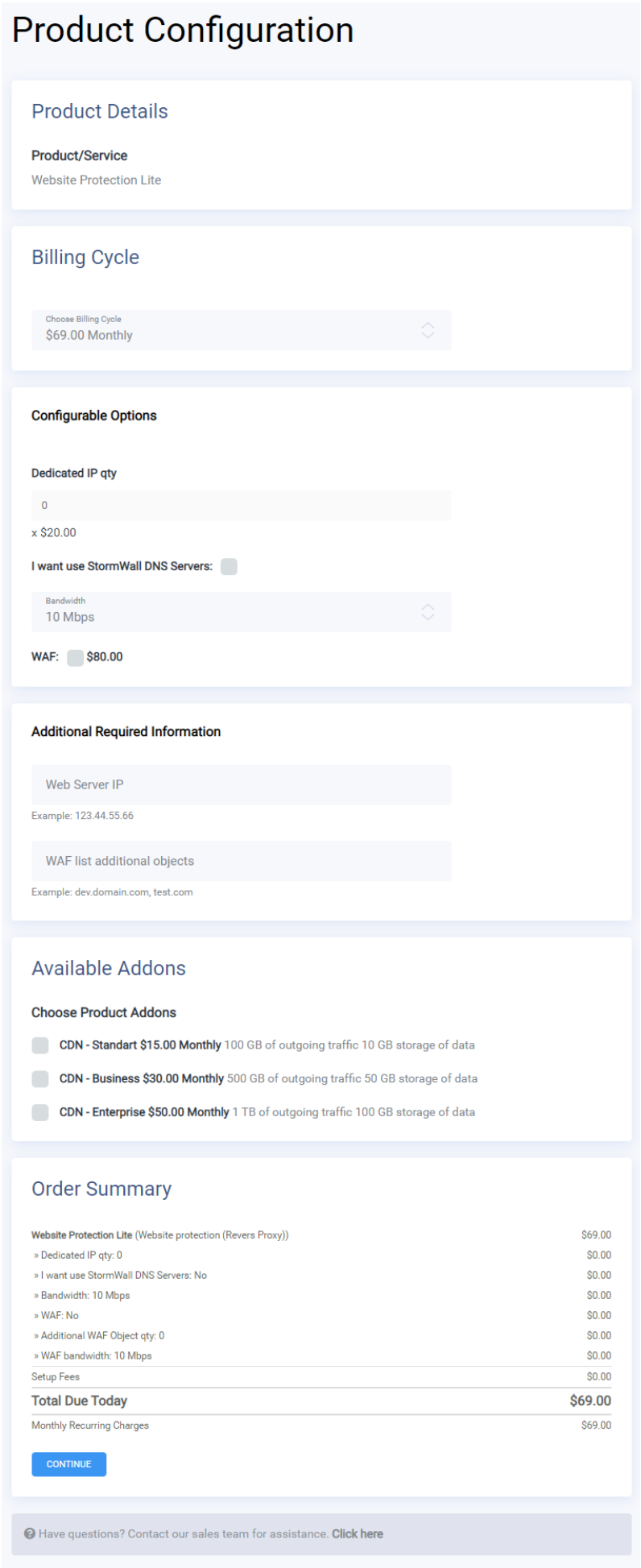
Ordering a service

Enter the directory **Available Services** as listed in the **StormWall Services** section. Select **Web site Protection**. On the page that opens, find the **Select a Subscription plan** table. Carefully study the features and limitations of each tariff, choose the most suitable for your organization. If necessary, consult with the specialists of the StormWall company (**Client area - Recent requests - Create a new request**). After you have decided on the optimal rate, click **Order** or **Contact us**.

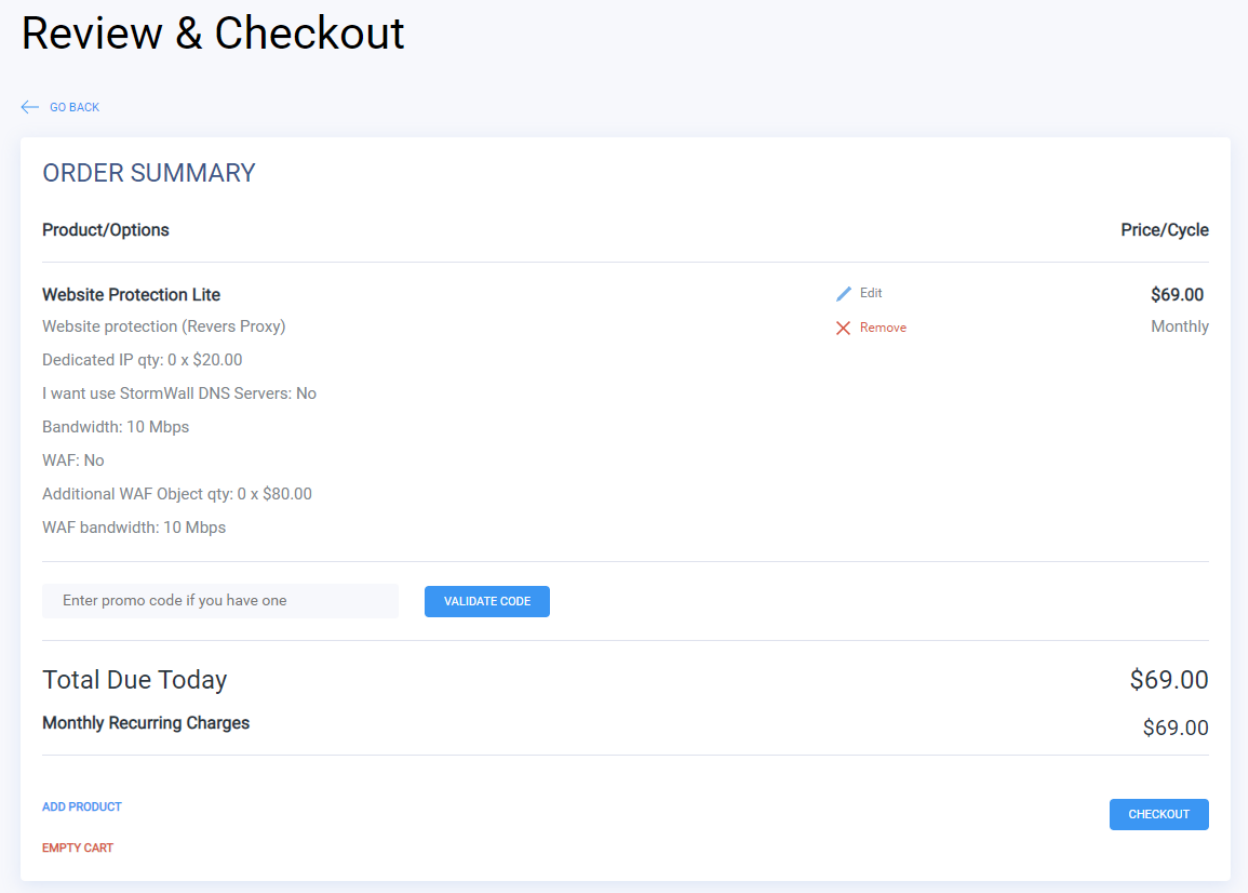
As an example, let's give the most affordable **Lite** tariff, optimal for small sites. When you click **Order**, the **Product configuration** page opens. Here's what you need to do here:

- **Billing cycle** (monthly, quarterly, every six months, annually);
- Number of connected domains (maximum 1 on **lite** tariff);
- Number of plug-in sub-rooms (maximum 5 on **Lite** tariff);
- Necessity to use your own DNS servers or StormWall DNS servers;
- Maximum channel throughput (maximum 10 Mbit/s on the **Lite** tariff);
- Necessity to use **StormWall WAF** to protect web applications (additional cost);
- Connecting domain IP;
- (Optional) one of the CDN tariffs to speed up the site (extra charge);
- Currency for service payment and invoicing.

Check out the list of options and the total cost. Click **Continue**.


Product Configuration
Product Details
Product/Service
Website Protection Lite
Billing Cycle
Choose Billing Cycle
$69.00 Monthly
Configurable Options
Dedicated IP qty
0
x $20.00
I want use StormWall DNS Servers:
Bandwidth
10 Mbps
WAF: $80.00
Additional Required Information
Web Server IP
Example: 123.44.55.66
WAF list additional objects
Example: dev.domain.com, test.com
Available Addons
Choose Product Addons
CDN - Standart $15.00 Monthly 100 GB of outgoing traffic 10 GB storage of data
CDN - Business $30.00 Monthly 500 GB of outgoing traffic 50 GB storage of data
CDN - Enterprise $50.00 Monthly 1 TB of outgoing traffic 100 GB storage of data
Order Summary
Website Protection Lite (Website protection (Revers Proxy)) $69.00
» Dedicated IP qty: 0 $0.00
» I want use StormWall DNS Servers: No $0.00
» Bandwidth: 10 Mbps $0.00
» WAF: No $0.00
» Additional WAF Object qty: 0 $0.00
» WAF bandwidth: 10 Mbps $0.00
Setup Fees $0.00
Total Due Today $69.00
Monthly Recurring Charges $69.00
CONTINUE
Have questions? Contact our sales team for assistance. Click here

Review & Checkout page opens. Here you can once again check the connected settings, options and components of the service. If you need to change anything, click on the **Edit**. If you change your mind ordering a service, click **Remove**. If you have a promo code for a discount, enter it in the appropriate box and click **Validate code**. To start the payment procedure, click **Checkout**.

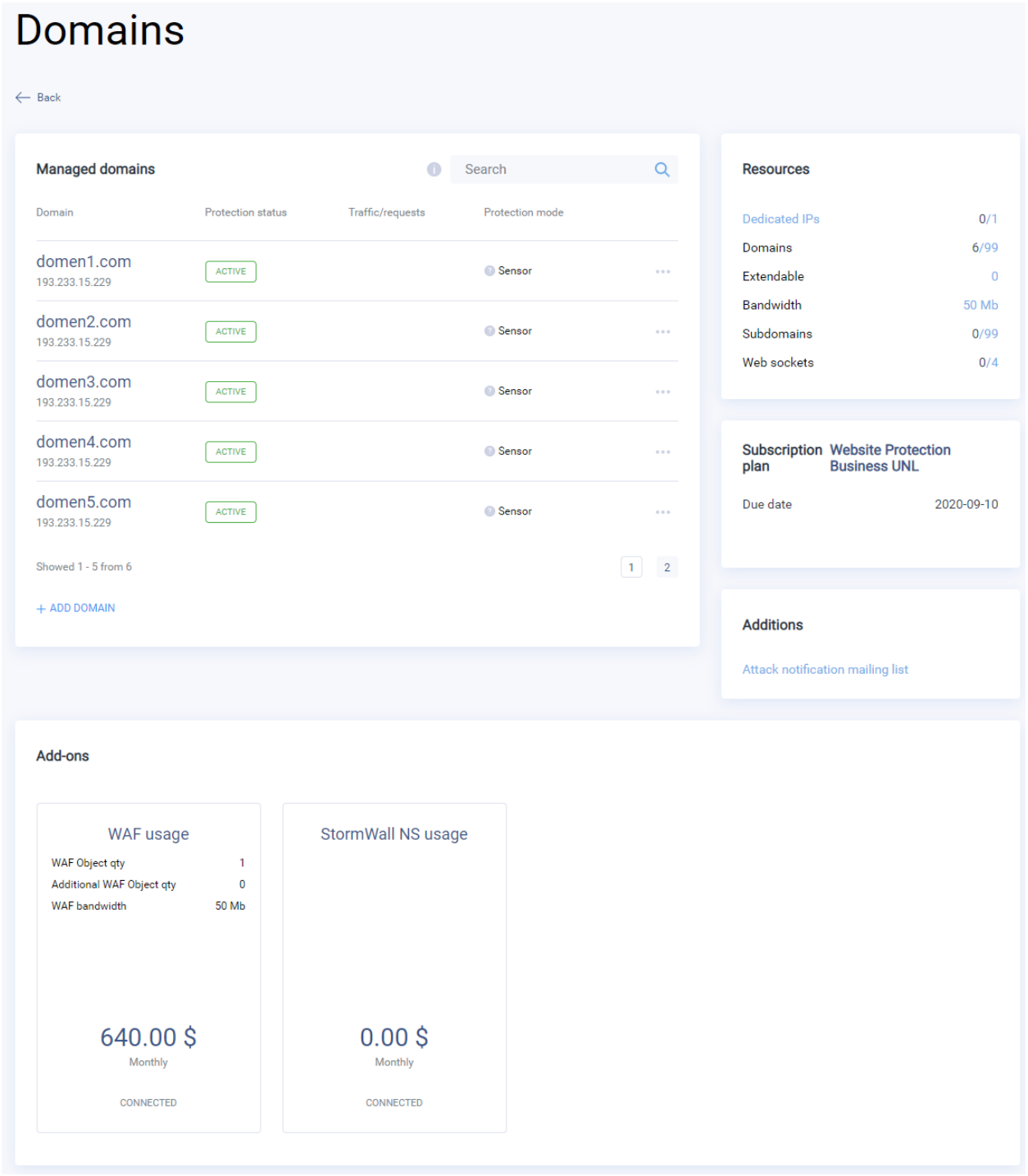


You can defer payment for later, in which case this page will be available in **Cart** in top menu.

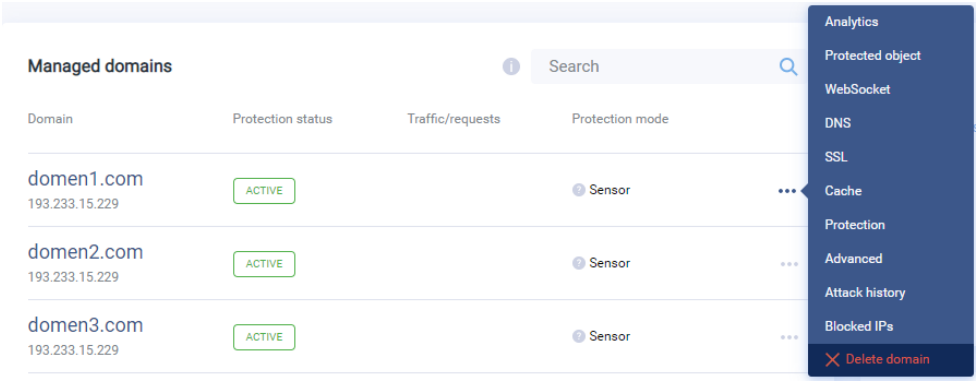
When you click on the **Checkout** button, a page opens offering a choice of payment method. On it, you should choose a convenient method, put a checkmark confirming familiarization with the Terms of Service, and then click on the **Complete Order** button. A page with an invoice will open. This account will be available in the **Billing** section of the **Client area**. The service you have connected will be available in the **Active products/services** section of the **Client Area**. Until the invoice for the service is paid, it will not be launched, but will be in the **Pending** status. After payment, the order goes through the pre-moderation procedure in the technical support service. After successful completion of pre-moderation, its status will change to **Active**.

Service management

In the **Client Area,** select **My Services** block. In the list of connected services in the **Active** status, select the **Website Protection** service. Click on her line on the list. Below there is a screenshot of the service page.



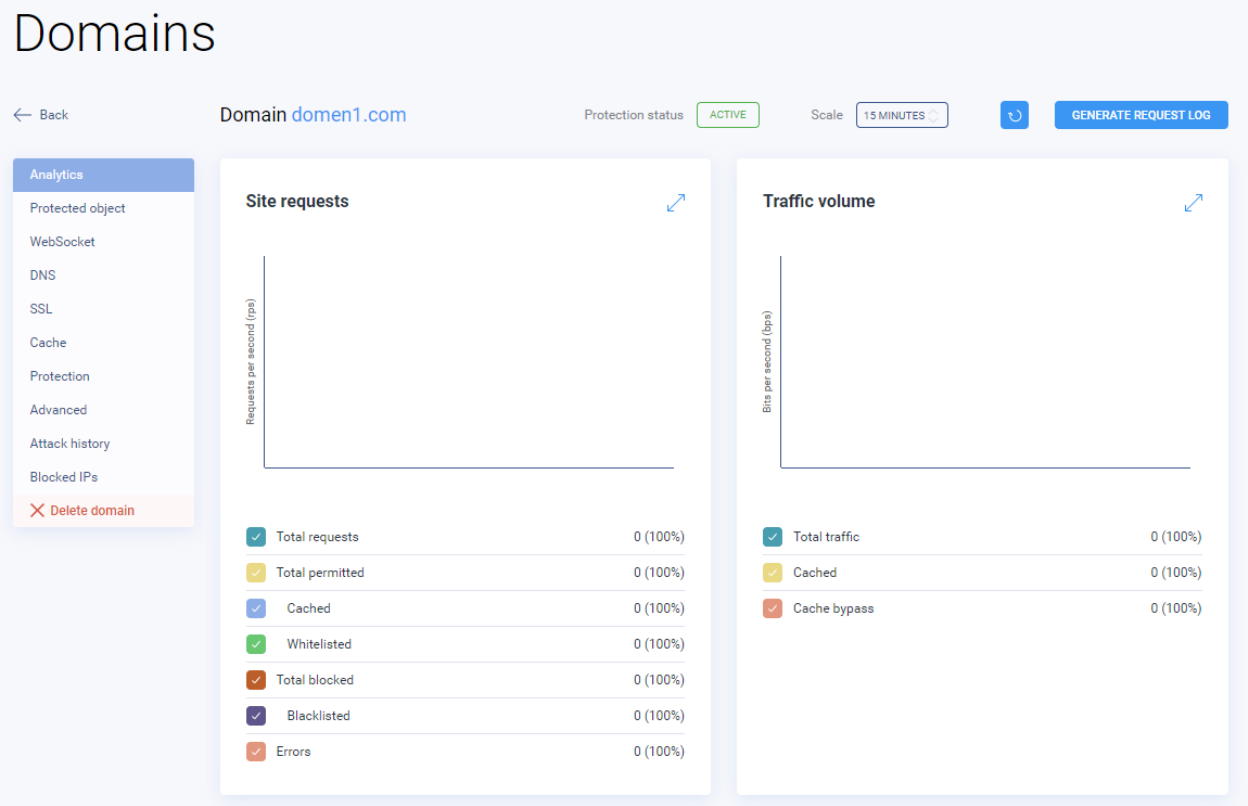
Choose from managed domains and click on the dot image on the right side of the line.



There is a drop-down menu, which includes the following items:

- **Analytics**. The following options are displayed in real time:
  - Requests to the site (including blocked and blacklisted);
  - Traffic (from cache and not from cache);
  - Time and response code;
  - Heat map and top cities and countries from which visitors came;
  - Top locations of the site viewed by visitors.

When you click **Generate request log,** you can get a CSV log that contains information about domain requests over a selected period of time.



- **Protected Object**. Manage the list of designated IP addresses and backend servers, set up balancing methods, turn the HTTP protocol on and off.
- **WebSocket**. WebSocket Port List Management.
- **DNS**. Managing DNS records for the domain.
- **SSL**. Here you can get a free SSL-a certificate from Let's Encrypt service, or set your own certificate, if any, and turn on and off redirects from HTTP to HTTPS.
- **Cache**. Manage the list of file extensions to cache and set the time it takes to store them.
- **Protection**. Protection settings:
  - Protection mode. The default **Sensor** mode (all requests) is recommended; When using this mode, no requests are filtered, filters work in passive mode. The sensor monitors the total number of requests, their bursts, the presence of errors in server responses, and when signs of an attack on the site are detected, it switches the filters to active mode, after which the attack is suppressed. The sensor response time usually does not exceed one minute, but can vary depending on the type and intensity of the attack. You can also set the required operating mode yourself, in this case all requests will be validated constantly.
    - **Sensor -** when using this mode, no requests are filtered, filters work in passive mode. The sensor monitors the total number of requests, their bursts, the presence of errors in server responses, and when signs of an attack on the site

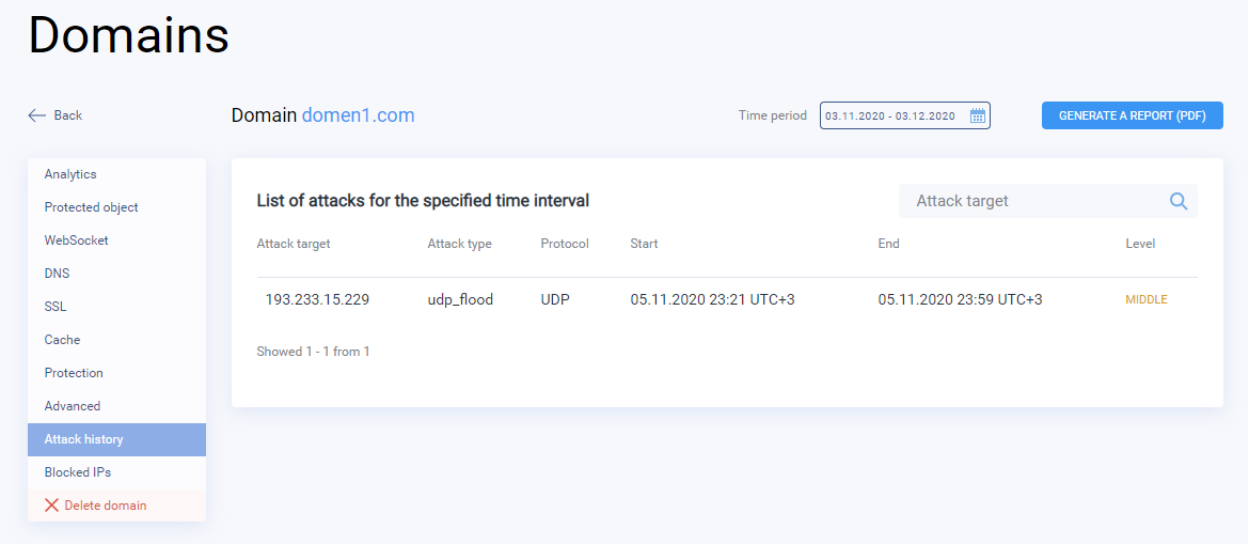
are detected, it switches the filters to active mode, after which the attack is suppressed. The sensor response time usually does not exceed one minute, but can vary depending on the type and intensity of the attack. You can also set the required operating mode yourself, in this case all requests will be validated constantly.

- Disabled – In this mode, the protection is completely disabled.
- Redirect - additional redirection to the requested location is applied for visitor requests.
- JS - JavaScript validation is used for regular IP queries.
- JSA - Extended validation using JavaScript is used for regular IP queries.
- Captcha – request to the site will require the passage of Captcha for validation.

- Enabling and disabling proactive protection. You can also use proactive protection mode for your domain. When activated in sensor mode, filtering of all requests is not performed, but each new visitor is checked according to many parameters, such as: visited site locations, whether keepalive connections were used, whether it carried out attacks on other sites, which User Agent uses, does not exceed the limits requests. In case of violations, requests from the client's IP address will be sent for validation and further monitoring of its behavior will be made. This mode allows for selective validation of suspicious requests without the need to switch the entire configuration to the active mode of operation.
- Cookie. Setting the storage time on the user's computer and generating a new protection key. This tab will allow you to set the lifetime of the visitor's session, after which it will be re-checked. You can also reset all installed user sessions by clicking "GENERATE NEW SECURITY KEY". In this case (with an active operating mode), all users will be validated again. The lifetime of the cookies used to operate the security system does not in any way affect the session time on the site itself, the system does not make any changes to the original site cookies.
- Whitelist. Protection using a "white" list of addresses. Allows you to add a list as a txt file. Allows you to add specific IP addresses to the whitelist to allow requests from these IP addresses to be passed without filtering.
- Blacklist Protection using the "black" list of addresses. Allows you to add a list as a txt file. When requesting from an IP address in this list, the error "HTTP 403 Forbidden ".
- Exception by file type. You can set up an exception to the site locations that will not be filtered.
- Exceptions by location. Allows you to add a list as a txt file. Adds specific paths (part of the request URL) to the whitelist. Locations work as a match rule, if the specified path is found in the request - the request will be sent to the whitelist.
- Filtration by headers. Based on the received headers, you can create rules for both blocking unwanted requests and allowing rules. This functionality will be relevant if you use the API on the website or a separate application makes requests to it. It can be used as a single title, or in combination.
- Filtering by country (Geo Filter). Allows you to add a list as a txt file;
- Safe Metrics (for Yandex Metrics and Google Analytics). If you are using Yandex or Google metrics, you need to specify their identifiers in the Safe Metrics fields. In the absence of this data, in the active filtering mode, metrics may receive incorrect data and count all transitions to the site as internal.
- Advanced sensor settings (for more see **Website Protection** – **Service management** – **Advanced sensor settings**).

- **Advanced**. Set up the redirect and choose the look of the error page (standard or in StormWall design);
- **Attack history.** List of recorded and reflected attacks to the specified domain within the selected time interval. Attacks are sorted by the following characteristics:
    - Attack target;
    - Attack type;
    - Protocol;
    - Start;
    - End;
    - Level.

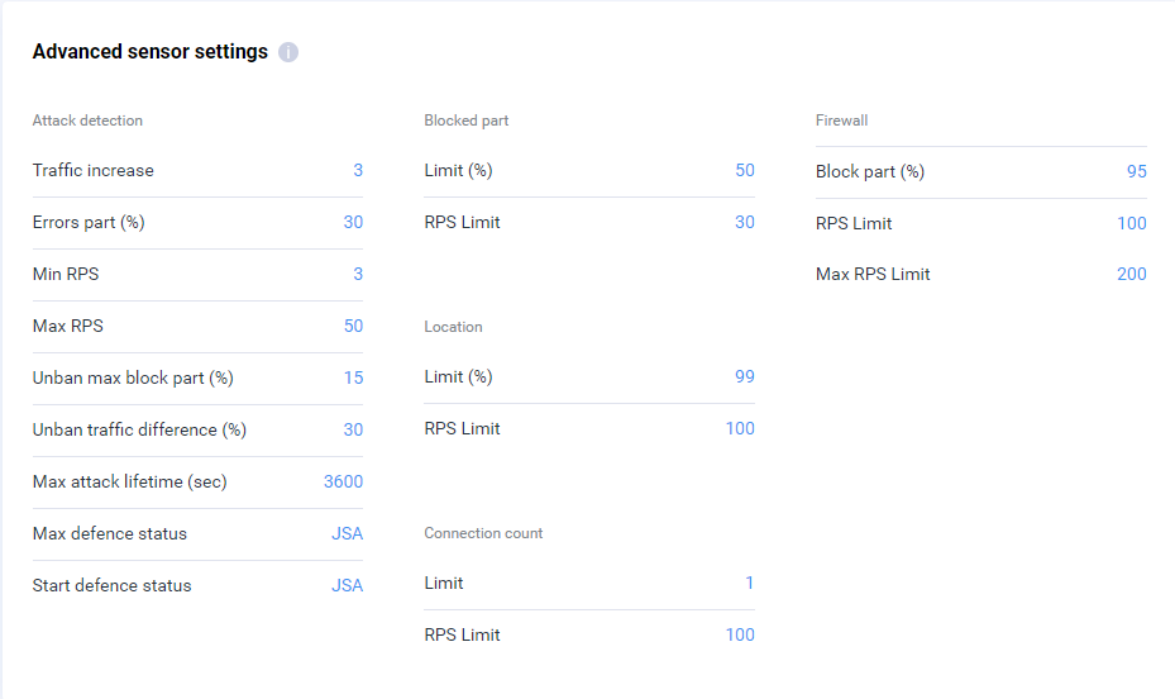
When you click **Generate a Report (PDF),** you can unload it from the system and save it as a PDF document.



- **Blocked IPs.** Blocked IPs list and lock history;
- **Delete domain.** Disconnecting the domain from **Website protection** service**.**

Advanced sensor settings

Experienced users can independently carry out "fine" adjustment of the sensor parameters. To change a parameter, move the mouse cursor to the digital value of this parameter and click on the pencil image that appears next to it.



Left column of the menu **Advanced sensor settings** allows you to adjust the parameters of attack detection:

- **Traffic increase**. How many times the number of requests should increase in a short period of time to go into active mode;
- **Error part**. Percentage of erroneous queries that filters will go into active mode;
- **Min RPS**. A value below which the **Traffic increase** and **Error part** check is not performed. The **Min RPS** value helps to avoid unnecessary checks when the RPS values "float" and should not be equal to zero, since such domains will be frequently checked and a lot of false positive sensor responses are possible.;
- **Max RPS**. Number of requests that will trigger the go-to-active mode if it's exceeded;
- **Max attack lifetime**. Time after the attack starts after the filter will attempt to switch to sensor mode;
- **Max defense status**. Maximum type sewn up when triggers automatically work;
- **Start defense status**. The type of protection that will be installed when the filter initially moves from sensor mode to active mode.

The center column of the **Advanced Sensor Settings** menu allows you to configure the Blocked part. There are two parameters here: **Limit** (in%) and **RPS limit** in RPS. If more requests are received from any IP address than indicated in the **RPS limit** value, and of them there are more blocked in percentage terms than in Limit, then the IP is placed on the "gray" lists (rating +1 to the protection type).

In the same column, you can configure the location (Location). There are also two parameters available here: **Limit** (in%) and **RPS limit** in RPS. If more requests are received from any IP address than indicated in the **RPS limit** value, and there is a certain URL location that receives more requests as a percentage than Limit, then the IP is placed on the gray lists (rating +1 to the type protection).

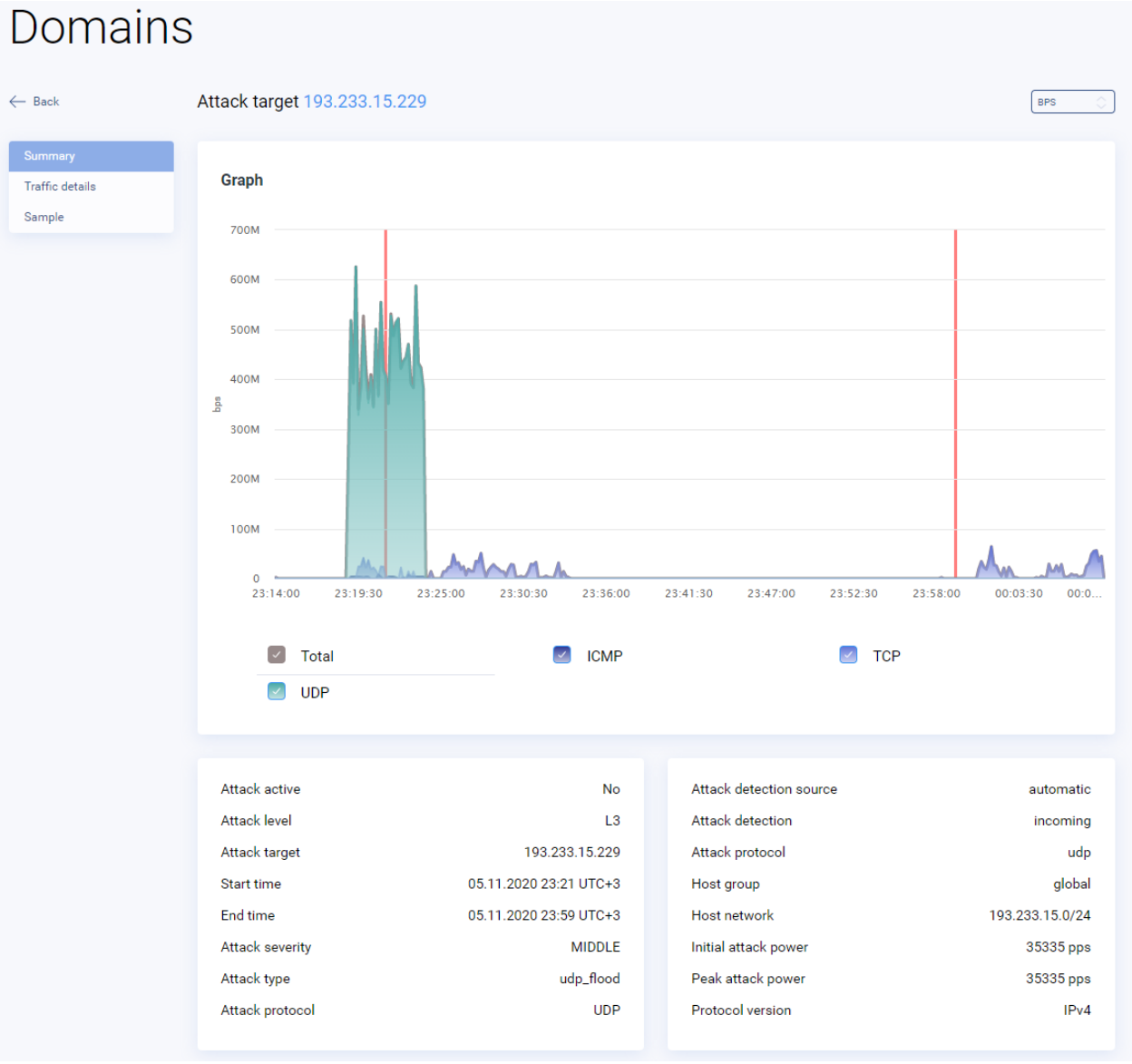
In the same column, you can configure the number of connections (Connection count). The **Limit** parameter displays the average number of requests per IP. If IP supports keep alive, then this value will differ greatly from 1, if it does not, it will tend to 1. The **RPS limit** parameter, as in other filters, means the minimum number of requests for analysis.

The right column of the **Advanced Sensor Settings** menu contains Firewall options. They regulate the values at which a specific IP address can be blocked by a firewall.:

- Max **RPS limit**. If Max **RPS limit** is exceeded, IP is included in the lock lists, without any additional checks;
- There are two related parameters: **Block Part** and **RPS limit.** If **the RPS limit** is exceeded and the share of blocked requests from a particular IP exceeds Block Part (value in), the IP will also be transferred to the list of blocked.

View attack history

When you select the **Attack history** menu item, a list of attacks aimed at the protected domain opens. Select one of the attacks in the list and click on its row to see the details.

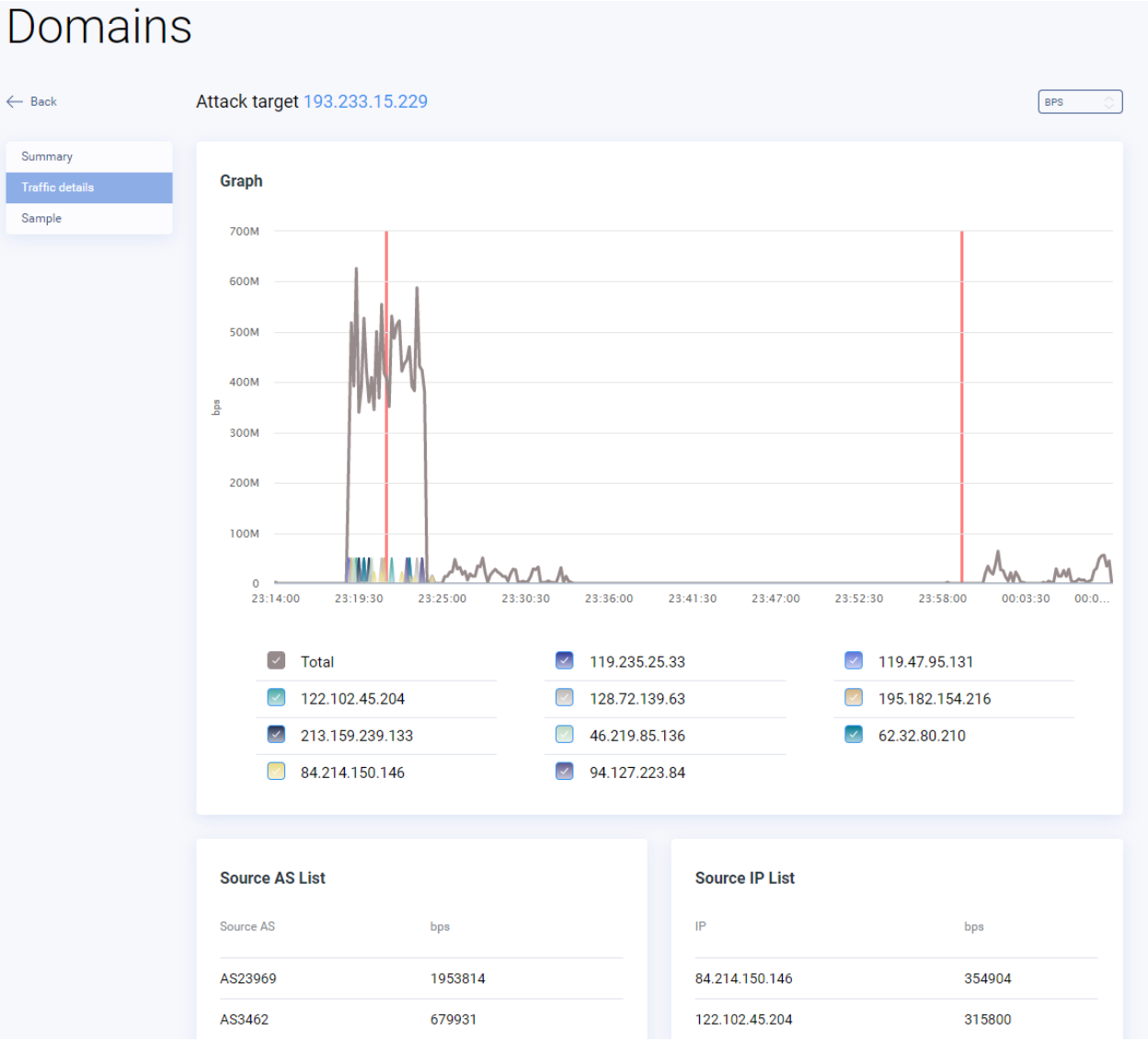


The following options are displayed in the preview window:

- **Attack active.** Attack activity at the moment;
- **Attack level**. The TCP stack level on which the attack is carried out;
- **Attack target**;
- **Start time**. Recorded start time of attack;
- **End time.** Registered end time of attack;

- **Attack severity**. Assessment of attack force;
- **Attack type**. Type of attack;
- **Attack protocol**. The protocol used to attack;
- **Attack detection source**. The source of the attack detection;
- **Attack detection**. Attack detection;
- **Host group**. Group of hosts involved in the attack;
- **Host network.** Host network;
- **Initial attack power.** The initial force of the attack;
- **Peak attack power.** Peak attack force;
- **Protocol version.** Version of the protocol.

Traffic details

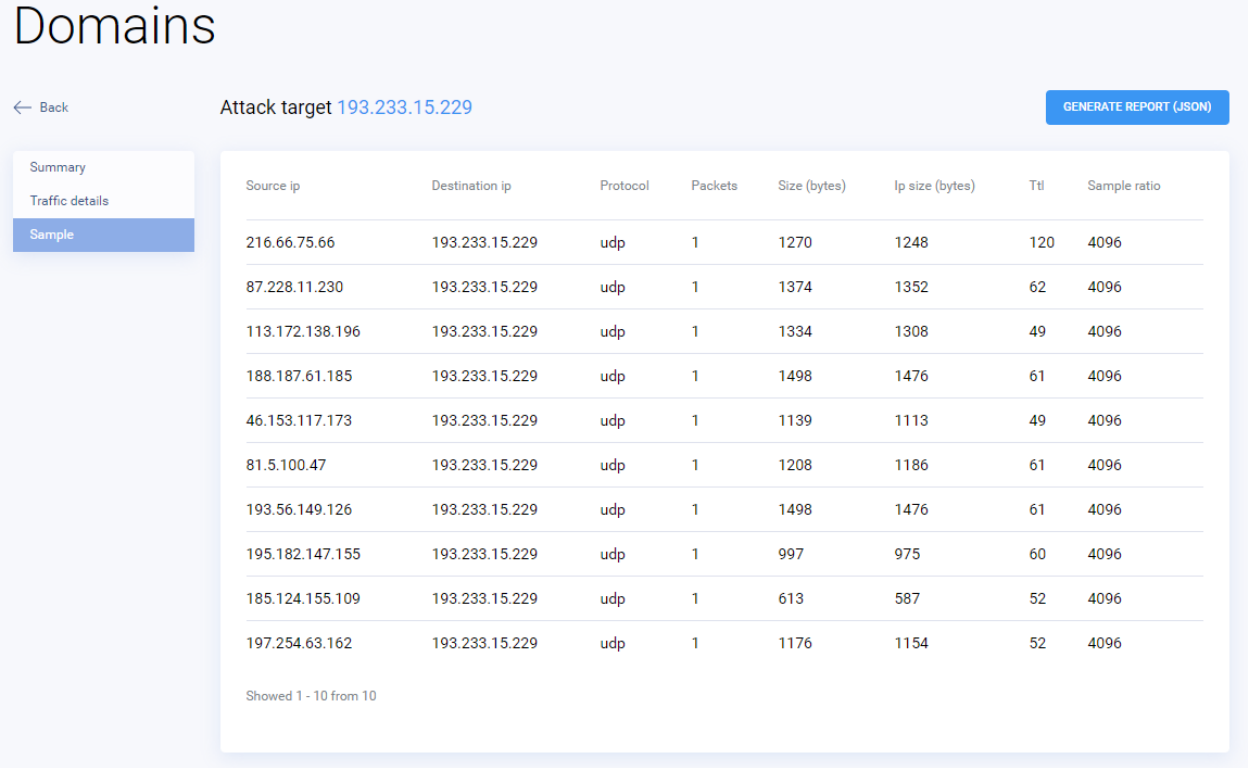


The **Attack History - Traffic Details** menu displays data that allows you to determine who, how, from where and how attacks are carried out:

- **Source AS List**. Top AS networks from which traffic was received;
- **Source IP List**. Top IP addresses from which traffic was received;
- **Protocol list**. Minutes that were recorded during the attack;
- **Source TCP Port List**. Top outgoing TCP ports from which packages were received during attack;

- **Destination TCP Port List**. TCP ports services directly targeted;
- **Source UDP Port List**. Top outgoing UDP ports from which packages were received during the attack;
- **Destination UDP Port List**. UDP ports services to which the attack was directly targeted.

Sample



In the **Attack History - Sample** menu, you can see the details of each attack separately:

- **Source IP**. The address from which the package came;
- **Destination IP**. Destination Address (address to which the attack was carried out);
- **Protocol**. Package Protocol;
- **Packets**. Number of packets on record;
- **Size (bytes).** Total packet size;
- **IP size (bytes).** Packet header size;
- **Ttl**. Installed maximum TTL (the life of the packet);
- **Sample ratio**. 1 package out of every N packages was collected (4096).

When you click the **Generate report (JSON)** button, you can get the entire list of attack samples in JSON format.

Anti-DDoS Hosting

Unlike **website protection,** in which your site does not change its hosting, and attack protection is done through forward, the **Anti-DDoS hosting** service provides quality hosting for websites with already connected protection against DDoS attacks (see the Website Protection section for more information.). Ordering this service, you'll get the following benefits:

- Hosting and protection from DDoS attacks from one hand;
- Effective filtering of any DDoS attack;
- Speeding up your websites;
- The optimal tariff for you with a monthly payment;

- No additional costs for hardware, software and protection against DDoS attacks;
- Ability to connect the required number of domains and subdomains within the tariff plan;
- Mail server, databases, DNS server, dedicated IP addresses and solid-state storage (SSD) disk space;
- Simple and fast migration of your Internet resources to our facilities, incl. by the specialists of the StormWall company;
- Daily data backup.

How the service works

The customer's web server is located on the secure network of StormWall. Incoming web traffic arrives with <1 millisecond latency before filtering. High quality of service is ensured by triple traffic filtering (**Triple Filter**):

1. **Border routers.** Located all over the world, cut off inter-zone traffic;
2. **Hardware filters**. Block the bulk of TCP / UDP floods;
3. **Stateful filters.** A fine filtering level where the most sophisticated attacks, including bot attacks, are blocked. When it comes to protecting the site, next comes the HTTP filtering layer with **BanHammer** cleaning system.

BanHammer's HTTP-flood filtration system uses intelligent methods and algorithms "trained" on tens of thousands of attacks on StormWall customer websites. **FlowSense** constantly monitors all data streams going to the server, tracks anomalies and automatically determines the type of attack that starts, and the results of which dynamically adjust the security settings.

High speed sites within the Service **Anti-DDoS Hosting** is guaranteed thanks to the use of **HyperCache** technology. It caches large files in server RAM, so site users get them almost instantly. When StormWall security is connected, traffic from the nearest to the customer's filtering point to the server is directed through StormWall's own leased communication channels between data centers, which provide minimal ping, minimal delay fluctuations, and no shaping.

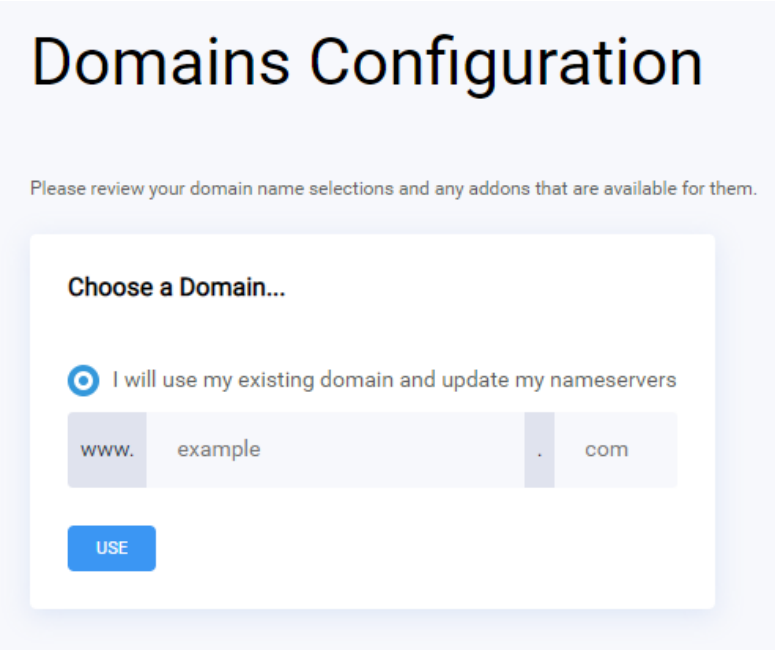
StormWall's global failures are protected with **Global Session** technology. StormWall's filtering nodes around the world "know" that the customer has connected to your server, and if one node is unavailable, the traffic is automatically directed to another site closest to the customer.

For more information about the service, please visit: https://stormwall.pro/antiddos-hosting.

Ordering a service

Enter StormWall's **Available Services** catalog as listed in **StormWall Services**. Select **Anti-DDos Hosting**. On a new page find the **Select a subscription plan** table. Carefully study the features and limitations of each tariff, choose the most suitable for your organization. If necessary, consult with StormWall specialists (**Client Area** – **Recent Requests** – **Create a new request**). Once you have decided on the optimal tariff, click **Order** or **Contact us**.

As an example, let's give the most affordable **Lite** tariff, optimal for small sites. When you click **Order**, the **Domain Configuration** page opens. It is necessary to indicate the address of the web resource to which you connect the service. After the instructions click **Use**.



On the **Product Configuration** page that opens, specify the following parameters:

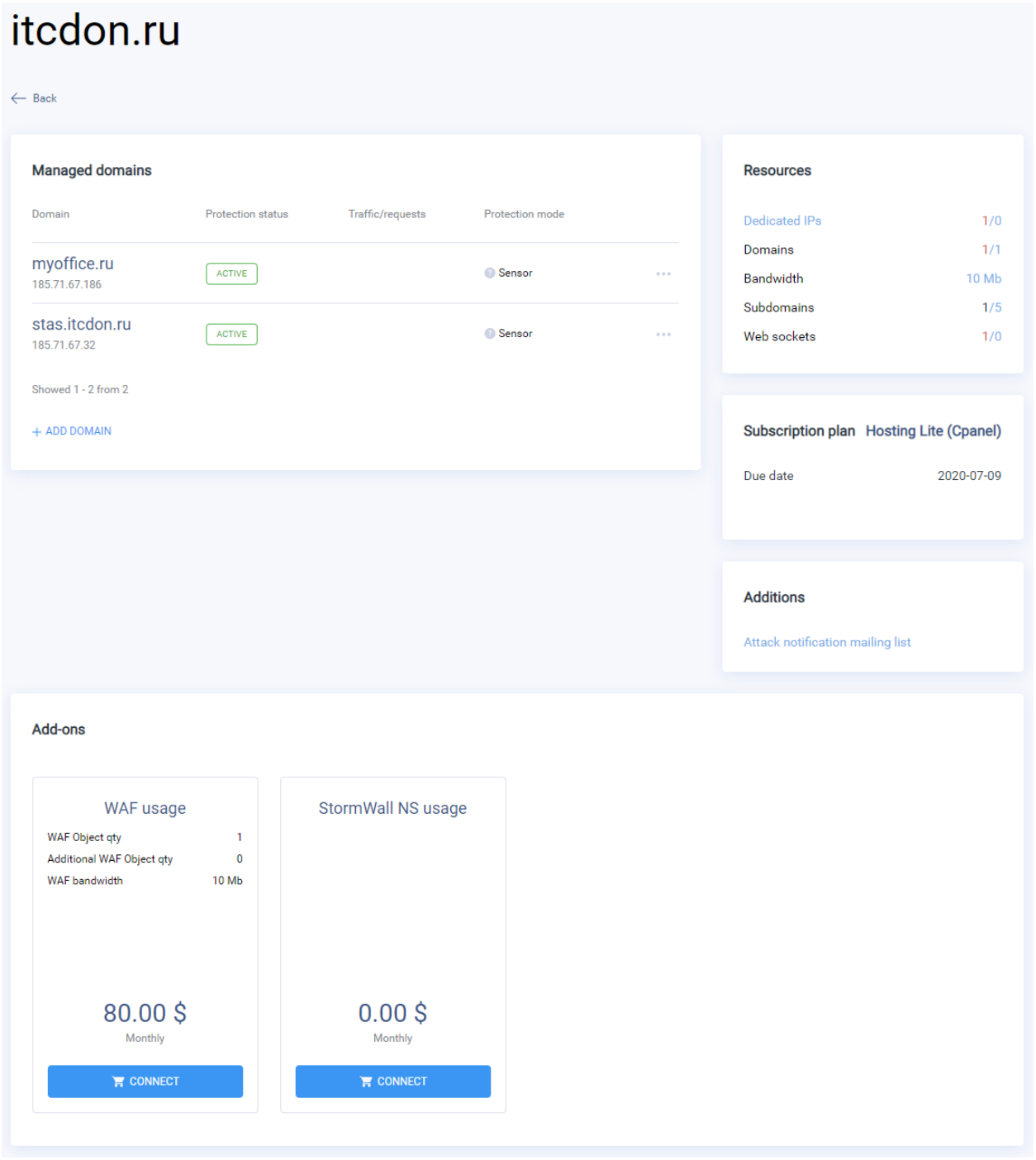
- **Billing cycle** (monthly, quarterly, once every six months, annually);
- Select a data center to host;
- The number of dedicated IP addresses (1 - maximum at the **Lite** tariff);
- Necessity to use StormWall's own DNS servers;
- Maximum channel throughput (maximum 10 Mbit/s on the **Lite** tariff);
- Necessity to use **StormWall WAF** to protect web applications (additional cost);
- List of additional domains for **WAF** (optional);
- Connect one of the CDN tariffs to speed up the site (for an additional fee);
- Select the currency for service payment and invoicing.

Check the list of options and the final cost. Click **Continue**. The **Review & Checkout** page opens. Here you can once again check the connected settings, options and components of the service. If you need to change anything, click **Edit**. If you change your mind ordering the service, click **Remove**. If you have a promo code for a discount, enter it in the appropriate box and click **Validate Code**. To start the payment procedure, click **Checkout**.

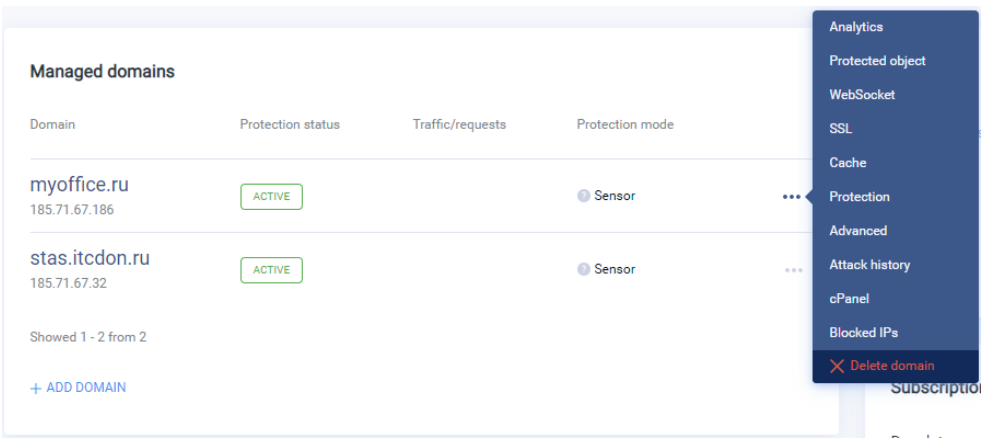
When you click **Checkout**, a page opens, offering a choice of payment method. On it, you should choose a convenient method, put a checkmark confirming familiarization with the Terms of Service, and then click **Complete Order**. A page with an invoice will open. This account will be available in the **Billing** block of the **Client Area**. The service you have connected will be available in **the Active products/services** block of the **Client Area**. As long as the bill for the service is not paid, it will not be launched, and will be in the status of **Pending**. After payment, the order is approved by the technical support service. Once the premoderation is successfully completed, its status will change to **Active**.

Service management

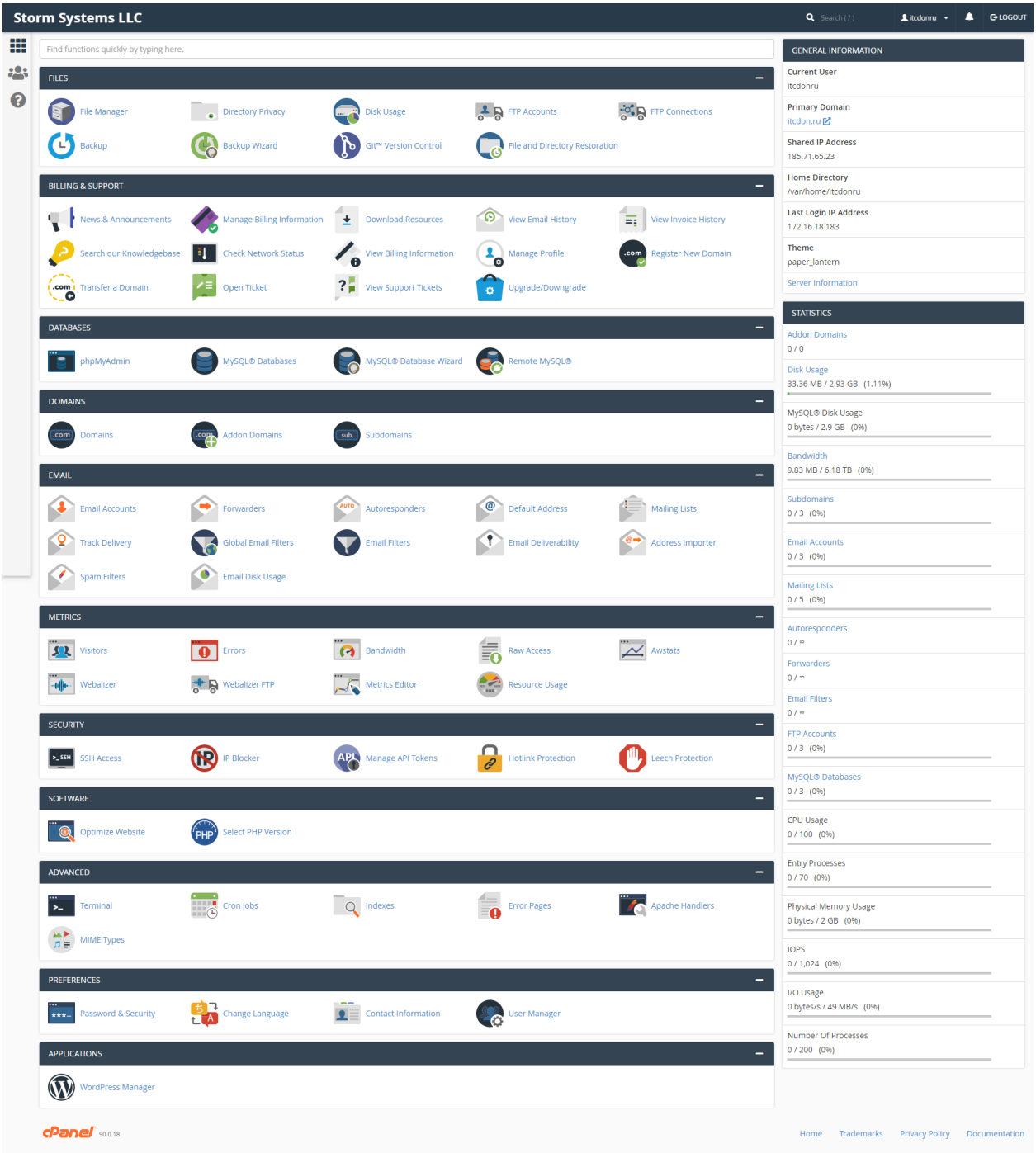
In the **Client Area**, select the **My Services** block. In the list of connected services in the **Active** status, select the **Hosting** service. Click on its line in the list. Below is a screenshot of the **Hosting Lite** service page.



Choose from managed domains and click on the dot image on the right side of the line.



A dropdown menu appears. Its items are similar to the **website protection** service (see the **Site protection - Service management** section). The only difference is the **cPanel** item. StormWall is not the developer of **cPanel**. It is a third-party product, a multifunctional control panel used to manage web hosting.



cPanel is used by many hosting providers around the world. cPanel User Guide can be found on the official page of this product at: https://docs.cpanel.net/cpanel/.

DDoS protection for TCP/UDP services

The StormWall service for protecting TCP / UDP services from DDoS attacks provides for filtering any type of malicious traffic, connected through a tunnel based on the IPIP / GRE protocol, proxying, or directly on the hosting site.

DDoS protection for TCP/UDP services is aimed at both end customers (web services, game services, VoIP, web applications for business, etc.) and service providers (data centers, hosting and Internet service providers, telecom operators, etc.).

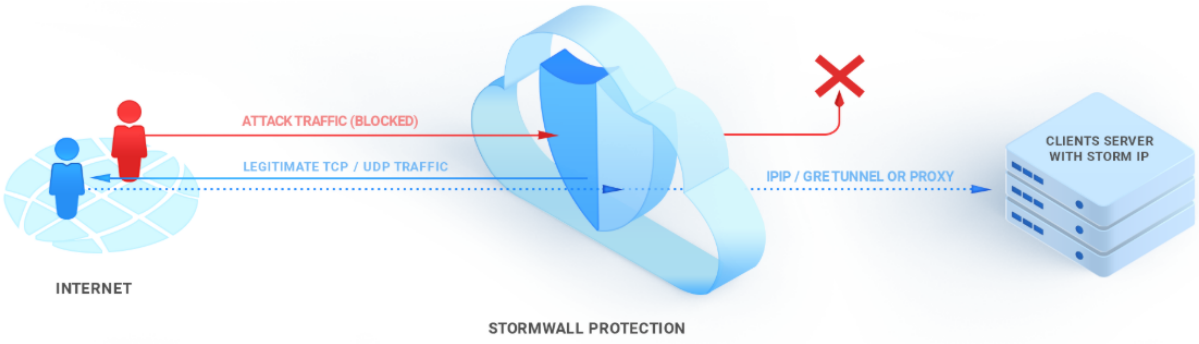
By ordering the service, you will receive the following benefits:

- Reliable protection of TCP / UDP services from DDoS attacks;
- Unlimited amount of filtered traffic;
- The number of ports on your server is unlimited;
- Filtering at 3-5 OSI levels.

How the service works

Connection to the service **DDoS Protection of TCP/UDP services** is carried out in one of two ways:

1. **With IPIP/GPE - tunneling.** This method is used if you are using an operating system such as Unix (for example, Linux or FreeBSD) or a specialized router (Cisco, Mikrotik, etc.). In this case, StormWall will "teleport" an external protected Storm IP to your equipment, with which clients communicate. In fact, another address just appears on the server - a secure one, while you see all the IP addresses of users.
2. **Using proxying**. This method is used if your server is running Microsoft Windows. In this case, all requests to the server will come from the same IP address, and you will not know the real addresses of users.



Triple Filter is used to filter traffic, **BanHammer** technology is used to filter HTTP flood, **Global Session** technology is used to protect against failures on the StormWall network nodes, and **HyperCache** technology is used to speed up work. For more information on these technologies, see the section **Anti-DDoS Hosting - How the Service Works**.

StormWall uses **ZeroNAT Tunnels** technology to reduce response times and minimize NAT issues. As a result, the customer receives a real IP address directly on his server. In addition, there is no limit on the number of ports used.

For more information about the service, please visit: https://stormwall.pro/service-protection.

Ordering a service

Enter StormWall's **Available Services** catalog as listed in **StormWall Services**. Select **Servers and Network Protection**. On a new page find **Select a subscription plan** table. Carefully study the features and limitations of each tariff, choose the most suitable for your organization. If necessary, consult with StormWall specialists (**Client Area** – **Recent Requests** – **Create a new request**). Once you have decided on the optimal tariff, click **Order** or **Contact us**.

As an example, let's give the most affordable **Standard** tariff, optimal for small Internet applications. When you click **Order**, the **Product Configuration** page opens. Here you should indicate the following data:

- **Billing cycle** (monthly, quarterly, every six months, annually);
- The need to connect UDP ports;
- The need to connect application level protection (L7) for an additional fee. When you connect L7 protection, you need to choose the speed of traffic;
- A version of an operating system running a server with a protected web application;
- Backend IP addresses;
- UDP ports.

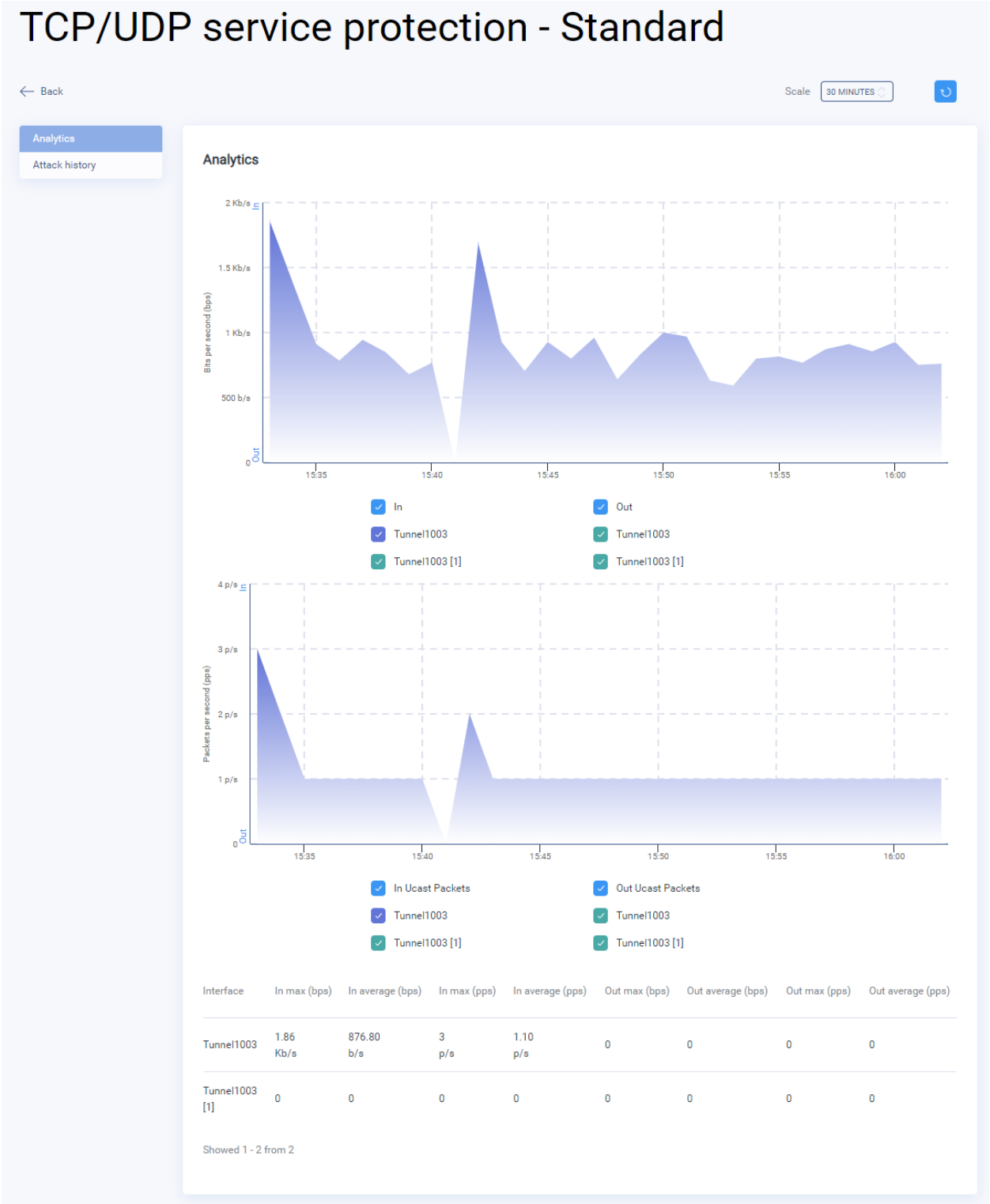
Check the list of options and the final cost. Click **Continue**. The **Review & Checkout** page opens. Here you can once again check the connected settings, options and components of the service. If you need to change anything, click **Edit**. If you change your mind ordering the service, click **Remove**. If you have a promo code for a discount, enter it in the appropriate box and click **Validate Code**. To start the payment procedure, click **Checkout**.

When you click **Checkout**, a page opens, offering a choice of payment method. On it, you should choose a convenient method, put a checkmark confirming familiarization with the Terms of Service, and then click **Complete Order**. A page with an invoice will open. This account will be available in the **Billing** block of the **Client Area**. The service you have connected will be available in the **Active products/services** block of the **Client Area**. As long as the bill for the service is not paid, it will not be launched, and will be in the status of **Pending**. After payment, the order is approved by the technical support service. Once the premoderation is successfully completed, its status will change to **Active**.

Service management

In the Client Area, select the **My Services** block. Select the **TCP/UDP Service Protection** service from the list of connected services in the **Active** status. Click on its line in the list. The service management page consists of two tabs: **Analytics** and **Attack History**.

The Analytics tab shows information about the service's work, traffic, etc.



The **Attack History** tab shows the history of attacks over the user's specified period of time. You can also generate a report in PDF format.

View attack history

When selecting a menu, **the History of Attacks** opens a list of attacks that targeted the protected service. Select one of the attacks in the list and click on her line to see the details.

The following options are displayed in the preview window:

- **Attack active.** Attack activity at the moment;
- **Attack level**. The TCP stack level on which the attack is carried out;
- **Attack target**;
- **Start time**. Recorded start time of attack;
- **End time.** Registered end time of attack;
- **Attack severity**. Assessment of attack force;
- **Attack type**. Type of attack;
- **Attack protocol**. The protocol used to attack;
- **Trigger type**. The trigger on which the attack was initially detected;
- **Trigger value**. The trigger value set;
- **Reason message**. The overall trigger message when it's activated;
- **Reason value**. The trigger value that was directly recorded at the time of the attack;
- **External in total**. The amount of traffic at the time of the attack;
- **External blocked**. Number of blocked traffic at the time of attack;
- **External whitelisted**; Number of requests missed by list of exceptions at the time of attack.

Traffic details

Attack History - Traffic Details reflect data to determine who, how, where and how requests:

- **Site requests.** Statistics on the number of allowed / blocked requests sent from the cache;
- **Traffic volume.** The amount of data transferred from the site. There is a division of statistics into the data given from the cache and directly from the project server;
- **Time and response code.** Statistics on site response time to requests and statistics on response codes for requests;
- **Heatmap and TOP countries.** Map of distribution of IP addresses from which requests are made. It can be useful for visual analysis of the geo-distribution of an attack on a site. There are also statistics directly by country. Further, this data can be used, for example, to configure the blocking of requests by geo-attribute;
- **Top locations.** Chart of site locations to which requests were made during the attack.

Protecting the network from DDoS attacks using BGP

Protecting the network from DDoS attacks using BGP service minimizes the consequences of the most sophisticated and sophisticated DDoS attack on your network. After all, even an attack on one of your IP addresses can make your entire IT infrastructure, or much of it, inaccessible to users. For more information on what DDoS attacks are, when they are used, and what threats and consequences they carry for business, you can read in **the DDoS Protection** section - **Website Protection**.

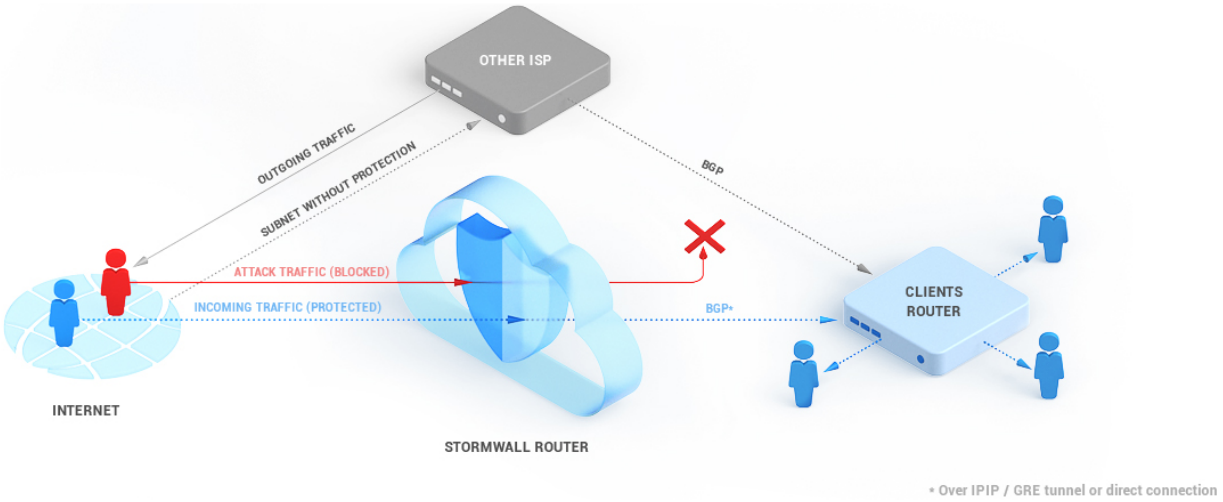
Protecting the network from DDoS attacks using BGP Service is designed for Internet providers, data centers, hosting companies, and corporate customers with their own autonomous system - the service will help ensure that IT infrastructure and networks work in a stable way, protecting them from DDoS attacks. Internet service providers can also provide this service to their customers, both for a fee and as an attractive bonus.

How the service works

StormWall specialists connect protection using an IPIP / GRE tunnel, through a traffic exchange point (IX - Internet Exchange) or by physically connecting to the StormWall network at one of the StormWall sites.

The connection is in the following order:

- We establish a connection with you;
- We launch a BGP session in which you advertise the necessary IP prefixes;
- We accept your announcements, filter all traffic and direct traffic to you that is free from attacks.



There are options for protecting against BGP-connected DDoS attacks:

1. Enabling real-time protection (Always-ON) with the passage of all incoming traffic through the StormWall filters. In this case, all of the customer's networks will be under constant protection (a DDoS attack will never be caught by surprise), but the flexibility to control incoming traffic will be limited.
2. Connecting protection manually. At the same time, not all customer networks will be announced, but only those that need protection at a certain point in time. For example, if you are expecting an attack, or it has already begun, you can manually send the network announcement to StormWall (by removing it from other providers).
3. Automation of advertising of protected networks at the start of an attack, thanks to the connection of a free **Anti-DDoS** sensor. This sensor, installed on the client's side, immediately after detecting the beginning of an attack, automatically switches the attacked network to the protection mode and removes this network from unprotected providers, and after the attack ends, returns it back.
4. Deployment of the **Anti-DDoS** sensor on a virtual machine. This allows the sensor to acquire traffic information using NetFlow, sFlow or Mirror / SPAN and integrates with your border router or router group using BGP, sending arming signals using BGP Community.

The **Anti-DDoS** sensor works according to the following scenario:

*(If **the Anti-DDoS** sensor is on the customer's side)*

1. The sensor detects the onset of an attack on one or more IP addresses;
2. The sensor then launches an attack network announcement through StormWall;
3. The sensor then removes the attack network from unprotected providers.

(Regardless of whether there is a sensor on the customer's side)

1. The sensor on the StormWall side (FlowSense system) detects which IP addresses are being attacked and redirects traffic to those addresses to filtering;
2. The attack is cut off by StormWall filters;
3. At the end of the attack, the traffic stops directing through the filters and goes directly.

(If the sensor is on the customer's side)

1. The network's announcement returns to its providers and is removed from StormWall.

To filter traffic, **Triple Filter** is used, to search for anomalies and automatically detect the type of attack - **FlowSence** technology, to protect against failures on StormWall network nodes - **Global Session** technology. For more information on these technologies, see the section **Anti-DDoS Hosting - How the Service Works**.

For more information about the service, please visit: https://stormwall.pro/network-protection.

Ordering a service

Enter StormWall's **Available Services** catalog as listed in **StormWall Services**. Select **Servers and Network Protection**. On the page that opened, click **Network Protection (BGP)**. On a new page find **Select a subscription plan** table. Carefully study the features and limitations of each tariff, choose the most suitable for your organization. If necessary, consult with StormWall specialists (**Client Area** – **Recent Requests** – **Create a new request**). Once you have decided on the optimal tariff, click **Order** or **Contact us**.

As an example, let's take a **Business** tariff, which is optimal for business applications and services. Clicking the **Order** button opens the **Product Configuration** page. It must indicate the following data:

- **Billing cycle** (monthly, quarterly, every six months, annually);
- Number of additional leased IP addresses;
- The need to connect UDP ports;
- The need to connect application layer protection (L7), at an additional cost;
- The version of the operating system under which the server running the protected web application is running;
- Backend IP addresses;
- UDP ports;

Check the list of options and the final cost. Click **Continue**. The **Review & Checkout** page opens. Here you can once again check the connected settings, options and components of the service. If you need to change anything, click **Edit**. If you change your mind ordering the service, click **Remove**. If you have a promo code for a discount, enter it in the appropriate box and click **Validate Code**. To start the payment procedure, click **Checkout**.

When you click **Checkout**, a page opens, offering a choice of payment method. On it, you should choose a convenient method, put a checkmark confirming familiarization with the Terms of Service, and then click **Complete Order**. A page with an invoice will open. This account will be available in the **Billing** block of the **Client Area**. The service you have connected will be available in the **Active products/services** block of the **Client Area**. As long as the bill for the service is not paid, it will not be launched, and will be in the status of **Pending**. After payment, the order is approved by the technical support service. Once the premoderation is successfully completed, its status will change to **Active**.

Service management

The service is managed by StormWall specialists on the customer's network equipment. If you have any questions, please contact StormWall technical support (see the **Recent Requests** section).

IP-transit

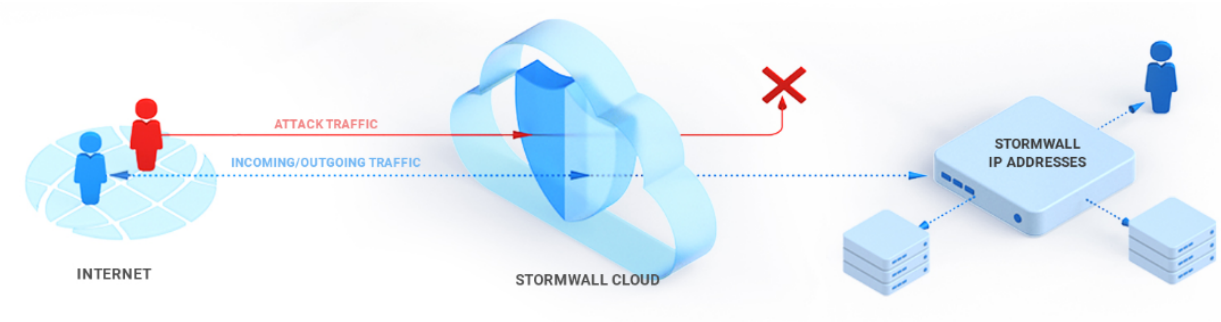
IP-transit service is designed for telecom operators, content providers and other telecom service providers. They are provided with broadband access to the networks of world providers, which is ensured through the use of modern optical networks for data transmission. The service customer receives high-speed Internet access with the allocation of a block of external IP addresses or using their

own IP addresses, which are announced: either with an autonomous system (AS) of StormWall, or with their own AS connected to the StormWall network via BGP. The StormWall network is deployed in Russia, Germany, the USA and China, and its bandwidth is more than 2 Tbit/s.

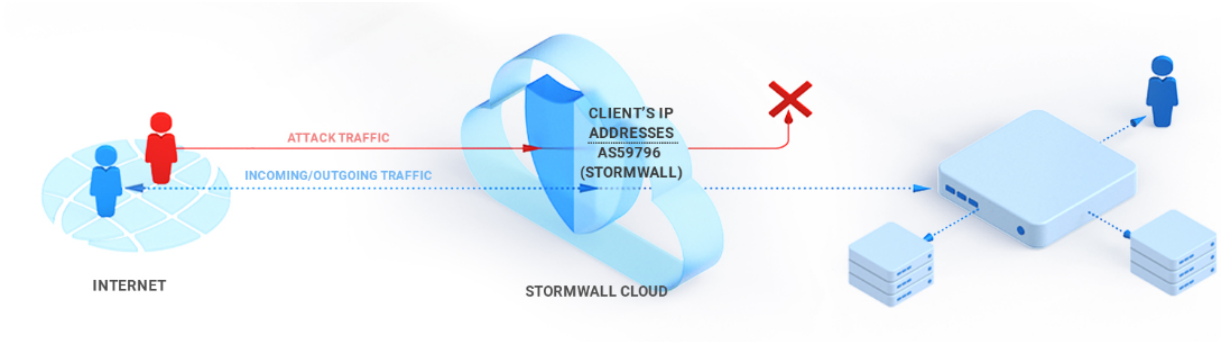
How the service works

For physical connection, you need to order marshalling to the StormWall rack at one of the company's computing platforms (Russia, Germany, USA, Kazakhstan, China (Hong Kong)).

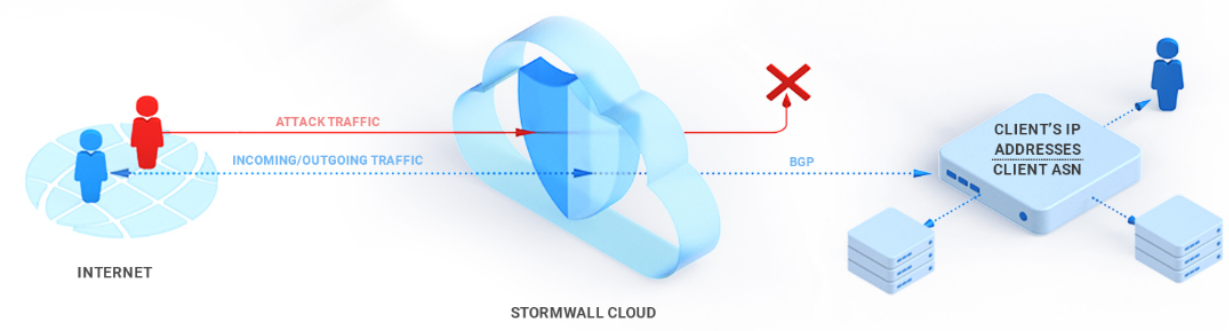
- For static routing, we allocate our clients IP addresses from our own pool for the. The client then configures their equipment with the provided IP addresses and uses them to access the Internet.



- If the client has PI (provider-independent) addresses, we add them to our autonomous system and advertise them on the Internet as our own. In this case, StormWall would accept all traffic for the allocated PI addresses and forward it to the client.



- During a dynamic BGP session, our autonomous system communicates with the client's AS (autonomous system). Next, the client advertises its IP addresses, we accept them and advertise the client's networks on the Internet.



For more information about the service, please visit: https://stormwall.pro/ip-transit.

Ordering a service

For detailed advice on fares and ordering the service, contact StormWall. To send a request, go to the **Client area - Recent requests** and click on the **Create new request** button.

Service management

The service is managed by StormWall specialists. To send a request, go to the **Client area - Recent requests** and click the **Create new request** button.

Servers & VPS

VDS/VPS DDoS servers

As part of the **DDoS protected VDS/VPS hosting**, the customer is provided with a dedicated virtual server with administrator rights for rent. All applications or sites hosted on this server, from the moment of launch, in accordance with the purchased tariff plan, will be automatically protected from various types of DDoS attacks. The customer can choose the configuration of a dedicated virtual server in accordance with their needs.

How the service works

- Protected VDS / VPS servers are deployed on a failover cluster.
- The traffic filtering system works. The traffic directed to VDS / VPS is processed by the StormWall system at 3-4 levels of the OSI model, protecting the customer's resources from infrastructure attacks that are aimed at overflowing the communication channel and overloading computing power.
- If the customer uses VDS / VPS to host websites, it is advisable to enable protection of incoming HTTP / HTTPS traffic, including analysis of requests to your server, optimization and delivery of cleaned traffic.

The VMWare platform is used to create virtual servers. **Triple Filter** is used to filter traffic, **BanHammer** technology is used to filter HTTP flood, and **FlowSence** technology is used to search for anomalies and automatically detect the type of attack. For more information on these technologies, see the section **Anti-DDoS Hosting - How the Service Works**.

For more information about the service, please visit: https://stormwall.pro/vds-vps.

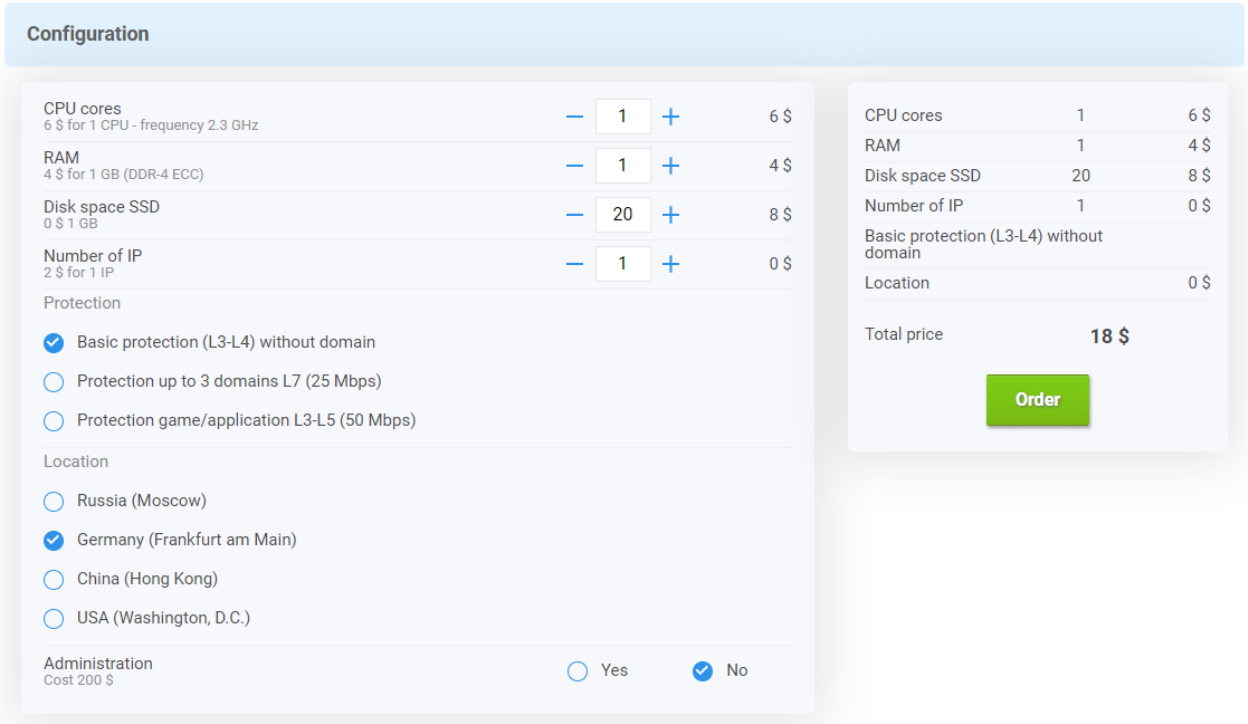
Ordering a service

Two options are available to order **DDoS protected VDS/VPS hosting.**

1. You can contact StormWall for consultation and activation of the service. Go to the **Client area - Recent requests** and click **Create new request**.
2. You can order the service yourself using the StormWall portal.

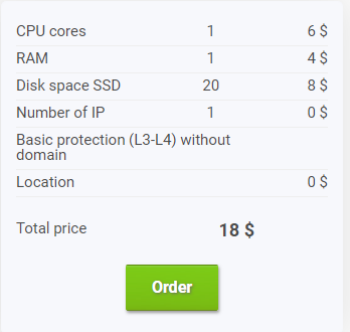
For self-order, enter StormWall's **Available Services** catalog, as stated in **StormWall Services**. Click **VPS for Web**. Find the table **Subscription plans**. Each of the tariffs (**VDS1**-**VDS4**) already offers a ready-made virtual server with a pre-configured configuration. Carefully examine the features and limitations of each fare, choose the most suitable for your organization. Consult StormWall if you need to (**Client area** – **Recent requests** – **create new request**). Please note that for each tariff **(VDS1-VDS4)** you can choose the level of protection and the physical location of the StormWall site (Moscow, Frankfurt am Main, Hong Kong). The cost of each tariff automatically changes from the choice. Below the **Subscription plans** table is the **Configuration** menu. In it you can specify:

- Dedicated virtual server hardware configuration (number of CPU cores, RAM size, SSD storage, number of IP addresses);
- Protection level (basic (no domain), protection up to 3 domains, protection of games and applications);
- Geographic location of the StormWall site;
- Enable or disable server administration by StormWall employees (for an additional fee).



So, you can choose a pre-configured configuration in the **Subscription plans** table, or set up the future virtual server in the **Configuration** menu yourself.

The right side of the **Configuration** menu displays the final configuration you have selected, as well as its cost. Make sure that you have made the right choice and click the **Order** button.



When you click **Order** in the **Subscription plans** table or **Order** in the **Configuration** menu opens the **Product Configuration** page. On it you can note the additional parameters of the **DDoS protected VDS/VPS hosting** (**VDS Constructor**), then proceed to payment. You can adjust the following parameters:

- Billing cycle;
- Physical platform StormWall, where your virtual server will be located;
- DDoS protection level;
- Enabling or disabling server administration by StormWall employees (extra charge);
- Add sites (domains) for protection;
- Select the operating system that will be installed on your virtual server. When choosing Linux or Windows, in the additional field you can specify a specific Linux distribution option or Microsoft Windows Server version.
- Configure the hardware parameters of your virtual server.

Once you've completed all the parameters you need, check the result carefully and click **Continue**.

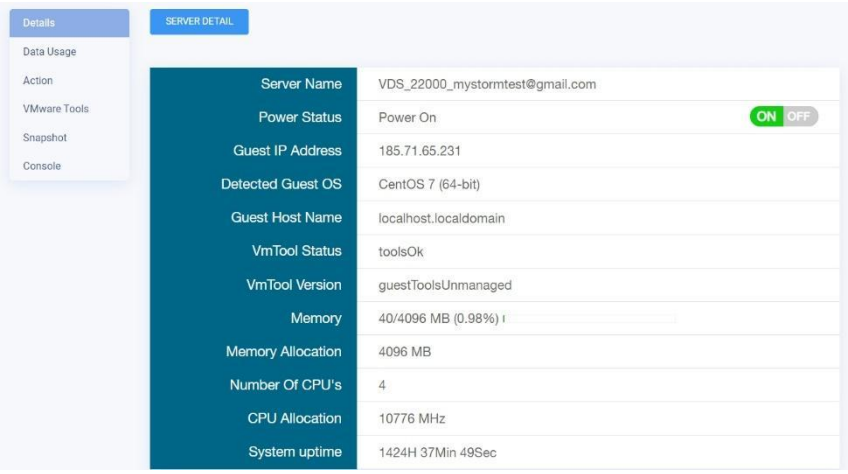
The **Review & Checkout** page opens. Here you can once again check the connected settings, options and components of the service. If you need to change anything, click **Edit**. If you change your mind ordering the service, click **Remove**. If you have a promo code for a discount, enter it in the appropriate box and click **Validate Code**. To start the payment procedure, click **Checkout**.

When you click **Checkout**, a page opens, offering a choice of payment method. On it, you should choose a convenient method, put a checkmark confirming familiarization with the Terms of Service, and then click **Complete Order**. A page with an invoice will open. This account will be available in the **Billing** block of the **Client Area**. The service you have connected will be available in the **Active products/services** block of the **Client Area**. As long as the bill for the service is not paid, it will not be launched, and will be in the status of **Pending**. After payment, the order is approved by the technical support service. Once the premoderation is successfully completed, its status will change to **Active**.

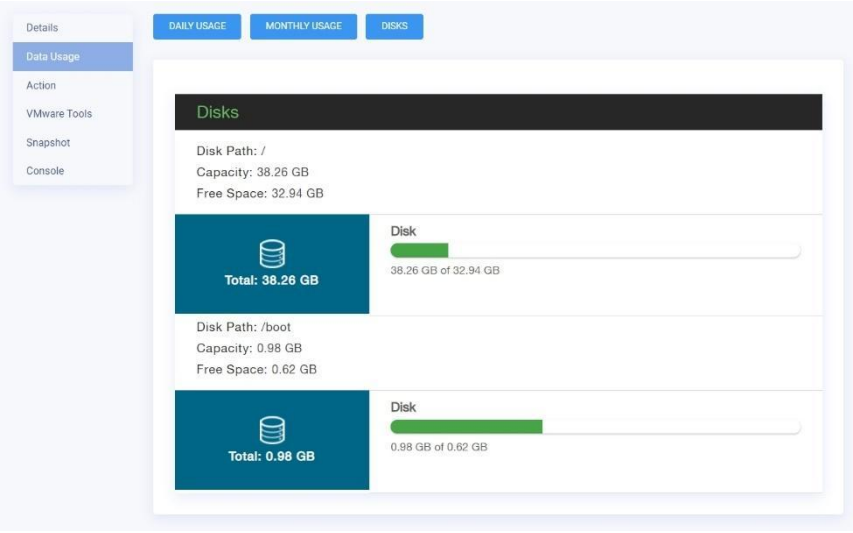
Service management

In **Client Area**, select **My Services**. On the list of your services that are in status **Active**, select service**VDS Constructor**. Click on her line on the list.

The service management menu includes several tabs. By default, the **Details** tab opens.



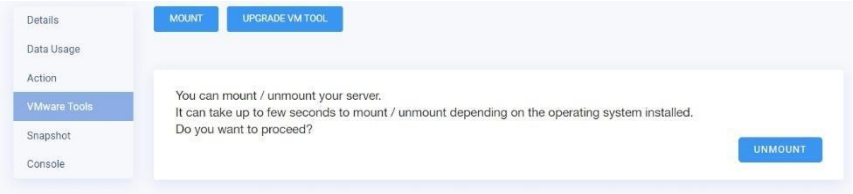
It displays all information about your server, its hardware resources, installed OS, IP addresses, etc. In the **Power Status** item, you can turn on or off your server by clicking on the switch image.



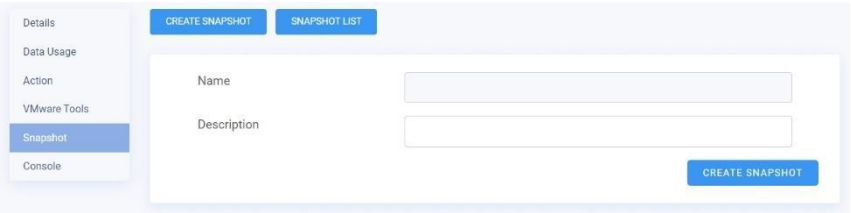
In the **Data Usage** tab, you can see the statistics of server usage during the day and during the month, as well as statistics on the use of disk drives.

With action, you can do the following server-like operations:

- Switch off;
- Pause;
- Reload programmatically;
- Reload hardware;
- Reinstall the operating system.



The **VMWare Tools** tab allows you to edit or edit an image with a virtual server.



The **Snapshot** tab allows you to take a quick snapshot of the current state of the system, if necessary, restore the system from such a snapshot. You can create at most one picture.

The **Console** tab allows you to start a virtual server with an installed operating system. You can also use the **RDP** protocol to connect to a virtual server with Windows installed, and **SSH** to connect to a virtual

server with Linux installed. You will receive the credentials for entering the operating system (login and password) by e-mail upon activation of this service.

Dedicated servers

The **Dedicated Servers** service allows the customer to rent and manage specific server equipment for a period determined by the contract. Dedicated server management is accessed remotely. All dedicated StormWall servers are physically located in France and provide excellent connectivity both with the European segment of the Internet and with Russia and the CIS countries. Renting a dedicated server allows you to avoid the cost of purchasing your own expensive equipment, as well as purchasing and equipping special server rooms. **Note**: Dedicated servers are non-refundable.

How the service works

A dedicated server works in a similar way to conventional hardware located on your computing site. All management of a dedicated server is carried out remotely. At the same time, the reliability of such equipment is higher, since it is located in data centers that meet the Tier III standard and is provided with Russian-language technical support 24/7.

For more information about the service, please visit: https://stormwall.pro/dedicated.

Ordering a service

Enter StormWall's **Available Services** catalog as listed in **StormWall Services**. Select **Dedicated Servers**. On the next page, check out StormWall's server hardware ranges and select the configuration you want. If necessary, seek advice from StormWall staff (**Client Area** – **Recent Request** – **Create New Request**). After choosing a configuration, click **Order** next to it.

On the **Product Configuration** page that opens, specify the following parameters:

- Billing Cycle;
- The number of additional IP addresses (at an additional cost);
- Inclusion or refusal of technical support and OS optimization (for an additional fee);
- Enabling or discontinuing the use of a CDN (additional cost).

Check the list of options and the final cost. Click **Continue**. The **Review & Checkout** page opens. Here you can once again check the connected settings, options and components of the service. If you need to change anything, click **Edit**. If you change your mind ordering the service, click **Remove**. If you have a promo code for a discount, enter it in the appropriate box and click **Validate Code**. To start the payment procedure, click **Checkout**.

When you click **Checkout**, a page opens, offering a choice of payment method. On it, you should choose a convenient method, put a checkmark confirming familiarization with the Terms of Service, and then click **Complete Order**. A page with an invoice will open. This account will be available in the **Billing** block of the **Client Area**. The service you have connected will be available in the **Active products/services** block of the **Client Area**. As long as the bill for the service is not paid, it will not be launched, and will be in the status of **Pending**. After payment, the order is approved by the technical support service. Once the premoderation is successfully completed, its status will change to **Active**.

Service management

The service is managed by StormWall specialists (**Client Area - Recent requests - Create new request**).

Colocation

The colocation service provides for the placement of the customer's physical server equipment in the StormWall data centers for a period determined by the contract. Placing servers in StormWall Tier III data centers will increase the reliability and availability of the customer's information systems, ensure

their connection to high-speed communication channels, reduce regulatory and business risks, and further simplify system scaling. In addition, the **Colocation** service will allow you to create a backup site in the shortest possible time to quickly restore the operability of the main systems. StormWall protection services will help protect customer equipment and applications and services installed on it from DDoS attacks and other incidents. All equipment is provided with technical support 24/7 with an average response time of 5-7 minutes.

How the service works

StormWall specialists help the customer to choose the best server hardware placement option. Currently there are two sites available for placement:

1. Moscow (MMTC-9);
2. Frankfurt am Main (Germany) (e-Shelter).

For more information about the service, please visit: https://stormwall.pro/collocation.

Ordering a service

To order the service and get all the necessary advice on the cost of the service and technical issues, please contact StormWall (**Client Area - Recent requests - Create a new request**).

Service management

The service is managed by StormWall specialists (**Client Area - Recent requests - Create new request**).

CDN&WAF

Content delivery network (CDN)

The Content Delivery Network (CDN) service is designed to transmit content at the maximum possible speed to an unlimited number of users around the world with the maximum download speed regardless of the location of both the content source and its consumer. Customers of the service do not need to bear the costs of deploying and operating their own infrastructure, software and high-performance communication channels for storing and quickly simultaneously providing large volumes of content, especially since the cost of technical support for such infrastructures is growing steadily as they age.

How the service works

Data from the content owner to the consumer follows the shortest (and therefore fastest) route. At the same time, each user around the world receives content from the content owner from the CDN server closest to him (user).

The service is implemented as follows:

- The customer's content is uploaded to the **CDN**;
- It is distributed to all local servers within the network;
- The data goes to each user from the nearest CDN server.

The total bandwidth of the CDN network is 500 Gbps. CDN data centers are located in more than 40 cities around the world.

For more information about the service, please visit: https://stormwall.pro/cdn.

Ordering a service

To order the service and get all the necessary advice on the cost of the service and technical issues, please contact StormWall (**Client Area - Recent requests - Create a new request**).

Service management

The service is managed by StormWall specialists (**Client Area - Recent requests - Create new request**).

Cloud WAF

The **Cloud WAF** service allows you to protect your web applications (online stores, information systems, web services, etc.) from attacks. Protection is provided by an application layer firewall hosted in the cloud by StormWall. Unlike solutions made in the form of software or hardware and software systems, **SolidWall Cloud Web Application Firewall (WAF)** is a cloud service that does not require a separate infrastructure, software, and the costs associated with their purchase, configuration, installation, connection and support: payment is made by subscription. The SolidWall WAF product was developed by the Russian company SolidSoft and StormWall provides it to customers using the cloud model, in integration with DDoS protection.

How the service works

The use of the most detailed models of operation of the protected application, along with signature and semantic methods for detecting anomalies, make it possible to protect it from both widespread simple types of attacks and complex targeted attacks. An effective mechanism for early suppression of false positives has been implemented. Special machine learning algorithms allow you to increase WAF performance, better detect false positives, automatically build application operation models, and effectively use the solution in an active development cycle.

Integration with StormWall DDoS protection makes it easy to protect applications from all vectors of hacker attacks.

For more information about the service, please visit: https://stormwall.pro/waf and https://solidwall.ru.

Ordering a service

Enter StormWall's **Available Services** catalog as listed in **StormWall Services**. Select **Cloud WAF**. On a new page find **Select a subscription plan** table. Carefully study the features and limitations of each tariff, choose the most suitable for your organization. If necessary, consult with StormWall specialists (**Client Area** – **Recent Requests** – **Create a new request**).

Click **Order**. Since StormWall's DDoS attack protection is integrated with the Cloud WAF service, after clicking Order on the Cloud WAF service page, the **Website Protection** service page opens. Here you can choose a tariff for DDoS protection. After choosing, click on the **Order** on the **Website Protection** service page. The **Product Configuration** page opens. It already shows the cost of the WAF tariff that you have

chosen. Do not forget to check this box and mark the number of domains protected by WAF. Otherwise, the procedure for filling out, ordering and paying is similar to that described in the section **Website protection - Ordering a service**.

Service management

In the **Client Area**, select the **My Services** block. Select **Website Protection** from the list of connected services in **Active** status. Click on her line in the list.

On a new page, in the **Add-ons - WAF Usage** block, click **Connect**. On a new page, configure the WAF settings, if you have not configured them before, and then click **Update configuration**. Thus, you can add the **Cloud WAF** service to the previously ordered **Website Protection** service.

Upon activation of the **Cloud WAF** service, the customer receives by email a link to the WAF control panel, as well as login credentials (login and password). The control panel is a standalone product. It has its own reference documentation (**Link**). We recommend that you read it before starting to manage the **Cloud WAF** service.

API for clients

The **API for clients** service is an auxiliary tool (software interface) that includes a set of commands that automates work with the StormWall protection system.

The StormWall API supports the following features:

- Domain management, load balancing, redirect and cache configuration;
- Working with SSL certificates and private keys;
- Manage DDoS protection settings, blacklists and whitelists;
- Manage DDoS sensor settings for different IP addresses;
- Managing StormWall Network Connection Settings;
- Getting information about attacks and access to other statistics.

How the service works

You can find detailed information on how the Client API Service works in the StormWall Knowledge Base at: https://stormwall.pro/my/index.php?rp=%2Fknowledgebase%2F79%2F--API.html.

You can find a complete list of supported API commands at: https://api.stormwall.pro/documentation?_ga=2.189643439.527849805.1599325704-1454448139.1594127873#/

Glossary

API - is an application programming interface, which is a set of ready-made classes, procedures, functions, structures and constants that are provided by the service for use in external software products.

Backend- server - is a server on which websites can be located, with the help of which the website logic is implemented and is also used to process data.

Backend IP - a unique network address of the Backend server in a computer network built on the basis of the TCP/IP protocol stack.

BGP - border gateway protocol. Dynamic routing protocol, which belongs to the class of external gateway routing protocols.

CDN - data transfer service to an unlimited number of users around the world with the maximum download speed regardless of the location of both the content source and its consumer.

DoS - Denial of Service, an attack on a system to cause a denial of service: a stream of garbage requests to it creates an excessive load, making it impossible to process requests from bona fide users.

DDoS attack - Distributed Denial of Service, a distributed DoS attack executed simultaneously from a large number of devices over which attackers were able to gain control and generate streams of garbage requests on command. Such an attack can cause denial of service to systems of a large company or network.

DNS - Domain Name System, a system that stores information about Internet domains. Its key function is to provide the IP address of a host or resource by its fully qualified domain name. The system consists of multiple servers and has a distributed hierarchical architecture. In order to minimize the risks of hacker attacks on the DNS and improve the integrity and reliability of the data stored in it, security and protection tools are built into the DNS servers: DNSSEC, TSIG, DANE, etc...

DNS record - is a record of the correspondence between the name and service information in the domain name system, for example, the correspondence of a domain name and an IP address.

GRE - a network packet tunneling protocol developed by Cisco Systems. Its main purpose is to encapsulate network layer packets of the OSI network model into IP packets.

HTTP-Headers - are special parameters that carry certain service information about the HTTP connection.

HTTP-flood - it is a type of DDoS attack in which an attacker manipulates GET or POST requests to attack a Web Server or application.

IPIP - is an IP tunneling protocol that encapsulates one IP packet into another IP packet. Encapsulation of one IP packet into another IP packet, this is the addition of an external header with Source IP - the entry point into the tunnel, and Destination - the exit point from the tunnel.

L7 - system for aggregation and analysis of HTTP / HTTPS requests.

Mirror/SPAN - duplicate packets from one port of a network switch (or VPN) to another.

NAT - Network Address Translation, a mechanism in TCP / IP networks to translate the IP addresses of transit packets. Used by many service providers and private users to solve the problem of the lack of real IP addresses and ensure the security of local networks connected to the Internet.

NetFlow - a network protocol designed for accounting for network traffic, developed by Cisco Systems. Is the de facto industry standard and is supported not only by Cisco equipment, but also by many other devices.

PI-адрес - Provider Independent, ISP-independent IP addresses are addresses that can be routed by a small number, regardless of the upstream ISP.

RDP - proprietary application-level protocol used to provide remote user interaction with the server running the terminal connection service.

RPS

sFlow - is a general-purpose network traffic measurement system technology. Designed to be embedded in any network device and provide continuous statistics on any protocol (L2, L3, L4 and up to L7) so that all traffic on the network can be accurately characterized and monitored.

SSH - network protocol. Used for remote operating system management and file transfer. The key feature is that SSH encrypts traffic, making connections secure.

SSL - Secure Sockets Layer, cryptographic protocol, which implies more secure communication. It uses asymmetric cryptography to authenticate exchange keys, symmetric encryption to preserve confidentiality, message authentication codes for message integrity.

Swagger - is a small collection of scripts for creating interactive documentation for web application APIs with REST protocol.

TCP - Transmission Control Protocol, OSI model transport layer protocol, one of the main protocols of the Internet. At one time it was developed to manage data transmission and ensure its reliability.

UDP - User Datagram Protocol, protocol for transmitting messages (datagrams) to other hosts without error checking and fixing.

VDS /VPS - Virtual Dedicated Server/Virtual Private Server, is a hosting service in which the client is allocated an entire virtual server with full administrative rights, which make it possible to install any software on the server. Functionally, a virtual server is no different from a physical one.

WAF - Web Application FireWall, a set of monitors and filters designed to detect and block network attacks on a web application.

WebSocket - a communication protocol over a TCP connection, designed to exchange messages between a browser and a web server in real time.

Botnet - is a network of computers that are infected with malware that allows attackers to remotely control them, send spam messages and viruses, serve as a location for software that carries out DDoS attacks - all without the knowledge of the real owners of computers.

Domain - is a symbolic identifier (name) of one of the regions of the Internet. The use of domain names is intended to facilitate the designation of individual nodes and resources deployed on them from the point of view of their perception by humans.

Ping - is a period of time during which a packet sent from a computer passes through the network to another computer or server, and returns back.

Subdomain - is a domain that is part of a higher-level domain. For example: if test.com is the main domain, then Subdomain.test.com is the subdomain.

Proxying - is the use of an intermediary program (proxy) that processes traffic in a certain way for its subsequent transmission to another program. In particular, security proxy servers process traffic in such a way as to prevent unauthorized access to traffic and to minimize the threat of network attacks.

Shaping - limiting packets to a specified speed limit in packets per second.