CASE STUDY

Securing High Network Availability and Performance at the Youth Olympic Games

Along with the Olympic Games and the Winter Olympics, the Youth Olympic Games are one of the largest international sporting events in the world. In each edition, the International Olympic Committee (IOC) works hand in hand with the host city to coordinate the organization of this competition that brings together—both in person and virtually—millions of spectators across the world. The latest Youth Olympic Games were held in Buenos Aires, Argentina, in October 2018. This 12-day competitive event brought together 4,012 young athletes representing 206 delegations from different countries. This latest edition also reached a record number of attending spectators, amassing a viewership of 1.1 million people across the 16 locations chosen for the different sports.

At events of this scale and magnitude, the athletes' physical safety has always been a priority. In this day and age, however, where all information and data are stored and carried through the network, computer security and IT infrastructure availability also proved to be critical aspects for the event organizers. The Government of Buenos Aires' IT Security team was tasked with managing all aspects of the event's cybersecurity, including a preliminary risk assessment for an international event of this nature, the definition of processes to address them, and the implementation of Fortinet advanced security next-generation firewalls to help guarantee network availability and prevent and mitigate any incidents.

Securing the IT Infrastructure of a Large-Scale International Event

The process kicked off three years prior to the games, following the selection of Buenos Aires as the host city for the 2018 Youth Olympic Games. The city government's IT Security team designed a plan to deploy the IT infrastructure, systems, and cybersecurity for the Buenos Aires games.

"We exchanged ideas with other entities until we ultimately defined the deployment of specific networks for the Olympic Games in each of the 16 venues. From a computer security standpoint, we set up three lines of work: one focused on prevention, one on operation, and another on incident resolution and forensic analysis," explained Gustavo Linares, managing director of IT Security for the Buenos Aires City Government.

"We needed to find a complete solution that ensured network availability, accessibility, and performance without compromising on security for the Youth Olympic Games. That is why we chose to deploy Fortinet's FortiGate full bundle solution with all of its capabilities, including IPS control, web filtering, advanced threat protection, and all associated services, at each venue as well as at central data centers."

– *Gustavo Linares, managing director of IT Security for the Buenos Aires City Government*

Details

Customer: Government of the City of Buenos Aires

Industry: Government

The most pressing requirements and requests made by the organizing committee were related to ensuring network availability and data security. The technology used for collecting data on the results of the Olympics was provided by OMEGA, the official timekeeper of the Olympic Games. However, it was the host city's responsibility to ensure the information's transmission, availability, and security. Given that an athlete cannot be asked to repeat a trial because of a data breach, the priority was always to ensure the information's availability and security as it circulated across networks at all times and throughout all venues.

There was a high level of traffic at the Olympic Park, where OMEGA was collecting data. Additionally, there was a medium-demanding volume of video transmission traffic and other considerably demanding traffic in the information centers where data was processed and passed on for international streaming. Web browsing availability was a key priority at the Olympic Village as well, which housed the athletes throughout the games' 19-day duration. Besides providing adequate availability and performance, there was also a concern for content filtering to avoid any inconvenience or complaint that could affect the participants—an aspect of utmost importance considering all athletes were minors.

Choosing the Right Security Solution

"We developed different network solutions at each of the Olympic Games' locations, all supported with Fortinet equipment to guarantee the information's availability, performance, and security. We deployed 48 FortiGate next-generation firewalls, all with different capacities in accordance with each location's requirements and network. A bidding process was launched for the interconnection service and we then incorporated Fortinet's security equipment into the telecommunications company's infrastructure," said Linares.

The IT Security team had to comply with a service-level agreement (SLA) imposed by the IOC that required the resolution of any incident in five minutes; however, they went further and lowered that requirement to one minute due to the reliability of the implemented technology.

"The Buenos Aires City Government was already working with Fortinet's firewall solutions in two of its data centers, so Fortinet was a natural choice. We knew we could find a complete solution to ensure traffic and accessibility at the Youth Olympic Games, which is why we chose Fortinet's complete FortiGate bundle, fully equipped with all its capabilities, including IPS control, web filtering, and all associated services, at each venue and at central data centers."

The Olympic Games are a multidisciplinary and international event; there is no other event involving 206 countries. The organizers knew cyber crime is used not only for economic purposes but also for political and ideological reasons. The risk potential multiplies when you consider the political and economic conflicts of each of these countries.

So, in addition to creating a Federal Security Committee with different Argentine security agencies and INTERPOL, the team created multiple conflict scenarios and developed resolutions for each of them based on the deployed Fortinet information security technology. Approximately 60 scenarios were created—some based on other Olympic Games' experiences, others based on government experience or imagination. This helped achieve rapid detection and resolution. For instance, the team found five fake domains similar to those of the games—created with the intention of generating phishing scams—which were eliminated.

Solution

FortiGate 300E-BDL, FortiGate 201E-BDL, FortiGate 1200D-BDL, FortiGate 1500D-BDL

Business Impact

- 24/7 availability to support demanding multinetwork information traffic at a large-scale event
- High-level security to prevent cybersecurity incidents and ensure data integrity in an elite international sports competition
- Fast detection and response capacity to comply with incident resolution SLAs in less than a minute
- Ability to filter web content for underage users
- Easy management of multiple networks with different levels of sophistication and strictness

"Being able to rely on a skilled technological partner allowed us to detect incidents we had already mapped, find the solution, and implement it swiftly to mitigate any potential cybersecurity risks, all while never slowing down critical network availability or performance."

– Gustavo Linares

Availability to Meet the Highest Standards

"We are extremely satisfied with the results we achieved. It was 12 activity-filled days with an IOC record participation of 1 million spectators and we had no cybersecurity incidents. We managed to prevent, detect, and mitigate any attempt to impact network availability or performance. In regard to administration, despite having more than 40 FortiGate firewalls of different capacities in operation, we did not experience any problem with the equipment, even though we had implemented the complete security package from Fortinet," added Linares.

Fortinet had already installed the Government of Buenos Aires' perimeter core security infrastructure system, greatly facilitating the administrative process of this project. Knowing the tools' capabilities and their administration made everything much easier. Additionally, Fortinet provided the solution most closely attuned to the needs of the event by connecting each of the event locations to a central data center with high availability and performance.

"We made a massive effort in prevention, analysis, research, and in creating a Computer Security Incident Response Team (CSIRT) specifically for the games. Generating known conflict scenarios combined with potential conflicts imagined through professional and political experience to test the security infrastructure is key. So is the ability to operate during the event and knowing how to work quickly and efficiently. Having this prior knowledge combined with the right technological partner allowed us to detect incidents that we had already mapped, thoroughly know which solution to apply, and then implement it quickly to mitigate cybersecurity risks," concluded Linares.

"We are extremely satisfied with the results we achieved. It was 12 activity-filled days with an IOC record participation of 1 million spectators and we had no cybersecurity incidents. We managed to prevent, detect, and mitigate any attempt to impact network availability or performance."

– Gustavo Linares

FORTINET

www.fortinet.com

March 7, 2019 10:34 PM

367290-0-0-EN

D:\Fortinet\Work\March\030719\cs-youth-olympics