



BITNINJA
SECURITY

2022

TECHNICAL SUPPORT **CHEATSHEET**

We created the following little guide or cheatsheet to help you understand and troubleshoot with BitNinja.
Of course you are free to contact us anytime you wish.

WWW.BITNINJA.COM



TEAM MESSAGE

INTRODUCTION

Let's make the internet a safer place together!

The team at BitNinja has been working together for more than four years. The idea to build a robust server security platform started at our partner company, which was the biggest shared hosting company in Hungary, providing top tier hosting services more than 15 years. We faced the same day-to-day frustrations with hackers and bots, and decided to build a better way to keep servers secure from the latest threats. Our goal is to provide the highest level of support at BitNinja, that's we handle all support requests ourselves.

Contact us via email: info@bitninja.io with any issue and we're always happy to help.

Becoming a server security ninja takes a little practice, so we designed this cheat sheet to help you quickly learn more about BitNinja and how it keeps your servers secure. We've collected some of the most frequent use cases and solutions to typical issues you may encounter. Once again, please don't hesitate to reach out to us with any questions you have. Even if it seems like a silly question or you don't know exactly what to ask, it's ok to email for help. We want to be sure you are totally satisfied with BitNinja and your customers are too.

BITNINJA TEAM

TABLE OF CONTENTS

TEAM MESSAGE	02	WEBSITES WITH CDN ARE NOT WORKING	12
UNDER ATTACK	04	BLOCKED CRAWLERS OR GOOD BOTS	13
DOS PROTECTION	05	WEBSITE HAS BEEN HACKED	14
IP IS GETTING GREYLISTED BECAUSE OF PORT SCANNING ON PORT 110	06	SOME FUNCTIONS OF THE WEBSITE AREN'T WORKING	15
UNABLE TO UPLOAD FILES	07	WAF 403 ERROR PAGE	16
BIC/CAPTCHA COMPLAINTS	08	WAF RULES WITH HIGH FALSE POSITIVE RATE	17
CUSTOMIZE CAPTCHA/BIC PAGE	09	SSL CERTIFICATE PROBLEMS	18
GREYLISTING DYNAMIC IP ADDRESS	10		
SERVICE IS NOT WORKING PROPERLY	11		

UNDER ATTACK

WHAT TO DO?

If you believe you are under attack or some of your customers might be, there are a few steps with BitNinja to protect your servers from more harm.

DDoS Attacks?

Against DDoS attacks there are some options we do recommend.

1. Adjust the Rate Limit in the SSL Terminating configuration by the perDomainRateLimitInterval variable.
2. If you are aware of which website/URL you host is being attacked you may setup our URL Captcha on it.
3. Block countries that the website not use.
4. Lower the threshold of the DosDetection module.

- ✓ In case the IP address was not blocked for some reason, you may blacklist it in the Firewall – Blacklist area.
- ✓ If the hacker targeted one of your customers, you may set up an URL captcha on the affected domain/URL pattern. This can be really helpful in case a botnet attack.
- ✓ If you are using our WAF module, in last scenario, you may also turn on the Lock Down mode on a specific domain pattern, keep in mind though, this will turn on readonly mode, preventing user from various actions such as: Payments, Posting, Forms. This can be effective if you don't want the infection to spread further.
- ✓ In the event you know a file is infected or malicious, you can also create a Malware Signature of it.



“One single vulnerability is all an attacker needs.”

Windows Snyder

DOS Protection

Network Attack

Our DoS Detection module helps whenever an IP address creates more than 80 connections to your server. You can adjust the number of connections to detect or set different thresholds for different ports, and services.

By default, BitNinja will block the IP address for a minute and put it on the greylist, this threshold can be also changed.

Thresholds can be configured in the file
`/etc/bitninja/DosDetection/config.ini`

```
; Thresholds set to DoS Detection
;
[tresholds]
general = 80
; Threshold for remote SMTP servers.
remote[25] = 200
remote[53] = 200
; Threshold for local ports
local[22] = 40
```

BitNinja DoS Detection also works in together with our AntiFlood module. When there are recurring DoS attempts, the IP will be greylisted for a longer period of time.

More customizations can be found on [DosDetection - BitNinja Docs](#)

IP IS GETTING GREYLISTED BECAUSE OF PORT SCANNING ON PORT 110

Your customer using desktop Email Client such as Outlook, Thunderbird, Windows Mail, etc



Date: 2022-09-07 11:55:01
Victim server: mail.bitninja.com
Attacker ip: 1.2.3.4
Severity label: lowest



```
{  
  "PORT HIT": "1.2.3.4:2919->8.8.8.8:110"  
}
```

If your customer is complaining that they are always greylisted by BitNinja and you are seeing port hit logs about port 110 (which is the POP3 port), it may be that the customer's email client settings are incorrect. Most likely, the issue is that their email client is trying to connect to the host server and not the appropriate address.

Please ask your customer to double-check the mail server settings in their email client.

UNABLE TO UPLOAD FILES

HOW TO SOLVE IT?

1. Ask them to send you their IP address (<https://www.whatsmyip.org/>), then search for it in the BitNinja Dashboard.
2. If the IP is greylisted, you can remove the IP address from the greylist with the -GL button. Make sure that the affected rules aren't enabled on this pattern (or you can disable the whole WAF on this domain).
3. If the reason for the greylisting was a WAF incident, we recommend that you create a domain pattern, then disable the affected WAF rule or the module for the newly created pattern. How can you create the domain pattern? BitNinja Dashboard -> WAF 2.0 menu -> Choose the appropriate server -> Create a new domain pattern for the affected domain. BitNinja WAF Overview
4. In the WAF menu if you see that the Lock Down option is enabled, please turn it off.

BEAWARE

If there are any issues related to the WAF, please do not disable the whole module on the server as this opens a security vulnerability on the affected server. Instead, follow the steps above to create a domain pattern or contact us for assistance.

BIC/CAPTCHA COMPLAINTS

HOW TO CHECK THEM?

- 1. To help your customers understand why they are seeing a BIC or CAPTCHA page, please feel free to send them the infographic that you can find in this package. It will help them understand how BitNinja protects their server while also allowing legitimate traffic through.
- 2. Ask them to send you their IP address (<https://www.whatsmyip.org/>), then search for the IP address in the BitNinja Dashboard.
- 3. Find the reason why the IP was greylisted. Scroll down to the very first incident or find the first log since the last delisting (=green incident icon):

Date: 2022-09-07 13:58:54
Attacker ip: 199.188.237.220
User id: 0000
Severity label: unknown

☐ Manually removed by user.

Blocked by WAF rule 930120 ⓘ
Date: 2022-09-07 13:58:35
Victim server: server123.bitninja.com
Victim domain: bitninja.com
Attacker ip: 199.188.237.220
Severity label: high

☐

DISABLE WAF RULE

```
Url: [project1080.website/]
Headers: [array (
  'X-Forwarded-Proto' => 'http',
  'User-Agent' => 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.27',
  'Accept-Language' => 'en-GB,en;q=0.9,en-US;q=0.8',
  'BN-Client-Port' => '22658',
  'Accept-Encoding' => 'gzip, deflate',
  'Cookie' => 'starstruck_b50d658936058597b7dd157217096dfd=839c013c9f95d5bf4f345b08da31b88c',
  'BN-Frontend' => 'waf-http',
  'Accept' => 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/;q=0.8,application/signed-exch'
```

- 4. If you see any malicious log entries, you should inform your sysadmins to investigate the issue further and determine the root cause. You can also contact us regarding the issue at info@bitninja.io, we're happy to help.
- 5. If the recent incidents appear to be valid actions, the infection has been fixed, and/or the IP is dynamic, you can remove the IP from the greylist with the -Greylist button. You can also whitelist the IP by using the +Whitelist button. This way, your customers won't see any BIC/ CAPTCHA pages even if the IP is greylisted again because of a new malicious action.

+ GREYLIST

+ WHITELIST

+ BLACKLIST

CUSTOMIZE CAPTCHA/BIC PAGE

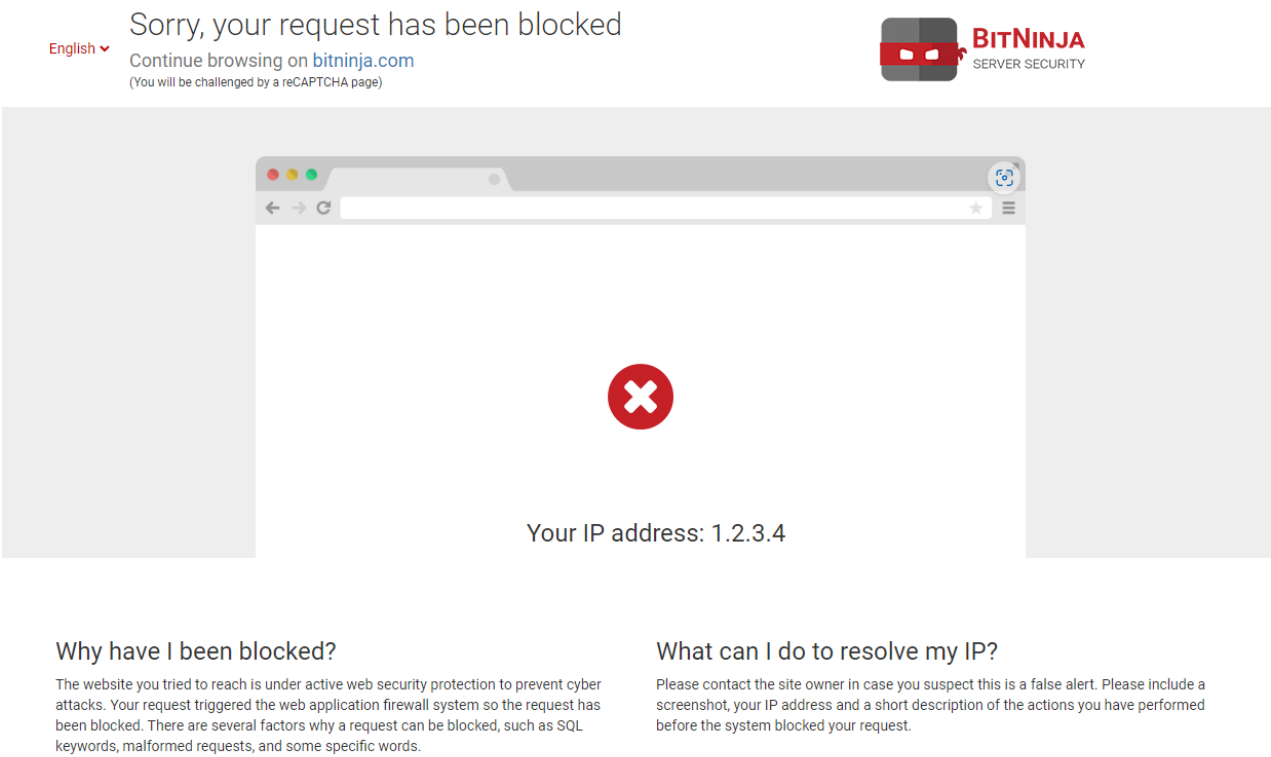
BitNinja supports multi-language templates for the Captcha/BIC page, which can be found within the directory `/etc/bitninja/CaptchaHttp/www`.

This directory will take over the default one, that would be replaced by BitNinja on each update.

Localization

Your own language can be also added in the file `v2/js/translations.js`.

Note that, the language depends on the browser language. If there is a Greek user with an English browser, it will display the English CAPTCHA page



GREYLISTED DYNAMIC IP ADDRESS

When a customer’s PC or mobile phone is using a dynamic IP address, it may be that a previous user of this IP performed a malicious action (e.g. DoS, malicious scan) which led to the IP being greylisted. When this happens, we recommend that you delist the IP so your customer can continue browsing without any issue. Don’t worry, if another malicious request comes from that IP in the future, it will be blocked and greylisted by BitNinja again.

Dynamic IPs	Static IPs
192.1.1.1	192.1.1.1
192.1.1.2	
192.1.1.3	
Periodically changes	Never changes

SERVICE IS NOT WORKING PROPERLY

MAKE IT WORK!

The Port Honeypot module randomly chooses ports from the most scanned/attacked 1000 ports. The Port Honeypot module never uses ports that are open at the time the module starts and also monitors port open requests to prevent conflicts. Ask them to send you their IP address ([https:// www.whatsmyip.org/](https://www.whatsmyip.org/)), then search for it in the BitNinja Dashboard.

SEARCH IP ADDRESS

Look for port hit logs and check for the destination port.



Date: 2022-08-12 07:55:33

Victim server: example.server.com

Attacker ip: 1.2.3.4

Severity label: unknown

```
{
  "PORT HIT": "1.2.3.4:40096->2.#.#.4:123456"
}
```

Here you can see the purpose of the different ports: [https:// www.speedguide.net/ports.php](https://www.speedguide.net/ports.php)

If your customer is using this port to run a service, here is how to set up the list of ports you never want to be used for honeypot purposes.

Config file location: /etc/bitninja/PortHoneypot/config.ini

```
;
; List of ports the module will never use for honeypot purposes
;
[ports_never_use]
ports[]=80
ports[]=25
ports[]=22
;
```

WEBSITES WITH CDN NOT WORKING

HOW TO RESOLVE?


Content Delivery Networks, CDN in short are really common these days to give extra boost for the website, in case you or your customers use it, you will want to enable the Trusted Proxy module as well as make sure the CDN provider is whitelisted.

The most popular CDNs IP ranges are included in our Trusted Proxy list by default. If your customers are using a CDN then you will need to enable the Trusted Proxy module. This will enable the BitNinja agent to see the real IP addresses behind the CDNs' proxies.

If your customer uses a CDN that is not included in the default list and experiences issues with accessing their site (the site is inaccessible, or it loads but CSS and scripts are missing), the source of the problem is that one or more IPs of the CDN are greylisted by BitNinja. When this happens, you should whitelist the CDN's IP ranges and the IP addresses of the CDN to the Trusted Proxy list.

You can add all of the IP ranges used by a CDN from the Firewall -> Trusted Proxy menu. Separate the IP ranges with a comma and space to add them in one shot.

If you experience this issue with other CDN's, please contact us at info@bitninja.io.

 Trusted Proxies

Module status:

ADD CUSTOM PROXY ADDRESS

IP address*:

Comment*:

+ ADD PROXY

✓ Known proxies

Filter...

Trusted proxies	IP address	Comment	Created At	Action
> Cloudflare (22)				
> QUIC.cloud (119)				
> BunnyCDN (375)				
> Fastly (21)				
> KeyCDN (2)				
> CDNSUN (78)				
> wao.io CDN (6)				
> EZOIC (29)				
> exactlywww (28)				
> CloudFront CDN (156)				
> MetaCDN (51)				

BLOCKED CRAWLERS OR GOOD BOTS

It's possible that BitNinja identifies internet crawlers as malicious bots due to their configuration and may greylist them due to security reasons. According to our policy about bots, we cannot whitelist them globally.

Our management decided it is the responsibility of our customers (the hosting providers) and the end-user to agree on what monitoring solutions, crawlers, and bots they allow. As it is always a risk of some level to whitelist IP, let alone on a global level. We do not want to bear the responsibility of deciding what bots and crawlers we whitelist.

As mentioned above the decision of what bots and crawlers to allow is the hosting providers and the end-users therefore please contact the hosting providers and or the endusers with the whitelisting request. If that is not possible we can disable the abuse email sent from the IP addresses used by the service.

WEBSITE HAS BEEN HACKED

HOW TO SCAN AND CLEAN?

By default, BitNinja's Malware Detection module only captures real-time infection attempts. It can be helpful to run a full scan to find previous infections. If a customer reports that their website has been hacked, please run a manual malware scan on the appropriate host.

You can start a malware scan from the Anti-Malware-> Scan settings menu. At the bottom of the page, you can add the path for the domain. Start a full scan on the server by running a scan on the / path.

Here is the command to run the scan:

```
bitninjacli --module=MalwareDetection --scan=/var/www
```

This command will look for malware in the /var/www folder.

You can also upload malware to the dashboard adding them to your account-level malware database. Our team will also check this uploaded malware and add it to the global malware database.

You can also set up a scheduled malware scan on each server from the Antimalware-> Scan settings menu. We recommend setting the scheduled malware scan to a time period when the server's traffic is the lowest. This will be a full malware scan.

If there would be malware that is not yet in our database you can upload the code to our database from the Anti-Malware -> Local malware signatures menu.

You can also find files that BitNinja suspects to be malware. After validating a file all files matching the signature will be quarantined on the server.

To prevent future infections, we recommend that you create honeypots and add a new domain pattern for the hacked domain and enable the medium or the high-risk WAF rulesets.

NOTE

Still can't fix?

Worry not, we can help you to get rid of the infection on the website and protect it.

Contact us for Website Cleaning service offers at info@bitninja.io

SOME FUNCTIONS OF THE WEBSITE AREN'T WORKING

HOW TO FIX?

There are many reasons why a website can stop functioning correctly, but if you think BitNinja is blocking some of the site's functionality, here is what you should check:

One reason the website may not be functioning correctly is when the Malware Detection module quarantines a file false positive.

You can check for quarantined files in the BitNinja Dashboard: Anti-Malware -> Infected files menu.

You can filter the results for the server's hostname. If you know which directory contains this user's files, you can also add the path.

You can manually restore files from the quarantine using the following command

```
bitninjacli --restore=/path/to/file
```

You can also restore all files that matched the same malware signature with the following command:

```
bitninjacli --module=MalwareDetection --discard-signature --id=<signatureId>
```

The "signatureId" parameter can be found if you click on the DETAILS button next to the files path and then select the Malware info section at the top.

Please do not hesitate to contact us if the above-described situation happens to you so we can check the malware signature and discard it if necessary.

Another reason the site may not be working correctly is when the Lock Down function of the WAF is enabled. You can check the Lock Down setting and disable it following these steps:

BitNinja Dashboard -> Firewall menu -> Web Application Firewall menu -> Choose the appropriate server at the top left -> Select the / pattern's settings or if there is a custom pattern for that domain, click on the settings icon -> Make sure that the Lock down function and the Virtual Honeypot Rules are disabled.

If a third-party service is being blocked then check their IP address in the BitNinja dashboard.

You can whitelist the service's IP address(es) from the Firewall -> Whitelist menu.

WAF 403 ERROR PAGE

HOW TO FIX?

If a visitor to one of your customer's sites sees the WAF 403 error page, it means their request has triggered the BitNinja WAF. By clicking on the domain on the top left side of the page, the IP will be removed from the greylist and the visitor can continue browsing.

SEARCH IP ADDRESS

Each delist by the visitor after the 403 error page will increase the false positive rate of the affected rule. Refer to the section on "WAF rules with high false positive rate" to learn more.

IMPORTANT

If there are any issues related to the WAF, please do not disable the whole module on the server as this opens a security vulnerability on the affected server. Instead, follow the steps on the next page to disable the rules with high false positives.

If customers continue to report seeing WAF 403 error pages, we recommend you investigate the situation for the following these steps:

Ask them to send you their IP address (<https://www.whatsmyip.org/>), then search for it in the BitNinja Dashboard.

If the IP is greylisted, you can remove the IP address from the greylist with the -GREYLIST button.



Look for WAF logs and collect the rule IDs which resulted in false positives. Then, disable these rules on the Dashboard.



Blocked by WAF rule 930120 ⓘ
Date: 2022-09-07 13:58:35
Victim server: server122.bitninja.com
Victim domain: bitninja.com
Attacker ip: 1.2.3.4
Severity label: unknown

☐

DISABLE WAF RULE

You can also click on the "DISABLE WAF RULE" button and select the pattern to quickly disable it.

How can you disable WAF rules for specific domains?

- BitNinja Dashboard -> Firewall -> Web Application Firewall -> Choose the appropriate server -> Create a new domain pattern for the affected domain.
-> Make sure that the affected rules aren't enabled on this pattern (or you can disable the whole WAF on the domain).

WAF RULES WITH HIGH FALSE POSITIVE RATE

⊞ BitNinja Ruleset (Enabled: 5/14)	Triggered	False	Forked
⊞ OWASP Core Ruleset (Enabled: 1/17)	Triggered	False	Forked
⊞ Scanner Detection (Enabled: 1/5)	3 times	0x	<input checked="" type="checkbox"/>
⊞ Protocol Attack (Enabled: 3/10)	0 times	0x	<input checked="" type="checkbox"/>

If you see a high false positive rate (above 2-3%) next to a WAF rule, it's recommended to switch off that rule in order to avoid false positives and customer complaints. Consider carefully which rules you enable on the server, for example, it's not always worth enabling the SQL injection rules on a website or a subdomain with a PHPMyAdmin installation, as some poorly-written websites can actually use SQL injection as part of their normal operation.

We are continuously fine-tuning the standard rule sets for BitNinja to avoid false positives and keep your customers happy.

SSL CERTIFICATE PROBLEMS

If a website shows a “Not secure” notification when viewed in your web browser or it isn’t accessible via HTTPS, there may be issues with confirming the SSL certificates for the site.

What can cause this issue?

- BitNinja’s SSL Terminating module can’t find the binary which is responsible for the web service.
- You aren’t using the standard Apache or Nginx settings.
- Your web server is not Apache or Nginx.

SSL certificate issues may require server configuration, please share the following steps with your IT Team and connect them with the BitNinja Team so we can help to resolve the issue quickly.

1. You can find instructions on our documentation site to create the certificate miner yourself.
2. Configure the web server settings in the SSL Terminating module’s config file (/etc/bitninja/SslTerminating/config.ini).

Here you can add the binary locations which are used and the main config file location as well.

```
;
; Web server settings
;
[webserver]
;; if binary location not set SslTerminating module tries to find where is apache.
;apachectlBinaryLocation = '/usr/sbin/apache2ctl'
;apachectlBinaryLocation = '/usr/sbin/httpd'
;apachectlBinaryLocation = '/opt/sp/apache/bin/apachectl'
;listVirtualHostParameter= '-S'
```

3. After these modifications, please run the following commands:

bitninjacli --module=SslTerminating --reload

bitninjacli --module=SslTerminating --regenerate (if it comes back with an error, don’t worry, run the bitninjacli --module=SslTerminating --enabled and try running the command again)

If these steps don’t solve the problem and the website is still inaccessible, please do the following:



WAF 2.0

HTTPS protection: ☐

Module status: ☒

i Add more WAF domain patterns

You can create patterns by combining a domain name, URL and*.
For example, the pattern "example.com/*" will match for any requests containing the example.com domain.

example.com/

Manage ruleset templates

1. Turn off the HTTPS protection on the WAF 2.0 menu temporarily.

Important: don't forget to enable it again as soon as the problem is resolved.

2. Please contact us (info@bitninja.io) with the following details and we'll investigate the situation and come up with a solution ASAP.

- What kind of web server are you using?
- Send us a sample config file.
- What kind of web server is responsible for the HTTPS connections?
- What compilation options are you using?
- Please also send us the log files from the `/var/log/bitninja/mod.ssl_terminating.log`

NOTE

If you are making a certificate request, please disable the WAF HTTPS protection while you are making your request. Don't forget to switch it back on as soon as the renewal is complete.

ADDITIONAL HELP

Don't forget that you can count on us anytime, drop us a message on the Dashboard or just send us a message via info@bitninja.io or contact your Customer Success Manager.

Education Program

If you are new to BitNinja, you can also check our Education Program.

1. [Network Attacks – What are they and how can you filter them with BitNinja?](#)
2. [IP filtering – Blacklists, whitelists, greylists and the BitNinja logic](#)
3. [WAF- Managing patterns and testing the BitNinja WAF](#)
4. [Malware Detection – Set up, schedule, catch and quarantine with BitNinja](#)

SiteProtection

Do you want to take off the load of your customer support and give more value to your products, while you earn some extra revenue?

Learn more about [SiteProtection here](#).

Premium Support

Would you like to turbocharge the customer support?
Check out our [Premium Support](#) options for exceptional assistance.

HAVE A NINJASTIC DAY!

DO YOU HAVE ANY QUESTIONS?
GET IN TOUCH WITH US



BitNinja Security

E-mail: info@bitninja.io

Facebook: <https://facebook.com/bitninja.io>

Twitter: <https://twitter.com/bitninjaio>

Linkedin: <https://www.linkedin.com/company/bitninja-io>