swpanel

ADVANCED SECURITY · NGFW

Threat report
swpanel.com

What the NGFW firewall has detected and blocked on swpanel.com (203.0.113.10) from 13 September to 12 October 2026.

• 47 of 58 threats blocked · 24 critical

CUSTOMER	SERVICE	PERIOD
SWPanel Demo, S.L.	swpanel.com · 203.0.113.10	13-09-2026 to 12-10-2026 · 30 days
DOCUMENT	**ISSUE DATE**	**SENSITIVITY**
SW-NGF-EJEMPLO-2026	16-10-2026	Blocks from medium severity

Contents of the report

Dashboard 2

01 The consultant's introduction 3

02 Threats 7
- By severity, type and application 8
- Most frequent, origin and destination 9
- What changed: the last 6 months 10

03 Access and files 11
- Authentication and suspicious files 12

04 What to do 13
- Most serious first 14

05 Per-host detail 16
- Host 203.0.113.10 17
- What each threat is 19

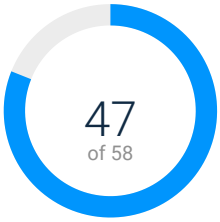
06 Conclusions of the analysis 22

Glossary 25

Annex: AI compute 27

NGFW report of swpanel.com generated by SWPanel

Dashboard



81 % BLOCKED

Of the detected events with a block action, from 13-09-2026 to 12-10-2026

swpanel.com · 203.0.113.10 · blocks from medium severity

11 of low severity were only logged, as the sensitivity requires.

• 24 critical, all blocked

58	47	11	1	0
THREATS DETECTED	BLOCKED	LOGGED	ILLEGITIMATE ACCESS ATTEMPT	SUSPICIOUS FILES

By severity



• Critical **24** • High **11** • Medium **12** • Low **11**

Compared with the customer average

58	1	0	1
threats per host Average: 944,7	intrusion attempt Average: 659,9	suspicious files Average: 70,3	application on the network Average: 1,2
93,9 % less	**99,8 % less**	**None**	**18,9 % less**

What you should do

CRITICAL

24 critical threats, all blocked. Most of them are «Code execution». Keep the server and its software up to date.

REVIEW

11 threats were only logged. They are low severity and the sensitivity blocks from medium severity. If you want to block them too, lower the sensitivity in the panel.

1 brute-force attempt(s) (WordPress Login Brute Force Attempt). If you use WordPress, limit login attempts.

NGFW report of swpanel.com generated by SWPanel

01

The consultant's introduction

Your situation in one minute, what we analysed and what deserves your attention.

NGFW report of swpanel.com generated by SWPanel

Introduction by the consultant

IA Written by the SWPanel AI security assistant

In the last 30 days, the NGFW detected 58 threat events, 47 of which were blocked.

ATTENTION

Your situation in one minute

The firewall blocked most detected threats, but a brute-force attempt and a critical PHP vulnerability require your attention. The priority is to verify and address these.

1. Check the PHP version and update if needed to address the known vulnerability.

2. Review the Cloudflare proxy logs to understand the brute-force attempt better.

3. Keep an eye on the low-severity events logged without block, in case they increase in frequency.

What I analysed

I reviewed the NGFW report for the last 30 days, which tracks threats detected and connections rejected by the firewall. The firewall is set to 'medium' sensitivity, meaning only events of that severity or higher are blocked. Lower events are logged but not blocked by design.

The number of threats is lower than the previous period, and no suspicious files or SSH sessions were observed. However, a few high-severity threats were blocked, and one brute-force attempt was recorded.

What needs your attention now is the one brute-force attempt and the applicability of some critical threats, especially the PHP-related one. These are manageable but should not be ignored.

Your SWPanel AI security assistant

Should I worry?

You should be alert but not alarmed. The firewall is working as expected, and the threats it blocked were serious but not confirmed to apply to your service. A few issues need checking, but they are not emergencies.

What this report covers and what it does not

This report shows what the NGFW observed: threats it detected and connections it rejected. It does not show normal allowed traffic, encrypted traffic it did not inspect, or what happened inside the server.

NGFW report of swpanel.com generated by SWPanel

What I found and why it matters

Each finding with what we saw, what it is based on, what it means for your service, what is still to be checked, what we recommend and how we will know it is solved.

MEDIUM IMPACT

Brute-force attempt against WordPress login

What we observed: One brute-force attempt was observed against the WordPress login page from a Cloudflare IP. The firewall applied a block action.

What it is based on: NGFW log entry for WordPress Login Brute Force Attempt against swpanel.com from IP 198.51.100.26.

What it means: Someone tried to guess the login credentials of your WordPress site. The firewall stopped it, but we need to understand if it was a real user or a bot, and if the login page is properly protected.

Still to be checked: We do not know if WordPress is installed or if the login page is exposed. We also do not know if this was a one-time event or part of a pattern.

What we recommend: Check the Cloudflare and application logs to see if this was a real user or a bot. Ensure the WordPress login is secured with two-factor authentication if needed.

How we will verify it: We will know it is solved when the logs show no further brute-force attempts and the WordPress login is properly secured.

HIGH IMPACT

Critical PHP vulnerability

What we observed: A threat related to a known PHP vulnerability was blocked 4 times. The service runs PHP 8.3, which may be affected.

What it is based on: NGFW log entry for phpunit Remote Code Execution Vulnerability, blocked 4 times.

What it means: An attacker tried to exploit a known PHP vulnerability that could allow them to run code on your server. The firewall blocked it, but we need to check if your PHP version is affected.

Still to be checked: We do not know if your PHP version is vulnerable. We also do not know if the vulnerability is exploitable in your current setup.

What we recommend: Verify the PHP version and update it if needed. Check if the affected versions include PHP 8.3.

How we will verify it: We will know it is solved when the PHP version is updated and the vulnerability is no longer relevant.

NGFW report of swpanel.com generated by SWPanel

What I found and why it matters

LOW IMPACT

Low-severity FTP evasion attempts

What we observed: Five low-severity FTP protocol evasion attempts were logged without block.

What it is based on: NGFW log entry for FTP Protocol Evasion Application Detection, logged without block.

What it means: Someone tried to bypass FTP security checks, but the firewall was set to log these without blocking them. These are low-severity and not blocked by design.

Still to be checked: We do not know if an FTP service is running or if it is needed. We also do not know if these attempts are part of a pattern.

What we recommend: Check if an FTP service is running and if it is needed. If not, consider disabling it.

How we will verify it: We will know it is solved when the FTP service is either secured or removed, and the evasion attempts stop.

NGFW report of swpanel.com generated by SWPanel

02

Threats

What has arrived, how severe and of what type, through which application and from where.

NGFW report of swpanel.com generated by SWPanel

Threats in the period

IA **The consultant's view**

The NGFW blocked most threats, especially high and critical ones. A few low-severity events were logged without block, as per the firewall's policy. The most common threats were code execution and information leak attempts.

The NGFW has detected 58 threats in the period. It has blocked the 47 of medium, high or critical severity and logged without blocking the 11 of low severity.

• 47 blocked • 11 logged

By severity



• Critical **24** • High **11** • Medium **12** • Low **11**

By type

Type	Severities	Blocked	Logged	Total
Code execution	• Critical • Low	**23**	**5**	28
Information leak	• High • Medium • Low	**19**	**1**	20
Protocol anomaly	• Low	**0**	**5**	5
Denial of service	• High	**4**	**0**	4
Brute force	• Critical	**1**	**0**	1
Total		47	11	58

By application

Application	Blocked	Logged	Total	Share
web-browsing	**37**	**5**	42	**72 %**
ftp	**0**	**6**	6	**10 %**
soap	**5**	**0**	5	**8,6 %**
ssl	**4**	**0**	4	**6,9 %**
portmapper	**1**	**0**	1	**1,7 %**

NGFW report of swpanel.com generated by SWPanel

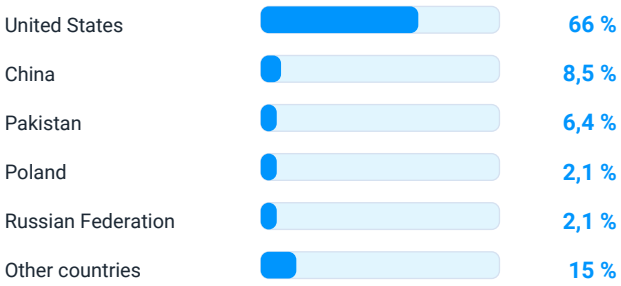
Most frequent, origin and destination

The 10 most frequent

Threat	Type	Severity	Attempts	Action
HTTP /etc/passwd Access Attempt ID 35107 · web-browsing	**Information leak**	• High	7	• Blocked
Apache Shiro Improper Authentication Vulnerability ID 58590 · web-browsing	**Code execution**	• Critical	6	• Blocked
HTTP Directory Traversal Request Attempt ID 30844 · web-browsing	**Information leak**	• Medium	6	• Blocked
D-Link DSL Soap Authorization Remote Command Execution Vulnerability ID 58483 · soap	**Code execution**	• Critical	5	• Blocked
FTP Protocol Evasion Application Detection ID 39826 · ftp	**Protocol anomaly**	• Low	5	• Logged
phpunit Remote Code Execution Vulnerability ID 55852 · web-browsing	**Code execution**	• Critical	4	• Blocked
Netgear DGN Device Remote Command Execution Vulnerability ID 40741 · web-browsing	**Code execution**	• Critical	4	• Blocked
OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability ID 58033 · ssl	**Denial of service**	• High	4	• Blocked
ZGrab Application Layer Scanner Detection ID 57955 · web-browsing	**Information leak**	• Medium	4	• Blocked
GPON Home Routers Remote Code Execution Vulnerability ID 37264 · web-browsing	**Code execution**	• Critical	3	• Blocked

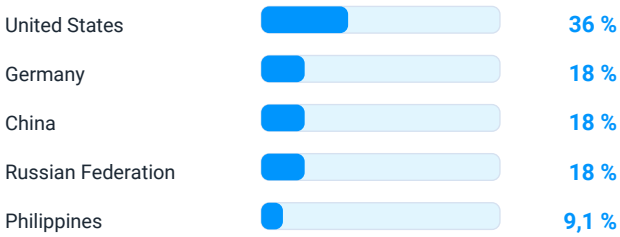
Origin of the blocked

47 threats, by country



Origin of the logged

11 threats, by country



NGFW report of swpanel.com generated by SWPanel

Most frequent, origin and destination (continued)

Destination

All 58 threats went to swpanel.com (203.0.113.10), the only service in this report.

What changed: the last 6 months

Month	Events	Blocked	Logged	Critical	High	Brute force
May 2026	**0**	0	0	0	0	0
June 2026	**0**	0	0	0	0	0
July 2026	**22**	11	11	11	0	0
August 2026	**51**	35	16	24	1	0
September 2026	**92**	77	15	38	16	1
October 2026	**0**	0	0	0	0	0

Calendar months; the last one, up to the end of this report's period. Comparing with your own history says more than any average.

NGFW report of swpanel.com generated by SWPanel

03

Access and files

Attempts to force your way in and suspicious files.

NGFW report of swpanel.com generated by SWPanel

Access and suspicious files

IA **The consultant's view**

No suspicious SSH sessions were observed. One brute-force attempt was recorded, but it was blocked.

Brute-force access attempts

The NGFW has blocked 1 attempt(s) to force entry, compared with 660 on average per host for other customers. Many of these attacks are automated and launched against any machine on the internet: with an up-to-date system, well-configured applications and strong passwords they pose no real risk.

Threat	Service	Source IP	Attempt	Action
WordPress Login Brute Force Attempt ID 40044	**swpanel.com**	**198.51.100.26** Cloudflare (proxy)	1	• Blocked

SSH sessions

Nobody reached the SSH login prompt in the period.

Suspicious files

No suspicious files were detected, blocked or logged. The customer average is 70 per host.

NGFW report of swpanel.com generated by SWPanel

04

What to do

What each type of threat detected is and how to protect yourself, in order of what is at stake.

NGFW report of swpanel.com generated by SWPanel

WHAT TO DO

How to protect yourself

Only the types detected in this period, from most to least serious.

Code execution · 28 attempts

• Critical • Low

Attempts to make the server run the attacker's commands. Exploits and ransomware fall into this category and can compromise the whole system. They reached swpanel.com through soap, web-browsing; 8 different threat(s).

WHAT TO DO

Filter threats at layer 7, install an antivirus and keep the server and its software up to date.

Brute force · 1 attempts

• Critical

Trying many usernames and passwords in a row until one works. They reached swpanel.com through web-browsing; 1 different threat(s).

WHAT TO DO

Strong passwords and automatic blocking of IPs that fail several times in a row, both in the firewall and in the application login.

Information leak · 20 attempts

• High • Medium • Low

Attempts to extract internal information from the server: configuration files, passwords or personal data. They reached swpanel.com through ftp, portmapper, web-browsing; 6 different threat(s).

WHAT TO DO

Make sure sensitive information cannot be read from outside: encrypt the files that hold it and grant access only to the user groups that need it.

Denial of service · 4 attempts

• High

Attempts to make a service stop responding by flooding it or making it fail. They reached swpanel.com through ssl; 1 different threat(s).

WHAT TO DO

Use layer 3 and layer 7 firewalls to detect and cut repeated connections, and keep exposed software up to date.

NGFW report of swpanel.com generated by SWPanel

How to protect yourself (continued)

Protocol anomaly · 5 attempts • Low

Traffic that does not behave like the protocol it claims to be, usually to go unnoticed. They reached swpanel.com through ftp; 1 different threat(s).

WHAT TO DO

Close the ports you do not use and let the NGFW identify the application before letting it through: whatever is not recognised is better blocked.

NGFW report of swpanel.com generated by SWPanel

05

Per-host detail

Every threat received by each service, with its reference.

NGFW report of swpanel.com generated by SWPanel

PER-HOST DETAIL

Host 203.0.113.10

IA **The consultant's view**

No suspicious files or internal server issues were observed. The firewall did not detect any signs of compromise.

swpanel.com has received 58 threats of 17 different kinds, from most to least serious.

ID	Threat	Severity	Attempts	Action
58590	**Apache Shiro Improper Authentication Vulnerability** Code execution · web-browsing	• Critical	6	• Blocked
58483	**D-Link DSL Soap Authorization Remote Command Execution Vulnerability** Code execution · soap	• Critical	5	• Blocked
55852	**phpunit Remote Code Execution Vulnerability** Code execution · web-browsing	• Critical	4	• Blocked
40741	**Netgear DGN Device Remote Command Execution Vulnerability** Code execution · web-browsing	• Critical	4	• Blocked
37264	**GPON Home Routers Remote Code Execution Vulnerability** Code execution · web-browsing	• Critical	3	• Blocked
54617	**Mirai and Reaper Exploitation Traffic** Code execution · web-browsing	• Critical	1	• Blocked
40044	**WordPress Login Brute Force Attempt** Brute force · web-browsing	• Critical	1	• Blocked
35107	**HTTP /etc/passwd Access Attempt** Information leak · web-browsing	• High	7	• Blocked
58033	**OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability** Denial of service · ssl	• High	4	• Blocked
30844	**HTTP Directory Traversal Request Attempt** Information leak · web-browsing	• Medium	6	• Blocked
57955	**ZGrab Application Layer Scanner Detection** Information leak · web-browsing	• Medium	4	• Blocked
32796	**RPC Portmapper DUMP Request Detected** Information leak · portmapper	• Medium	1	• Blocked
34804	**PHP CGI Query String Parameter Handling Information Disclosure Vulnerability** Information leak · web-browsing	• Medium	1	• Blocked
39826	**FTP Protocol Evasion Application Detection** Protocol anomaly · ftp	• Low	5	• Logged
58098	**Possible HTTP Malicious Payload Detection** Code execution · web-browsing	• Low	3	• Logged

NGFW report of swpanel.com generated by SWPanel

Host 203.0.113.10 (continued)

ID	Threat	Severity	Attempts	Action
54469	**Suspicious File Downloading Detection** Code execution · web-browsing	• Low	2	• Logged
40391	**Application Identification Evasion Attempt Through Malformed FTP Traffic** Information leak · ftp	• Low	1	• Logged

NGFW report of swpanel.com generated by SWPanel

What each threat is

ID 58590 · Code execution • Critical

Apache Shiro Improper Authentication Vulnerability

Apache Shiro is prone to an improper authentication vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable improper authentication vulnerability.

Attempts **6** Blocked CVE-2020-11989 Ref. **lists.apache.org**

ID 58483 · Code execution • Critical

D-Link DSL Soap Authorization Remote Command Execution Vulnerability

Dlink DSL is prone to a command injection vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable command injection.

Attempts **5** Blocked CVE-2018-19986 Ref. **github.com**

ID 55852 · Code execution • Critical

phpunit Remote Code Execution Vulnerability

phpunit is prone to a remote code execution vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable remote code execution.

Attempts **4** Blocked CVE-2017-9841 Ref. **phpunit.vulnbusters.com**

ID 40741 · Code execution • Critical

Netgear DGN Device Remote Command Execution Vulnerability

Netgear DGN devices is prone to a remote code execution vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of privilege checks on the request, leading to an exploitable remote code execution.

Attempts **4** Blocked Ref. **seclists.org**

ID 37264 · Code execution • Critical

GPON Home Routers Remote Code Execution Vulnerability

GPON Home Routers are prone to a Remote Code Execution vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable Remote Code Execution vulnerability.

Attempts **3** Blocked CVE-2018-10561 Ref. **blog.netlab.360.com**

ID 54617 · Code execution • Critical

Mirai and Reaper Exploitation Traffic

This signature detects exploitation attempts from Mirai and Reaper malware families. Detection of this traffic indicates an attempt to exploit various IoT device vulnerabilities including: the D-Link DSL-2750B - OS command injection vulnerability, the MVPower DVR unauthenticated command execution...

Attempts **1** Blocked

ID 40044 · Brute force • Critical

WordPress Login Brute Force Attempt

This event indicates that someone is using a brute force attack to gain access to WordPress wp-login.php.

Attempts **1** Blocked

ID 35107 · Information leak • High

HTTP /etc/passwd Access Attempt

There is a /etc/passwd access attempt has been detected while parsing certain crafted HTTP request. A successful attack could allow an attacker to access sensitive information that could launch further attacks.

Attempts **7** Blocked

NGFW report of swpanel.com generated by SWPanel

What each threat is (continued)

ID 58033 · Denial of service • High

OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability

OpenSSL is prone to a NULL pointer dereference vulnerability while parsing certain crafted SSL requests. The vulnerability is due to the lack of proper checks on SSL requests, leading to an exploitable NULL pointer dereference vulnerability.

Attempts **4** Blocked CVE-2020-1967 Ref. **openssl.org**

ID 30844 · Information leak • Medium

HTTP Directory Traversal Request Attempt

A directory traversal vulnerability has been discovered in parsing malformed HTTP requests. This vulnerability is due to a lack of proper checks in HTTP URI requests.

Attempts **6** Blocked Ref. **imperva.com**

ID 57955 · Information leak • Medium

ZGrab Application Layer Scanner Detection

This signature indicates that an attacker is trying to collect information about the network by using the ZGrab Scanner.

Attempts **4** Blocked

ID 32796 · Information leak • Medium

RPC Portmapper DUMP Request Detected

Most Unix server can be retrieved information through a normal portmapper request.

Attempts **1** Blocked

ID 34804 · Information leak • Medium

PHP CGI Query String Parameter Handling Information Disclosure Vulnerability

PHP-CGI based setups such as Apache's mod_cgid, contain a vulnerability when parsing query string parameters from php files. In such a setup php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the p...

Attempts **1** Blocked CVE-2012-1823 Ref. **kb.cert.org**

ID 39826 · Protocol anomaly • Low

FTP Protocol Evasion Application Detection

This signature detects applications or tools that tunnel SSH traffic over FTP protocol traffic.

Attempts **5** Logged Ref. **room362.com**

ID 58098 · Code execution • Low

Possible HTTP Malicious Payload Detection

This signature detects malicious payload in HTTP traffic.

Attempts **3** Logged Ref. **unit42.paloaltonetworks.com**

ID 54469 · Code execution • Low

Suspicious File Downloading Detection

This signature detects WGET and CURL command execution in HTTP request URL parameters, which is pervasively exploited by attackers to get subsequent malicious payload.

Attempts **2** Logged

NGFW report of swpanel.com generated by SWPanel

What each threat is (continued)

ID 40391 · Information leak • Low

Application Identification Evasion Attempt Through Malformed FTP Traffic

The signature detects an application identification evasion attempt which sends malformed traffic through tcp port 21.

Attempts **1** Logged Ref. **jira-hq.paloaltonetworks.local**

NGFW report of swpanel.com generated by SWPanel

06

Conclusions of the analysis

What your consultant concludes after seeing all the figures, and your action plan.

NGFW report of swpanel.com generated by SWPanel

Conclusions of the analysis

IA **Written by the SWPanel AI security assistant**

The NGFW blocked 47 out of 58 detected threats, showing strong protection against known attacks. The drop from 72 events in the previous period is a positive sign of reduced exposure or improved filtering.

A WordPress login attempt from a Cloudflare IP stands out. It's important to check if it was a real user or a bot, and ensure the login is secured with two-factor authentication if needed.

A critical vulnerability in PHP 8.3 was targeted. Verifying the exact version and applying updates if needed is key to closing this potential risk.

Low-severity FTP evasion attempts were logged but not blocked. This suggests a possible misconfiguration or unused service that could be reviewed for removal or tightening.

The NGFW is working as configured, but it only sees what reaches it. A deeper security layer, like Seguridad 360, could help detect and respond to threats inside the server and beyond the firewall.

Your action plan

THIS MONTH

Check Cloudflare and WordPress logs for the login attempt from 198.51.100.26

Why: To determine if it was a real user or a bot and ensure the WordPress login is secured with two-factor authentication if needed.

Who: You

How we will check it: Review the logs and confirm if two-factor authentication is enabled.

THIS MONTH

Verify the PHP version and update if needed

Why: A critical vulnerability in PHP 8.3 was targeted. Confirming the exact version and applying updates if needed is key to closing this potential risk.

Who: You

How we will check it: Check the PHP version in SWPanel and confirm any updates applied.

NGFW report of swpanel.com generated by SWPanel

Conclusions of the analysis

MEDIUM TERM

Review and disable or secure the FTP service if not needed

Why: FTP evasion attempts were logged. If the service is not in use, it's better to disable it to reduce the attack surface.

Who: You

How we will check it: Confirm the FTP service is disabled or secured in the server configuration.

Seguridad 360: one step further

TRY IT

Seguridad 360 adds an extra layer of protection beyond the NGFW, including a WAF, bot blocking, and a SOC that actively monitors and responds to threats. Given the detected attacks on PHP and WordPress, it could help detect and prevent similar threats more proactively. You can activate it directly from SWPanel to test it.

You're doing well in keeping threats at bay, but staying a step ahead is always better. Let me know if you want to explore how Seguridad 360 could help you with that.

Your SWPanel AI security assistant

Text written by the SWPanel AI Assistant from the data in this report, with a model running on SW Hosting's own servers: your data never leaves our infrastructure. The figures are computed by the system; the AI only interprets them.

NGFW report of swpanel.com generated by SWPanel

Glossary

The technical terms used in this report, in alphabetical order.

Application
Type of traffic the NGFW recognises by its content (web-browsing, ssl, ftp), not only by its port.

Blocked threat
One the NGFW stopped before it reached the server, according to the chosen sensitivity.

Brute force
Trying many passwords in a row until one works.

Code execution
Attack that tries to make the server run the attacker's commands.

CVE
Public code that identifies a known vulnerability, for example CVE-2020-1967.

Denial of service
Attack that floods or breaks a service until it stops responding.

Exploit
Program or request that takes advantage of a specific vulnerability.

Inbound and outbound traffic
Data arriving at your services and data leaving them.

Information leak
Attempt to extract internal data from the server, such as configuration files or passwords.

Logged threat
One detected and recorded but not blocked, because its severity is below the sensitivity.

NGFW
Next Generation Firewall: a firewall that inspects traffic content to detect and block threats.

Protocol anomaly
Traffic that does not behave like the protocol it claims to be.

Sensitivity
Severity from which the NGFW blocks. Below it, it only logs.

NGFW report of swpanel.com generated by SWPanel

Glossary (continued)

Session

A complete connection between two machines, from the first packet to the last.

Severity

Risk level of a threat: critical, high, medium or low.

SQL injection

Sneaking database commands into the data sent to an application.

Threat ID

Identifier of the threat in the NGFW vendor's catalogue.

Vulnerability

Security flaw in a program that an attacker can exploit.

NGFW report of swpanel.com generated by SWPanel

Annex: AI compute

IA **What it took to write this report with AI**

The assistant and the translations in this report were generated by a language model running on SW Hosting's own servers: your data never leaves our infrastructure.

AI compute

qwen3-32b MODEL	**vLLM** ENGINE	**3** MODEL CALLS
6.447 TOKENS READ	**2.954** TOKENS WRITTEN	**62.0 s** COMPUTE TIME

Infrastructure

NVIDIA A100 GPU	**80 GB** HBM2E	**312 TFLOPS** FP16/BF16

Energy and cost

0.0099 kWh COMPUTE ENERGY	**0.0248 kWh** TOTAL ENERGY (WITH COOLING)	**6.2 g** CO2 EMITTED
0.0356 € COMPUTE COST		

Estimate: GPU at 575 W, cooling of 1.5 kW per kW of compute, 0.185 EUR/kWh, 1.8 EUR per GPU hour and 250 g of CO2 per kWh.

NGFW report of swpanel.com generated by SWPanel

swpanel

https://www.swpanel.com

Document: SW-NGF-EJEMPLO-2026

Report automatically generated by SWPanel · https://www.swpanel.com