CASO DE ESTUDIO

Fortinet asegura una alta disponibilidad y el rendimiento de la red en los Juegos Olímpicos de la Juventud

Los Juegos Olímpicos de la Juventud son uno de los eventos deportivos internacionales de mayor escala a nivel mundial, junto con los Juegos Olímpicos y los Juegos Olímpicos de Invierno. En cada edición, el Comité Olímpico Internacional (COI) trabaja junto a la ciudad sede para coordinar la organización de esta competición que reúne de manera presencial y virtual a millones de espectadores de todo el mundo. En octubre de 2018, se llevaron a cabo los Juegos Olímpicos de la Juventud en la Ciudad de Buenos Aires, Argentina. Este evento de 12 días de competencia reunión a 4.012 jóvenes atletas representantes de 206 delegaciones de diferentes países. Esta última edición contó además con una cifra récord de espectadores; 1,1 millón de personas se hicieron presentes en las 16 locaciones elegidas para las diferentes disciplinas deportivas.

En un evento de esta escala, la seguridad física de los atletas siempre ha sido prioritaria. Sin embargo, en este momento donde todos los datos y la información son transportados a través de la red, la seguridad informática y la disponibilidad de la infraestructura de TI fueron aspectos críticos para los organizadores de la competencia. El equipo de Seguridad Informática del Gobierno de la Ciudad de Buenios Aires estuvo a cargo de la gestión de todos los aspectos relacionados a la ciberseguridad del evento, incluyendo la evaluación previa de los riesgos que representa un evento internacional de estas características, la definición de los procesos para abordarlos y la implementación de la seguridad avanzada de los firewall de próxima generación de Fortinet que ayudó a garantizar la disponiblidad de la red, y a prevenir y mitigar los incidentes.

El reto de asegurar la infraestructura tecnológica de un evento de gran escala internacional

El proceso comenzó más de tres años antes de la realización de los juegos, luego de que la Ciudad de Buenos Aires fuera elegida como sede para los Juegos Olímpicos de la Juventud 2018. El equipo de Seguridad Informática del Gobierno de la Ciudad delineó el proyecto de despliegue de la infraestructura informática, los sistemas y la ciberseguridad para los juegos de Buenos Aires.

"Necesitábamos encontrar una solución completa que garantizara la disponibilidad, accesibilidad y rendimiento de la red sin comprometer la seguridad de los Juegos Olímpicos para la Juventud, por lo que contratamos el full bundle de FortiGate de Fortinet con todas las capacidades, incluyendo control IPS, filtrado web y todos los servicios asociados en cada uno de los venues y en los centros de datos centrales. Contar con el socio tecnológico adecuado nos permitió detectar incidentes que ya teníamos mapeados, conocer la solución e implementarla rápidamente para mitigar los riesgos a la ciberseguridad."

– Gustavo Linares, director general de Seguridad Informática del Gobierno de la Ciudad de Buenos Aires

Detalles

Cliente: Gobierno de la Ciudad de Buenos Aires.

Industria: Gobierno

Location: Buenos Aires, Argentina

"Fuimos intercambiando ideas con otros organismos hasta que definimos el despliegue de redes específicas para los juegos olímpicos en cada uno de los venues, 16 en total. Desde el aspecto de la seguridad informática, armamos tres líneas de trabajo: una enfocada en la prevención, una en la operación y otra en la resolución del incidente y el análisis forense", explicó Gustavo Linares, director general de Seguridad Informática del Gobierno de la Ciudad de Buenos Aires.

Los principales requerimientos y exigencias que recibieron por parte del comité organizador estuvieron relacionadas con garantizar la disponibilidad de la red y la seguridad de los datos. La tecnología utilizada para la toma de datos de los resultados de las pruebas olímpicas la aportó la empresa OMEGA, firma cronometradora oficial en los Juegos Olímpicos. Sin embargo, la responsabilidad de que la información se transmitiera, estuviera disponible y no fuera vulnerada era de la ciudad sede. Dado que no es posible pedirle a un atleta que repita una prueba por una pérdida de datos, la prioridad fue la disponibilidad y el aseguramiento de la información que circulaba por las redes en todo momento y desde todos los venues.

En el Parque Olímpico se tenía un nivel de tráfico súper exigente que era el de los datos tomados por OMEGA, a esto se agregó un tráfico medianamente exigente para el transporte de video y otro tráfico muy exigente en los centros donde se procesaban los datos y se pasaban al streaming internacional. Por su parte, la disponibilidad para la navegación web fue prioridad en la Villa Olímpica donde residieron los atletas durante los 19 días. Además de proveer adecuada disponibilidad y performance, se añadió la preocupación por el filtrado de contenido para evitar cualquier inconveniente o denuncia que pudiera afectar a los participantes. Máximo si se toma en cuenta que todos los atletas eran menores de edad.

La elección de la adecuada solución de seguridad informática

"Sobre cada una de las locaciones de los juegos olímpicos nosotros armamos diferentes soluciones de red, todas apoyadas con equipo de Fortinet para garantizar la disponibilidad, el desempeño y la seguridad de la información. Desplegamos 48 firewall de próxima generación FortiGate, con distintas capacidades de acuerdo a los requerimientos de cada locación y su respectiva red. Se realizó una licitación para el servicio de interconexión y sobre la infraestructura de la empresa de telecomunicaciones fuimos incorporando el equipamiento de seguridad de Fortinet", dijo Linares.

El equipo de Seguridad Informática debía cumplir un acuerdo de nivel de servicio (SLA, por sus siglas en inglés) impuesto por el COI que exigía la resolución de cualquier incidente en 5 minutos, sin embargo, fueron más allá y bajaron esa exigencia a 1 minuto por la confiabilidad de la tecnología desplegada.

"En el Gobierno de la Ciudad de Buenos Aires ya trabajamos con las soluciones de firewall de Fortinet en nuestros dos centros de datos, por lo que Fortinet fue la elección natural. Nosotros sabíamos que podíamos obtener una solución completa para asegurar el tráfico y la disponibilidad en los Juegos Olímpicos de la Juventud, por lo que contratamos el full bundle de Fortinet con todas las capacidades, incluyendo control IPS, filtrado web y todos los servicios asociados en cada uno de los venues y en los centros de datos centrales", agregó Linares.

Los Juegos Olímpicos son un evento multidisciplinar e internacional, no hay otro evento donde participen 206 países. Los organizadores sabían que el delito cibernético no solo se utiliza con fines económicos, sino también por razones políticas e ideológicas. El riesgo potencial se multiplica cuando se consideran los conflictos políticos y económicos de cada uno de estos países.

Solución

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

Impacto de negocios

- Disponibilidad 7x24 para soportar tráfico exigente de información sobre múltiples redes en un evento a gran escala
- Alta seguridad para prevenir incidentes de ciberseguridad y asegurar la integridad de los datos en una competencia deportiva de élite internacional
- Rápida capacidad de detección y respuesta para cumplir con SLA de resolución de incidentes en menos de 1 minuto
- Capacidad de filtrado de contenido web para usuarios menores de edad
- Facilidad de administración de múltiples redes con diferentes niveles de exigencia y criticidad.

"Sobre cada una de las locaciones de los juegos olímpicos nosotros armamos diferentes soluciones de red, todas apoyadas con equipo de Fortinet para garantizar la disponibilidad, el desempeño y la seguridad de la información."

– Gustavo Linares

Entonces, además de crear un Comité Federal de Seguridad con la inclusión de diferentes organismos de seguridad de Argentina e INTERPOL, el equipo creó múltiples hipótesis de conflicto y desarrolló la resolución para cada escenario en base a la tecnología de seguridad informática que desplegaron con Fortinet. Se armaron aproximadamente 60 escenarios, algunos basados en la experiencia de otros juegos olímpicos, otros basados en experiencia de gobierno y en la imaginación. Eso ayudó a lograr una detección y una resolución rápida. Por ejemplo, se encontraron cinco dominios falsos similares a los de los juegos, creados con la intención de generar estafas por phishing y fueron eliminados.

> *"Estamos sumamente satisfechos con los resultados logrados, fueron 12 días de actividades con la participación récord para el COI de 1 millón de espectadores, y no tuvimos ningún incidente de ciberseguridad."*
>
> *– Gustavo Linares*

Disponibilidad a prueba de las más altas exigencias

"Estamos sumamente satisfechos con los resultados logrados, fueron 12 días de actividades con la participación récord para el COI de 1 millón de espectadores, y no tuvimos ningún incidente de ciberseguridad. Logramos prevenir, detectar y mitigar cualquier intento sin perjuicio de la disponibilidad ni el desempeño de las redes. En lo que tiene que ver con la administración, si bien teníamos más de 40 firewalls FortiGate de distintas capacidades en funcionamiento, no tuvimos ningún problema con los equipos. Implementamos el paquete completo de seguridad de parte de Fortinet", dijo Linares.

Toda la infraestructura de seguridad de core perimetral de la red del Gobierno de la Ciudad de Buenos Aires es de Fortinet, por lo que implementar Fortinet en los Juegos Olímpicos de la Juventud no fue una novedad para ellos. El conocimiento de las capacidades de las herramientas y su administración hizo que todo fuera mucho más sencillo. Además, Fortinet ofreció la plataforma que mejor se adaptaba a la necesidad de interconectar con alta disponibilidad y desempeño cada una de las locaciones a un centro de datos central y asegurar desde el core hacia toda la plataforma de los juegos.

"Nosotros hicimos un esfuerzo gigante en la prevención, el análisis, la investigación y en la creación de un Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT) específico para los juegos. Generar escenarios de conflicto conocidos o los que se puedan imaginar para probar la infraestructura de seguridad y estar verdaderamente preparados es clave. También lo es la capacidad de operación durante el evento, saber cómo hacerlo de manera rápida y eficiente. Este conocimiento previo, combinado con el socio tecnológico adecuado, nos permitió detectar incidentes que ya teníamos mapeados, conocer la solución e implementarla rápidamente para mitigar los riesgos a la ciberseguridad", concluyó Linares.

FORTINET®

www.fortinet.com