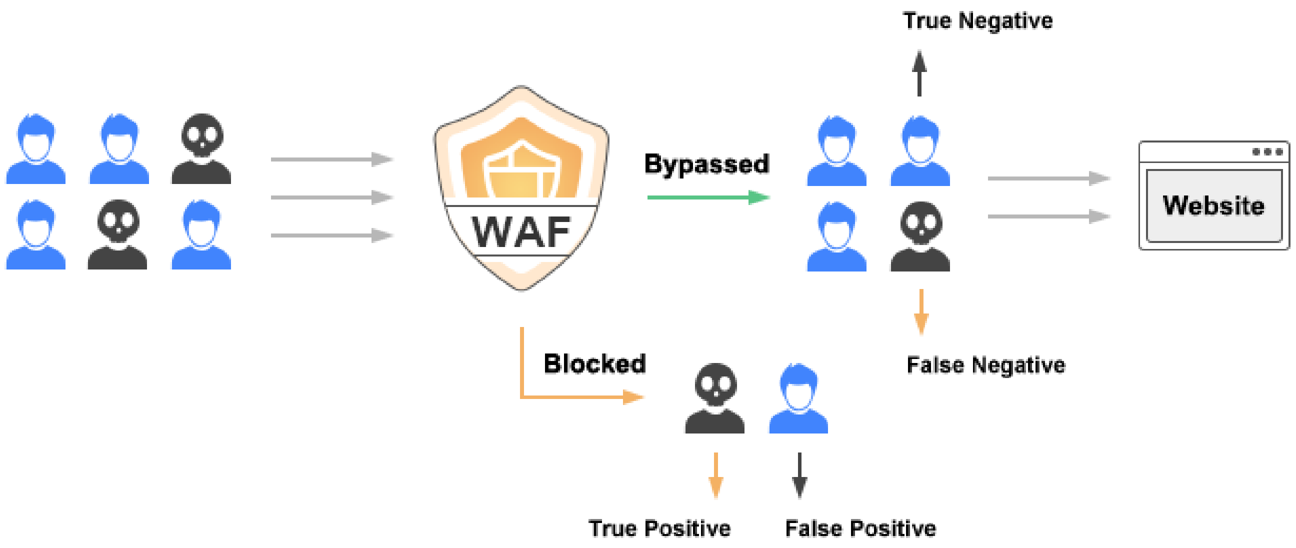
One Article Clarifies Four Very Brain-Burning WAF Terms

Gartner's prediction in 2012 that 70% of organizations will use WAF services in 2024 seems to be quite accurate. WAF (Web Application Firewall) has become a website security necessity, not just for classified protection, but to ensure the reliable operation of the website system. You can purchase WAF hardware devices or cloud WAF services to achieve WAF protection. However, users are confused by the dazzling array of WAF devices and WAF cloud services on the market and various protection indicators of WAF, this article will explain clearly the four brain-burning terms of WAF: True Negative, False Negative, True Positive, False Positive, and explain the actual meaning and significance of these terms in WAF protection with examples.

1. What is True Negative, False Negative, True Positive, False Positive?

These 4 terms are very tongue-twisting, but users who really want to use WAF can't get around it. WAF works by allowing normal traffic and blocking attack traffic, which some vendors also call traffic scrubbing. As shown in the figure below, the blue user is the good user who accesses the website normally, and the black user is the hacker who tries to attack the website, and these users are mixed traffic to visit the website. The WAF must be able to correctly detect normal traffic and allow it, which is the **True Negative** traffic and does not block it. If WAF fails to identify the attack traffic and bypass it, this is the **False Negative** traffic, which is a leak, indicating that WAF's detection capability is problematic. If WAF does successfully block the attack traffic, this is the **True Positive** traffic, and if it is really blocked, it means that WAF is truly capable of blocking the real attack traffic. However, if WAF blocks normal traffic, which is the **False Positive** traffic, it is an incorrect block, indicating that there is still a problem with WAF's distinguishing ability.



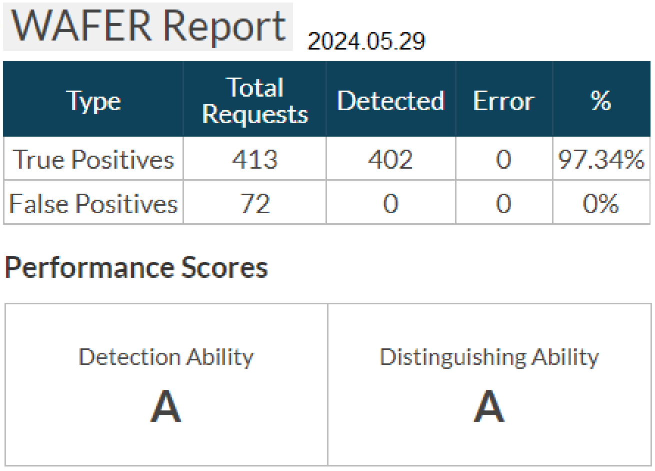
Maybe there are some readers who are still confused by these 4 terms, the author thinks of the Pandemic just past, many people have been "Positive", and the comparison to this situation should be clearer to understand. If everything is normal and there is no sign of "Positive ", then to do the test, and the result is Negative, this is the **True Negative**, you can go to work normally, and you will not be blocked anywhere. However, if you are really "Positive", but the test result is still Negative, this is the **False Negative**, but you can still go to work unhindered, which means that there is something wrong with the detection system, which is very dangerous. And if you are really "Positive", and you are really detected during the test, you are the **True Positive**, it means that the detection system is very effective, and you have to isolate at home or go to isolation for treatment. However, if you are not Positive, but the test results say you're Positive, it's miserable, it's **False Positive**, but it will be mistakenly blocked and isolated for treatment.

The worst-case scenario is False Negative, which does not block the malicious attack traffic that should be blocked. The next worst case is False Positive, which mistakenly blocks normal traffic, so that normal traffic cannot access the website normally. Both are important indicators to measure a WAF's detection ability and distinguishing ability, and the most ideal indicators are, of course, 100% no False Negative and 100% no False Positive.

2. Interpret the WAFER Test Report of ZoTrus Gateway built-in WAF module

Understanding the above 4 important terms of WAF, let's look at the WAFER Test Report of the ZoTrus

Gateway built-in WAF module. As shown in the figure below, the first row is True Positives, and a total of 413 real attacks were launched during the test, and 402 were detected, with a detection rate of 97.34%, which means that the Detection Ability is A-level. The second line is a False Positive, a total of 72 false positive attacks were launched during the test, and there was no false block (0), so the Distinguishing Ability is A-level. Overall, the ZoTrus Gateway has a very good WAF protection performance.



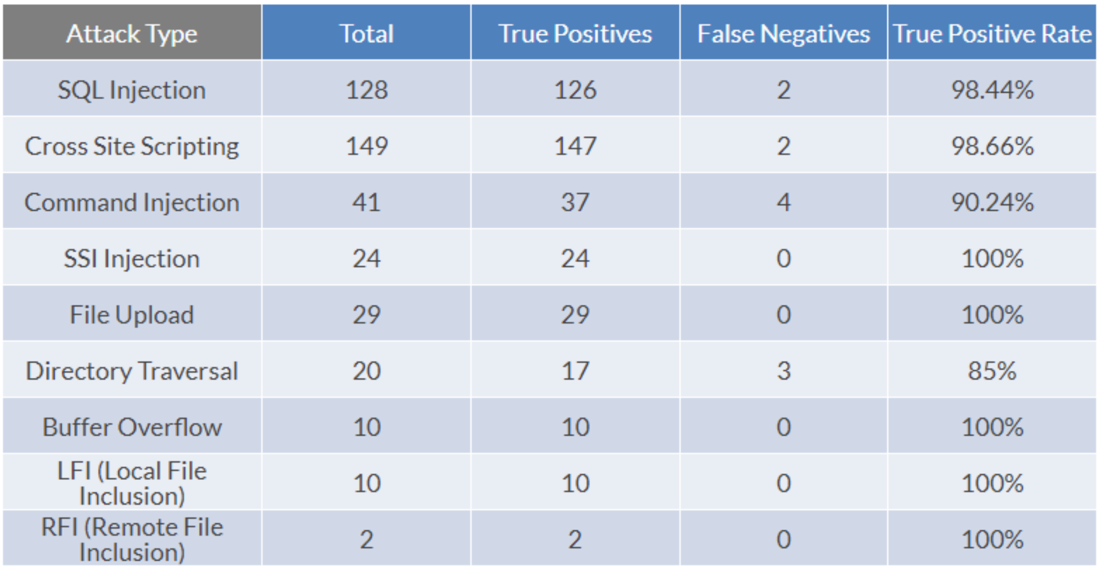
WAFER Report 2024.05.29

Type	Total Requests	Detected	Error	%
True Positives	413	402	0	97.34%
False Positives	72	0	0	0%

Performance Scores

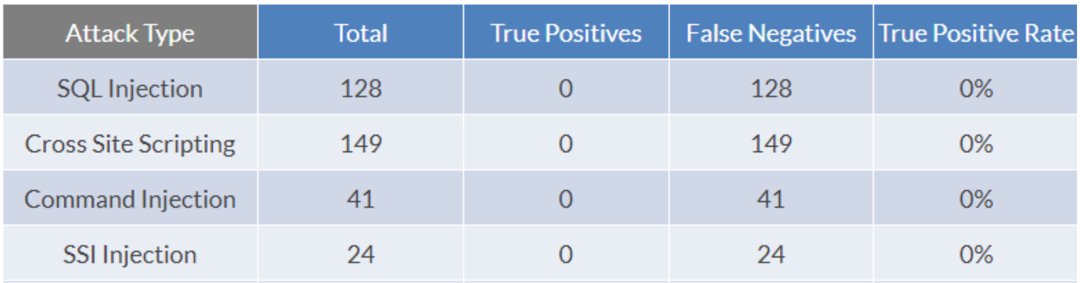
Detection Ability	Distinguishing Ability
A	A

Let's look at the detection and blocking of specific attack types. SQL Injection launched a total of 128 attacks and blocked 126 times. There were also 2 false negatives, that is, missed blocks, with a True Positive Rate of 98.44%. For Cross Site Scripting, a total of 149 attacks were launched and 147 were blocked. There were also 2 false negatives, that is, missed blocks, and the True Positive Rate was 98.66%. For Command Injection attacks, a total of 41 attacks were launched and 37 were blocked. There were also 4 false negatives, that is, missed blocks, with a True Positive Rate of 90.24%. For SSI Injection, a total of 24 attacks were launched and 24 were blocked. There are no false negative, and the True Positive Rate is 100%. Other test results are not analyzed one by one. For attacks that are not blocked, the Gateway WAF Module needs to be continuously improved in the WAF protection rules and the rules need to be updated regularly. Of course, customer also need to pay attention to analyzing WAF logs and constantly customize protection rules based on attacks.



Attack Type	Total	True Positives	False Negatives	True Positive Rate
SQL Injection	128	126	2	98.44%
Cross Site Scripting	149	147	2	98.66%
Command Injection	41	37	4	90.24%
SSI Injection	24	24	0	100%
File Upload	29	29	0	100%
Directory Traversal	20	17	3	85%
Buffer Overflow	10	10	0	100%
LFI (Local File Inclusion)	10	10	0	100%
RFI (Remote File Inclusion)	2	2	0	100%

To let readers intuitively feel the difference between a website without WAF protection and a website with WAF protection, the author also used WAFER to test a website without WAF protection, and the test results are shown in the following figure. According to the test results of WAF protection above, the True Positive Rate of four type attacks, including SQL Injection attacks, Cross Site Scripting attacks, Command Injection attacks, and SSI Injection attacks, is 0%. That is to say, all kinds of attacks have been successfully implemented, you can imagine what the consequences are, which is why websites must have WAF protection.



Attack Type	Total	True Positives	False Negatives	True Positive Rate
SQL Injection	128	0	128	0%
Cross Site Scripting	149	0	149	0%
Command Injection	41	0	41	0%
SSI Injection	24	0	24	0%

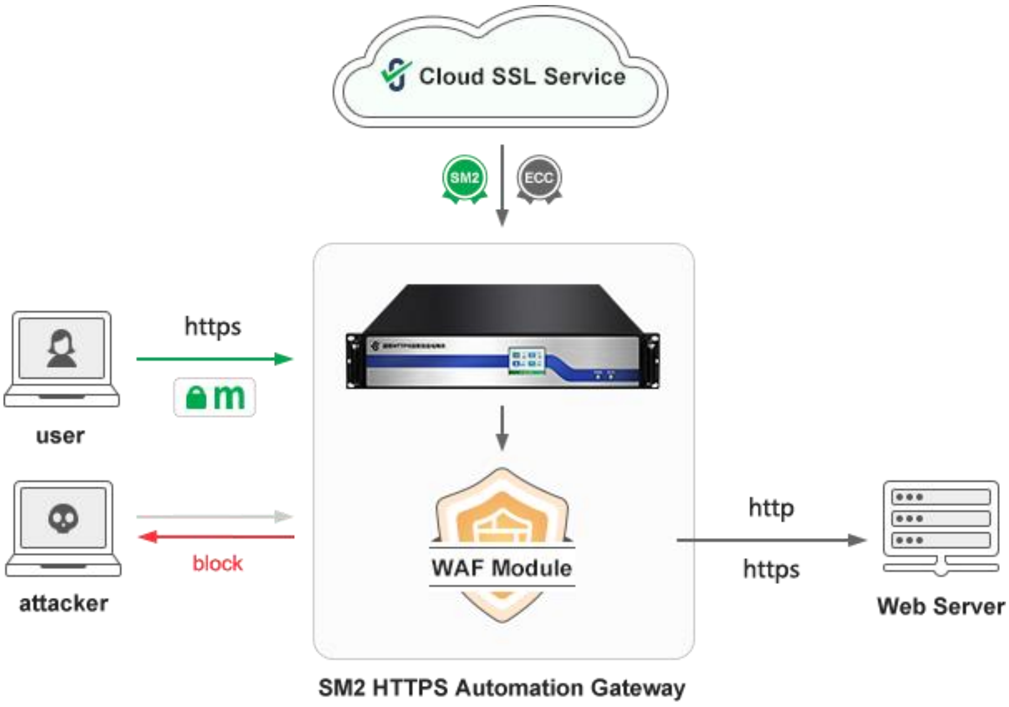
3. Further Reading: WAF devices must support automatic SSL certificate management

The author believes that readers can really understand the four terms that are difficult to understand through the content of the first part, "True Negative", "False Negative", "True Positive", and "False Positive", because we have all been "Positive" and "Negative" during the Pandemic. By interpreting the WAF performance test data of ZoTrus Gateway, we should be able to further understand these four terms, and the author summary the four terms to the actual action results as: True Negative - bypassed, False Negative - leaky block, True Positive - block, False Positive - false block.

This section briefly explains that WAF devices or WAF cloud services must support automatic SSL certificate management.

As we all know, websites must implement HTTPS encryption to ensure the security of data transmission, and WAF protection must be able to read plaintext traffic data to analyze whether it is the attack traffic, which requires WAF to support HTTPS encryption and offloading. The traditional method is that users must apply for an SSL certificate from a CA and deploy it on a WAF device to enable WAF protection. In addition, to meet the cryptography compliance requirements, both WAF devices and cloud WAF services must support SM2 SSL certificates to implement SM2 HTTPS encryption.

ZoTrus Technology's innovative solutions can be used as a reference, ZoTrus Gateway, or third-party WAF equipment or WAF cloud services, can automatically connect to ZoTrus Cloud SSL Service, automatically configure dual-algorithm dual-SSL certificates for websites that need WAF protection, realize HTTPS encryption and offloading of adaptive algorithms, and hand it over to WAF module to achieve WAF protection, so that normal traffic can be transferred to the web server to process business and block attack traffic. ZoTrus Gateway supports automatic configuration of dual SSL certificates (SM2 OV SSL certificate + ECC DV SSL certificate) for up to 255 websites for 5 years, to realize SM2 HTTPS encryption with zero change of the original web server, and it is compatible with RSA algorithm HTTPS encryption, to achieve 5 years of security and worry-free, and use HTTPS plus WAF to ensure business data security.



In other words, ZoTrus SM2 HTTPS Automation Gateway perfectly combines HTTPS encryption automation and WAF protection automation into one device, to kill two birds with one stone, and meet the application requirements of cybersecurity protection compliance and cryptography protection compliance, which is the innovation of the ZoTrus Gateway, and it is also the most value-added point. ZoTrus Gateway can be treated as a WAF device that can automatically implement HTTPS encryption, which can meet the application requirements of customers who need WAF protection and SM2 HTTPS encryption automation.

Richard Wang

May 29, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.