Trabajo practico integrador
Counter-Trique II Cup Argentina
Mariano Cavallo sassi
mariano.cavallosassi@gmail.com

1. Resumen ejecutivo

Este evento propone una competencia de eSports de alto nivel, en la cual varios equipos deben participar en partidas de videojuegos simultáneas.
La naturaleza de la competencia exige que se ponga un énfasis en la disponibilidad para que la continuidad del torneo no sea afectada, porque cualquier interrupción en las partidas simultáneas comprometería la integridad de la competencia.
Otro aspecto a tener en cuenta en las partidas es la precisión, un tiempo de respuesta mínimo, donde las milésimas de segundo pueden determinar el resultado de una partida.
Esto requiere una infraestructura de red robusta, servidores de juego dedicados de alto rendimiento y una gestión de ancho de banda impecable para asegurar que la experiencia competitiva sea justa y responda instantáneamente a las acciones de los jugadores.
Además de los requisitos técnicos operativos, dado que se trata de un evento de gran prestigio con patrocinios, es necesario establecer un riguroso enfoque en la seguridad, para que no ocurra ningún imprevisto, y también en la seguridad de los jugadores, esto abarca la protección contra *cheating*, ataques de denegación de servicio, *hacking* a cuentas de jugadores o servidores de juego, y prevención de *stream sniping*. Se deben implementar mecanismos de ciberseguridad y contar con un equipo de árbitros y técnicos dedicados a monitorear la integridad de la competición en tiempo real.
y por último un enfoque en el rendimiento, garantizar que todo el *hardware* (ordenadores, periféricos, monitores) y el *software* de juego funcione consistentemente a sus máximas capacidades para ofrecer una experiencia fluida y sin contratiempos, permitiendo a los competidores no tengan limitaciones técnicas.
Se brindará conectividad WiFi al público presencial para que se logre una exposición del evento en internet y crezca.
Teniendo en cuenta estas consideraciones podremos armar un torneo donde la calidad y el profesionalismo sea lo primordial.

2. Características principales del diseño

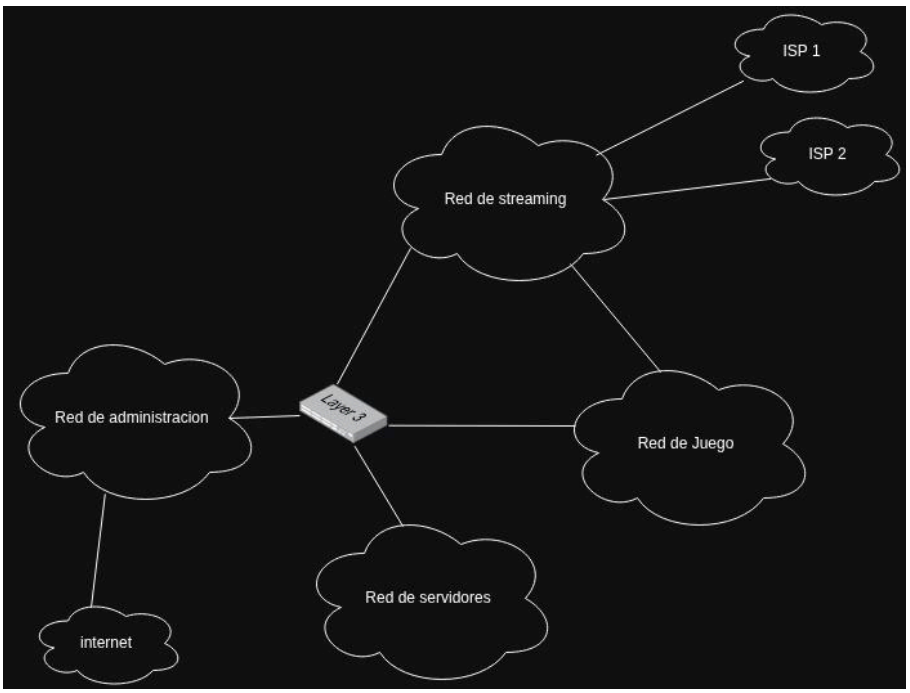
El diseño propuesto se basa en 3 zonas interconectadas entre sí,

En la red de juego podemos encontrarnos con el switch de capa 3 principal del cual se conectan a 2 switches para los equipos y en estos se van a separar en 4 equipos por switch y serán separados en una VLAN por equipo y otra para los equipos de VoIP.
contaremos con otro switch capa 3 troncal en el cual se conecta una red de servidores y otra red de administración que será clave a la hora de configurar o modificar alguna característica de los equipos en la red, se dispondrá también de conexión Wi-Fi, lo que permitirá al equipo técnico gestionar el evento sin necesidad de una conexión por cable y la posibilidad de los espectadores a conectarse a internet.
Para garantizar la máxima seguridad, se establecerá una VPN que permitirá a los patrocinadores del evento conectarse sin problemas para llevar a cabo sus tareas promocionales y además se implementa un firewall para que no puedan ocurrir accidentes y generar un control de acceso.
Por último la red de streaming, donde se procesa y emite el video tanto de las partidas como el de las 13 cámaras ip del evento.
Contarán con 2 routers de borde y cada uno implementa un firewall, tienen diferentes contrataciones de ISP obteniendo redundancia, por si cualquiera de estos enlaces falla tener uno de repuesto y poder seguir con la transmisión de streaming, estas contrataciones vienen con características de QoS que le darán máxima prioridad a los paquetes enviados del streaming para que el espectador pueda tener una experiencia fluida.

3. Topología de alto nivel

La arquitectura general de la red se basa en cuatro sectores, red de administración, red de streaming, red de juego y la red de servidores.

Topología de alto nivel de abstracción:



Las interconexiones entre todos los equipos físicos dentro del establecimiento se harán a través de cables de cobre UTP, para las conexiones con los ISPs se utilizará fibra óptica.

Para garantizar una experiencia de streaming fluida en 1080p a 60 fps, cada host de transmisión requiere un ancho de banda mínimo de 10 Mbps.

Dado que hay 5 hosts realizando streaming, la tasa mínima de ancho de banda requerida aumenta a 50 Mbps (5 hosts * 10 Mbps/host).

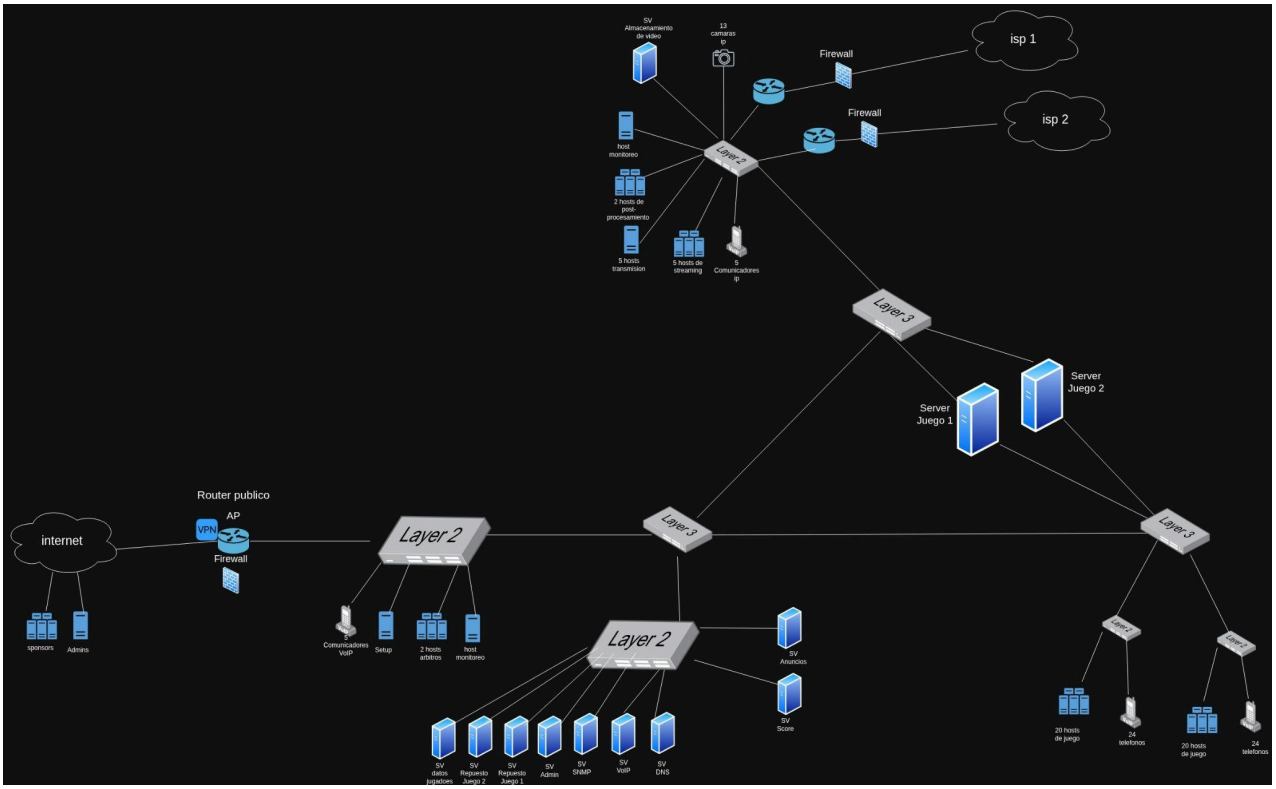
Aplicando un margen de seguridad del 20%, el ancho de banda total necesario se establece en 60 Mbps (50 Mbps * 1.20).

Respecto a los SLA con los ISP se pedirá
-Ancho de banda mínimo de 60 Mbps
- Disponibilidad de enlace: > 99,5 %
- Latencia promedio : <= 100 ms
- Pérdida de paquetes: < 1 %
- Jitter: < 20 ms

QoS:
En los routers de borde se dará máxima prioridad a los paquetes que sean de streaming.

4. Topología física

Topología de bajo nivel de abstracción:



(Adjunto imagen para mejor visualización)

Switch juego:
cuenta con 5 interfaces:
eth0: Enlace con el Switch de administración cuenta con la ip 192.168.1.1
eth1: Enlace con el servidor de juego N1 cuenta con la ip 10.99.0.100
eth2: Enlace con el servidor de juego N2 cuenta con la ip 10.99.0.101
eth3: Enlace con los equipos número 1, 2, 3 y 4, cuentan con varias interfaces virtuales con las ip 10.0.1.100, 10.0.2.100, 10.0.3.100, 10.0.4.100.
eth4: Enlace con los equipos número 5, 6, 7 y 8, cuentan con varias interfaces virtuales con las ip 10.0.5.100, 10.0.6.100, 10.0.7.100, 10.0.8.100.

Direccionamiento de los equipos de juego:

- **Formato de IP:** `10.0.N.0 /24`
- **Asignación de VLAN:** Cada equipo pertenece a la VLAN `N0`.
    - Donde **N** es el número del equipo.

Ejemplo:

- **Red Equipo 1:** IP `10.0.1.0 /24`, perteneciente a la **VLAN 10**.

Direccionamiento de los equipos de VoIP:

- **Formato de IP:** `10.1.N.0 /24`
- **Asignación de VLAN:** Cada equipo pertenece a la VLAN `NN`.
    - Donde **N** es el número del equipo.

Ejemplo:

- **Red VoIP Equipo 1:** IP `10.1.1.0 /24`, perteneciente a la **VLAN 11**.

Para los comunicadores VoIP del equipo de streaming se generan las direcciones como si fueran el equipo 9 y lo mismo ocurre con los comunicadores de la red de administración, perteneciendo al equipo 10, pero en una VLAN combinada 90.

Ejemplo:

- **Red VoIP streaming :** IP `10.1.10.0 /24`, perteneciente a la **VLAN 90**.

Switch admin:
Contará con cuatro interfaces, dos de ellas son de conexiones punto a punto con otros switches y las otras dos, una se conecta al switch de los servidores y la otra al switch de administración.

En el switch de servidores estos se dividen en dos VLAN una para los servidores privados y otra para los que el público pueda acceder.

Direccionamiento de los servidores privados:

- **Formato IP:** `10.99.1.0 /24`
- **Asignación de VLAN:** VLAN `98`

Direccionamiento de los servidores públicos:

- **Formato IP:** `10.99.2.0 /24`
- **Asignación de VLAN:** VLAN `99`

Router público:
Router que funciona como AP que implementa un firewall.

Aquí es donde se conecta el público para navegar a internet y también ver los servidores de score y anuncios.
Los sponsors y Admins también se pueden conectar al él mediante una VPN.
para los usuarios conectados al AP dispondrán de las direcciones de la red: `10.4.0.0 /16`

Switch de Streaming:
Este router se encarga de la conectividad con los servidores del juego y, a su vez, con un switch al que está conectado todo el equipo necesario para la transmisión en vivo del evento.

El switch de streaming cuenta con doble redundancia de enlace, conectándose a dos Proveedores de Servicios de Internet (ISPs) diferentes. Esto asegura la continuidad de la transmisión en caso de que uno de los enlaces falle.

Direccionamiento de los equipos de streaming:

- **Formato de IP:** `10.2.0.0 /24`
- **Asignación de VLAN:** VLAN `200`.

Ejemplo:

- **Host streaming 1:** IP `10.2.0.1 /24`, perteneciente a la **VLAN 200**

Direccionamiento de los equipos de administración:

- **Formato de IP:** `10.3.0.0 /24`
- **Asignación de VLAN:** VLAN `300`.

Ejemplo:

- **host admin 1:** IP `10.3.0.1 /24`, perteneciente a la **VLAN 300**

Direccionamiento de los equipos de administración remoto:

- **Formato de IP:** `10.4.0.0 /24`
- **Asignación de VLAN:** VLAN `400`.

Ejemplo:

- **host admin remoto 1:** IP `10.4.0.1 /24`, perteneciente a la **VLAN 400**

Direccionamiento de los equipos de sponsor:

- **Formato de IP:** `10.5.0.0 /24`

- **Asignación de VLAN:** VLAN `500`.

Ejemplo:

- **host sponsor 1:** IP `10.5.0.1 /24`, perteneciente a la **VLAN 500**

Direccionamiento de la audiencia (AP):

- **Formato de IP:** `10.6.0.0 /22`
- **Asignación de VLAN:** VLAN `600`.

Ejemplo:

- **host audiencia 1:** IP `10.6.8.1 /24`, perteneciente a la **VLAN 600**

Direccionamiento de los equipos de cámaras IP:

- **Formato de IP:** `10.7.0.0 /24`
- **Asignación de VLAN:** VLAN `700`.

Ejemplo:

- **Red Camaras:** IP `10.10.0.0 /24`, perteneciente a la **VLAN 700**

Dispositivos físicos:
3 TP-Link TL-SG1048 - Switch de 48 puertos.
3 DGS-1210-10 switch capa 3 con 10 puertos.
58 comunicadores VoIP para todas las comunicaciones para los equipos, administradores y personal del streaming.

5. Ingeniería de tráfico

Red de Juego:

- **Flujo de datos principal:** Datos de Juego (partida)
- **Fuentes:** computadoras de la red de juego (todos los equipos)
- **Destino:** Servidores de juego
- **Tipo de comunicación:** cliente servidor
- **Tasa de transferencia requerida y estimada:**
  - 60 kbps por jugador
  - 300 kbps por equipo

- **Prioridad:** Máxima, tiene que estar por encima de cualquier otro flujo ya que cualquier retraso afectará al rendimiento de las partidas y jugadores.

Red de streaming:

- **Flujo de datos principal:** transmisión de video
- **Fuentes:** Camaras de video IP y equipo de streaming
- **Destino:** Servidores internos de almacenamiento y plataformas de streaming
- **Tipo de comunicación:** Comunicación multicast, la transmisión de video se distribuye a varios destinatarios simultáneamente
- **Tasa de transferencia requerida y estimada:**
    - 5 Mbps por cada cámara IP que transmita a 1080p 30 fps
    - 10 Mbps por host de streaming
    - 60 Mbps para los 5 host de streaming más un margen de seguridad
- **Prioridad:** Alta, al darle prioridad alta estamos mejorando la calidad de video y disponibilidad, para los espectadores que no estén presencialmente en el evento.

Red Operacional:

- **Flujo de datos principal:** Datos de control y monitoreo del evento
- **Fuentes:** host de monitoreo, setup, árbitros.
- **Destino:**servidor de administración, servidor de datos de jugadores, servidores de juego,servidores de score y anuncios.
- **Tipo de comunicación:** Cliente servidor.
- **Tasa de transferencia requerida y estimada:**
    - Tasa por operación(setup,control de partida,etc): 500 kbps a 2 Mbps
- **Prioridad:** Media, la latencia no es crítica para este flujo.

Sponsors:

- **Flujo de datos principal:** Datos de anuncios, promociones y actualizaciones
- **Fuentes:** Hosts conectados a través de la VPN en el Router de administración
- **Destino:** Servidores de anuncios, servidor de datos de jugadores.
- **Tipo de comunicación:** Cliente servidor
- **Tasa de transferencia requerida y estimada:**
    - Tasa por conexión: 100-500 kbps (actualizaciones de anuncios o análisis de audiencia).
- **Prioridad:** Baja, no es un flujo crítico así que le asignamos una baja prioridad.

Red VoIP:

- **Flujo de datos principal:** Chat de voz y comunicaciones de los jugadores

- **Fuentes:** Comunicadores VoIP de jugadores y del staff
- **Destino:**Equipos de voz de jugadores, equipos del staff y servidor VoIP
- **Tipo de comunicación:** Unicast
- **Tasa de transferencia requerida y estimada:**
    - Tasa por cada jugador: 100 kbps
    - tasa por equipo: 500 kbps
- **Prioridad:** Maxima, este flujo es de máxima importancia para la comunicación entre los equipos en las partidas, por esto mismo la latencia tiene que ser baja.

Monitoreo Continuo y Acceso Remoto

- **Flujo de datos principal:** Monitoreo de red y métricas de rendimiento
- **Fuente:** Estaciones de monitoreo,servidores de control
- **Destino:** Estaciones de trabajo de monitoreo
- **Tipo de comunicación:** Modelo Cliente-Servidor
- **Tasa de transferencia requerida y estimada:**
    - Tasa por estación de monitoreo: 1-10 Mbps (dependiendo de la cantidad de métricas que se recopilen).
    - Total para monitoreo continuo: ~10-50 Mbps.
- **Prioridad:** Media.

6. Administración y gestión de la red

Tecnologías de Monitoreo

Simple Network Management Protocol (SNMP): Se empleará para la recopilación de datos esenciales, tales como el estado operativo, contadores de tráfico, métricas de utilización de CPU y memoria, y el estado de las interfaces de todos los equipos activos en la red (incluyendo Routers, Switches, Puntos de Acceso y Servidores).

NetFlow/sFlow: Se habilitará en los Routers y Switches Capa 3 para obtener datos detallados sobre los flujos de tráfico (origen, destino, puertos, protocolos), esencial para detectar anomalías y realizar análisis de ingeniería de tráfico.

Syslog: Se configurará en todos los dispositivos activos para enviar mensajes de eventos y logs al servidor de monitoreo, lo que facilita la auditoría y la detección temprana de fallos de hardware o configuraciones.

ICMP: Se utilizará para la verificación básica de la disponibilidad (latencia) de los hosts y dispositivos principales, especialmente en la Red de Juego y la Red de Voz.

Dispositivos a Monitorear Activamente y Características Observadas

Routers/Firewalls de Borde (ISP 1/2)

- **tecnologías:** SNMP, Syslog, NetFlow
- **Características a observar:** Disponibilidad (Uptime) , Estado de Enlaces (Up/Down) , Utilización del Ancho de Banda (QoS y Consumo Total), Errores de Seguridad (Intentos de acceso/Denegaciones del Firewall).

Switches Capa 3

- **Tecnologías:** SNMP,Syslog,NetFlow
- **Características observadas:** Estado de Interfaz , Uso de CPU/Memoria (crítico para la capacidad de enrutamiento), Estadísticas de Tráfico (detección de congestión/broadcasts).

Switches Capa 2 (Juego/Producción/admin)

- **Tecnologias:** SNMP, Syslog
- **Características a observar:** Estado de Puertos (PoE), Errores/Drops por Interfaz (crítico para la Red de Juego), Uso de CPU, Estado de la Fuente de Alimentación (para redundancia).

Servidores de Juego y equipos de juegos (PC)

- **Tecnologias:** SNMP, ICMP
- **Características a observar:** Latencia (Ping/Jitter), Uso de CPU/Memoria (performance del juego), Uso de Disco, Proceso del Servidor de Juego (estado).

Servidores de Producción y equipos streaming (Almacenamiento de video, Streaming, Post-Prod)

- **Tecnologias:**SNMP, Syslog
- **Características a observar:** Tasa de Transferencia de Disco (Escritura/Lectura Sostenida), Uso de CPU/Memoria (para *encoding*), Disponibilidad de Servicios (HTTP, RTMP).

Puntos de Acceso (APs)

- **Tecnologías:** SNMP

- **Características a observar:** Carga de Clientes, Calidad de Señal/Interferencia, Errores de autenticación.

Alertas Automatizadas para Tratamiento de Incidentes

El sistema de monitoreo debe configurarse para generar y enviar alertas automáticas, por correo electrónico y mensajes SMS, al personal técnico en caso de que se sobrepasen los siguientes umbrales críticos:

Red de Juego

- **Alerta Crítica:** La **latencia** hacia los Servidores de Juego excede los **100 ms**, ya que este nivel interrumpe la fluidez de la experiencia de juego.
- **Alerta:** Se detecta una alta tasa de errores o pérdidas de paquetes (*drops*) en las interfaces de los *switches* de juego.

Red de Producción

- **Alerta:** Se identifica la caída del proceso de *streaming* o fallas de conexión con plataformas como Twitch o YouTube.

Red e Infraestructura General

- **Alerta Crítica:** Se produce la **caída de un Enlace Principal** o la **falla de cualquier componente redundante** (como una fuente de poder).
- **Alerta:** El uso de CPU en cualquier Router o Switch es superior al **85%.**

7. Seguridad en redes de datos

Herramientas de Protección de Confidencialidad e Integridad del Tráfico de Red

Para salvaguardar la confidencialidad e integridad del tráfico de red, se implementarán las siguientes herramientas y protocolos:

Cifrado de Tráfico (Confidencialidad)

Acceso remoto de los sponsors y administradores

- **herramienta:** OpenVPN, y garantizamos que el tráfico que viaja por internet sea confidencial.

Servidores Web/Anuncios

- **Herramienta:** TLS/HTTPS, protege las comunicaciones entre los clientes (público/patrocinadores) y los servidores de score y anuncios públicos, impidiendo la intercepción de credenciales o datos sensibles.

Administración de dispositivos

- **Herramienta:** SSH/HTTPS, asegurar las sesiones de administración remota de Routers y Switches.

Mecanismos de Integridad (Anti-Manipulación)

Firewalls aplicados en los routers de borde, monitoreando el estado de las conexiones para asegurar que solo el tráfico legítimo y esperado pueda fluir, bloqueando paquetes anómalos.

IDS/IPS aplicados tanto en la red de juego como en la de servidores, para el monitoreo del tráfico en tiempo real, identificar y bloquear patrones de ataques conocidos, incluyendo intentos de inyección, DDoS o cheating mediante la manipulación de red.

Gestión de las Herramientas de Protección

La gestión efectiva de estas herramientas es crucial para mantener un entorno seguro y de alto rendimiento.

Gestión de VPN y Cifrado

1. **Generación y Rotación de Claves:** Implementar una política estricta para la generación, almacenamiento y rotación periódica de claves de cifrado (para IPsec y TLS) para minimizar el riesgo de compromiso de claves a largo plazo.
2. **Certificados:** Usar una infraestructura de clave pública (PKI) interna para gestionar certificados TLS en servidores, asegurando que sólo los hosts autorizados puedan establecer comunicaciones cifradas.
3. **Control de Acceso VPN:** Mantener una whitelist de IPs y credenciales para los administradores y patrocinadores que acceden a través de la VPN, aplicando autenticación de dos factores (2FA) si es posible.

Gestión de Firewalls y IDS/IPS

1. **Políticas de Mínimo Privilegio:** Configurar los Firewalls (tanto en el borde como el interno del Router público) con políticas de denegación por defecto, permitiendo únicamente el tráfico estrictamente necesario.
2. **Actualización de Firmas:** Asegurar que el sistema IDS/IPS se actualice diariamente con las últimas firmas de amenazas para proteger contra vulnerabilidades y técnicas de ataque recientes.
3. **Revisión de Logs:** Integrar los logs de Firewalls e IDS/IPS con el sistema Syslog centralizado para la monitorización continua. Las reglas de alerta críticas deben estar enfocadas en intentos de DDoS, port scanning o hacking a los servidores de juego.

Switches y Routers

1. **Desactivación de Servicios Innecesarios:** Deshabilitar cualquier servicio de red no esencial (ej. Telnet, HTTP) en todos los dispositivos para reducir la superficie de ataque.

2. **VLANs Separadas:** Mantener la estricta separación de tráfico mediante VLANs para evitar que un compromiso en la red de invitados afecte a la red de juego o la red de administración.

Tabla firewall borde 1 y 2

Cadena	IP origen	IP destino	Protocolo	Port orig	Port dest	Acción	Comentario
Forward	desde 10.2.0.1 hasta 10.2.0.5	*	TCP	*	443	ACCEPT	streaming hacía web
Forward	*	desde 10.2.0.1 hasta 10.2.0.5	TCP	443	*	ACCEPT	respuesta del streaming
output	10.2.0.100	10.3.0.10	TCP	22	*	ACCEPT	ssh respuesta
input	10.3.0.10	10.2.0.100	TCP	*	22	ACCEPT	ssh ida
input	*	10.2.0.100	TCP	*	22	REJECT	ssh bloqueo
*	10.3.0.10	10.2.0.100	ICMP	*	*	ACCEPT	Acepta ICMP
*	*	*	*	*	*	DROP	Política por

							defecto

Tabla firewall Admin

Cadena	IP origen	IP destino	Protocolo	Port orig	Port dest	Acción	Comentario
Forward	desde 10.4.0.1 hasta 10.4.0.100	10.99.1.1 y 10.99.2.1	TCP	443	*	ACCEPT	server datos jugadores y anuncios (sponsors)
Forward	10.99.1.1 y 10.99.2.1	desde 10.4.0.1 hasta 10.4.0.100	TCP	*	443	ACCEPT	server datos jugadores y anuncios (sponsors)
Forward	desde 10.5.0.1 hasta 10.5.0.100	10.3.0.10	TCP	22	*	ACCEPT	host de monitoreo y config
Forward	10.3.0.10	desde 10.5.0.1 hasta 10.5.0.100	TCP	*	22	ACCEPT	host de monitoreo y config
Forward	desde 10.6.0.1 hasta 10.6.2.254	10.99.2.1 y 10.99.2.2	TCP	443	*	ACCEPT	server anuncios y score (audiencia)
Forward	10.99.2.1 y 10.99.2.2	desde 10.6.0.1 hasta 10.6.2.254	TCP	*	443	ACCEPT	server anuncios y score (audiencia)
output	10.3.0.100	10.3.0.10	TCP	22	*	ACCEPT	ssh

							respuesta
input	10.3.0.10	10.3.0.100	TCP	*	22	ACCEPT	ssh ida
input	*	10.3.0.100	TCP	*	22	REJECT	ssh bloqueo
*	10.3.0.10	10.3.0.100	ICMP	*	*	ACCEPT	Acepta ICMP
*	*	*	*	*	*	DROP	Política por defecto