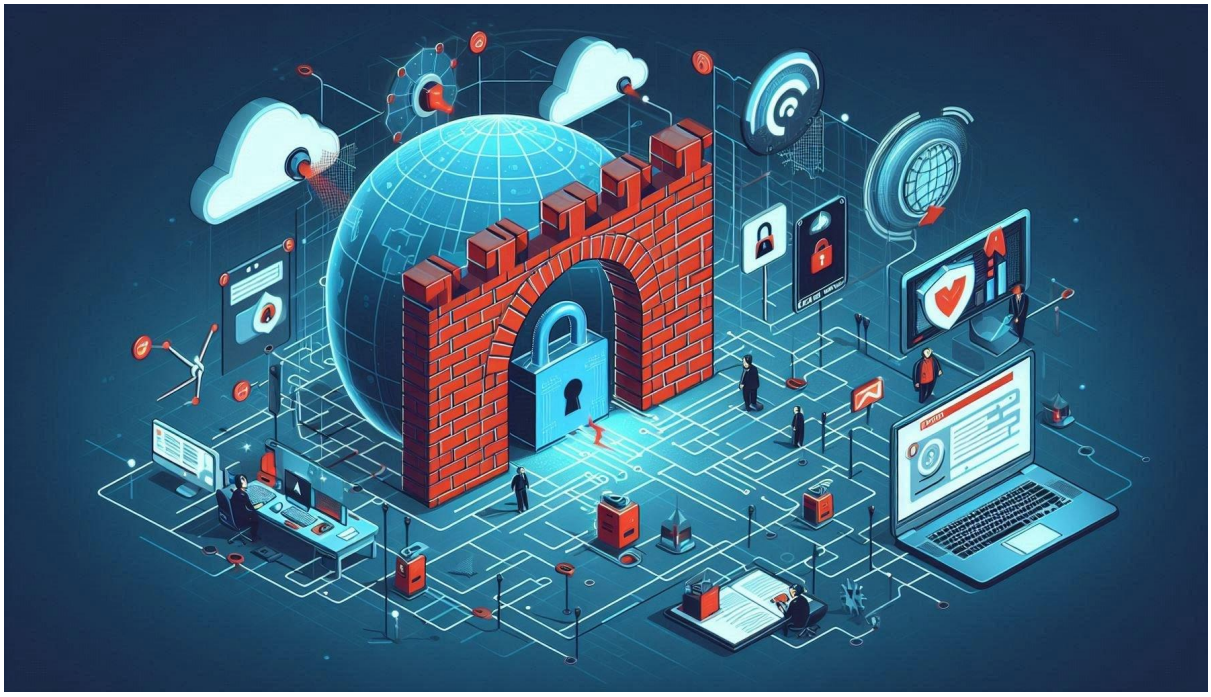
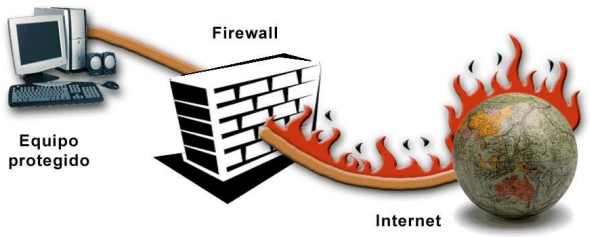


Firewalls

¿Qué es un Firewall?

Los datos fluyen dentro y fuera de los dispositivos a través de lo que llamamos puertos. Un firewall es lo que controla lo que -y lo más importante no- permite pasar a través de esos puertos. Se puede considerar como un guardia de seguridad de pie en la puerta, comprobando el id. de todo lo que intenta entrar o salir.

En la mayoría de los equipos normales o redes domésticas, el firewall debería permitir muy poco tráfico entrante, si procede. Rara vez hay motivos legítimos para que otros dispositivos tengan que conectarse a tu dispositivo o a la red doméstica, no solicitados.



¿Cómo funcionan los firewalls?

Un firewall decide qué tráfico de red se admite y qué tráfico se considera peligroso. Básicamente, separa el tráfico bueno del malo, o el seguro del no fiable. Sin embargo, antes de entrar en detalles, es útil entender la estructura de las redes basadas en la web.

Los firewalls tienen como objetivo proteger las redes privadas y los dispositivos de punto de conexión que se encuentran en ellas, conocidos como hosts de red. Los hosts de red son dispositivos que se "comunican" con otros hosts en la red. Envían y reciben tráfico entre las redes internas, además de enviar y recibir tráfico de redes externas.

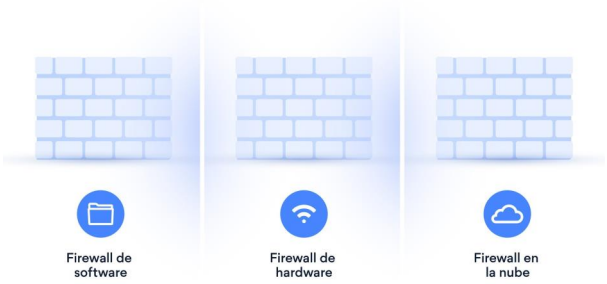
Las computadoras y otros dispositivos de punto de conexión utilizan redes para acceder a Internet y comunicarse entre ellos. Sin embargo, el Internet está segmentado en subredes por motivos de seguridad y privacidad. Los segmentos de subredes básicos son los siguientes:

1. Las **redes públicas externas**, que suelen referirse al Internet público o global, o a varias extranets.
2. Las **redes privadas internas**, que son redes domésticas, intranets de empresas y otras redes "cerradas".
3. Las **redes de perímetro**, que hacen referencia a las redes fronterizas compuestas por *hosts bastión*: computadoras host dedicadas con seguridad reforzada que están preparadas para soportar ataques externos. A modo de búfer asegurado entre redes internas y externas, estas también se pueden usar para alojar cualquier servicio orientado al exterior brindado por la red interna (por ejemplo, servidores para sitios web, correo electrónico, FTP, VoIP, etc.). Son más seguras que las redes externas pero menos seguras que las internas. *No siempre están presentes en las redes más simples, como las redes domésticas, pero se utilizan con frecuencia en las intranets de empresas o nacionales.*

¿Qué tipos de firewalls hay?

Existen firewall de hardware y de software. Además, según el método de filtración, pueden ser firewall proxy, firewall de inspección activa y firewall NGFW.

Los cortafuegos pueden clasificarse en dos categorías principales: los que se encuentran integrados en dispositivos específicos, conocidos como firewall de hardware, y aquellos que pueden instalarse en diversos dispositivos electrónicos, denominados firewall de software.

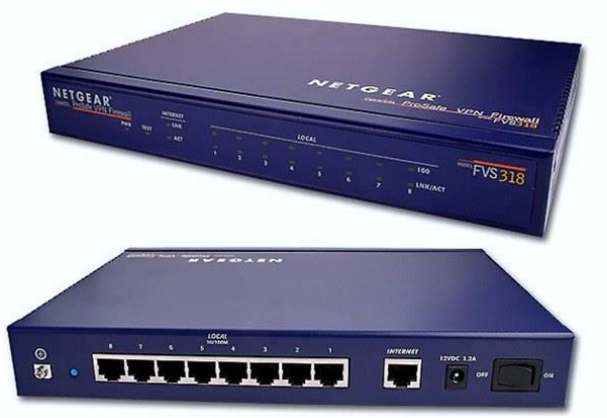


Firewall de hardware

El firewall de hardware se encuentra **instalado en un dispositivo**, por ejemplo un *router* o en algunos casos *Firewall* físicos dedicados, de manera que todos los ordenadores que se conecten a él están protegidos.

Esto es de suma utilidad si se necesita proteger múltiples dispositivos que deben interconectarse entre sí. La complejidad de estos sistemas varía, y en sistemas caseros, que nos brinda nuestro proveedor de internet, el Firewall se encuentra dentro de nuestro "Módem", y en la mayoría de los casos no necesita modificaciones para funcionar.

En sistemas más complejos como redes industriales o corporativas, pueden llegar a ser equipos muy robustos y costosos que requieren personal calificado para hacerlos funcionar, administrarlos y configurarlos.



Firewall de software

Este es el tipo de *firewall* que **viene incluido en el sistema operativo de un ordenador o que puede instalarse** posteriormente en uno, por lo que no protege a una red de ordenadores sino a un único dispositivo.

Es sumamente útil como complemento a un *firewall* de hardware, pues actúa como una segunda capa de protección en caso de que la primera falle, o un ataque provenga de otro

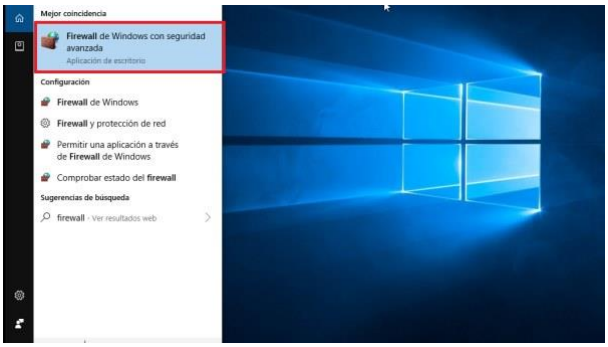
dispositivo, o incluso protege en algunos casos cuando nos conectamos a redes que no conocemos o no tenemos el control.

Configurar el firewall de Windows

Veamos dos de las diversas configuraciones de firewall que nos permite realizar Windows:

- Configurar el firewall de Windows para evitar contestar a peticiones de red de eco entrante. ¿Es posible realizar una configuración para cada puerto de red?
- Configurar el firewall para evitar que tu navegador web tenga acceso a Internet.

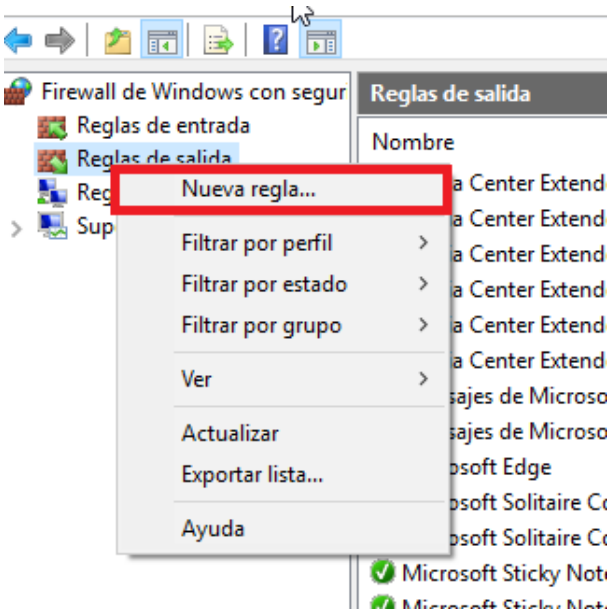
Para realizar estos apartados, debemos de dirigirnos a la configuración avanzada de firewall:



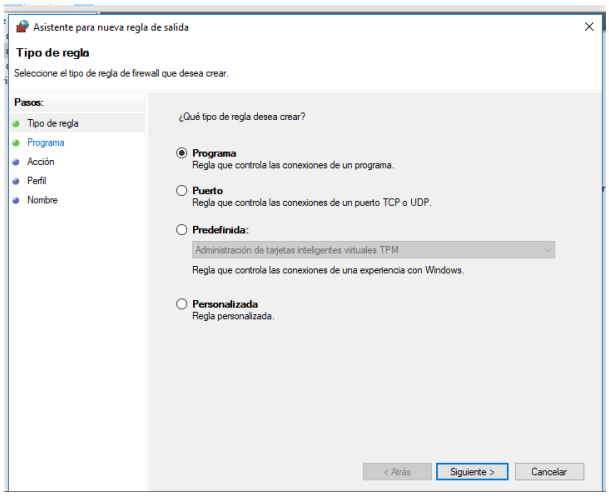
Configuración del firewall de Windows para evitar contestar a peticiones de red de eco entrante. ¿Es posible realizar una configuración para cada puerto de red?

Sí, ya sea como regla de entrada a de salida.

Por ejemplo, si queremos realizar una regla de salida para un puerto (para ambos casos se hace igual), debemos de irnos al apartado de regla de salida y con el botón derecho elegimos *Nueva regla…*

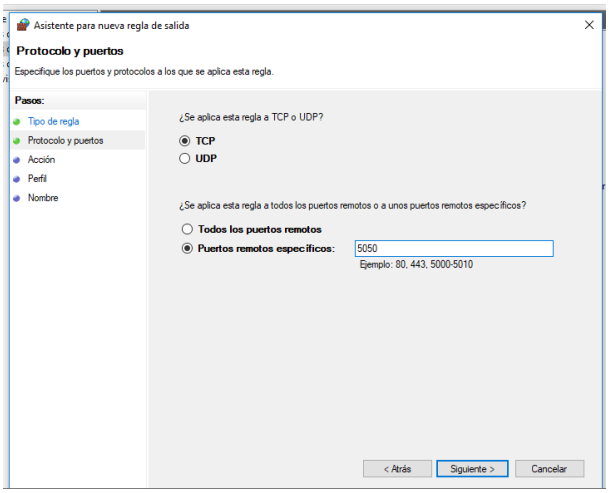


Se nos abrirá la siguiente ventana:

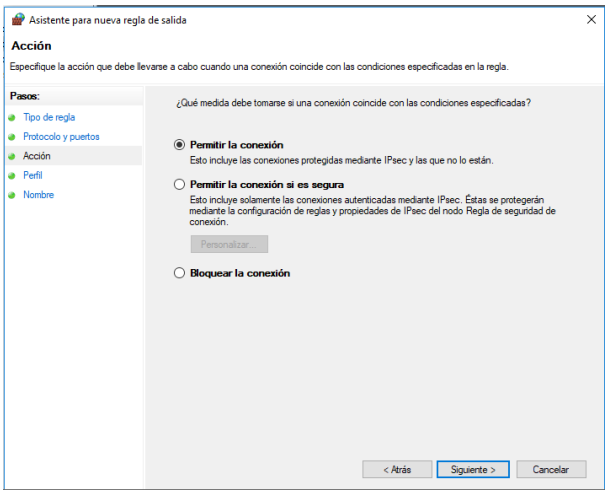


Como podemos ver, nos pregunta que tipo de regla queremos aplicar. Marcamos *Puerto* y pulsamos *Siguiente*.

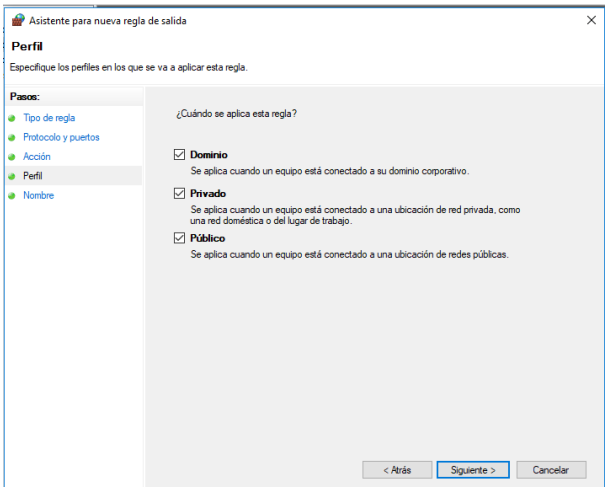
Lo próximo que debemos de indicar es si es un puerto TCP o UDP y de que puerto se trata. En este ejemplo, pondremos que es el puerto TCP 5050.



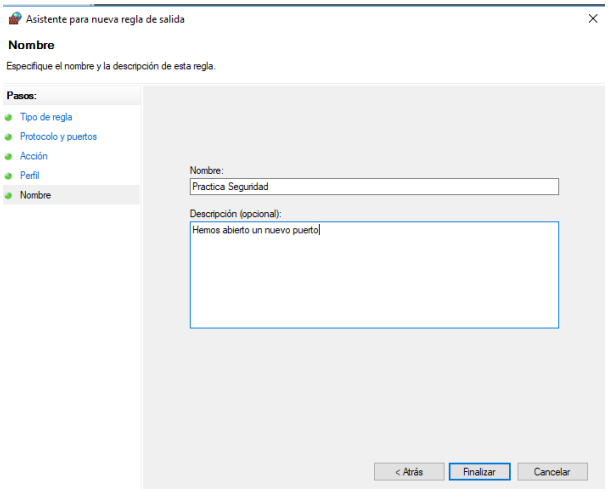
Lo Siguiente que debemos de hacer, es elegir que queremos hacer con el puerto, es decir, permitir conexión mediante ese puerto, bloquear la conexión o permitir la conexión en el caso de que sea una conexión segura. Elegimos la opción de permitir conexión en este caso.



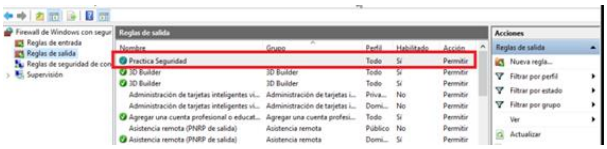
Lo próximo que tendremos que elegir, es cuándo se aplica esta regla. En este caso queremos que se aplique siempre, por lo que marcamos todas las opciones.



Pulsamos *Siguiente,* y para finalizar, asignamos un nombre y una descripción.



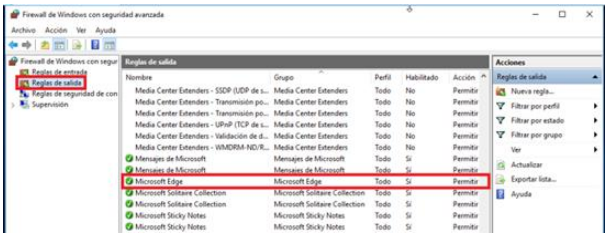
Pulsamos en *Finalizar* y ya tendremos nuestra regla creada.



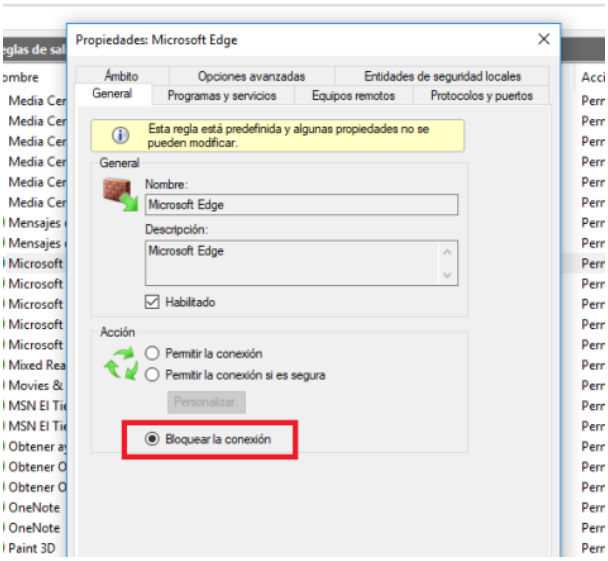
Configurar el firewall para evitar que tu navegador web tenga acceso a Internet.

Para esta apartado, usaremos como ejemplo el navegador Microsoft Edge.

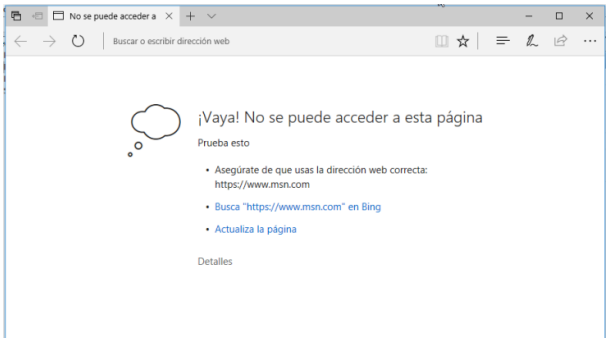
Nos vamos a reglas de salida y buscamos el navegador Microsoft Edge.



Pulsamos botón derecho sobre Microsoft Edge y elegimos la opción Propiedades. Una vez dentro marcamos la opción Bloquear Conexión.



Como podemos ver, no tiene acceso a Internet.



Tipos de firewall según los métodos de filtración de tráfico

Existen distintas maneras de filtrar el tráfico de red y lograr la protección que ofrecen los *firewall*. En este sentido, se puede clasificar a los cortafuegos como sistemas proxy, sistemas de inspección o *firewalls* de nueva generación.

Firewall proxy

Este tipo de *firewall* es lo más parecido a una verdadera barrera física o intermediario que evita conexiones directas entre redes externas y privadas. Tal como un guardia, examina toda la información entrante y si esta cumple con las reglas de seguridad, toma una función permisiva, autorizando su paso hacia el dispositivo o red privada.

Los *firewall* proxy realizan un filtrado de paquetes completos. Esto quiere decir que revisan el paquete de red completo en lugar de enfocarse en detalles superficiales, como el número de puerto o la dirección IP. La desventaja de esto es que puede consumir recursos y afectar el rendimiento del sistema, disminuyendo su funcionalidad y creando un punto débil para ser atacado.

Firewall de inspección de estado o inspección activa

Al hablar de inspección de estado o inspección activa nos referimos a un sistema de protección casi omnipresente, pues estos *firewall* filtran el tráfico de la red según una serie de propiedades técnicas de la data, como el estado, el puerto o los protocolos específicos.

La decisión de permitir o bloquear el paso de datos depende de una serie de reglas definidas por la persona que haya configurado el *firewall*; con la particularidad de que este tipo de *firewall* es capaz de tomar decisiones con base en el aprendizaje de interacciones previas. Así, por ejemplo, podría bloquear un tipo de tráfico que causó problemas anteriormente, o incluso bloquear ataques de fuentes de las cuales ya han sido catalogadas como maliciosas.

Firewall de próxima generación (NGFW)

Los ciberataques evolucionan cada vez de manera más acelerada, obligando a que todas las medidas de seguridad se adapten y mejoren a su ritmo. Así nacen los *firewalls* de próxima generación o NGFW (siglas del inglés *new generation firewall*), que combinan las funciones clásicas de los cortafuegos con la prevención de otras amenazas.

Estos firewall examinan el tráfico de red más allá, o en mayores capas que los firewall convencionales, buscando de manera detallada *malware* avanzado, ataques de capa de aplicación y otros tipos de peligros cibernéticos.

Funciones de NGFW

Los NGFW se consideran de mayor utilidad para la protección de redes empresariales, pues cumplen con las siguientes tareas:

- Inspección activa de la red, como un *firewall* clásico.
- Reconocimiento avanzado de aplicaciones peligrosas y bloqueo de comunicaciones asociados a aplicaciones específicas.
- Actualización continua, para mejorar sobre la marcha.
- Prevención de intrusiones y afrontamiento de amenazas cibernéticas.

El uso de un firewall es considerado una medida costoefectiva para proteger los activos digitales tanto de individuos como de organizaciones. Al actuar como una barrera defensiva, ayuda a salvaguardar la integridad de la información frente a los ciberataques más comunes. Sin embargo, **por sí solo no garantiza una protección absoluta**.

Para robustecer la ciberseguridad de una organización, es fundamental acompañar el uso del firewall con otras medidas de protección.

Cortafuegos: Lista de verificación de auditoría

Lista de verificación previa a la auditoría

1. Obtener documentos de trabajo/informes de auditoría anteriores.
2. Obtenga la política, los estándares y los procedimientos de Internet relevantes para la revisión del firewall.
3. Obtenga diagramas de red actuales e identifique las topologías de firewall.
4. Identifique el tipo y la versión de los firewalls implementados.
5. Identifique los objetivos de la instalación del firewall.
6. Identifique el sistema operativo que soporta el firewall.
7. Identifique todos los proveedores de servicios de Internet (ISP) y redes privadas virtuales (VPN).
8. Obtener una comprensión de los contratos de ISP y VPN.
9. Identifique si se utilizan métodos distintos del firewall para proporcionar acceso a Internet (desde redes de confianza) y desde Internet (desde redes que no son de confianza) (es decir, módem, marcado, etc.).
10. Obtenga la configuración predeterminada del firewall, la documentación y la disponibilidad de actualizaciones.

Revisión de la administración

1. ¿Existe documentación que defina claramente las funciones y responsabilidades de la administración del firewall, incluida la capacitación y las pruebas de la configuración del firewall?
2. ¿Existe una lista de administradores de firewall autorizados? (Identifique a los administradores principales y de respaldo).
3. ¿Se ha probado la eficacia de los administradores de copias de seguridad en el soporte del firewall?
4. ¿Hay alguien que sea responsable de mantenerse al día con los avisos de seguridad actuales?

Control de acceso

1. ¿Se utiliza algún proceso para autorizar el acceso de empleados y no empleados (agregar, cambiar, eliminar) a Internet?
2. ¿Qué niveles de acceso se otorgan a los privilegios?
3. Evaluar la oportunidad y exhaustividad de los métodos utilizados.
4. ¿Existe una política de contraseñas?
5. ¿Se han implementado funciones de control de contraseñas para todas las cuentas? (Es decir, uso requerido, longitud mínima, cambios periódicos, etc.).
6. ¿Se han deshabilitado las cuentas predeterminadas o se ha cambiado la contraseña original de los valores proporcionados por el proveedor?
7. ¿Existen controles que garanticen que el acceso a Internet se conceda sólo a las personas autorizadas?
8. Obtenga una lista de usuarios con acceso al firewall y concélelo con las solicitudes aprobadas documentadas. ¿Es cada usuario identificable de forma única?
9. Evalúe si las metodologías de autenticación (es decir, proxy) utilizadas son efectivas.
10. ¿Es apropiado el acceso de personas que no son empleados?
11. ¿El administrador de seguridad revisa periódicamente a los usuarios que tienen acceso a Internet? ¿Cuándo fue la revisión más reciente?
12. ¿Hay revisiones periódicas de las cuentas inactivas? ¿Cuáles son las acciones tomadas para resolver las discrepancias?
13. ¿Cuáles son los controles de seguridad utilizados por la VPN para proteger el acceso a las redes de confianza xyz?
14. ¿Existen controles de seguridad sobre el uso de módems y otros métodos (es decir, acceso telefónico) utilizados para acceder a las redes de confianza de xyz?
15. ¿Cómo se protege el acceso público a los servidores web mediante el cortafuegos?

Configuración del cortafuegos

1. Evalúe la idoneidad de las topologías de firewall implementadas.
2. ¿Cuál es la configuración actual de hardware y software del Firewall?
3. Que se hayan aplicado todas las actualizaciones identificadas por el proveedor.

4. ¿Hay una zona desmilitarizada? ¿El firewall separa correctamente la DMZ de la red interna y la red externa?
5. ¿Existe un único punto en el que se pueda separar la red interna de Internet?
6. Revise la documentación del firewall para comprender las capacidades y limitaciones del firewall.
7. ¿Existe un procedimiento de control de cambio de filtro de firewall?
8. Identifique las reglas que debe aplicar el firewall (qué servicios están permitidos entre el origen y el destino).
9. ¿Se utiliza el cifrado para los servicios autorizados?
10. ¿Cuáles son las reglas de firewall vigentes actualmente?
11. ¿Cuáles son las técnicas de filtrado utilizadas para permitir o denegar servicios a sistemas host especificados?
12. ¿Se está realizando la traducción de direcciones de red y, de ser así, está configurada correctamente?
13. Evalúe el orden de las reglas de firewall para comprobar su eficacia.
14. ¿El firewall tiene los siguientes controles? Cribado de URLs. Bloqueo de puertos. Suplantación de IP. Cribado de paquetes. Evite los ataques de denegación de servicio. Cribado entrante de Java o ActiveX. Protección antivirus.
15. ¿El firewall admite una política de "denegar todos los servicios excepto aquellos específicamente permitidos"?
16. ¿El firewall está configurado de acuerdo con los estándares y pautas xyz y el firewall aplica de manera efectiva la política de seguridad de Internet?
17. ¿Se informa a la administración de la eficacia del firewall para hacer cumplir la política de seguridad?

Monitorización

1. ¿Existe un sistema de detección de intrusos (IDS)?
2. ¿Cuáles son las amenazas para las que se ha automatizado la respuesta (por ejemplo, ataques de denegación de servicio, suplantación de identidad)?
3. Si no se ha implementado IDS, determine el alcance de la automatización de la detección de intrusiones.

4. ¿Se registran las actividades del firewall? ¿Existen procedimientos para monitorear y actuar sobre cualquier actividad inapropiada?
5. ¿Se autentican, supervisan y revisan las acciones del personal que tiene acceso privilegiado al cortafuegos?
6. ¿Existen procedimientos de registro y presentación de informes para supervisar y actuar sobre cualquier actividad inapropiada?
7. Todos los servicios de entrada, los servicios de salida y los intentos de acceso a o a través del firewall que infringen la política se registran y supervisan.
8. ¿Con qué frecuencia se realiza el monitoreo?
9. ¿Se han configurado alarmas para eventos o actividades importantes?
10. ¿Qué herramientas se utilizan para ayudar en el análisis de tendencias?
11. ¿Los registros contienen datos suficientes para la responsabilidad del usuario, el tipo de transacción, la marca de fecha y hora, la ubicación del terminal, etc.? ¿Están protegidos los registros para evitar modificaciones? ¿Cuánto tiempo se conservan los registros? ¿En qué medios se almacenan los registros?
12. ¿Qué proceso se utiliza para informar, dar seguimiento, evaluar y resolver todos los incidentes?
13. Obtenga copias de los informes de firewall para su revisión.
14. ¿Son los informes de firewall adecuados para proporcionar al personal administrativo la información necesaria para ayudar a analizar las actividades del firewall (ataques, defensas, configuraciones y actividades de los usuarios)?
15. ¿Cuáles son los procesos que se utilizan para dar seguimiento y resolver incidencias?
16. Es el firewall probado periódicamente desde las redes confiables y no confiables de xyz.
17. ¿Cuál es la eficacia del cortafuegos para hacer cumplir la política de seguridad de xyz según lo informado a la dirección?

Seguridad Física

1. ¿Existen métodos físicos para evitar que personal no autorizado acceda a los sistemas de firewall?
2. ¿Existe una lista de personal autorizado que puede acceder a las salas de computadoras del Firewall?
3. ¿Todo el personal autorizado necesita acceso?

4. ¿Existen métodos físicos para evitar que personal no autorizado acceda a consolas, armarios, enrutadores, etc.?

Controles de cambio de firewall

1. ¿Existe un procedimiento de control de cambios de firewall? ¿Existe documentación para todos los cambios en el firewall? ¿Se han autorizado todos los cambios?
2. ¿Existen procedimientos para informar al administrador del firewall de cualquier nuevo problema relacionado con la seguridad o parches disponibles y se aplican de manera adecuada y oportuna?

Copia de seguridad y recuperación

1. ¿Existe un plan de contingencia de recuperación ante desastres? ¿Se ha probado la recuperación?
2. Evaluar la idoneidad de los procedimientos de copia de seguridad y recuperación (incluida la retención).
3. ¿Con qué frecuencia se realizan las copias de seguridad?
4. ¿Se utiliza el cifrado al realizar copias de seguridad?
5. ¿Cuáles fueron los resultados de la última prueba de copia de seguridad exitosa?

Sistema operativo

1. Verifique el tipo y la versión del sistema operativo, incluido el historial de parches.
2. Evaluar el proceso de gestión de cuentas.
3. Evaluar la idoneidad del proceso de aprobación.
4. Identifique los tipos de cuentas autorizadas para tener acceso.
5. Evaluar la idoneidad de los controles de acceso y autenticación.
6. Evalúe la idoneidad de todas las cuentas.
7. Evalúe la idoneidad de los controles de contraseñas.
8. ¿Es necesario que todos los servicios de red estén implementados?
9. Identificar y evaluar la efectividad del procedimiento de monitoreo y control del desempeño.

Firewall Rules

Firewall Rules

1. Allow SSH (port 22) from a specific IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.2" port protocol="tcp" port="22" accept' --permanent

sudo firewall-cmd --reload

2. Block incoming ICMP (ping) requests:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" protocol value="icmp" drop' -permanent

sudo firewall-cmd --reload

3. Allow traffic from a specific network range:

sudo firewall-cmd --zone=public --add-source=192.168.0.0/24 --permanent

sudo firewall-cmd --reload

4. Open a custom port range (e.g., 5000-6000):

sudo firewall-cmd --zone=public --add-port=5000-6000/tcp --permanent

sudo firewall-cmd --reload

5. Block outgoing traffic on a specific port (e.g., 8080):

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" port protocol="tcp" port="8080" drop' --permanent

sudo firewall-cmd --reload

6. Allow FTP (port 21) for a specific interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" interface="eth0" port protocol="tcp" port="21" accept' --permanent

sudo firewall-cmd --reload

7. Block specific service (e.g., Telnet):

sudo firewall-cmd --zone=public --remove-service=telnet --permanent

sudo firewall-cmd --reload

8. Allow multicast traffic:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="224.0.0.0/4" drop' --permanent

sudo firewall-cmd --reload

9. Allow specific application traffic (e.g., Apache):

sudo firewall-cmd --zone=public --add-service=http --permanent

sudo firewall-cmd --reload

10. Block traffic from a specific country (e.g., Russia):

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="0.0.0.0/0" invert source="country" destination country="RU" drop' --permanent

sudo firewall-cmd –reload

11. Allow DNS (port 53) for both TCP and UDP:

sudo firewall-cmd --zone=public --add-port=53/tcp --add-port=53/udp --permanent

sudo firewall-cmd --reload

12. Allow incoming traffic on a specific network interface (e.g., eth1):

sudo firewall-cmd --zone=public --add-interface=eth1 --permanent

sudo firewall-cmd --reload

13. Block all incoming traffic except for established connections:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="0.0.0.0/0" drop' --permanent

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="0.0.0.0/0" accept' --permanent

sudo firewall-cmd --reload

14. Allow only specific IP addresses on a certain port (e.g., 8080):

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" port protocol="tcp" port="8080" source address="192.168.1.2" accept' --permanent

sudo firewall-cmd --reload

15. Open port 123 for NTP (Network Time Protocol):

sudo firewall-cmd --zone=public --add-port=123/udp --permanent

sudo firewall-cmd --reload

16. Allow ICMP echo requests (ping) from a specific subnet:

sudo firewall- --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.0.0/24" protocol="icmp" accept' --permanent

sudo firewall-cmd --reload

17. Block traffic to a specific IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="0.0.0.0/0" destination address="192.168.1.2" drop' --permanent

sudo firewall-cmd --reload

18. Allow SSH on a non-default port (e.g., 2222):

sudo firewall-cmd --zone=public --add-port=2222/tcp --permanent

sudo firewall-cmd --reload

19. Allow traffic based on a custom service:

sudo firewall-cmd --zone=public --add-service=my_custom_service --permanent

sudo firewall-cmd --reload

20. Block all incoming and outgoing traffic:

sudo firewall-cmd --zone=public --set-target=DROP --permanent

sudo firewall-cmd --reload

21. Allow RDP (Remote Desktop Protocol - port 3389) from a specific IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.2" port protocol="tcp" port="3389" accept' --permanent

sudo firewall-cmd --reload

22. Allow traffic for a specific application (e.g., PostgreSQL):

sudo firewall-cmd --zone=public --add-service=postgresql --permanent

sudo firewall-cmd --reload

23. Allow incoming connections on a specific port range (e.g., 8000-9000) for UDP:

sudo firewall-cmd --zone=public --add-port=8000-9000/udp --permanent

sudo firewall-cmd --reload

24. Allow SIP (Session Initiation Protocol - port 5060) for VoIP:

sudo firewall-cmd --zone=public --add-port=5060/udp --permanent

sudo firewall- --reload

25. Block specific MAC address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source

mac="00:11:22:33:44:55" drop' --permanent

sudo firewall-cmd --reload

26. Allow traffic for a specific user:

sudo firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -m owner --uid-owner username -j ACCEPT

sudo firewall-cmd --reload

27. Allow NFS (Network File System - port 2049) for file sharing:

sudo firewall-cmd --zone=public --add-port=2049/tcp --permanent

sudo firewall-cmd --reload

28. Allow Docker containers to communicate on a bridge network:

sudo firewall-cmd --zone=trusted --add-source=172.17.0.0/16 --permanent

sudo firewall-cmd --reload

29. Block outgoing traffic to a specific IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" destination address="203.0.113.10" drop' --permanent

sudo firewall-cmd --reload

30. Allow SNMP (Simple Network Management Protocol - port 161) for monitoring:

sudo firewall-cmd --zone=public --add-port=161/udp --permanent

sudo firewall-cmd --reload

31. Allow incoming traffic on a specific port for IPv6 (e.g., port 8080):

sudo firewall-cmd --zone=public --add-port=8080/tcp --permanent --ipv6

sudo firewall-cmd --reload

32. Block all traffic except for a specific service (e.g., SSH):

sudo firewall-cmd --zone=public --add-service=ssh --permanent

sudo firewall- --zone=public --remove-service={http,https} --permanent

sudo firewall-cmd --reload

33. Allow traffic from and to a specific network interface (e.g., eth0):

sudo firewall-cmd --zone=public --add-interface=eth0 --permanent

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source interface="eth0" accept' --permanent

sudo firewall-cmd --reload

34. Allow DNS traffic only for a specific domain:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="0.0.0.0/0" destination domain="example.com" accept' --permanent

sudo firewall-cmd --reload

35. Block traffic from a specific country for a specific service (e.g., SSH):

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="0.0.0.0/0" invert source="country" destination port="22" protocol="tcp" drop' --permanent

sudo firewall-cmd --reload

36. Allow multicast traffic for IPv6:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv6" source address="fe80::/10" drop' --permanent

sudo firewall-cmd --reload

37. Allow traffic for a specific UDP service (e.g., syslog - port 514):

sudo firewall-cmd --zone=public --add-port=514/udp --permanent

sudo firewall-cmd --reload

38. Allow traffic from a specific MAC address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source

mac="00:11:22:33:44:55" accept' --permanent

sudo firewall-cmd --reload

39. Allow outgoing SMTP traffic (port 25) for a specific IP range:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.0/24" port protocol="tcp" port="25" accept' --permanent

sudo firewall-cmd --reload

40. Allow traffic on a custom port range for both TCP and UDP (e.g., 7000-8000):

sudo firewall-cmd --zone=public --add-port=7000-8000/tcp --add-port=7000-8000/udp -permanent

sudo firewall-cmd --reload

41. Allow traffic on a specific port range for both TCP and UDP, limiting it to a specific IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.2" port port="8000-9000" protocol="tcp" accept' --permanent

sudo firewall-cmd --reload

42. Block traffic to a specific port from a range of IP addresses:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.0.0/24" port port="1234" protocol="tcp" drop' --permanent

sudo firewall-cmd --reload

43. Allow traffic for a specific user on a custom port:

sudo firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -m owner --uid-owner username -p tcp -dport 9876 -j ACCEPT

sudo firewall-cmd --reload

44. Block outgoing traffic to a specific domain:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" destination domain="example.com" drop' --permanent

sudo firewall-cmd --reload

45. Allow NTP traffic (port 123) for both TCP and UDP:

sudo firewall-cmd --zone=public --add-port=123/tcp --add-port=123/udp --permanent

sudo firewall-cmd --reload

46. Allow traffic from a specific country on a specific port (e.g., 8080):

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="0.0.0.0/0" source country="US" port port="8080" protocol="tcp" accept' --permanent

sudo firewall-cmd --reload

47. Allow traffic for a specific service on a custom interface (e.g., eth1):

sudo firewall-cmd --zone=public --add-service=http --add-interface=eth1 --permanent

sudo firewall-cmd --reload

48. Allow incoming and outgoing traffic on a specific port only for a specific time:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" port port="9876" protocol="tcp" accept' --permanent --active-from=Mon-Fri 08:00-17:00 sudo firewall-cmd --reload

49. Allow traffic for a specific service from a specific IP address range:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.0.0/24" service name="ftp" accept' --permanent

sudo firewall-cmd --reload

50. Allow traffic from and to a specific port for a range of IP addresses:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.0.0/24" port port="5432" protocol="tcp" accept' --permanent

sudo firewall-cmd –reload

51. Allow traffic on a specific port range for both TCP and UDP, limiting it to a specific MAC address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source mac="00:11:22:33:44:55" port port="8000-9000" protocol="tcp" accept' --permanent

sudo firewall-cmd --reload

52. Block traffic from a specific user on a custom port:

sudo firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -m owner --uid-owner username -p tcp -dport 9876 -j DROP

sudo firewall-cmd --reload

53. Allow traffic on a specific port range from a specific country:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source country="US" port port="8000-9000" protocol="tcp" accept' --permanent

sudo firewall-cmd --reload

54. Block traffic to a specific domain for a specific service (e.g., SSH):

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" destination

domain="example.com" service name="ssh" drop' --permanent

sudo firewall-cmd --reload

55. Allow traffic on a custom port range for a specific service (e.g., SNMP):

sudo firewall-cmd --zone=public --add-service=snmp --add-port=6000-7000/tcp --permanent

sudo firewall-cmd --reload

56. Allow traffic for a specific user and specific service:

sudo firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -m owner --uid-owner username -p tcp -dport 1234 -j ACCEPT

sudo firewall-cmd --reload

57. Block ICMP echo requests (ping) from a specific IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.2" protocol="icmp" icmp-type="8" drop' --permanent

sudo firewall-cmd --reload

58. Allow traffic on a specific port range for a specific application:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent

sudo firewall-cmd --reload

59. Block traffic from a specific IP address range on a specific port:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.0.0/24" port port="9876" protocol="tcp" drop' --permanent

sudo firewall-cmd --reload

60. Allow incoming traffic on a specific port for both TCP and UDP, limiting it to a specific user:

sudo firewall-cmd --direct --add-rule ipv4 filter INPUT 0 -m owner --uid-owner username -p tcp -dport 8080 -j ACCEPT

sudo firewall-cmd --direct --add-rule ipv4 filter INPUT 0 -m owner --uid-owner username -p udp -dport 8080 -j ACCEPT

sudo firewall-cmd --reload

61. Allow traffic on a specific port for a range of IP addresses during specific days and times:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.10-

192.168.1.20" port port="8080" protocol="tcp" accept' --permanent --activeon=Mon,Tue,Wed,Thu,Fri --active-at="08:00-17:00"

sudo firewall-cmd --reload

62. Allow traffic on a specific port range for both TCP and UDP, limiting it to a specific user and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.2" port port="8000-9000" protocol="tcp" accept' --permanent --interface=eth0

sudo firewall-cmd --reload

63. Block traffic from a specific MAC address for a specific service:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source mac="00:11:22:33:44:55" service name="ftp" drop' --permanent

sudo firewall-cmd --reload

64. Allow traffic on a custom port range for a specific application and user:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -j ACCEPT

sudo firewall-cmd --reload

65. Block incoming and outgoing traffic on a specific port for a specific user:

sudo firewall-cmd --direct --add-rule ipv4 filter INPUT 0 -m owner --uid-owner username -p tcp -dport 9876 -j DROP

sudo firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -m owner --uid-owner username -p tcp -dport 9876 -j DROP

sudo firewall-cmd --reload

66. Allow traffic on a specific port for a specific service and network interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" accept' --permanent --interface=eth1

sudo firewall-cmd --reload

67. Allow traffic on a specific port for a specific service and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="ssh" port port="2222" protocol="tcp" source address="192.168.1.2" accept' --permanent

sudo firewall-cmd --reload

68. Block traffic from a specific country on a specific port for a specific service:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source country="CN" port port="80" protocol="tcp" service name="http" drop' --permanent

sudo firewall-cmd --reload

69. Allow traffic on a specific port range for a specific application and destination IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" destination address="192.168.1.2" accept' --permanent

sudo firewall-cmd --reload

70. Block traffic from a specific MAC address for a specific service and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source mac="00:11:22:33:44:55" service name="ftp" drop' --permanent --interface=eth0

sudo firewall-cmd –reload

71. Allow traffic on a specific port range for a specific application, user, and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -o eth1 -j ACCEPT

sudo firewall-cmd --reload

72. Block incoming traffic on a specific port range for a specific country:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source country="RU" port port="3000-4000" protocol="tcp" drop' --permanent

sudo firewall-cmd --reload

73. Allow traffic on a specific port for a specific service, source IP address, and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source address="192.168.1.2" accept' --permanent --interface=eth1

sudo firewall-cmd --reload

74. Allow traffic on a specific port range for a specific application, user, and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -s 192.168.1.2 -j ACCEPT

sudo firewall-cmd --reload

75. Block traffic on a specific port for a specific service and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source address="192.168.1.2" drop' --permanent

sudo firewall-cmd --reload

76. Allow traffic on a specific port range for a specific application, user, and destination IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -d 192.168.1.2 -j ACCEPT

sudo firewall-cmd --reload

77. Allow traffic on a specific port for a specific service, source MAC address, and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source mac="00:11:22:33:44:55" accept' --permanent --interface=eth0

sudo firewall-cmd --reload

78. Block incoming traffic on a specific port range for a specific application:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" drop' --permanent

sudo firewall-cmd --reload

79. Allow traffic on a specific port for a specific service, source MAC address, and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source mac="00:11:22:33:44:55" source address="192.168.1.2" accept' --permanent

sudo firewall-cmd --reload

80. Allow traffic on a specific port range for a specific application, user, source IP address, and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -s 192.168.1.2 -o eth1 -j ACCEPT

sudo firewall-cmd --reload

81. Allow traffic on a specific port range for a specific application, user, source IP address, and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -s 192.168.1.2 -o eth1 -j ACCEPT

sudo firewall-cmd --reload

82. Block incoming traffic on a specific port range for a specific application and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" source address="192.168.1.2" drop' --permanent

sudo firewall-cmd --reload

83. Allow traffic on a specific port for a specific service, source MAC address, and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source mac="00:11:22:33:44:55" accept' --permanent --interface=eth0

sudo firewall-cmd --reload

84. Block incoming traffic on a specific port range for a specific application and destination IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" destination address="192.168.1.2" drop' --permanent

sudo firewall-cmd --reload

85. Allow traffic on a specific port range for a specific application, user, and destination IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -d 192.168.1.2 -j ACCEPT

sudo firewall-cmd --reload

86. Allow traffic on a specific port for a specific service, source MAC address, and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source mac="00:11:22:33:44:55" source address="192.168.1.2" accept' --permanent

sudo firewall-cmd --reload

87. Block incoming traffic on a specific port range for a specific application and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" drop' --permanent --interface=eth0

sudo firewall-cmd --reload

88. Allow traffic on a specific port for a specific service, source IP address, and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source address="192.168.1.2" accept' --permanent --interface=eth1

sudo firewall-cmd --reload

89. Block incoming traffic on a specific port range for a specific application, user, and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" source address="192.168.1.2" drop' --permanent --direct -add-rule ipv4 filter OUTPUT 0 -m owner --uid-owner username -s 192.168.1.2 -j DROP

sudo firewall-cmd --reload

90. Allow traffic on a specific port range for a specific application, user, and destination IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -d 192.168.1.2 -j ACCEPT

sudo firewall-cmd --reload

91. Allow traffic on a specific port range for a specific application, user, and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -s 192.168.1.2 -j ACCEPT

sudo firewall-cmd --reload

92. Block incoming traffic on a specific port range for a specific application and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" source address="192.168.1.2" drop' --permanent

sudo firewall-cmd --reload

93. Allow traffic on a specific port for a specific service, source MAC address, and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source mac="00:11:22:33:44:55" accept' --permanent --interface=eth0

sudo firewall-cmd --reload

94. Block incoming traffic on a specific port range for a specific application and destination IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" destination address="192.168.1.2" drop' --permanent

sudo firewall-cmd --reload

95. Allow traffic on a specific port for a specific service, source MAC address, and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source mac="00:11:22:33:44:55" source address="192.168.1.2" accept' --permanent

sudo firewall-cmd --reload

96. Block incoming traffic on a specific port range for a specific application and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" drop' --permanent --interface=eth0

sudo firewall-cmd --reload

97. Allow traffic on a specific port for a specific service, source IP address, and interface:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" port port="8080" protocol="tcp" source address="192.168.1.2" accept' --permanent --interface=eth1

sudo firewall-cmd --reload

98. Block incoming traffic on a specific port range for a specific application, user, and source IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" source address="192.168.1.2" drop' --permanent --direct -add-rule ipv4 filter OUTPUT 0 -m owner --uid-owner username -s 192.168.1.2 -j DROP

sudo firewall-cmd --reload

99. Allow traffic on a specific port range for a specific application, user, and destination IP address:

sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" application="my_custom_app" port port="8000-9000" protocol="tcp" accept' --permanent --direct --add-rule ipv4 filter OUTPUT 0

-m owner --uid-owner username -d 192.168.1.2 -j ACCEPT

sudo firewall-cmd --reload

100. Block incoming and outgoing traffic on a specific port for a specific user:

bash

sudo firewall-cmd --direct --add-rule ipv4 filter INPUT 0 -m owner --uid-owner username -p tcp --dport 9876 -j DROP

sudo firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -m owner -uid-owner username -p tcp --dport 9876 -j DROP

sudo firewall-cmd --reload