

WEBFRONT-K: Web Application Firewall Specialized for the SSL

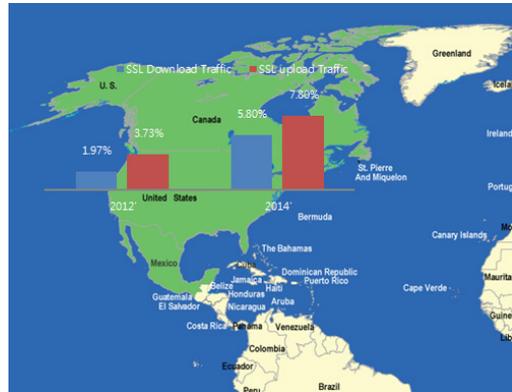
The Basis for Selecting the Web Application Firewall: SSL

The web application firewall (WAF) is the web security solution for protecting web servers and data by checking the requests and responses between the web servers and web service users.

WEBFRONT-K maintains the performance of the servers by performing the encryption/decryption of the SSL traffic in front of the web servers and storing/monitoring the SSL certificates as well as keys in front of the web servers. The SSL traffic is processed with more stability and speed while using 2048-bit RSA keys — which is recently recommended for more secure SSL communication.

According to the sales of PIOLINK’s WAFs from 2010 to 2014, the total amount for the sales of the SSL model had increased about 35%. (2010: 43% → 2014: 78%) This suggests that there are more needs for the SSL from the customers.

Moreover, for the wired/wireless network traffic around the world from 2012 to the first half of 2014, the encrypted traffic has increased for both downloading (about 3 times) and uploading (about 2 times). This result is closely connected to the expectancy for the quality improvement due to strengthening the security and increasing the speed of the web service by applying the encryption.



As Google doubled the size of RSA keys from “1024-bit” to “2048-bit” in 2013, the 2048-bit keys are currently used for most parts of the web service. Therefore, the WAFs should support the keys with the sizes of 2048 bits or more with more stability.

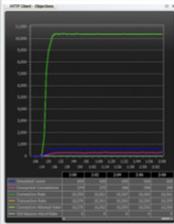
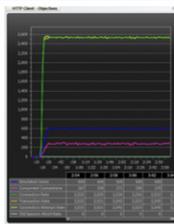
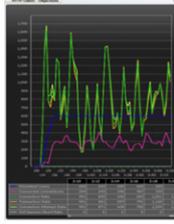
WEBFRONT-K for the Advanced SSL

1. Standards for SSL Performance (CPS and TPS)

The value of CPS (connection per second) represents the maximum number of creating TCP connections for each second, and the value of TPS (transaction per second) represents the maximum number of transactions processed in one second. While measuring the TPS, the results vary widely according to the numbers of transactions which are included in each session. However, in Korea, the numbers are inconsistent for each manufacturer as tests are performed with 10 or more transactions for each session, to exaggerate the values. Therefore, it is better to compare the SSL performances of WAFs with their CPS values. In case of using the TPS values, it is necessary to check how many transactions are included in each session.

2. SSL Performance on WEBFRONT-K

While processing SSL, the loads on WAFs increase as a lot of resources are used. WEBFRONT-K reduces the waiting time by reducing the loads on the devices drastically and improving the speed of response through the SSL accelerator card (hardware). This reduces the extra cost of purchasing additional devices for processing SSL traffic. In **Table 1**, there are cases of the performance of WEBFRONT-K. Compare to the WAF of another company, WEBFRONT-K demonstrates the superiority on the performance and stability, even for processing traffic with 2048-bit RSA keys.

	1024-Bit RSA Key	2048-Bit RSA Key	Result
PIOLINK's WEBFRONT-K			Stability for 1024/2048-bit RSA keys
A Company's WAF			Not enough stability as RSA keys become bigger *Service is stopped

[Table 1 Performance Test for SSL Traffic]

In **Table 2**, the performances of the 2 models of WEBFRONT-K are displayed for SSL traffic. The performances are measured according to the 2048-bit RSA keys. The CPS is measured as “1 session = 1 get” while the TPS is measured as “1 session = 10 gets”. WEBFRONT-K models have the superior performances compare to the models from other companies for processing traffic with 2048-bit RSA keys.

WEBFRONT	K4200	K4400
HTTP Throughput	8 Gbps	12 Gbps
HTTPS CPS	7,000	7,500
HTTPS TPS (RPS)	40,000	50,000
HTTPS Throughput	6.5 Gbps	7.2 Gbps

[Table 2 SSL Performance Test for WEBFRONT-K Models^①]

WEBFRONT-K for the EV SSL Certificates

1. EV SSL Certificate

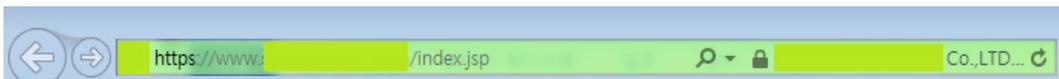
The EV SSL certificates enhance the security of the user interface by applying various methods for displaying the statuses of the websites which have been approved for security. This standard of certificates has been created to ensure protections for the users against continuously developing phishing and pharming methods. The color of the address bar is changed to green for the websites where the users’ data is protected by EV SSL certificates. More companies will use these certificates to gain more credibility from the users. Therefore, the WAFs should support EV SSL certificates.

^① **Standards for Measuring the SSL Performance**

- **Encryption Key Size:** 2048 bits (RSA)
- **CPS:** 1 session = 1 get, 1 KB (response size)
- **TPS:** 1 session = 10 gets, 1KB (response size)
- **Throughput:** 1 session = 10 gets, 550KB (response size)

2. Supporting EV SSL Certificates

WEBFRONT-K supports EV SSL certificates which are used internationally. The following image indicates the address bar of the website for one of the WEBFRONT-K service users. The HTTPS service, as well as the HTTP service, is supported with the stability even after applying EV SSL certificates.



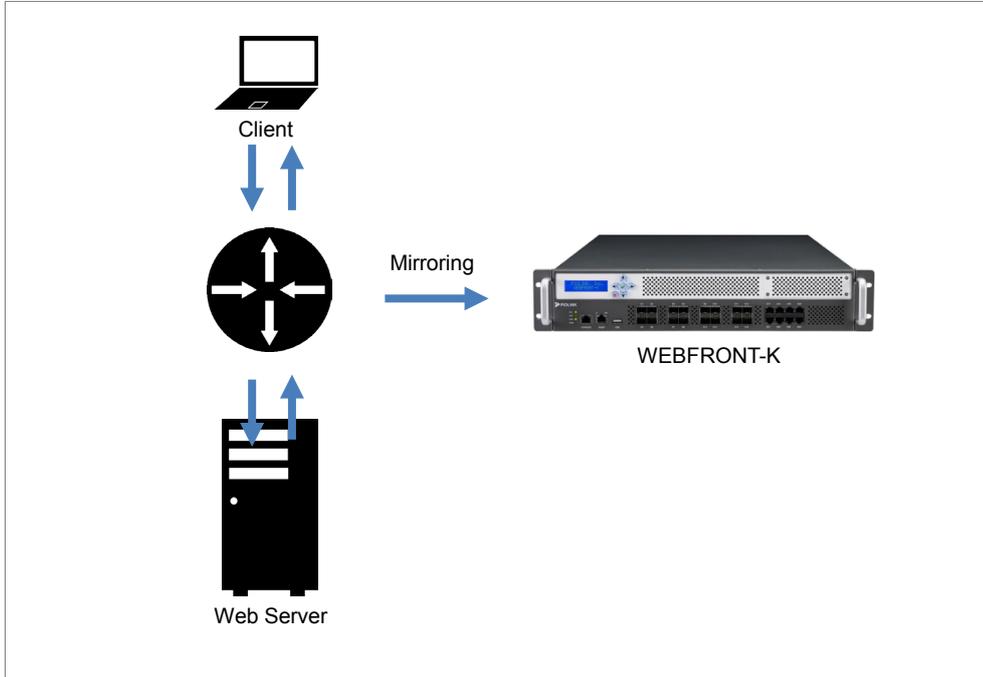
[Figure 1 Example of Applying the EV SSL Certificate]

WEBFRONT-K for the Stable SSL Service in the Mirroring Mode (Out-of-Path Mode)

1. Definition of the Mirroring Mode

The web traffic is ever increasing, and more parts of business and work involve the web service. There is more sensitivity for the response time, and more needs on the advanced web security features with high performance. It is becoming harder and harder to ensure the high capacity, quick response, and service availability on in-line proxy devices. PIOLINK has developed WEBFRONT-K, the WAF with high performance, along with the mirroring mode for the service availability. The mirroring mode monitors and analyzes packets by mirroring these packets between the clients and the servers. This mirroring mode is also optimized for the service availability as WEBFRONT-K does not interrupt any part of the current network structure. With the mirroring mode, the WAFs became available for the sections which have been sensitive to the service availability. (e.g. financial institutions and web portals) Moreover, both the HTTP and HTTPS are supported for the stability while processing continuously increasing amount of SSL traffic as well as blocking illegal requests.

2. Network Structure for the Mirroring Mode



[Figure 2 Network Structure of the Mirroring Mode]

3. Availabilities for the Mirroring Modes

	PIOLINK	A	B	C
Mirroring Mode	supported	supported	not supported	not supported
HTTPS in the Mirroring Mode	supported	not supported	not supported	not supported
Blocking in the Mirroring Mode	supported	not supported	not supported	not supported

[Table 3 Availabilities for the Features in the Mirroring Mode (September 2015)]

Case Studies in the Securities Sector

1. S Securities

This is the biggest securities firm in Korea. As the traffic is concentrated during specific periods of time, there were needs of the security and availability on the service for particular periods of time. This firm demanded more of the security and SSL acceleration. 5 units of WEBFRONT-K were installed in the one-arm structure, and they have provided the stability for the network system and the security for the web service. The SSL traffic is processed with the stability during the processes of trading stocks, and the availability is ensured for the stable service during the periods when there are increasing numbers of transactions.

2. A Airlines

This is the second biggest airline in Korea. It has to handle more than 600 applications, and bundles of traffic which are concentrated during the peak seasons in the spring, summer, and autumn. There were needs of the WAF for processing all of those applications as well as SSL traffic. A Airlines once used the WAF from X Company, but selected 4 units of WEBFRONT-K due to the lack of the features for processing SSL traffic. Currently, WEBFRONT-K is at the center of the web security part of this airline, providing safe and seamless web service for the customers by processing SSL traffic with the stability during the peak seasons.

WEBFRONT-K is gaining more recognition on the stability for processing SSL traffic of: the financial section, insurance section, colleges, medical service, public service, and companies.

To Satisfy All Customers

1. Low-End Web Application Firewalls for Small/Medium-Sized Businesses

Recently, the ranges of hacking are expanding from big websites to small and medium-sized websites. As most of these websites cannot afford high-priced WAFs, they are vulnerable against web attacks. They can be the direct targets or the slaves for other attacks. For these websites, WEBFRONT-K1600 (the low-end WAF model) is available with the options as follows.

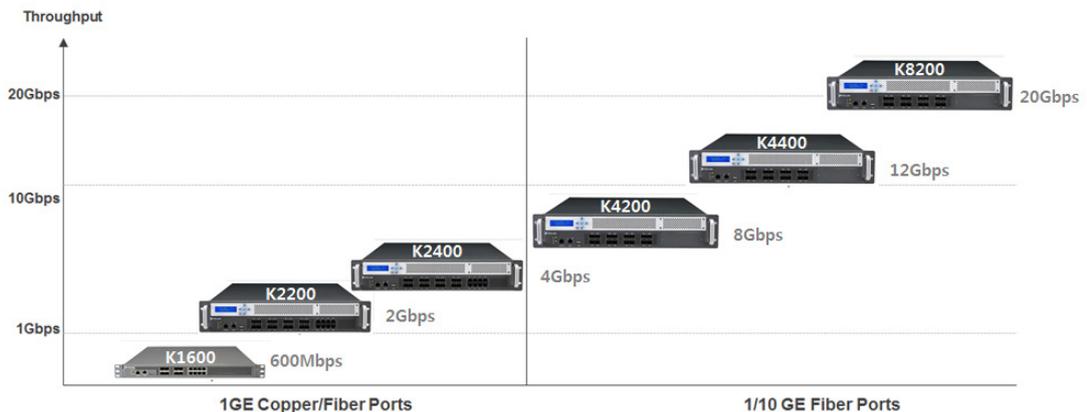
There are 3 types of SSL licenses.

HTTPS Throughput	HTTPS CPS	HTTPS TPS	Applied License
100Mbps	300	2,000	Software SSL (Free)
300Mbps	1,000	8,000	WAFK10,000TPS
600Mbps	2,000	16,000	WAFK22,000TPS

[Table 4 SSL Licenses for Small/Medium-Sized Businesses]

2. Full Line-up from the Mbps Level to the Gbps Level

The leader of the high-end WAFs, WEBFRONT-K is safer and faster. Once optimized only for the high-end market, WEBFRONT-K currently provides the full line-up of models for customers from small websites to huge websites (such as web portals, banking websites, game websites, and online shopping malls).



[Figure 3 WEBFRONT-K Line-up]

Check Points for Selecting a Web Application Firewall

You **must** consider the following points while selecting a WAF for the SSL.

- Is it stable for using the 2048-bit keys?
- Does it use the SSL for hardware to reduce the loads on the WAF's performance?
- Is it possible to extend the performance of the SSL?
- Are EV SSL certificates supported?
- Is the SSL supported in the mirroring mode with the out-of-path deployment?
- Can it support big websites which include large portions of SSL traffic?

- Depending on the product's upgrade and correction of printing errors, PIOLINK, Inc. reserves the right to change specifications at any time without notice.
- Actual products may vary due to product enhancement.
- Copyrights to the names of the companies and products on this document are the properties of those companies.
- For more information on how to order this product, please contact a local partner in your country, or use the following contact information.



Optimizing Your Cloud Data Center

global@piolink.com

www.PIOLINK.com

