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-cmd --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-cmd --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-cmd --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 --active-on=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