French Tennis Federation

SOLIDserver™ Protects Internet Services for Grand Slam Roland-Garros

Project Type:

- Improve DNS performance

- Enhance network security with DNS protection

- Overlay management of existing DDI components

Key Benefits:

- Availability of the DNS service ensured during the 2016 tournament

- Significantly enhanced user experience

- DNS resolution time reduced by a factor of 4 to 6

- Smooth, quick implementation with easy integration

- Ability to manage Microsoft DHCP in overlay

The French Tennis Federation (FFT) is the governing body of tennis in France, founded in 1920. Highly revered worldwide, it hosts and supports large events like the Grand Chelem Roland-Garros (French Open) and the BNP Paribas Masters tournaments. The internal IT department of the FFT supports 400 internal users at their Roland-Garros Stadium headquarters, and about 800 other users within the region (for a total of 1200). Franck Labat, FFT CTO, manages the infrastructure team and the relationship with its partner responsible for managing the network.

> "We knew that DNS was critical, and that it could be a target but also a vector of cyber-attacks. The insider threat is a reality we have to take care of, and be sure we have the best security in place."

> Franck Labat, FFT CTO

During the two weeks of the French Open in Paris, roughly 40 television stations broadcast every match. Additionally, more than 2,000 journalists (print, radio, and web) and 1,200 VIPs (players and their families and coaches) need an internet connection to cover the event and access applications and the web. The quality of these delivered services are key for the reputation of Roland-Garros.

The 2015 Internet Performance Issue

In 2015 during the French Open, the external DNS services suffered a decrease in performance due to a high volume of DNS queries during a short period of time. The DNS resolution times were too long, and Internet access appeared slow. The IT department found a workaround to ensure good service, but it was the catalyst to begin a project to internalize the external DNS service to avoid the situation again in the future. At the same time, an overall security audit of the site was being conducted, so it made sense to also secure the DNS infrastructure (thousands of devices would be connecting to the Roland-Garros network, without any guarantees that they will not bring malware or viruses with them). "We knew that DNS was critical, and that it could be a target but also a vector of cyber-attacks. The insider threat is a reality we have to take care of, and be sure we have the best security in place", said Franck Labat.

Availability and Performance as Main Objectives

FFT asked its partner managing their network to find a fast, reliable and secure DNS solution. The short list was relatively fast to make as the need for a high performing DNS solution reduced dramatically the list of possible solutions. During the two weeks of tournament, there are billions of DNS requests that have to be served.

There were three basic stipulations for the selection of the new product and solution. "As we are a French Sport Federation, we first looked to see if any French technology could fit our needs. Second, we wanted a hardware-like appliance that could be easily integrated into our existing IT environment. Lastly, the partner had to be confident with the performance and usability of the solution", explained Labat. They evaluated several products and vendors including Infoblox, but quickly selected EfficientIP: the network management partner discovered that no other solution available on the market was able to compete with SOLIDserver™ in terms of DNS performance. Labat added, "I was also very interested by the ability of SOLIDserver to manage DNS and DHCP at the same time, even managing Microsoft DHCP in overlay- it brings a single point of management to the team and facilitates the transition".

The objective was to not have any further internet performance issues during the tournament, and offer the best service to the press and VIPs.

Fast Implementation and Quick, Measurable Benefits

The implementation itself was made by the network partner with the help of EfficientIP engineers, installing redundant servers for high availability. Labat was pleased, declaring, "The implementation was so smooth that as a CTO, I didn't hear anything about it. It was a very good sign that our team and partner were confident with the solution and moved it in production. As we deployed SOLIDserver close to the start of the tournament, we were very busy with other projects, so it was essential that this deployment be smooth, on time and without problems."

The DNS Blast product was installed to ensure performance of DNS resolution. FFT was confident that with their newly-enabled 17 million QPS cache, they would be able to absorb tremendous traffic- or even malicious traffic coming from inside- during the two weeks. They will now always be able to answer legitimate traffic.

DNS Guardian was also deployed, with specific rules to monitor and analyze DNS traffic to discover "suspicious" behaviors. FFT cannot monitor all the devices connected to their network and cannot assume they are safe without malware. The risk can come from inside, and should be mitigated rapidly. The DNS Guardian rules analyze real-time traffic to detect:

- Volumetric attacks (DDoS)
- Data exfiltration
- Phantom or Random Subdomain attacks
- NXDomain attacks
- Syntax protection (cache poisoning)
- Water Torture attacks

In addition to the ability to absorb a huge amount traffic, FFT dramatically reduced their DNS resolution time by a factor of 4 to 6 during the peak period. The assigned objective to ensure the service during the two weeks of the tournament for VIPs and press was met, and performance was optimized at the same time. Latency time was also reduced to a minimum.

Looking Towards the Future

Change management for FFT will be facilitated with a step-by-step transition. The next step of the implementation is to integrate the DHCP management, as they have numerous IP plans and VLANs for security and organizational needs. The 10,000 RJ45 network connectors are placed all over the stadium (including in unexpected locations like plant gardens or the pit for photographers), with more to be installed when the new stadium is completed.

The next phase will be to manage the Microsoft DHCP in overlay with SOLIDserver, and benefit from the available features to optimize the IP address plan. A further step would be to use the SOLIDserver DHCP service to free up servers in the infrastructure, shutting down the Microsoft devices. In any case, SOLIDserver can start managing external DHCP services integrated with the DNS management, and when the organization is ready switch to its internal DHCP services.