

CIB201-198-223081-ONL-SEGURIDAD DE CABLEADO Y DATACENTER

Semana 4

Jonathan Joel Salinas Santibañez

Índice

[Introducción 4](#_Toc46485953)

[Desarrollo 5](#_Toc46485954)

[Conclusión 6](#_Toc46485955)

[Bibliografía 7](#_Toc46485956)

# Introducción

La modernización y optimización de los datacenters son cuestiones de suma importancia para las organizaciones que desean mejorar su funcionamiento, proteger su información y garantizar la disponibilidad de servicios críticos. En el contexto de la sede de AIEP en La Serena, se ha identificado la necesidad de renovar su datacenter actual. Esta iniciativa no solo busca implementar un modelo de eficiencia, sino también reforzar la seguridad de la red mediante la adopción de un Firewall UTM (Gestión Unificada de Amenazas).

Se pretende instruir al personal que no esté familiarizado con la nueva implementación de seguridad. Este informe tiene como objetivo explorar las ventajas del modelo de eficiencia propuesto, comparar el Firewall UTM con un firewall convencional y presentar una prueba de concepto (PoC) para demostrar cómo bloquear el puerto SSH en un sistema CentOS 7. De esta manera, se busca brindar una comprensión detallada sobre la importancia de estas mejoras tecnológicas en el contexto del datacenter de AIEP en La Serena.

# Desarrollo

Ventajas del Modelo de Eficiencia Propuesto:

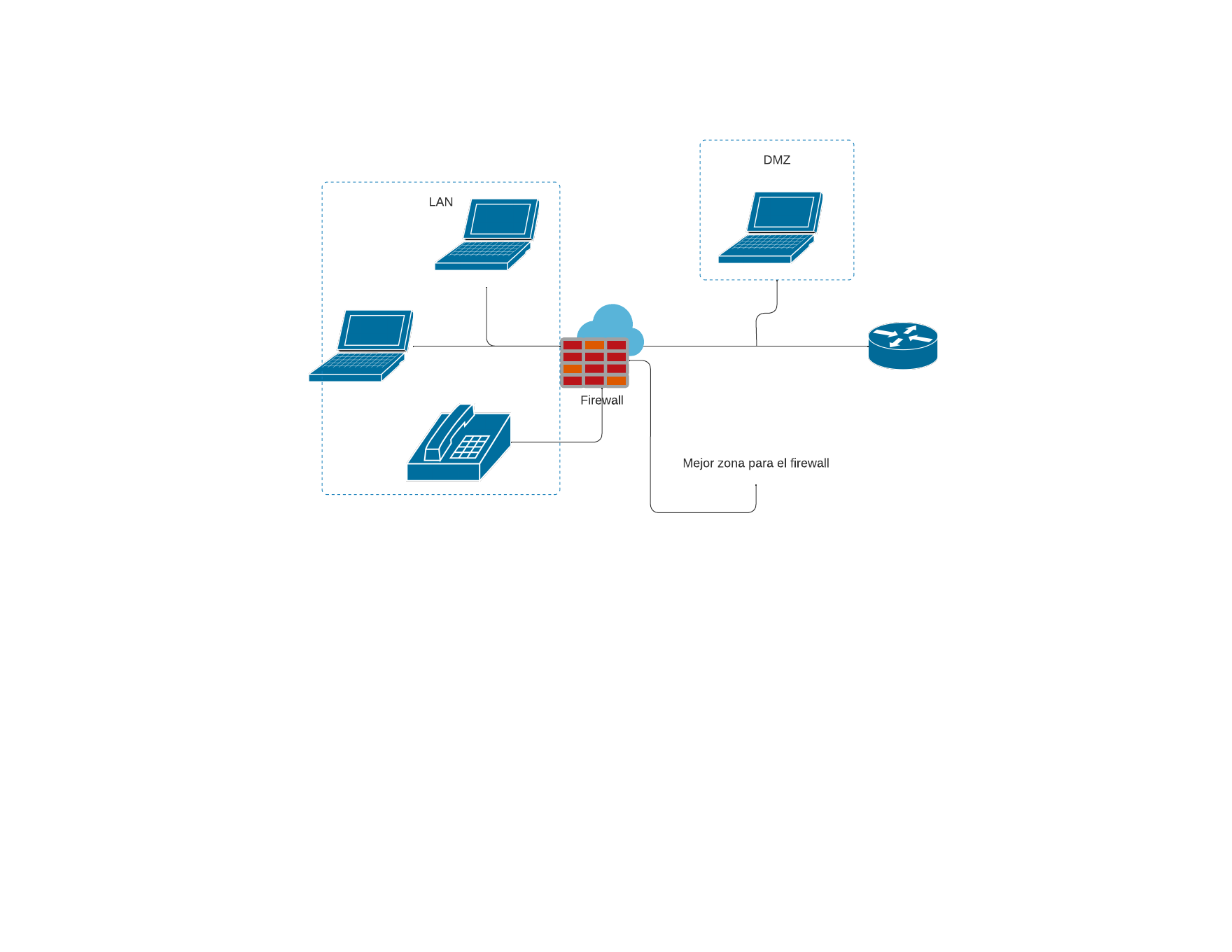
La renovación del datacenter de AIEP sede La Serena conlleva múltiples ventajas. En primer lugar, la eficiencia operativa mejorada permitirá una utilización más efectiva de los recursos de hardware y software. Esto se traduce en un rendimiento superior de las aplicaciones y servicios alojados en el datacenter, lo que mejora la experiencia del usuario y la productividad general. Además, la eficiencia conlleva un ahorro significativo en costos operativos y de energía, lo que es beneficioso tanto para el presupuesto de la institución como para el medio ambiente.

La redundancia y la alta disponibilidad, típicas de los modelos de eficiencia, reducen el tiempo de inactividad no planificado, lo que garantiza una mayor disponibilidad de los servicios esenciales. La incorporación de un Firewall UTM en este proceso de renovación también añade una capa de seguridad esencial. Esta solución unificada de gestión de amenazas ofrece una amplia gama de funcionalidades de seguridad, incluyendo filtrado de contenido, detección de intrusiones y antivirus, lo que fortalece la postura de seguridad de la red y minimiza las amenazas cibernéticas.

Ventajas del Firewall UTM vs. Firewall Convencional:

El Firewall UTM se destaca en comparación con un firewall convencional debido a su enfoque integral de seguridad. Al consolidar múltiples funciones de seguridad en un solo dispositivo, se simplifica la administración y se reduce la complejidad de la infraestructura de seguridad. Esto se traduce en una mayor facilidad de gestión y en la capacidad de responder más eficazmente a las amenazas en tiempo real.

Además, la amplitud de las capacidades de seguridad de un UTM permite una mayor detección y bloqueo de amenazas, mejorando la seguridad general de la red. Con el monitoreo en tiempo real y la generación de informes detallados, los administradores pueden tomar decisiones informadas y responder proactivamente a los riesgos cibernéticos.



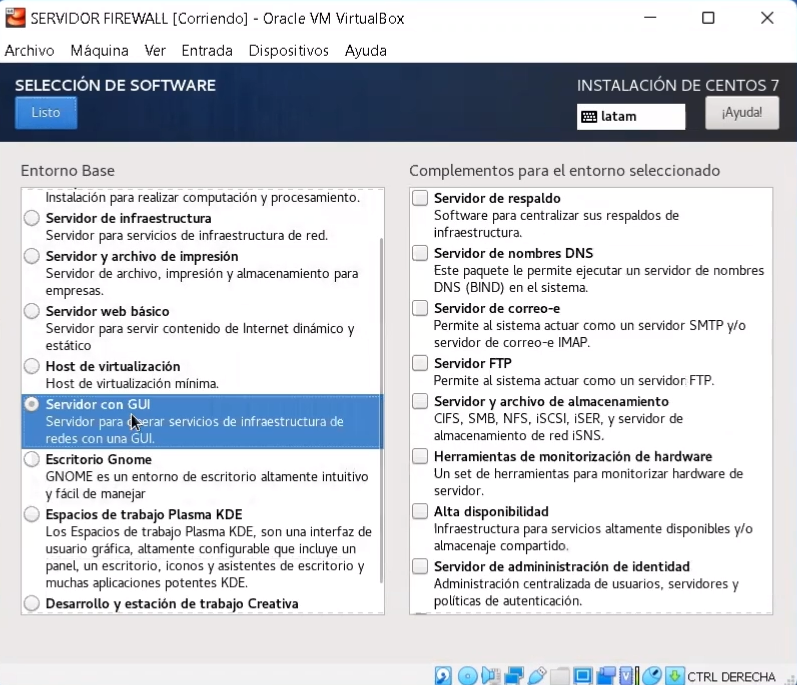
Prueba de Concepto para Bloquear el Puerto SSH:

Para ilustrar la implementación de una PoC, se proporciona un ejemplo evidenciado por capturas de pantalla de cómo bloquear el puerto SSH en un sistema CentOS 7 utilizando el firewall iptables. Se debe tener en cuenta que cualquier modificación en las reglas de seguridad debe realizarse con precaución y con un plan de recuperación en su lugar. Además, se deben ajustar las reglas de acuerdo con las necesidades y políticas de seguridad específicas de la organización.

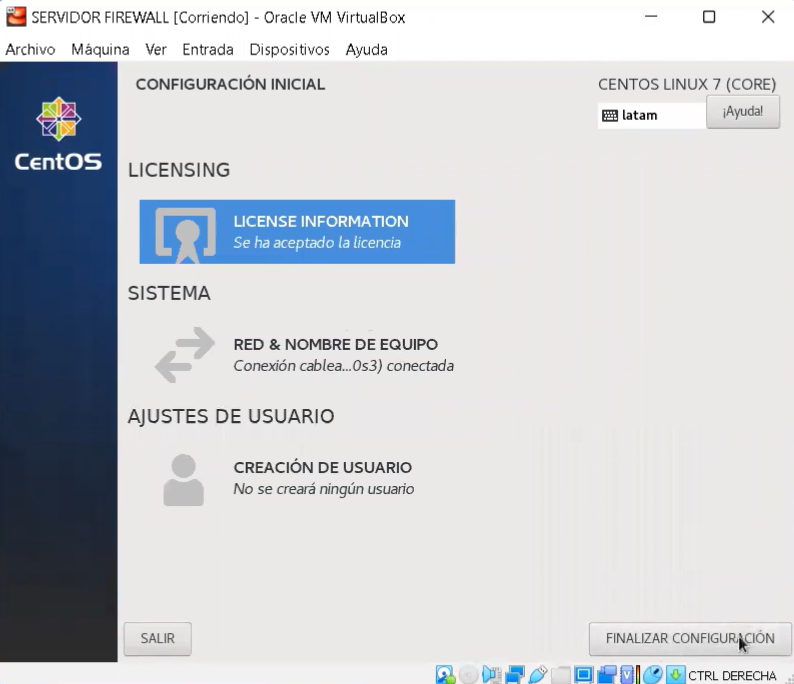
Debemos descargar la imagen iso de Centos 7 desde el siguiente link.

[Download (centos.org)](https://www.centos.org/download/)

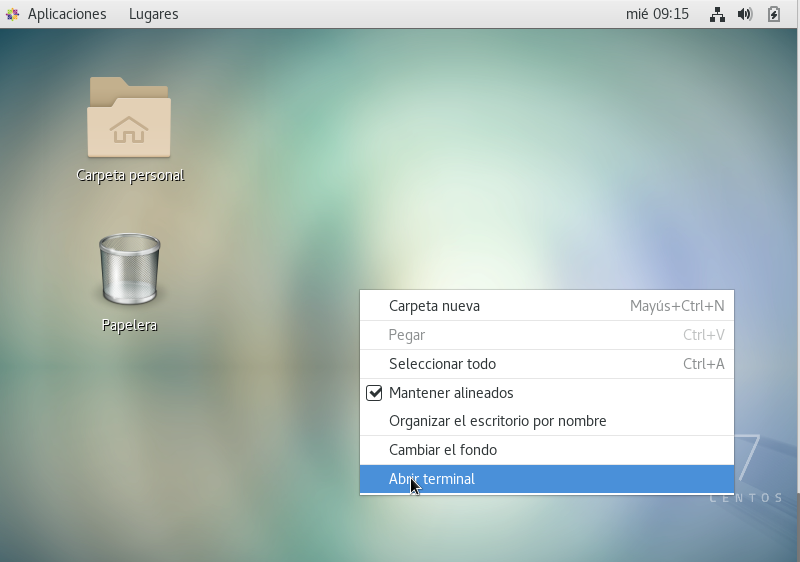
Debemos configurar una máquina virtual para nuestro nuevo sistema importante seleccionar la configuración GUI para poder trabajar con una interfaz gráfica.



Ahora solo hay que hacer click en finalizar configuración.



Abrimos una terminal haciendo click derecho sobre el escritorio y haciendo click en abrir terminal.



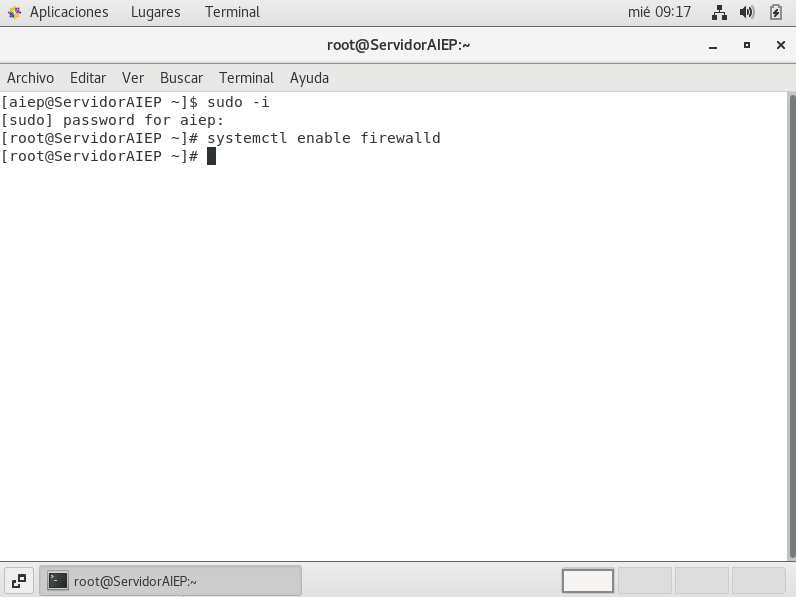
Primero debemos elevar privilegios con el siguiente comando:

Sudo -i



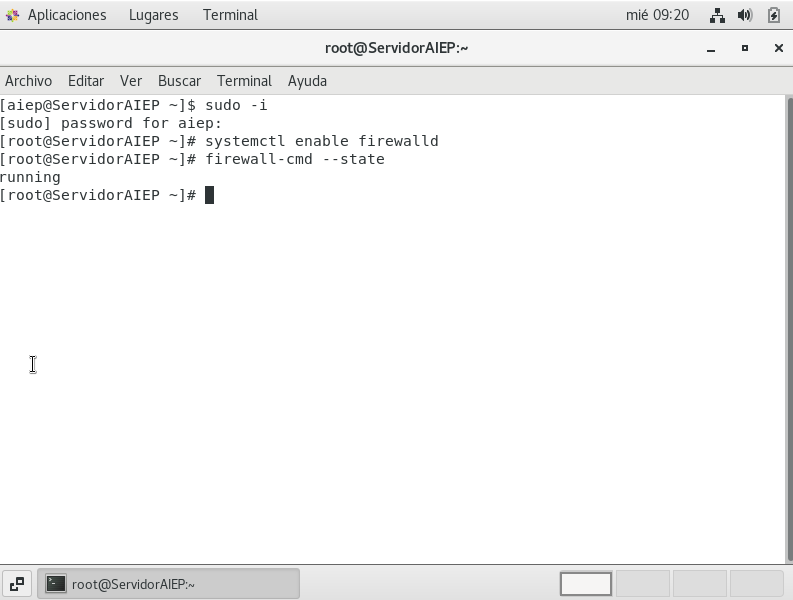
Debemos habilitar el firewall con el siguiente comando:

systemctl enable firewalld



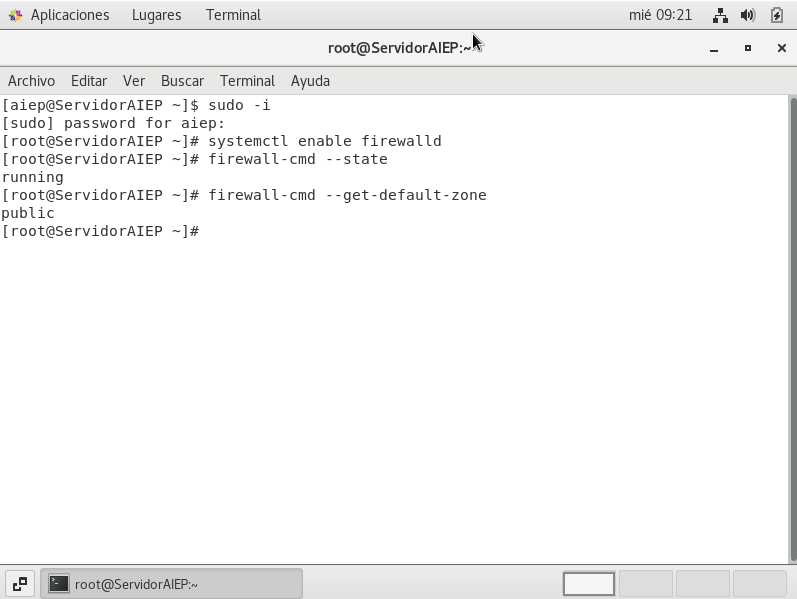
Podemos verificar si el firewall se encuentra corriendo con el siguiente comando:

firewall-cmd --state



Podemos verificar la zona actual con el siguiente comando:

firewall-cmd --get-default-zone



Podemos conocer las reglas que estan asociadas a la zona:

firewall-cmd --list-all

Podemos conocer el nombre del servicio con el siguiente comando:

firewall-cmd --get-services

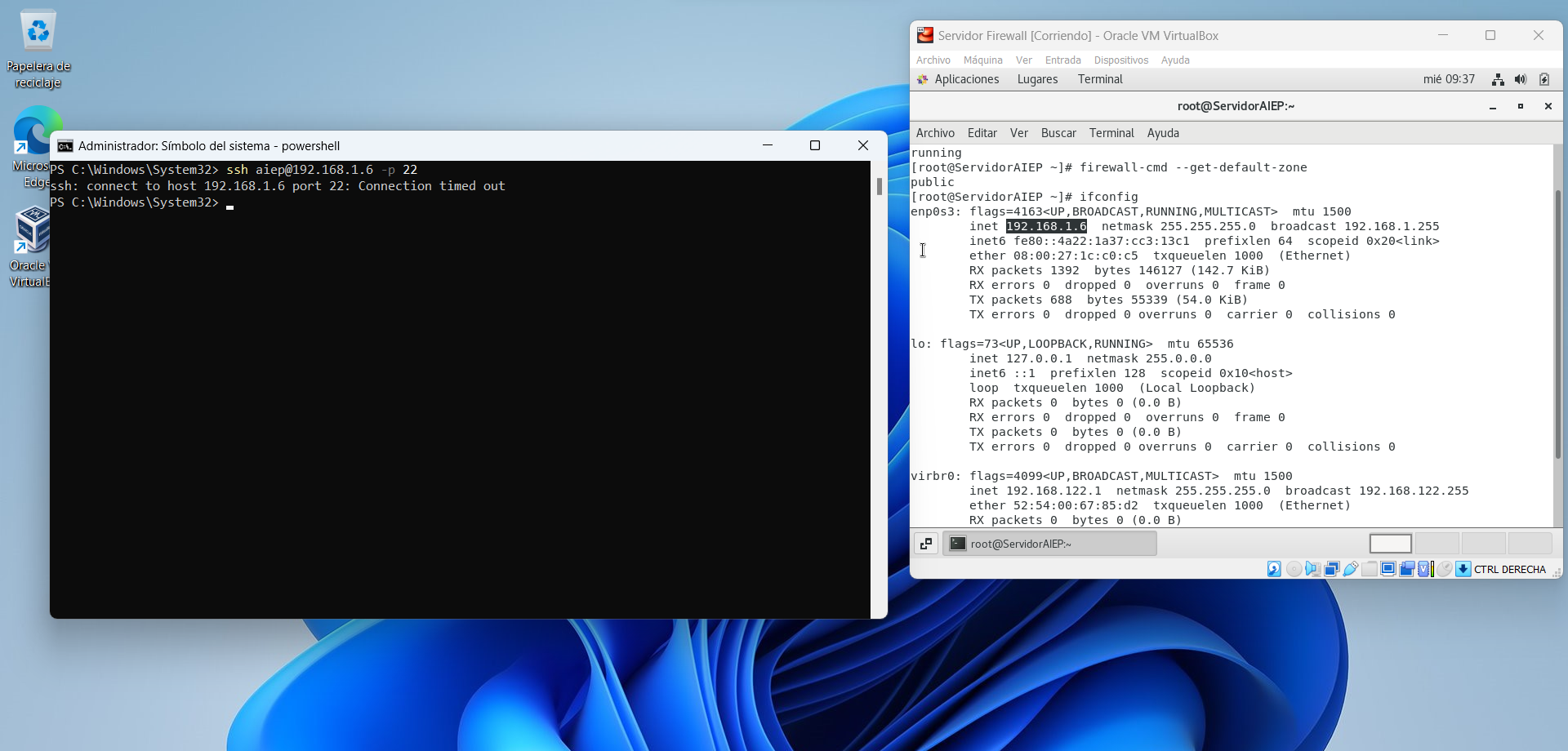
Podemos eliminar un servicio como por ejemplo en este caso ssh con el siguiente comando:

firewall-cmd --zone=public --remove-service=ssh --permanet

Podemos guardar con el siguiente comando:

firewall-cmd --reload

Para verificar si efectivamente no tenemos conectividad con Centos 7 intentamos establecer conexión por ssh



# Conclusión

La renovación del datacenter de AIEP sede La Serena conlleva una serie de ventajas significativas, que van desde la mejora en la eficiencia operativa hasta el fortalecimiento de la seguridad de la red. La implementación de un modelo de eficiencia permitirá un uso más efectivo de los recursos y una reducción en los costos operativos, al tiempo que garantiza una mayor disponibilidad de servicios. La adopción de un Firewall UTM ofrece una solución de seguridad integral que simplifica la administración y mejora la capacidad de detección y respuesta ante amenazas cibernéticas.

Es fundamental que el personal del datacenter se capacite y se familiarice con estas nuevas tecnologías y conceptos para aprovechar al máximo los beneficios que ofrecen. La PoC presentada demuestra cómo se puede aplicar un control de seguridad en un entorno CentOS 7, pero se debe proceder con precaución y con una comprensión completa de los riesgos asociados.

En resumen, la modernización del datacenter y la implementación de medidas de seguridad avanzadas son pasos esenciales para garantizar la eficiencia y la protección de los activos de TI en AIEP sede La Serena.

# Bibliografía

Información obtenida del material del modulo CIB201-198-223081-ONL-SEGURIDAD DE CABLEADO Y DATACENTER semana 4.