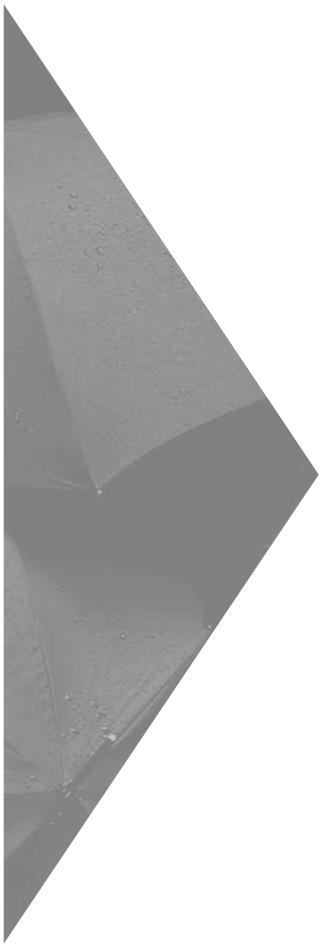
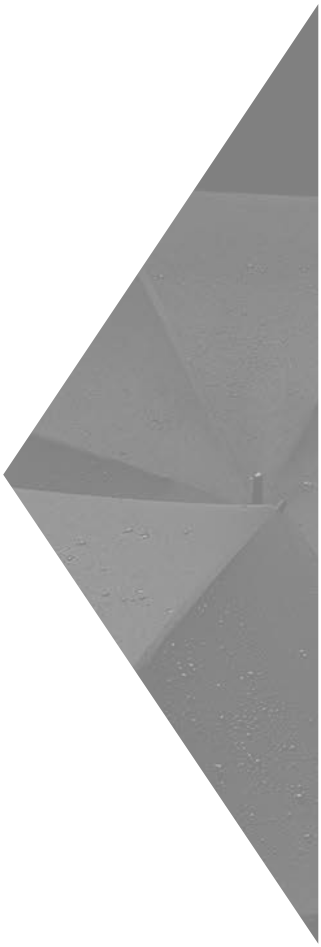
Portal Guide





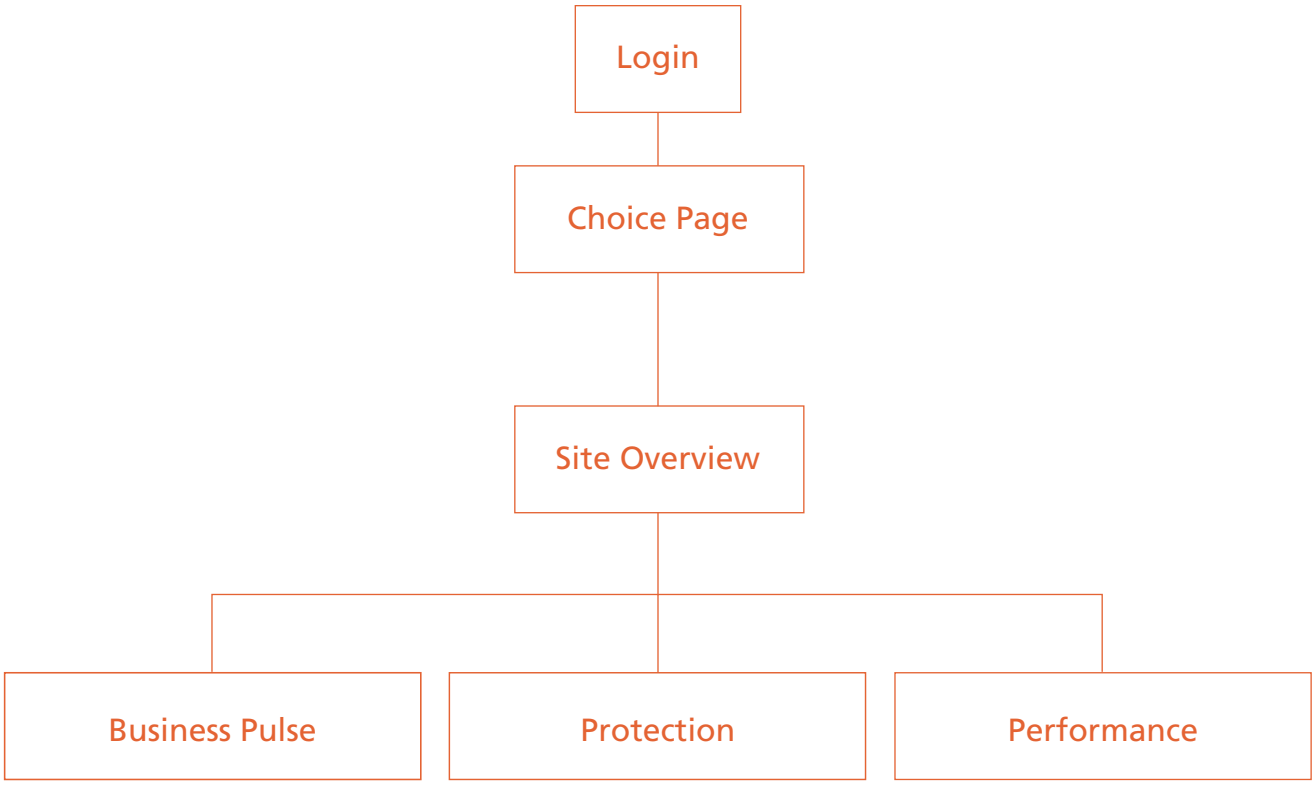
Nexusguard Application Protection

Ver 1.2.9

NEXUSGUARD™

Table of Contents

Site Map



Chapter 1

Introduction

The Application Portal reduces network security risk by delivering full network traffic visibility, advanced analytics and real-time threat defection for all traffic into your network. This enables you to identify, detect and respond to threats swiftly. A comprehensive report of all activity lets you conduct forensic investigations, perform proactive incident response and even make informed business decisions.

About Application Portal

Application Portal harnesses and combines the power of Big Data with visual and analytic technologies to deliver real-time, meaningful business and security intelligence to empower business leaders to make winning decisions. The Application Portal monitors your website from three perspectives: business status, threat protection and service performance.

Business Pulse

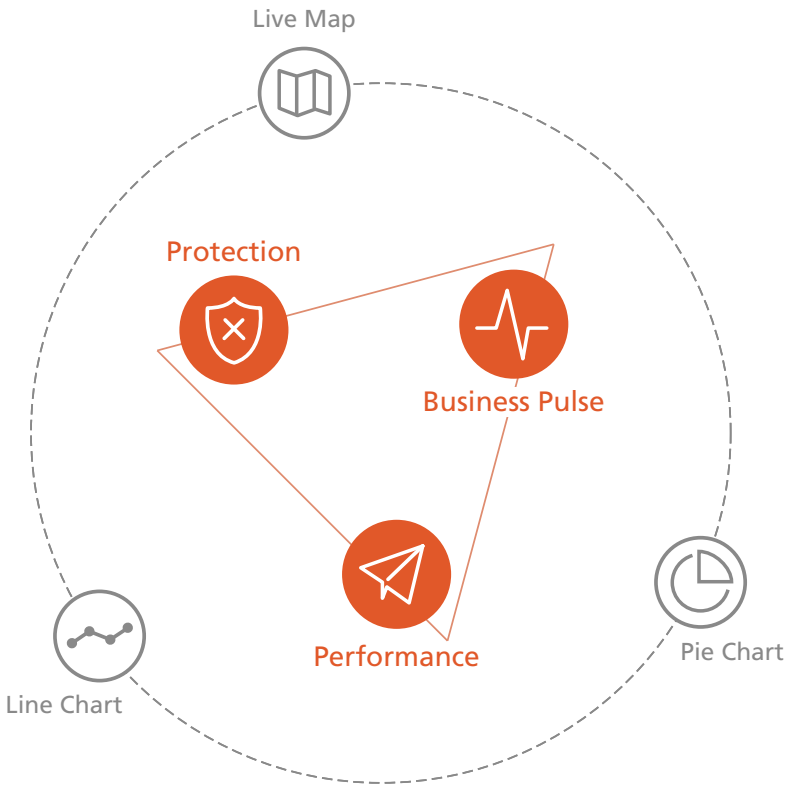
Business Pulse is a statistical analysis module that visually presents traffic trends, business trends and ultimately user experience.

Protection

The protection module provides real time visualisations of attacks as they happen. Global heat map allows users to quickly identify the geographical sources of attacks and to deploy strategic defense.

Performance

Through service performance monitoring, website owners can better understand the efficiency of content delivery and the level of performance improved by the Application Portal.



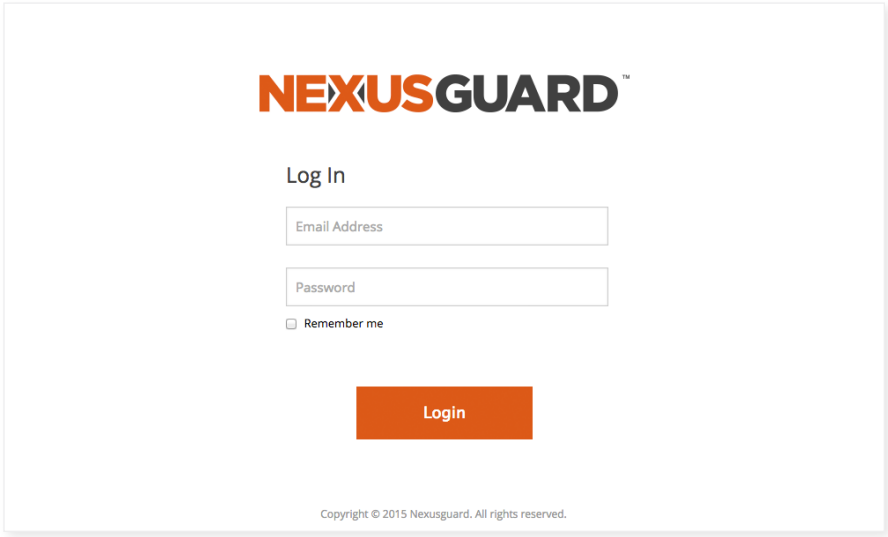
Chapter 2

Navigation

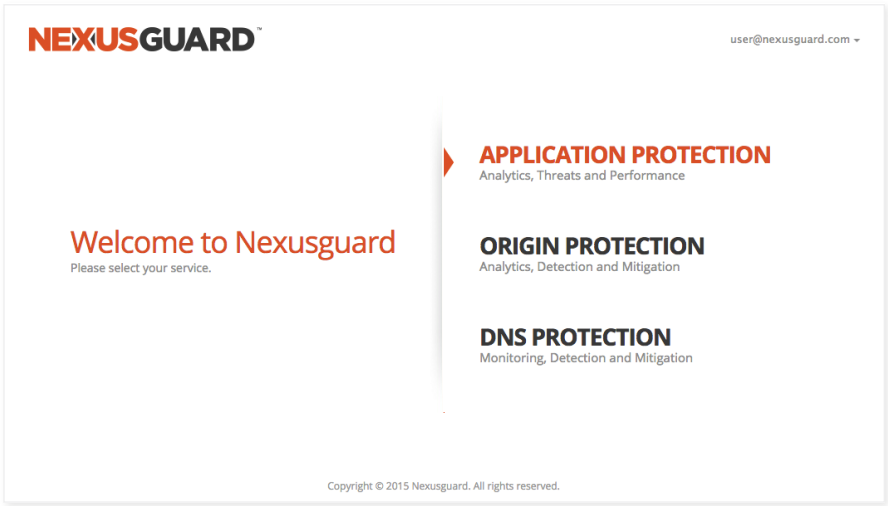
One would quickly get lost in the abundance of information available on Application Portal. This section guides you through how to make use of the interface tools to navigate around Application Portal so that you can efficiently examine business, protection and performance of your assets.

Quick Start

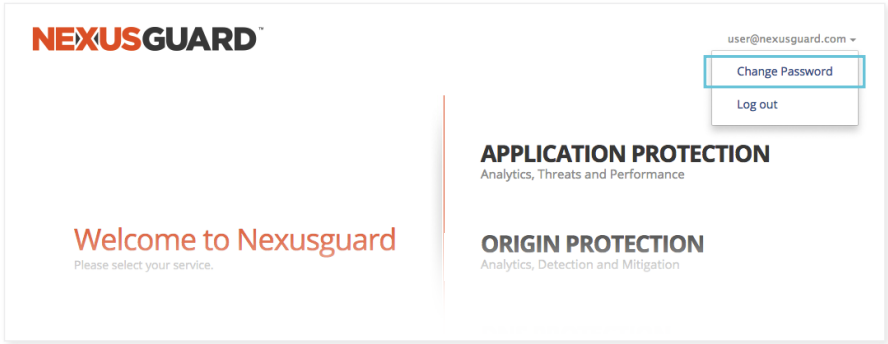
Step 1 : Go to https://login.nexusguard.com and login



Step 2 : Choose Application Protection



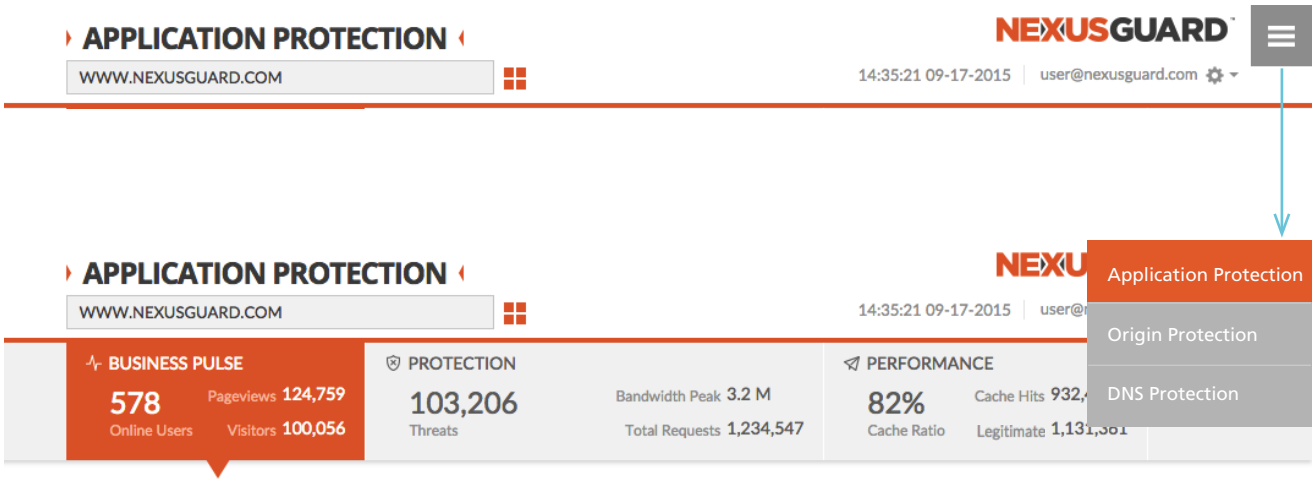
Step 3: Change Password



Step 4: Complete

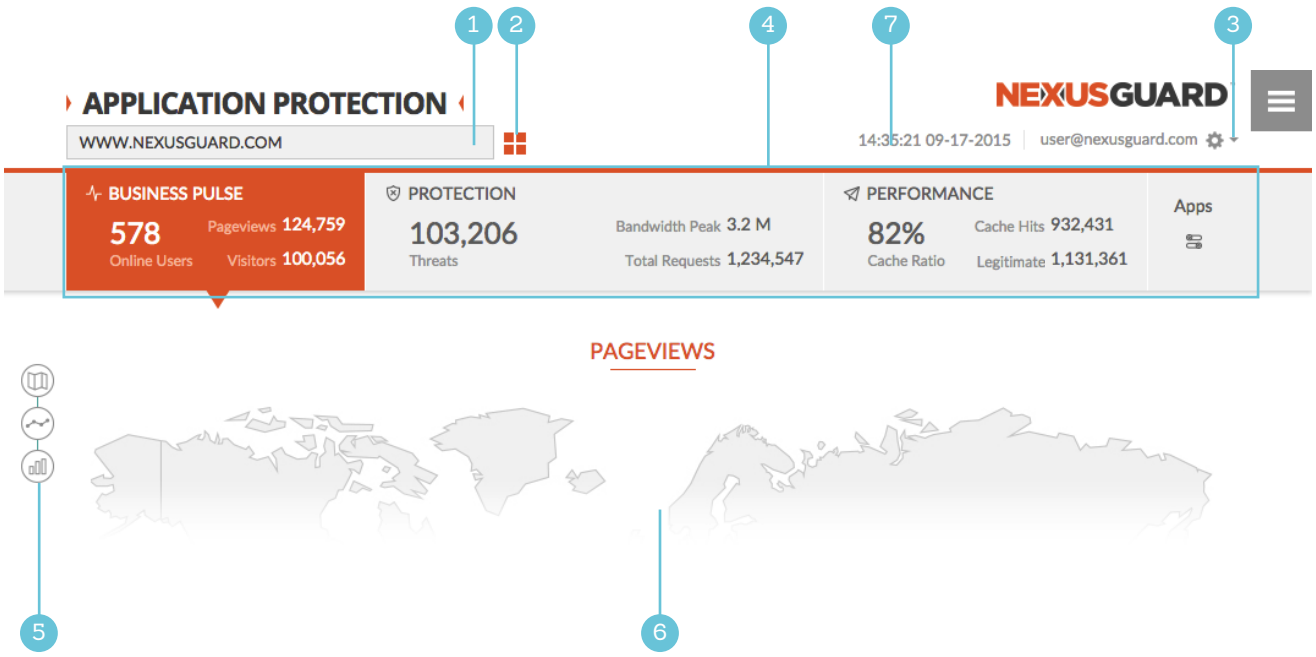
Switch Service

Click ☰ in the upper right corner to access different protection platforms.



User Interface (Best viewed in IE10.0, Firefox 38.0, Chrome 46 or Safari 9.0)

Application Portal comprises of six major functional modules.



1. IP / Domain Name

Displays the asset currently under management, showing either its URL or IP address

2. Site Navigation Drawer

Opens the site navigation drawer which allows you to select from a list of sites you are managing.

3. Account Settings

This section allows for changing user account settings and provides other support.

4. Horizontal Controls

Users can click or swipe on tabs to switch between the three perspective modules.

5. Vertical Controls

The floating bar and vertical scrolling selector provide users with shortcut access to different information.

6. Main Monitoring Area

This section displays the results of the selected module.

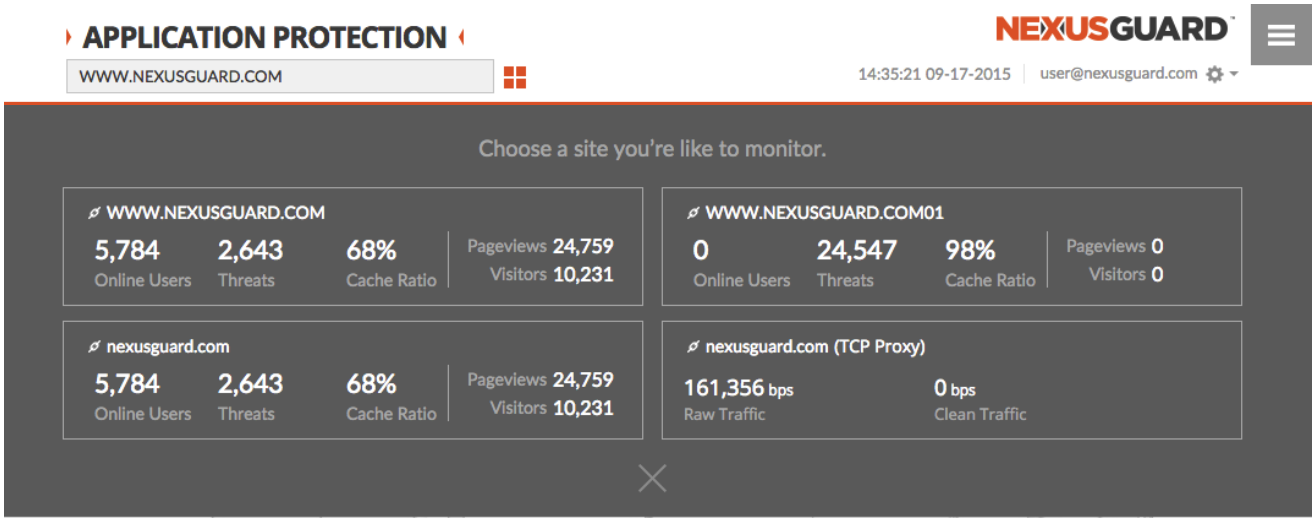
The analytics are presented in an immediately intuitive and visually appealing way, including live chart and interactive map—in real time.

7. Browser Time

Browser time.

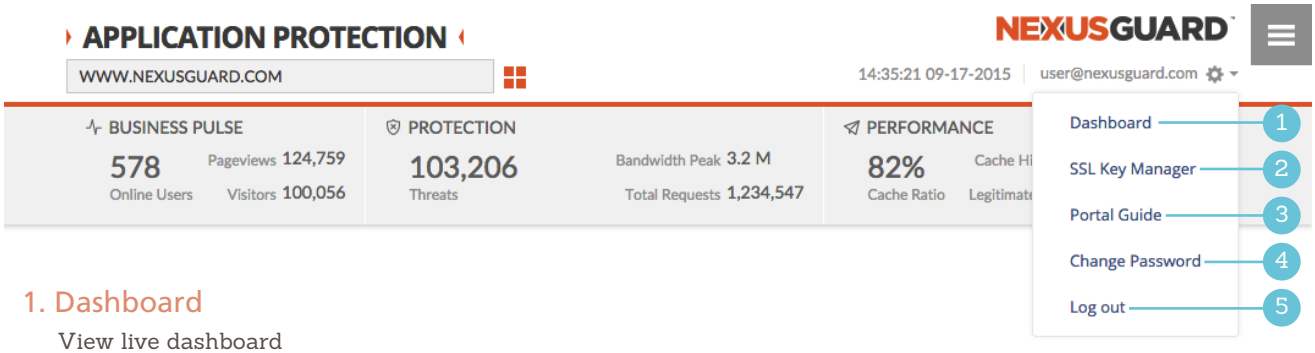
Site Information

Click ⊞ to roll out the site navigation drawer to view all sites under protection at a glance.



Account Settings

User account settings and other support provided by the platform.



1. Dashboard

View live dashboard

2. SSL Key Manager

Manage your SSL Key

3. Portal Guide

Download Portal Guide

4. Change Password

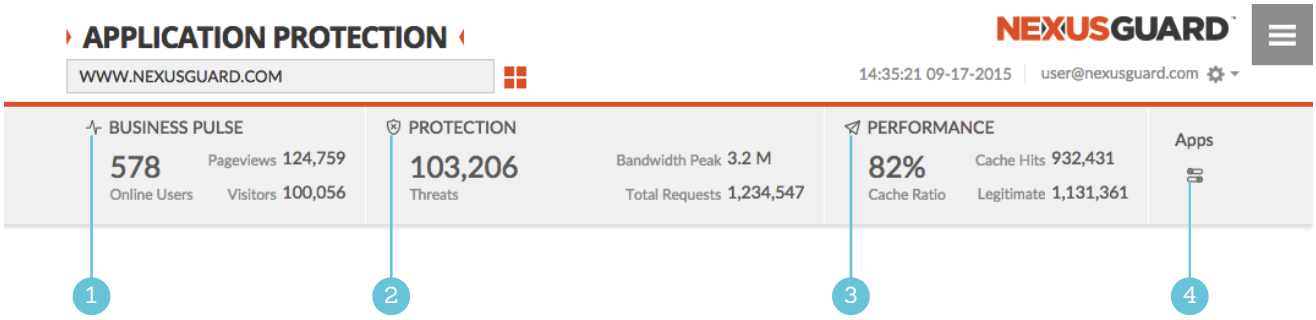
Reset your password

5. Log out

Log out

Horizontal Control

Users can click or swipe on tabs to switch between the three perspective modules.



1. Business Pulse

This module provides business related data and analytics to provide users with a better transparency of their business activities.

2. Protection

This module provides comprehensive information related to threats, attacks and mitigation.

3. Performance

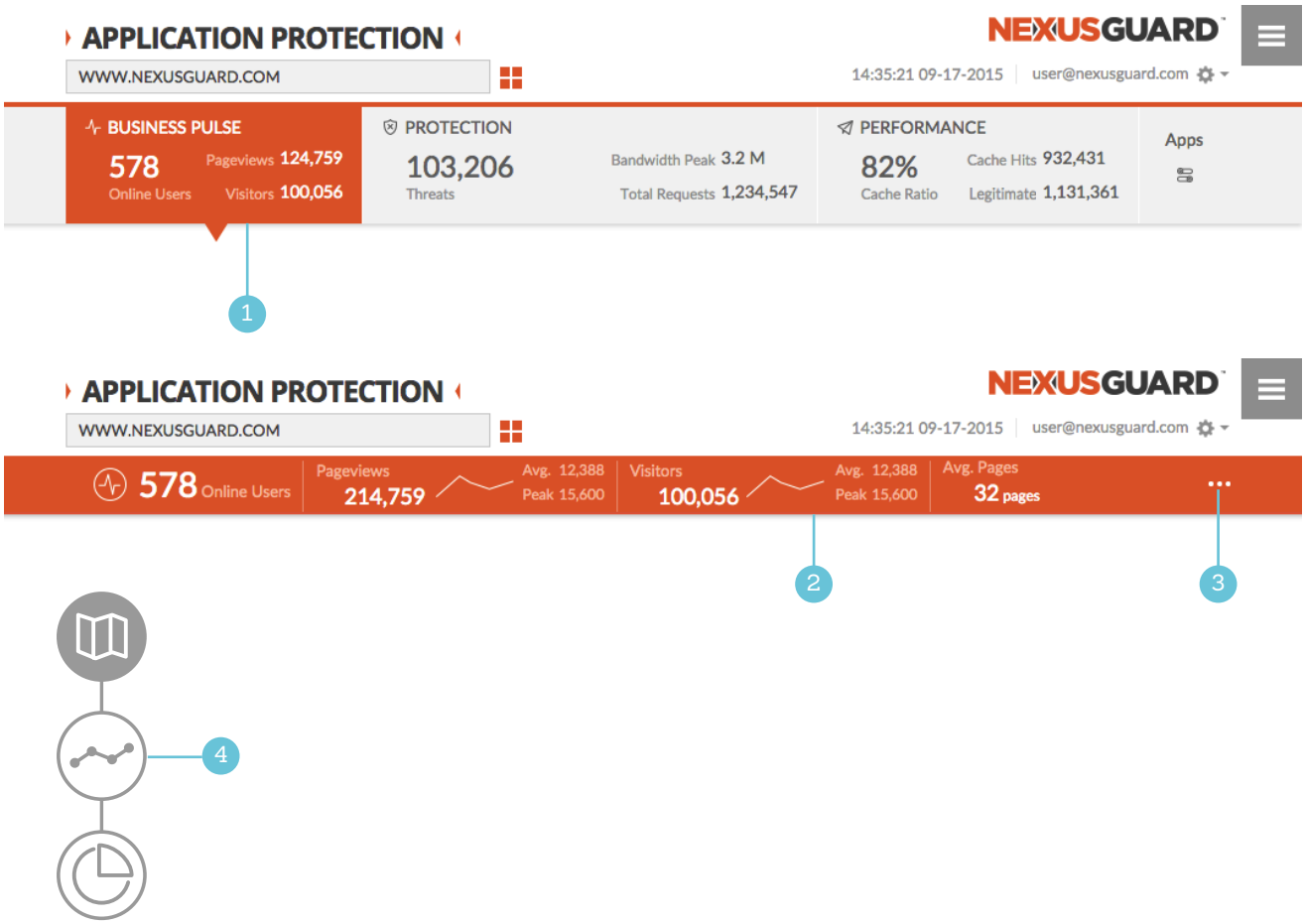
This module displays site performance and optimization information.

4. Apps

Provides an overview of value-added services provided under the Application Portal

Vertical Controls

When looking into each specific site, information is presented in three perspective modules - Business, Protection & Performance. Under each mode, users will find a wealth of valuable information and statistics carefully sectioned and indexed. The floating bar and vertical scrolling selector provide users with dynamic and quick access to these information.



1. Module Selector

Provides access to one of the three perspectives - Business Pulse, Protection & Site Performance. On this Module selector, you are also presented with respective key statistics in real time.

2. Floating Bar

As you scroll down the page, the module selector is replaced by a floating display which provides a more detailed view of the selected module.

3. Back Button

Return to module overview

4. Vertical Scroll Selector

Provides quick vertical scrolling to each section within the module.

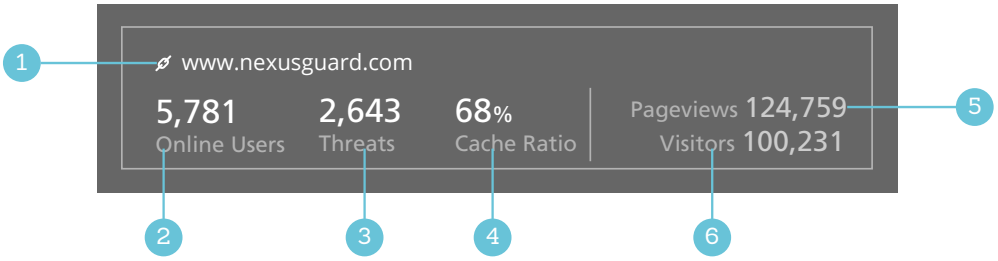
Chapter 3

Data Definition

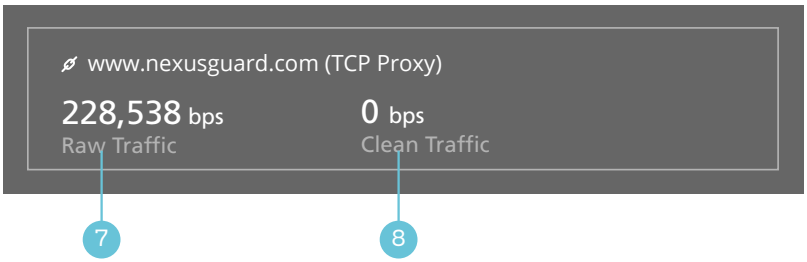
This section introduces data definitions, time zones and update frequency of all elements on the Application Portal. This allows for flexible analysis and comparison to maximize the efficiency and security level of all sites.

Site Overview

Site overview displays 5 sets of data that summarize the status of each site under protection. Displayed data are accumulated values beginning at 00:00:00 (UTC) and resets at 23:59:59 (UTC) of each day.



For some reason, such as protocol/port mismatch, some sites or applications may have to run in TCP proxy mode in order to get protection. If so, an additional box (below) is shown to display raw and clean traffic statistics.



1. IP / Domain Name

Website URL / IP Address.

2. Online Users

The number of online users browsing the website. Users displaying no activity within 50 seconds are considered offline.

3. Threats

Accumulated actual and potential threats on the site of the day. (1)

4. Cache Ratio

Proportion of content served from cache.

5. Pageviews

Accumulated page views of the day.

6. Visitors

The number of unique site visitors accumulated of the day.

7. Raw Traffic

The amount of raw traffic to the site in the TCP proxy mode observed in the past 24 hours.

8. Clean Traffic

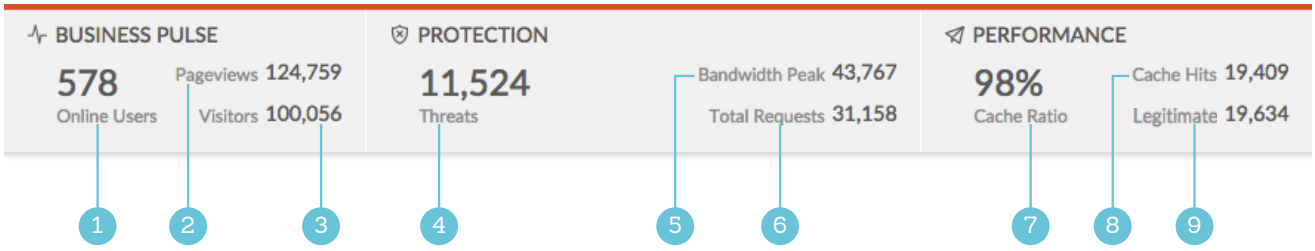
The amount of clean traffic routed to the client server after scrubbing in the past 24 hours.

(1) "of the day" means the time duration from GMT 00:00:00 to 23:59:59.

Overview

The Application Portal provides information on three fronts: business, protection and performance for analyzing and evaluating a site's status precisely. Three sets of critical data are shown from each perspective for comprehensive evaluation and monitoring.

Figures shown may be subject to a 0.3% variation due to Application Portal's computation methods.



1. Online Users (Real-time / updated every 50 secs)

The number of online users browsing the website. Users displaying no activity within 50 seconds are considered offline.

2. Pageviews (Last 24 hrs / real-time)

Accumulated page views of the day.

3. Visitors (Last 24 hrs / real-time)

The number of unique site visitors accumulated of the day.

4. Threats (Last 24 hrs / updated every 1 min)

Accumulated actual and potential threats on the site of the day.

5. Bandwidth Peak (Last 24 hrs / updated every 2 mins)

The peak bandwidth throughput (inbound + outbound) of the day in bits per second (bps), including both legitimate and non-legitimate traffic.

6. Total Requests (Last 24 hrs / updated every 1 min)

The accumulated number of all requests to the site of the day, including suspicious, malicious and legitimate requests.

7. Cache Ratio (Last 24 hrs / updated every 1 min)

The proportion of HTTP requests served from cache (cache hits/legitimate).

8. Cache Hits (Last 24 hrs / 1 min)

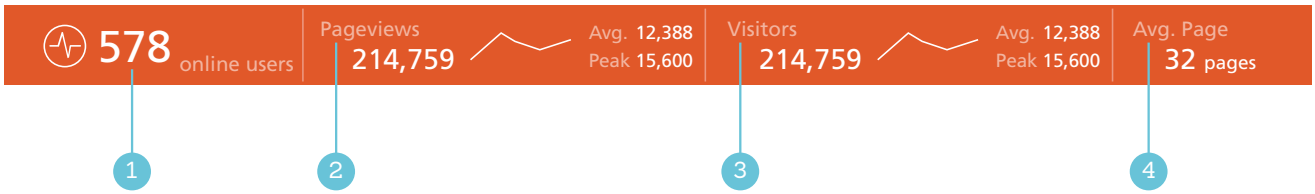
The accumulated number of HTTP requests served from cache.

9. Legitimate Traffic (Last 24 hrs / 1 min)

The accumulated number of legitimate requests, including authorized web crawlers, of the day.

Business Pulse

The Business Pulse module provides analytics on online business activity analytice.



1. Online Users

The number of online users browsing the website. Users displaying no activity within 50 seconds are considered offline.

2. Pageviews

Accumulated page views of the day.

- Avg. Pageviews - average number of page views per day over the last 7 days.
- Peak Pageviews - highest number of page views per day over the last 7 days.

3. Visitors

Accumulated number of unique site visitors of the day.

- Avg. Visitors - the average number of visitors per day over the last 7 days.
- Peak Visitors - the highest number of visitors a day over the last 7 days.

4. Avg. Page (Last 24 hrs / updated every 1 min)

Average page views per visitor of the day.

Pageviews (Real-Time/Real-Time)

Global distribution of page views in real time.

1. Pageviews by region

= 1 Pageview = 2-9 Pageviews =10-99 Pageviews

=100-999 Pageviews = 1,000-9,999 Pageviews

= 10,000-99,999 Pageviews

2. Live Data

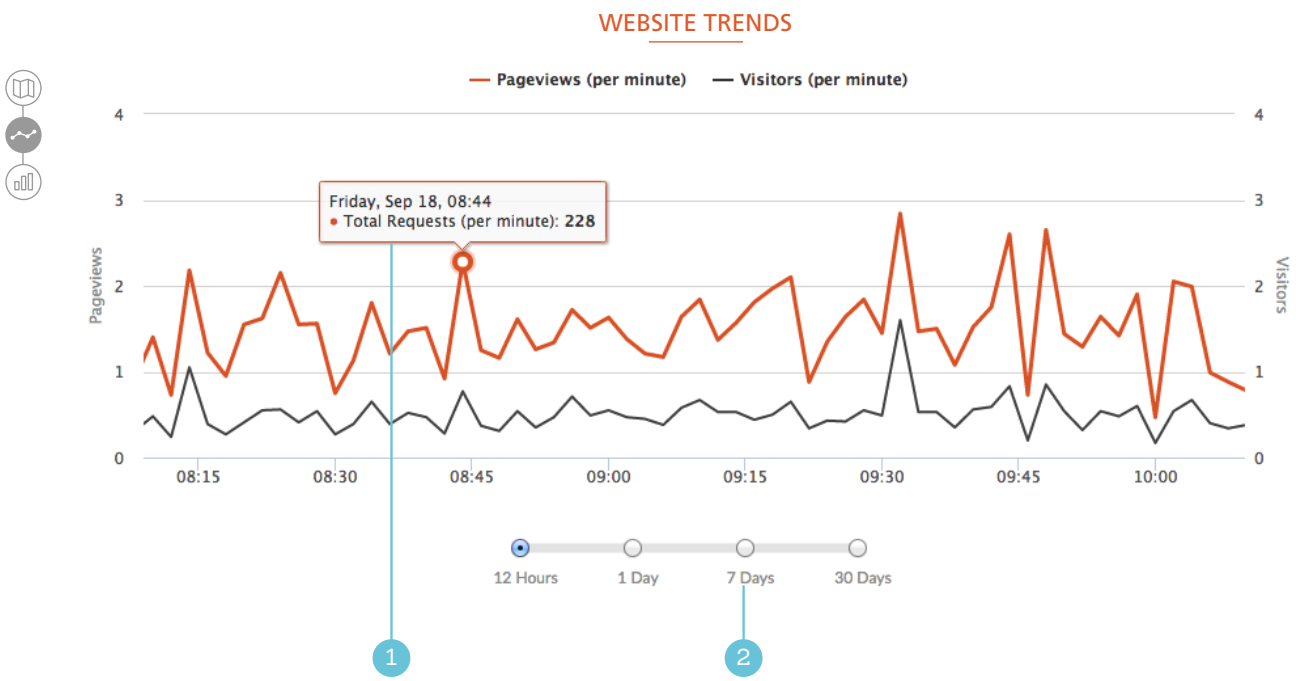
Page views by IP address, country, URL, etc.

3. PLT (Page Load Time)

The time it takes for a specific page to be loaded from the IP address.

Website Trends (Last 24 hrs / updated every 2 mins)

Pageview and visitor data are presented in line charts in order to visualize trends.



1. Detail

Mouse over the line chart to view the number of page views and visitors at the selected point of time.

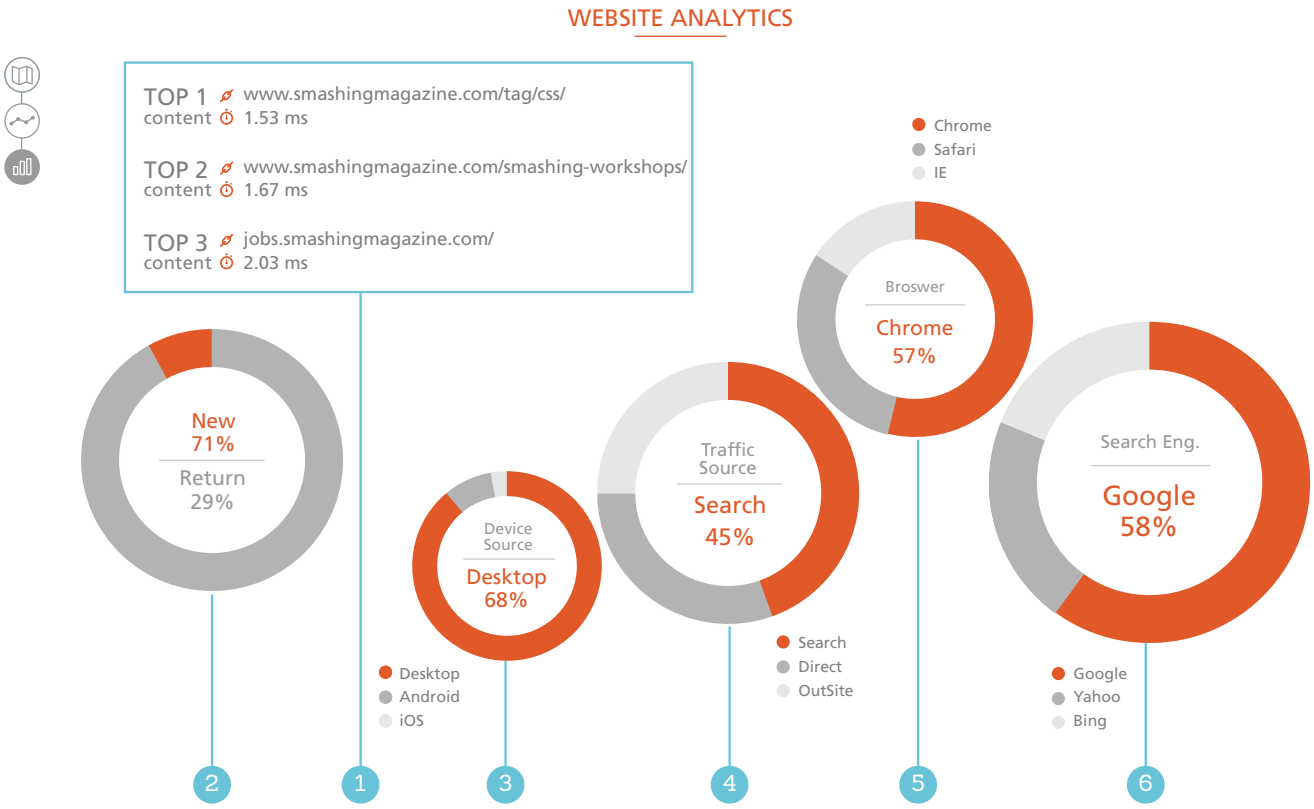
2. Time Frame Selector

The following time intervals are available:

- 12 hours - 2 minute/data point
- 1 day - 1 hour/data point
- 7 days - 1 hour/data point
- 30 days - 1 day/data point

Website Analytics (Last 24 hrs / updated every 1 mins)

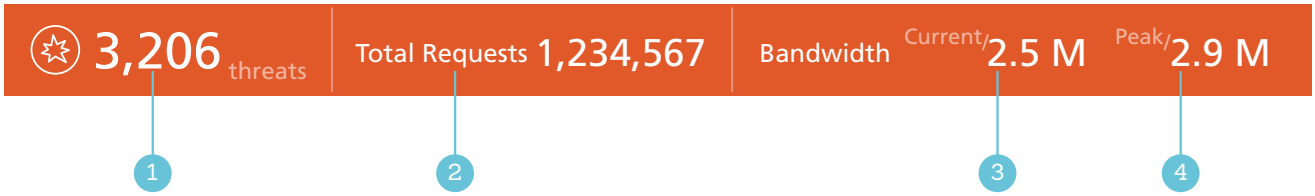
The pie charts summarize various types of site traffic data of the day.



1. The top 3 most visited pages of the day and the average time spent on each of them.
2. The split between new and return visitors.
3. Traffic by device type.
4. Traffic sources, i.e. direct, search and referral.
5. Traffic by browser type.
6. Traffic by search engine.

Protection

The Application Portal provides detailed data for users to monitor the site's protection status.



1. Threats

Accumulated numbers of actual and potential threats on the site of the day.

2. Total Requests

Accumulated number of requests to the site of the day, including suspicious, malicious and normal requests.

3. Bandwidth - Current (Last 24 hrs / updated every 2 mins)

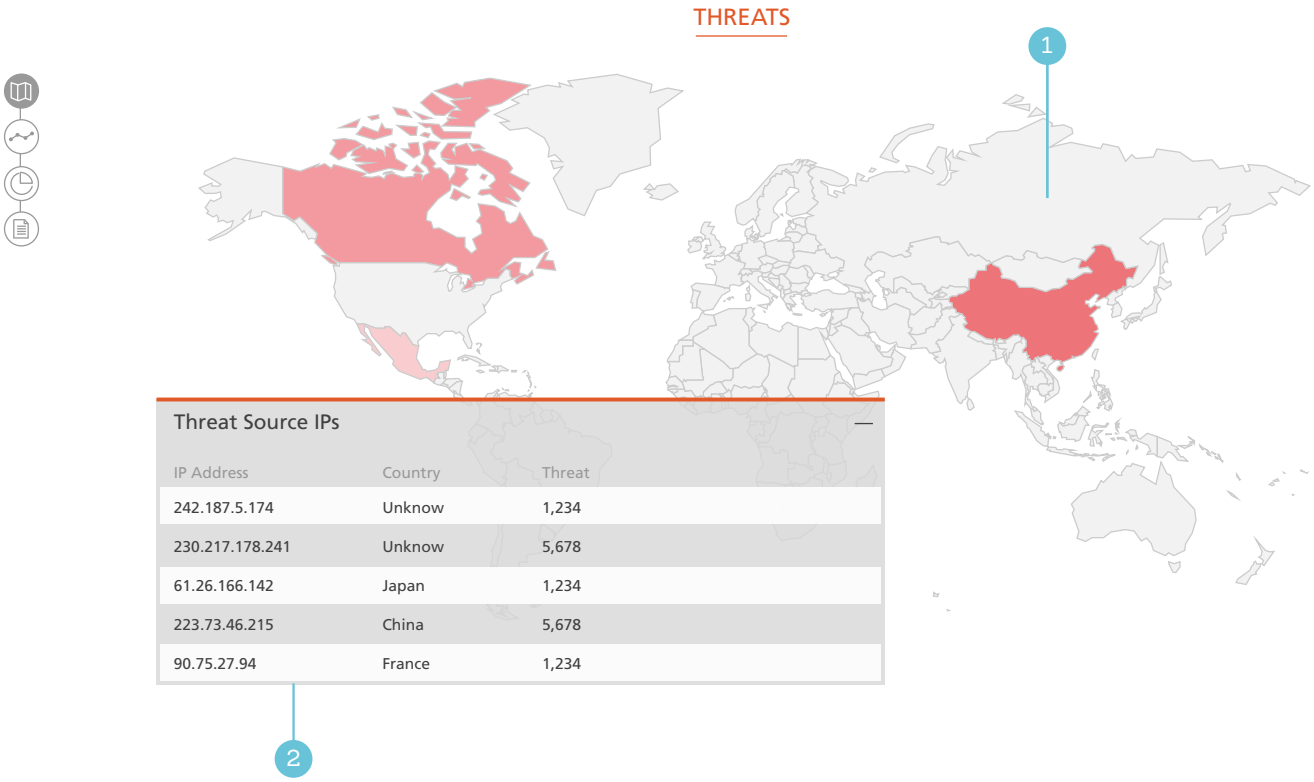
The site's current bandwidth throughput (bps), including both legitimate and non-legitimate traffic.

4. Bandwidth - Peak

The site's current bandwidth throughput (inbound + outbound, bps) of the day, including both legitimate and non-legitimate traffic.

Threats (Last 24 hrs / updated every 1 min)

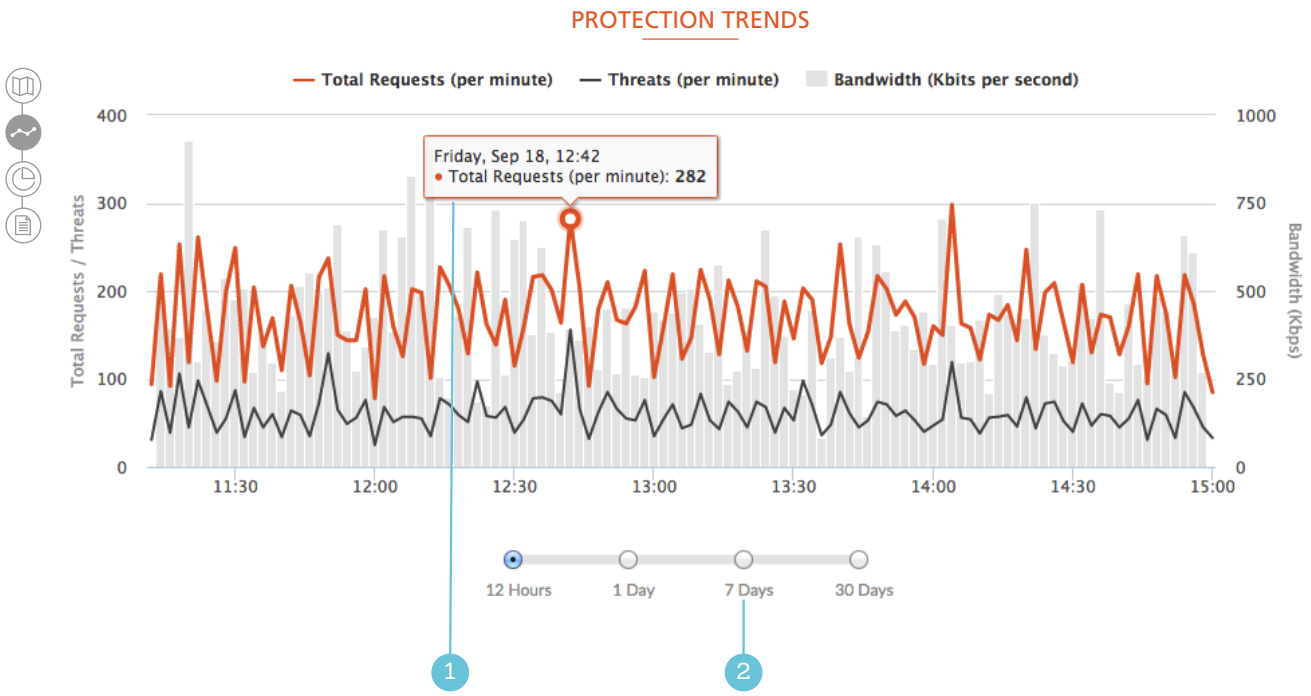
Geographical distribution of threats in real time and the details thereof, such as IP addresses, countries and numbers of threats from different regions.



1. Geographical distribution of threats in real time.
2. Threat sources, i.e. source IPs, countries and numbers of threats.

Protection Trends (24hrs/2mins)

Live chart showing bandwidth usage and numbers of threats and requests for on-the-fly analysis and formulation of security strategy.



1. Details

Mouse over the chart to see the total numbers of requests and threats as well as bandwidth usage at the selected point of time.

2. Time Frame Selector

The following time frames are available:

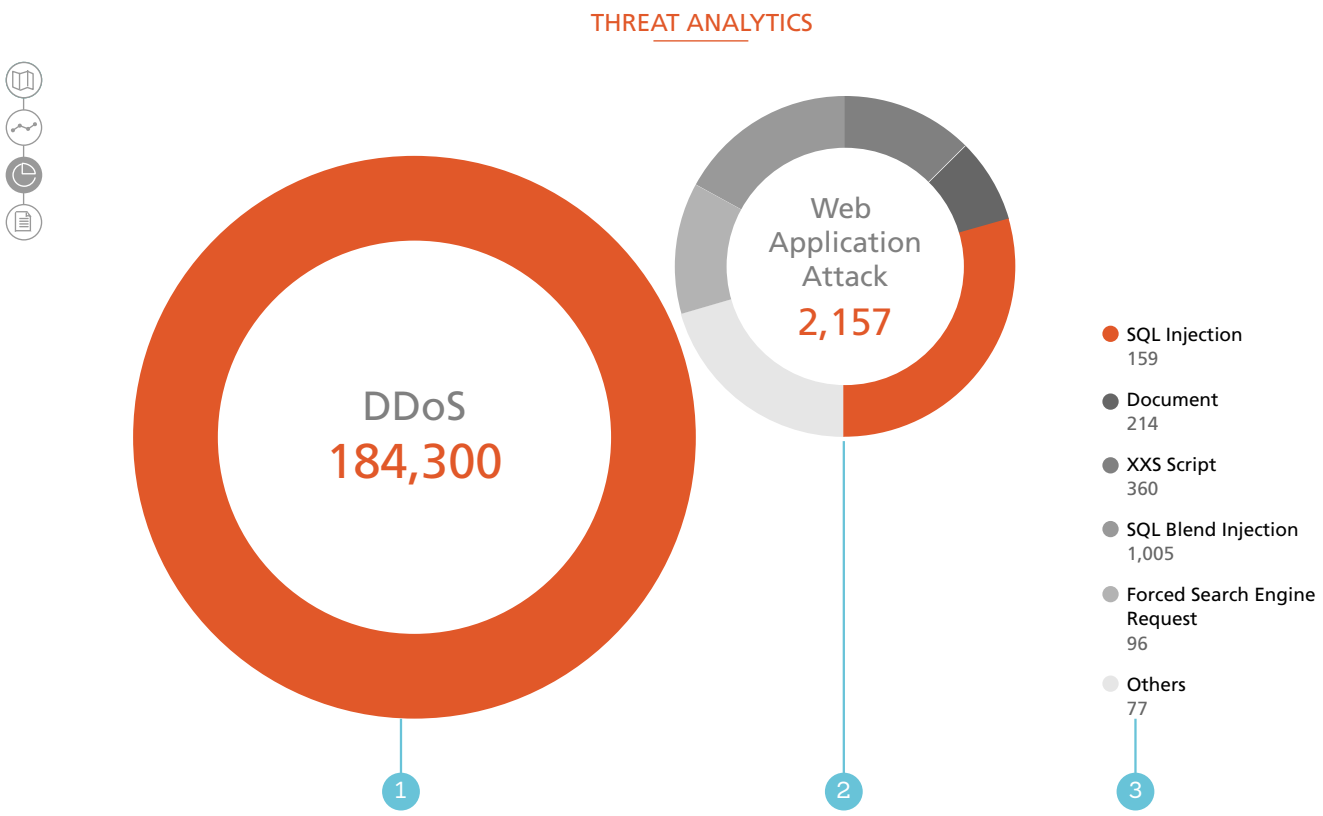
- 12 hours - 2 minutes/data point
- 1 day - 1 hour/data point
- 7 days - 1 hour/data point
- 30 days - 1 day/data point

— Data Unit

- Threats - threats per minute (tpm)
- Requests - requests per minute (rpm)
- Bandwidth - kbits per second (kbps)

Threat Analytics (24hrs/1min)

Visualized threat data are presented in pie charts.



1. DDoS Attacks

Number of DDoS attacks mitigated.

2. Web Application Attacks

Number of web application attacks mitigated.

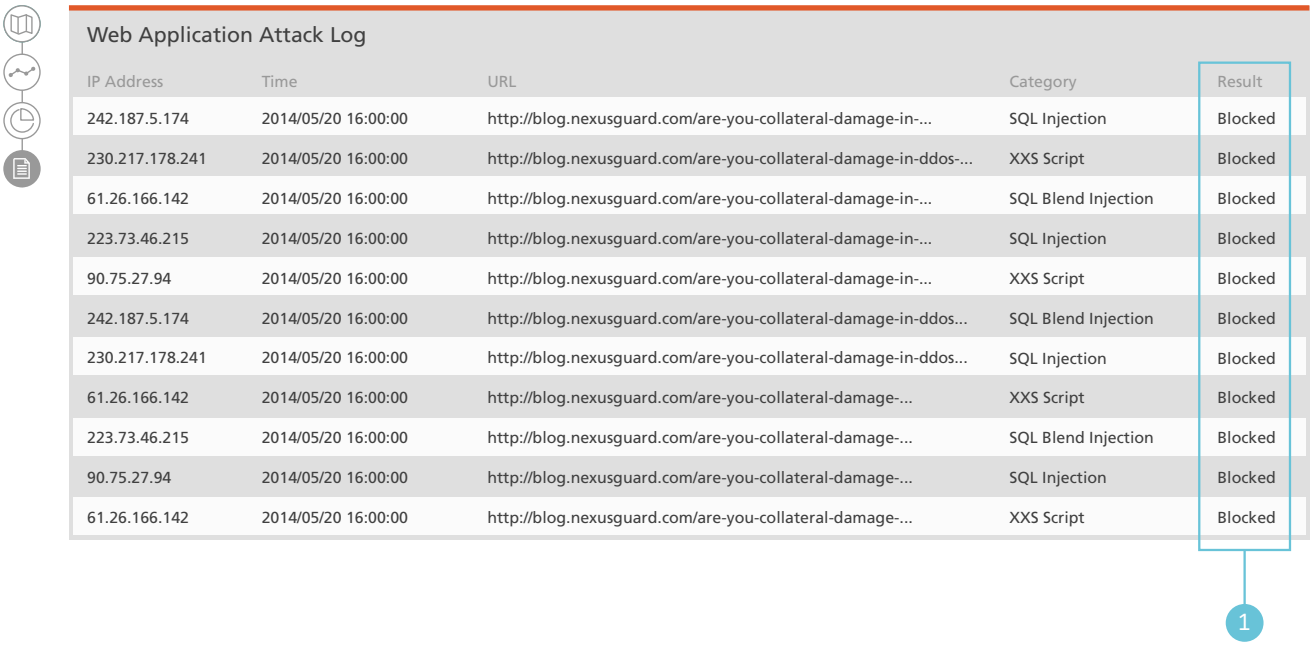
3. Category

Types of web application attacks on the site.

Web Application Attack Log

The Web Application Attack Log shows the threats the Application Portal has sucessfully blocked.

WEB APPLICATION ATTACK LOG



Web Application Attack Log

IP Address	Time	URL	Category	Result
242.187.5.174	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-in-...	SQL Injection	Blocked
230.217.178.241	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-in-ddos-...	XXS Script	Blocked
61.26.166.142	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-in-...	SQL Blend Injection	Blocked
223.73.46.215	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-in-...	SQL Injection	Blocked
90.75.27.94	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-in-...	XXS Script	Blocked
242.187.5.174	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-in-ddos...	SQL Blend Injection	Blocked
230.217.178.241	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-in-ddos...	SQL Injection	Blocked
61.26.166.142	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-...	XXS Script	Blocked
223.73.46.215	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-...	SQL Blend Injection	Blocked
90.75.27.94	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-...	SQL Injection	Blocked
61.26.166.142	2014/05/20 16:00:00	http://blog.nexusguard.com/are-you-collateral-damage-...	XXS Script	Blocked

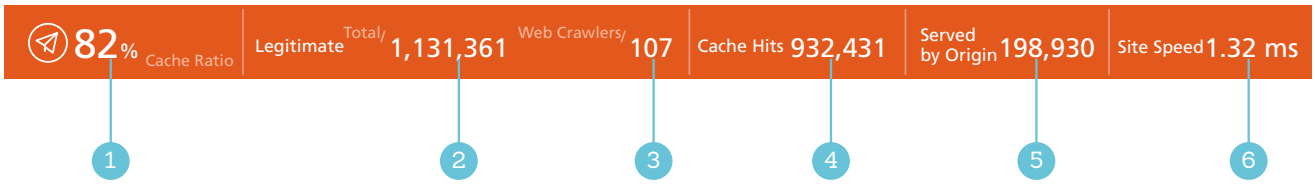
1. Result

This field indicates the action taken to address each specific attack.

Performance (24hrs/1min)

The Application Portal provides valuable analytics to help improve site performance.

Figures shown may be subject to a 0.3% variation due to Application Portal's computation methods.



1. Cache Ratio

The Ratio of HTTP requests served from cache. (Cache Hits / Legitimated).

2. Legitimate Traffic (Total)

The Number of legitimate requests (including authorized web crawlers) of the day.

3. Legitimate Traffic (Web Crawlers) (Last 24 hrs / updated every 1 min)

The number of web crawlers authorized of the day.
Web crawlers authorized to pass through by default includes: Google, Baidu, Bing, MSN, Yandex, Soso, Exa, Sogou, Facebook, Qihoo, Slurp.

4. Cache Hits

The accumulated number of requests served by cache of the day.

5. Served by origin (Last 24 hrs / updated every 1 min)

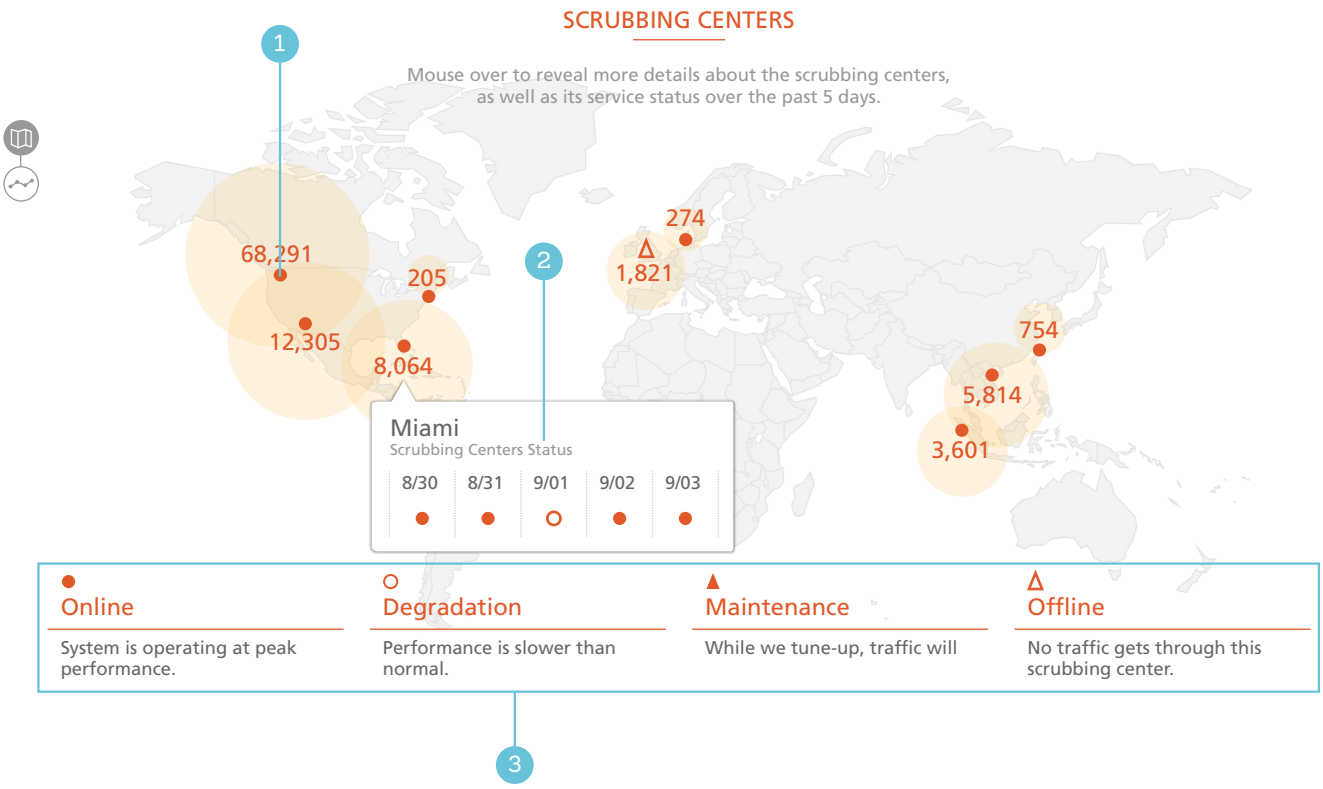
The amount of requests served directly by origin server of the day.

6. Site Speed (Last 24 hrs / updated every 1 min)

The average page loading time for all users and pages of the day.

Scrubbing Centers

Geographical distribution of Nexusguard's scrubbing centers and the amount of requests each of them handles.



1. Scrubbing Centers

Location of the 8 major scrubbing centers: San Jose, Los Angeles, Miami, Washington London, Amsterdam, Singapore, Hong Kong and Taipei.

2. Scrubbing Centers Traffic

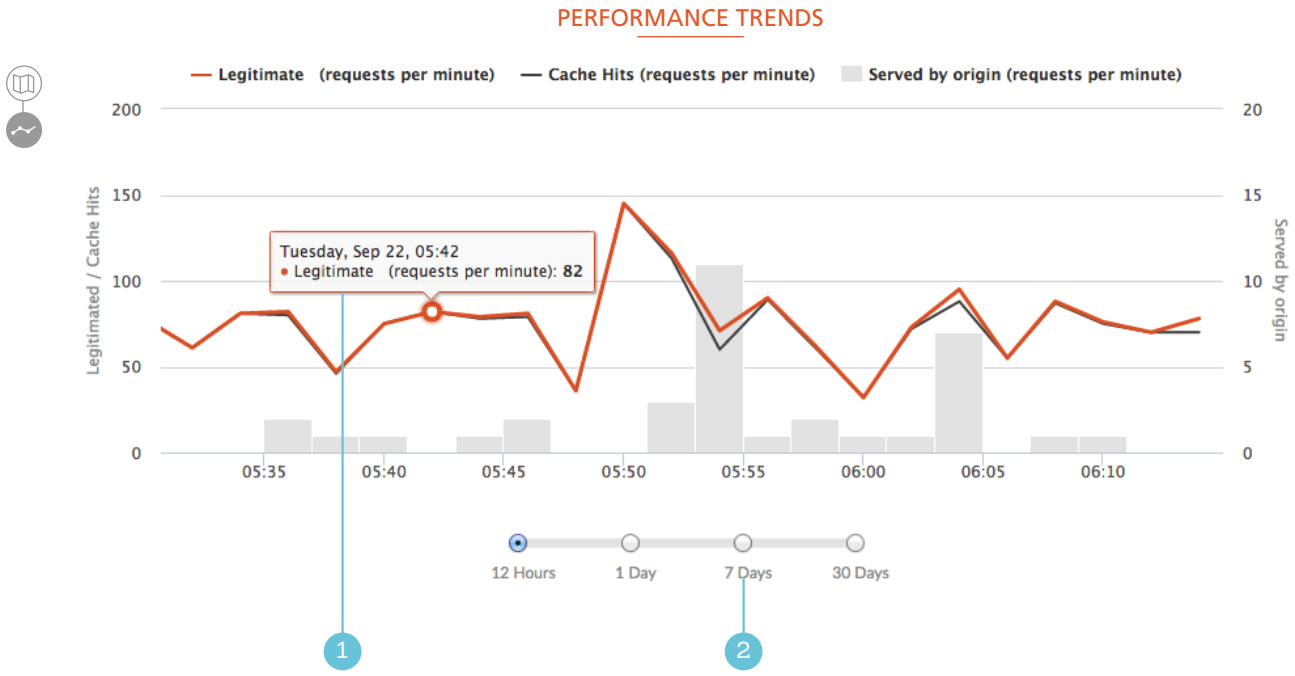
Scrubbing center status the during 5 days.

3. Scrubbing Centers Status

- Online - System is operating at peak performance.
- Degradation - Performace is slower than normal.
- Maintenance - While we tune-up, traffic will be re-routed elsewhere.
- Offline - No traffic gets through this scrubbing center.

Performance Trends (24hrs/2mins)

The number of requests and cached hits are visualized in line charts.



1. Details

Mouse over the chart to see the numbers of legitimate requests, cached hits and requests served at the selected point of time.

2. Time Frame Selector

The following time frames are available:

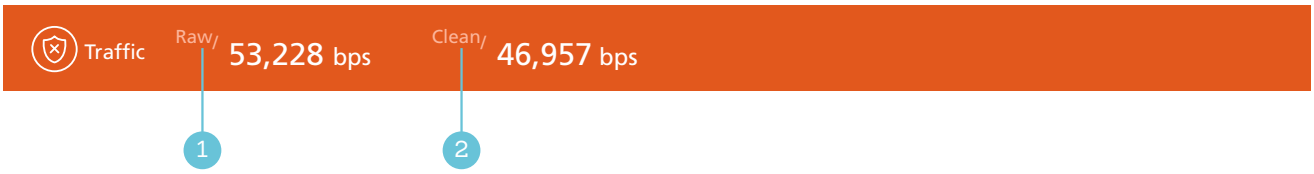
- 12 hours - 2 minutes/data point
- 1 day - 1 hour/data point
- 7 days - 1 hour/data point
- 30 days - 1 day/data point

— Data Unit

- Legitimate - requests per minute (rpm)
- Cache Hits - requests per minute (rpm)
- Served by origin - requests per minute (rpm)

TCP Proxy Protection

This section shows the amount of raw traffic to the site in the TCP proxy mode as well as the amount of clean traffic routed to the client network.



1. Raw Traffic (Last 24 hrs/updated every 1 min)

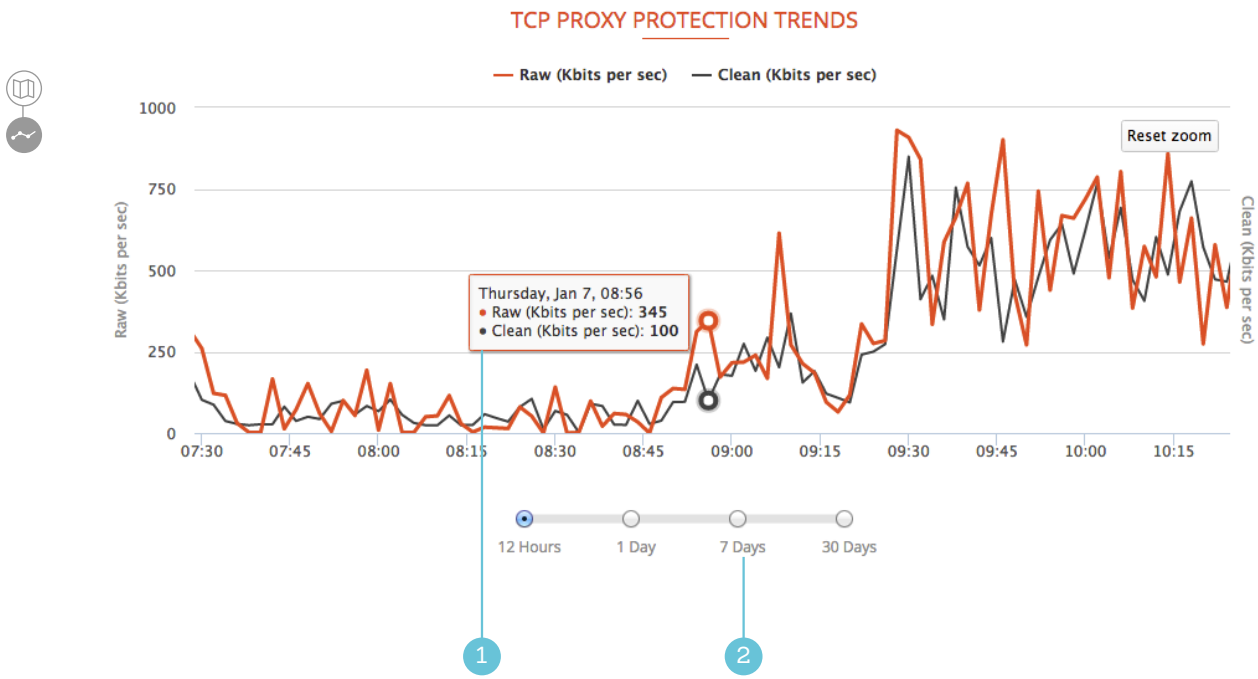
The amount of raw traffic to the site in the TCP proxy mode observed in the past 24 hours.

2. Clean Traffic (Last 24 hrs/updated every 1 min)

The amount of clean traffic routed to the client server after scrubbing in the past 24 hours.

TCP Proxy Protection Trends

Live chart showing bandwidth usage and numbers of threats and requests for on-the-fly analysis and formulation of security strategy.



1. Details

Mouse over the chart to see the numbers of legitimate requests, cached hits and requests served at the selected point of time.

2. Time Frame Selector

The following time frames are available:

- 12 hours - 2 minutes/data point
- 1 day - 1 hour/data point
- 7 days - 1 hour/data point
- 30 days - 1 day/data point

— Data Unit

- Raw Traffic - Kbits per second (Kbps)
- Clean Traffic - Kbits per second (Kbps)

Data Timetable

Item	Data Time Frame	Update Freq.
Online Users	Real-time	50 secs
Pageviews	24 hrs	Real-time
Visitors	24 hrs	Real-time
Threats	24 hrs	1 min
Total Requests	24 hrs	1 min
Bandwidth - Current	24 hrs	2 mins
Bandwidth - Peak	24 hrs	2 mins
Cache Ratio	24 hrs	1 min
Legitimate Requests - Total	24 hrs	1 min
Legitimate Requests - Web Crawlers	24 hrs	1 min
Cache Hits	24 hrs	1 min
Served by Origin	24 hrs	1 min
Avg. Pageviews	7 days	1 min
Peak Pageviews	7 days	1 min
Avg. Visitors	7 days	1 min
Peak Visitors	7 days	1 min
Avg. Page	24 hrs	1 min

Item	Data Time Frame	Update Freq.
Live Pageviews Distribution Map	Real-time	Real-time
Website Trends	24 hrs	2 mins
Website Analytics	24 hrs	1 min
Threat Distribution Map	24 hrs	1 min
Protection Trends	24 hrs	2 mins
Threat Analytics	24 hrs	1 min
Web Application Attack Log	Real-time	Real-time
Site Speed	24 hrs	1 min
Data Center	24 hrs	Manual
Performance Trends	24 hrs	2 mins
Raw Traffic	24 hrs	1 min
Clean Traffic	24 hrs	1 min
TCP Proxy Protection Trends	24 hrs	2 mins

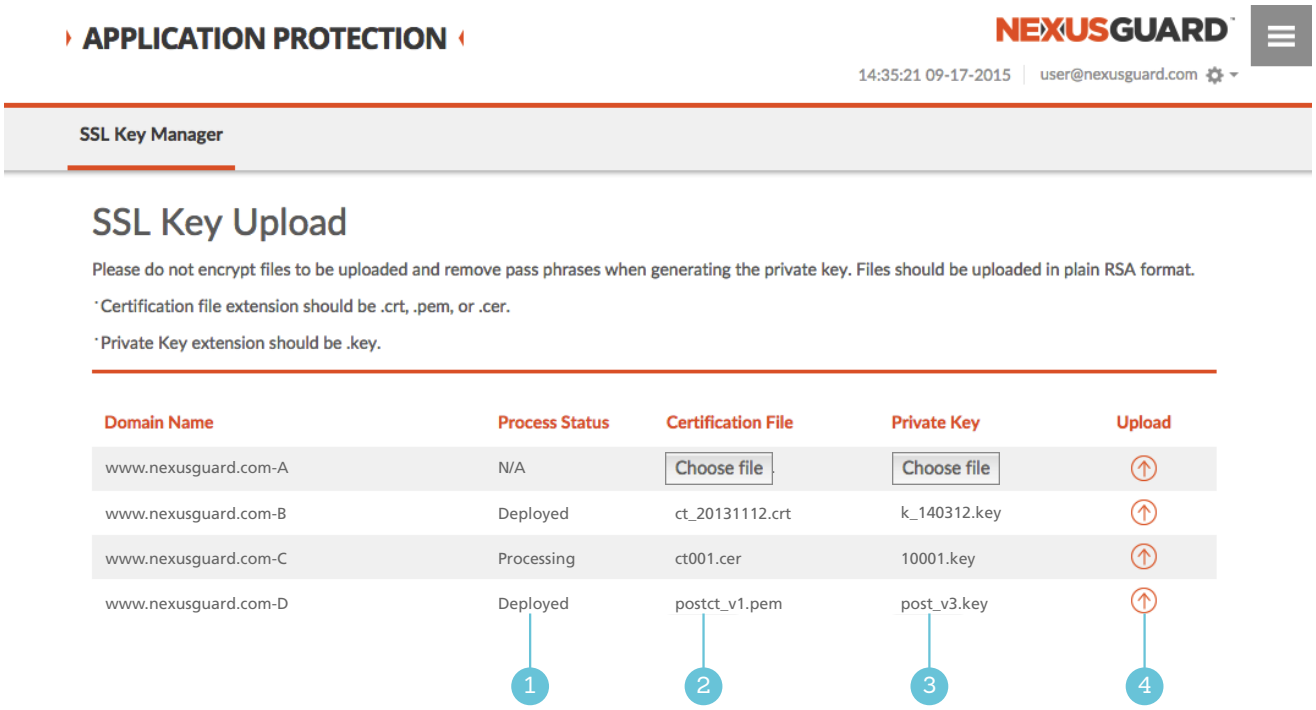
Chapter 4

SSL Key Management

We believe that SSL key management is one of the most difficult aspects of cryptography. That is why we have spared no resources in ensuring that your certificates are always handled with extreme care.

SSL Key management (24hrs/1min)

This section illustrates the user interface used for the upload and deployment of your SSL certificates. The entire process from receipt to deployment to AES 256-bit encrypted storage is automated and is strictly void of human intervention.



1. Process Status

Displays the status of your SSL certification deployment.

- N/A: No certificate has been uploaded.
- Processing: The system is processing your certificate.
- Deployed: The certificate has been successfully deployed.

2. Certification File

Displays the name of the selected SSL certificate file.

3. Private Key

Displays the name of the selected Private key file.

4. Upload

Click to upload the selected files.

Chapter 5

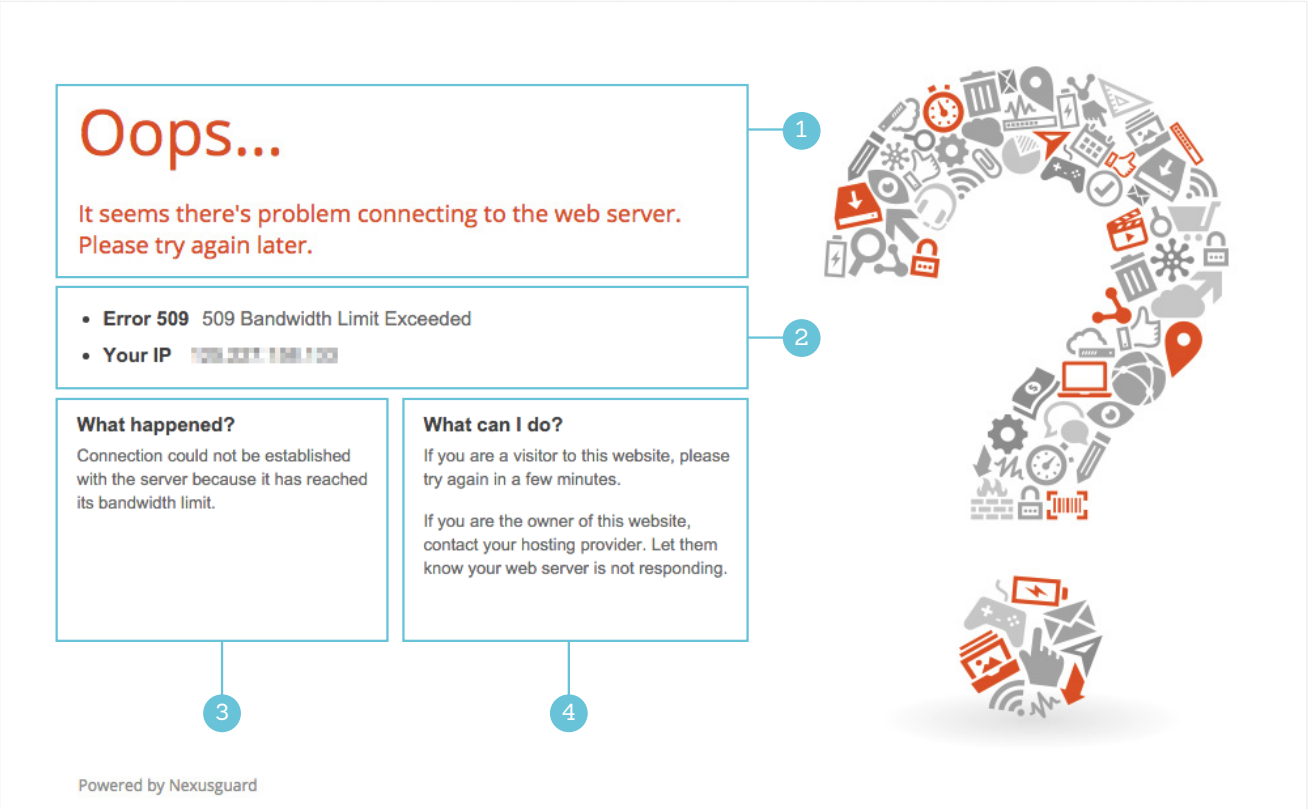
Error Status Codes

HTTP errors are sent from the web server to the end-user's browser if a problem is encountered when trying to view a webpage. By default, your web server is responsible for displaying those error pages. But when for any reason your web server is unable to display an error page when it is supposed to, Nexusguard will take charge by sending the corresponding error page to the user's browser.

This section provides a list of error pages used by Nexusguard to respond to different types of errors. Each error page includes an error code, the end-user's iP address and/or an Event ID, which can be easily be quoted as the reference in future troubleshooting. The end-user will also to see a brief explanation of what happened and get some ideas for how to solve the problem that is causing them.

Sample Error Codes

The following is a sample of how an error code page looks like on the end-user front when an error occurs.



1. Description

A quick explanation of what has happened and what the end-user can do.

2. Event Status

The error code and the end-user's IP address.

3. What happened?

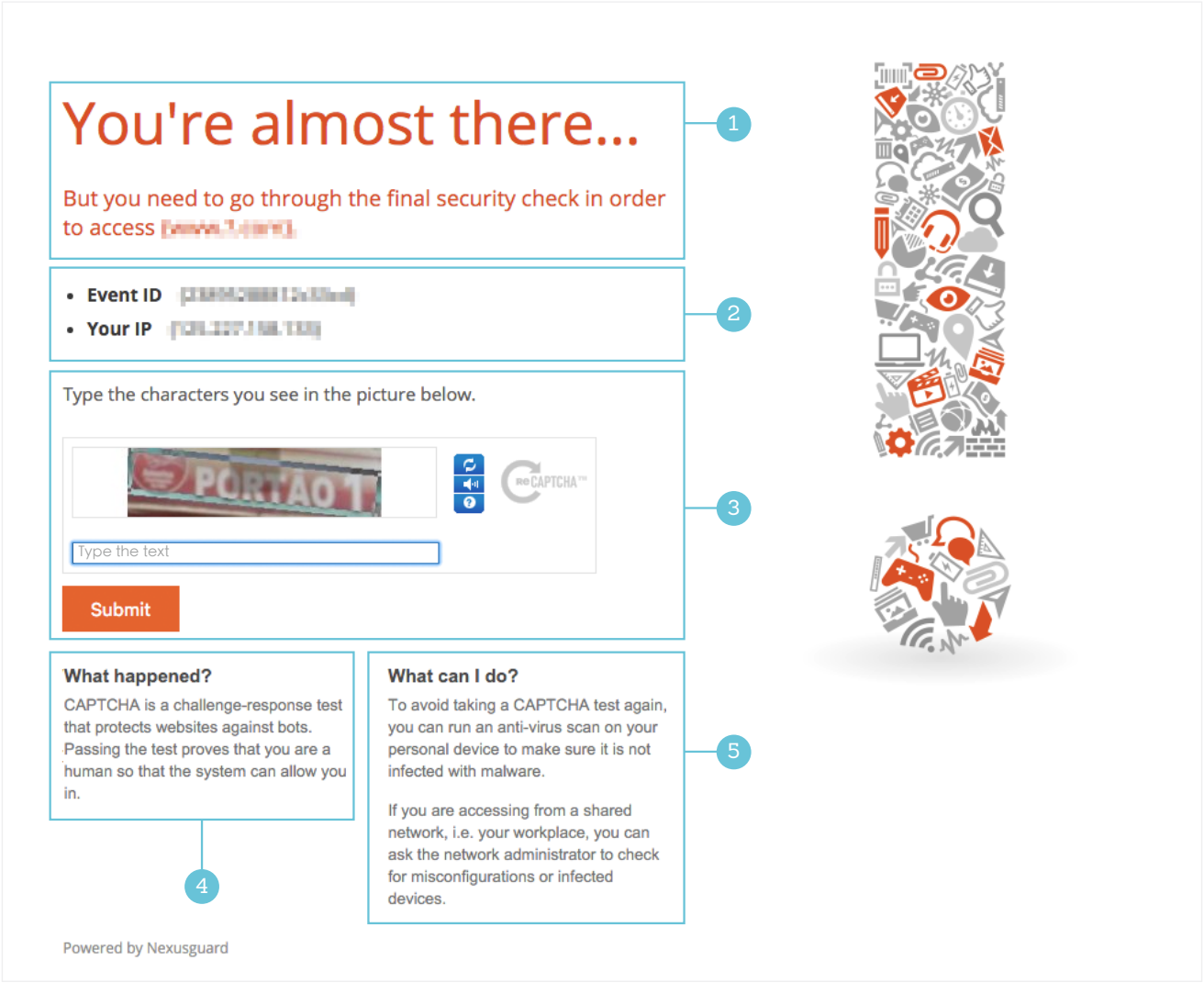
The reason behind the error explained in more detail.

4. What can I do?

What the site owner and/or the end-user can do to resolve the situation.

CAPTCHA Test

The user is challenged to a CAPTCHA test after suspicious browsing activity has been detected. CAPTCHA test is the last resort Nexusguard uses to separate humans from the bad bots.



1. Description

A quick explanation of what has happened and what the end-user can do.

2. Event Status

The error code and the end-user's IP address.

3. CAPTCHA

The user is required to type the letters from the text as verification.

4. What happened?

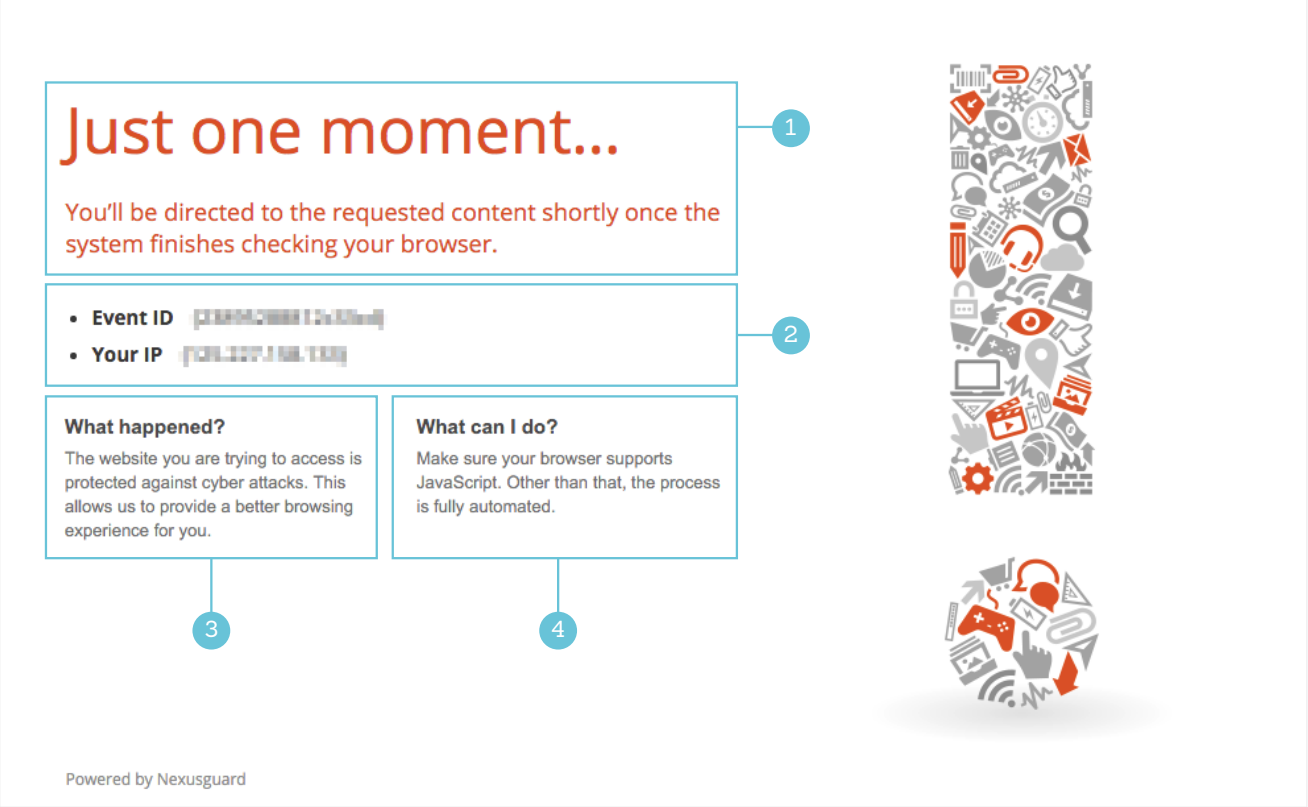
The reason behind the error explained in more detail.

5. What can I do?

What the site owner and/or the end-user can do to resolve the situation.

Human Activity Validation

Nexusguard uses a mix of non-disruptive techniques to monitor user behavior in order to separate humans from the bad bots. All this is done quietly in the background and most users are not bothered. If validation takes a longer time, the user will see this page to keep them patient. Highly suspicious users will be challenged to a CAPTCHA test if their activity fails the validation tests.



1. Description

A quick explanation of what has happened and what the end-user can do.

2. Event Status

The error code and the end-user's IP address.

3. What happened?

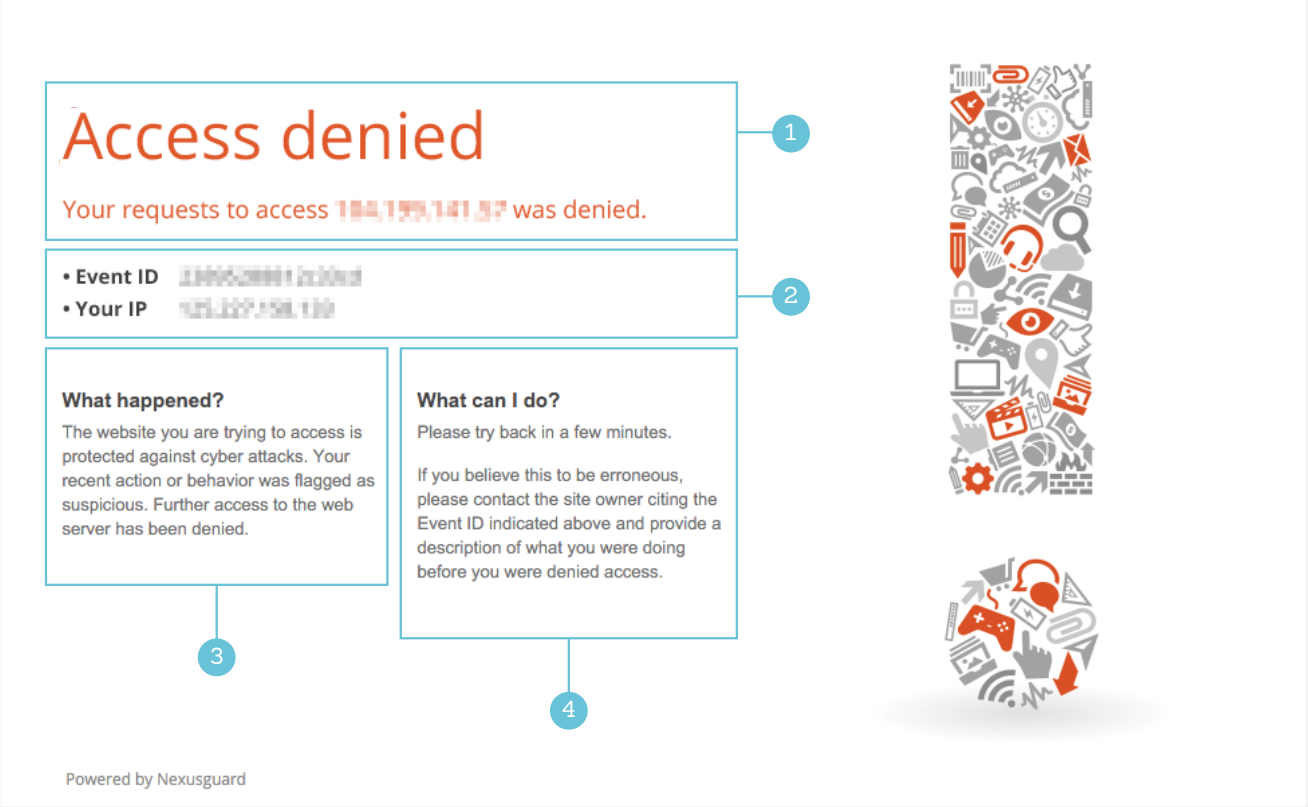
The reason behind the error explained in more detail.

4. What can I do?

What the site owner and/or the end-user can do to resolve the situation.

403 Error - Access denied

The end-user is temporarily blocked from accessing the site because his/her browser activity fails the validation tests, including the CAPTCHA challenge. When that happens our system thinks it's a bot, not a genuine user.



1. Description

A quick explanation of what has happened and what the end-user can do.

2. Event Status

The error code and the end-user's IP address.

3. What happened?

The reason behind the error explained in more detail.

4. What can I do?

What the site owner and/or the end-user can do to resolve the situation.

Error Code Summary

Error Code	What happened?	What can I do?
Error 500 Internal Server Error	The web server encountered an unexpected condition that prevented it from fulfilling your request for access to the requested URL.	Please try again later. If this problem persists, please contact the site owner.
Error 501 Not Implemented	The web server either does not recognize the request method, or it lacks the ability to fulfill the request.	If you are a visitor to this website, try again in a few minutes. If you are the owner of this website, contact your hosting provider so they can trace the exact reason for the error.
Error 502 Bad Gateway	This problem is caused by poor IP connection between backend computers, possibly including the web server at the site you are trying to visit.	Clear your browser cache completely and reload the page again. Sometimes a 502 Bad Gateway error is only a temporary problem. However, if this problem persists, please contact the site owner.
Error 503 Service Unavailable	The web server or gateway is unable to process the request due to an overload or maintenance problem.	If you are a visitor to this website, please try again in a few minutes. If you are the owner of this website, contact your hosting provider. Let them know your web server is not responding.
Error 504 (1) Gateway Timeout	This problem is entirely due to slow IP communication between backend computers, possibly including the web server.	If you are a visitor to this website, please contact the site owner whenever you encounter this problem. If you are the owner of this website, contact your hosting provider.
Error 505 HTTP Version Not Supported	The web server does not support, or refuses to support, the HTTP protocol version specified by your web browser in the HTTP request data stream sent to the server.	Please contact the site owner. There is nothing you can do to sort it out.
Error 506 Variant Also Negotiates	The web server has an internal configuration error: the chosen variant resource is configured to engage in transparent content negotiation itself, and is therefore not a proper end point in the negotiation process.	Please contact the site owner. There is nothing you can do to sort it out.

(1) As Nexusguard as the gateway/proxy server does not receive a response from your web server to complete the request, Nexusguard's Error 504 page is displayed.

Error Code	What happened?	What can I do?
Error 507 Insufficient Storage	The web server is unable to store the representation needed to complete the request.	Please try again later. If this problem persists, please contact the site owner.
Error 508 Loop Detected	The web server detected an infinite loop while processing the desired request.	Please try again later. Sometimes a 508 Loop Detected error is only a temporary problem. However, if this problem persists, please contact the site owner.
Error 509 Bandwidth Limit Exceeded	Connection could not be established with the server because it has reached its bandwidth limit.	If you are a visitor to this website, please try again in a few minutes. If you are the owner of this website, contact your hosting provider. Let them know your web server is not responding.
Error 404 Page Not Found	The page you are looking for cannot be found.	If you are a visitor to this website, please check with the administrator that the URL is correct. If you are the owner of this website, please make sure that the URL is correct.
Error 403 (2) Access denied	The website you are trying to access is protected against cyber attacks. Your recent action or behavior was flagged as suspicious. Further access to the web server has been denied.	Please try back in a few minutes. if you believe this to be erroneous, please contact the site owner citing the Event ID indicated above and provide a description of what you were doing before you were denied access.
Captcha Test	CAPTCHA is a challenge-response test that protects websites against bots. Passing the test proves that you are a human so that the system can allow you in.	To avoid taking a CAPTCHA test again, you can run an anti-virus scan on your personal device to make sure it is not infected with malware. If you are accessing from a shared network, i.e. your workplace, you can ask the network administrator to check for misconfigurations or infected devices.
Human Activity Validation	The website you are trying to access is protected against cyber attacks. This allows us to provide a better browsing experience for you.	Make sure your browser supports JavaScript. Other than that, the process is fully automated.

(2) A suspicious user would only see Nexusguard's Error 403 page if he/she has failed our progressive challenge-response authentication tests.

Nexusguard reserves the right to modify the above information without any prior notice.

NEXUSGUARD™

Nexusguard is leading the fight against malicious Internet attacks, protecting our customers from threats to their sites, their services, and most importantly, their reputations. As the global leader in DDoS defense, we've provided security against these threats for years. Continually evolving to face new threats as they come, we've got the tools, the instinct, and the know-how to cover our clients' backs no matter what gets thrown their way.

Contact us at
support@nexusguard.com
for any queries.

Follow us on Twitter
@Nexusguard

Join us on Facebook
www.facebook.com/NXG.PR

Follow our LinkedIn Page
www.linkedin.com/company/nexusguard