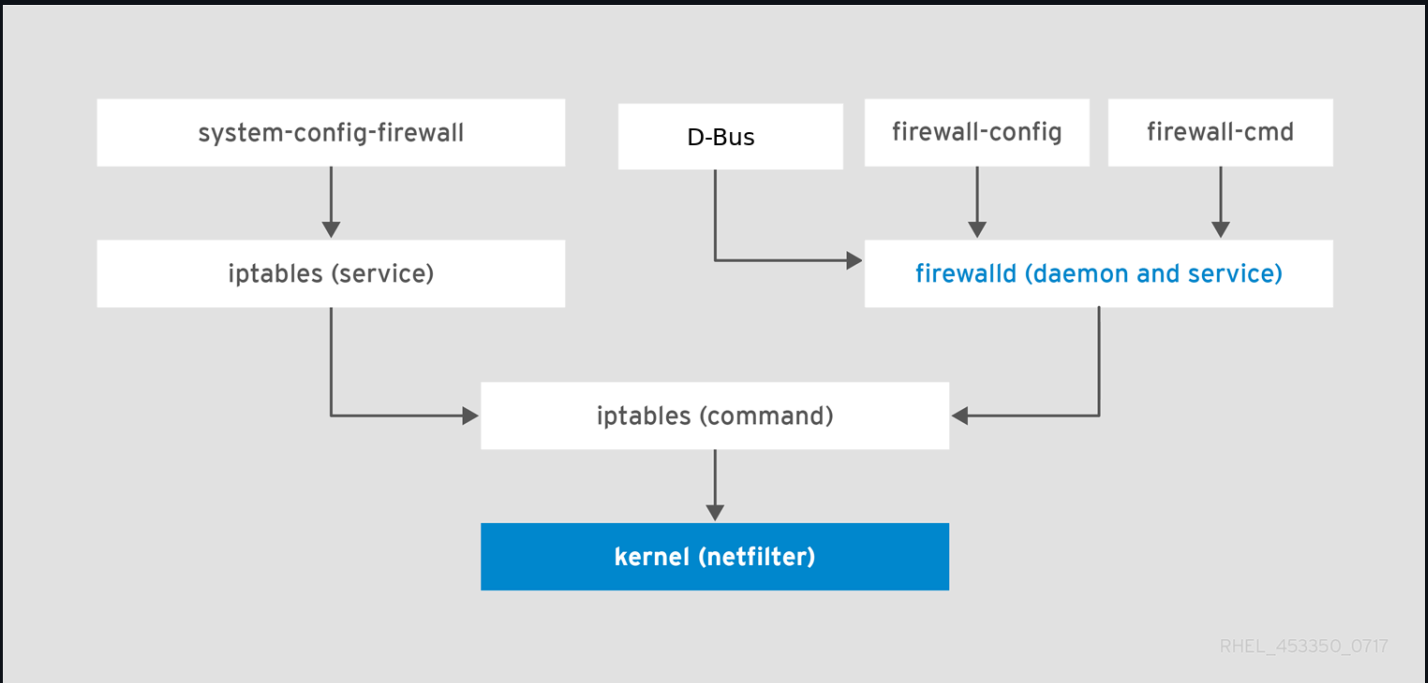
firewalld

firewalld에서 사용되는 용어



1. 런타임(Runtime)

런타임(실행시간)에만 설정한다는 것이다. 즉, 설정 내역이 메모리에 상주되어 있어 적용은 되지만, firewalld 서비스 중지와 함께 런타임 구성이 손실된다. (firewalld를 다시 불러오거나 시스템을 재시작 하면 설정된 내역은 지워지게 된다)

2. 영구적(Permanent)

영구적 설정한다는 것이다. (설정파일에 저장되어있다.)
즉, 시스템 재시작 또는 서비스 reload/restart 시 새로운 런타임 구성을 설정된 내역에서 불러온다. 런타임 설정내역을 저장할 수 있는 방법을 제공하지 않기 때문에 영구적 설정으로 관리하는 것이 효율적이다.

Runtime to Permanent

런타임 환경을 사용하여 필요에 맞는 방화벽 설정을 생성할 수 있다. 완료되면 해당 런타임 환경을 영구적으로 마이그레이션 할 수 있다.

- firewall-config : Firewalld 방화벽 관리 GUI 프로그램
- firewall-cmd : Firewalld 방화벽 관리 CUI 프로그램

/usr/lib/firewalld 디렉토리에는 icmptypes, 서비스(services) 및 영역(zones)에 대해 firewalld에서 제공하는 기본 및 대체 구성이 포함되어 있습니다.

3. 영역(Zone)

방화벽 영역(Firewall Zone)은 커넥션에 대한 신뢰 순준을 정의한다.
Zone은 특정 Source Address 또는 Network Interface와 일치하는 수신 패킷(Incoming Packets)에 적용되는 규칙(Rules)의 집합니다.
Firewalld는 기본적으로 들어오는(incoming) 패킷에만 적용되며 나가는(outgoing) 패킷에는 필터링이 발생하지 않는다.

시스템으로 들어오는 모든 패킷은 Source Address를 분석하고 해당 Source Address를 기반으로 Firewalld는 패킷이 특정 영역에 속하는지 여부를 분석한다.
그렇지 않은 경우 들어오는 네트워크 인터페이스의 Zone이 사용된다.
만약 특정 Zone을 사용할 수 없는 경우 패킷은 Default Zone의 설정에 따라 처리된다.
기억해야 할 중요한 사항은 Source Zone이 Interface Zone보다 우선된다는 것이다.

Predefined Zones - 기본적으로 정의된 영역	
영역(Zone)	*설명*
drop	*들어오는(incoming) 모든 패킷 폐기(drop)* *나가는(outgoing) 모든 패킷 허용(accept)*
block	*들어오는(incoming) 모든 패킷 거부(reject)* *나가는(outgoing) 모든 패킷 허용(accept)* *이 시스템 내에서 시작된 네트워크 연결만 가능*
public	*선택한 수신 연결을 제외하고 들어오는(incoming) 모든 패킷 거부(reject)* *나가는(outgoing) 모든 패킷 허용(accept)*
external	*특히 라우터에 대해 마스커레이딩이 활성화된 외부 네트워크에서 사용* *선택한 수신 연결을 제외하고 들어오는(incoming) 모든 패킷 거부(reject)* *나가는(outgoing) 모든 패킷 허용(accept)*
dmz	*DMZ는 비무장지대를 의미한다.* *내부 네트워크에 대한 엑세스가 제한된 조직의 외부 네트워크에 있는 공개적으로 엑세스할 수 있는 컴퓨터를 위한 것.*

영역(Zone)	설명
	선택한 수신 연결을 제외하고 들어오는(incoming) 모든 패킷 거부(reject) 나가는(outgoing) 모든 패킷 허용(accept)
work	선택한 수신 연결을 제외하고 들어오는(incoming) 모든 패킷 거부(reject) 나가는(outgoing) 모든 패킷 허용(accept)
home	선택한 수신 연결을 제외하고 들어오는(incoming) 모든 패킷 거부(reject) 나가는(outgoing) 모든 패킷 허용(accept)
internal	선택한 수신 연결을 제외하고 들어오는(incoming) 모든 패킷 거부(reject) 나가는(outgoing) 모든 패킷 허용(accept)
trusted	들어오는(incoming) 모든 패킷 허용(accept) 나가는(outgoing) 모든 패킷 허용(accept)

firewalld는 D-Bus 인터페이스가 있는 동적 사용자 정의 호스트 기반 방화벽을 제공하는 방화벽 서비스 데몬이다. 동적이므로 규칙이 변경될 때마다 방화벽 데몬을 다시 시작할 필요 없이 규칙을 생성, 변경 및 삭제할 수 있다.

firewalld는 트래픽 관리를 단순화하는 영역(Zones) 및 서비스(Services) 개념을 사용한다.
방화벽은 특정 서비스에 대해 들어오는 트래픽을 허용하고 Zone 내에서 적용하는 데 필요한 모든 설정를 포함하는 미리 정의된 규칙(Rules)이다.
그리고 서비스는 네트워크 통신을 위해 하나 이상의 포트 또는 주소를 사용한다. 방화벽은 포트를 기반으로 통신을 필터링한다. 따라서 서비스에 대한 네트워크 트래픽을 허용하려면 해당 포트가 열려있어야 한다.
연결은 하나의 Zone에만 속할 수 있지만 Zone은 여러 네트워크 연결에 사용될 수 있다.

firewall-cmd의 --new-zone, --add-port, --add-service등을 사용하여 서비스, 포트를 직접 추가할 수 있다. 그러나 새 영역(zone)을 정의하고 배포하는 더 빠른 방법은 전용 태그 집합으로 XMl설정파일을 직접 작성하는 것이다.
기본 영역(default zones)에 대한 설정파일은 /usr/lib/firewalld/zones 디렉토리에 있다.
기본 영역 중 하나가 수정되면 변경 사항이 원래 구성 파일에 직접 기록되지 않는다.
대신 /etc/firewalld/zones 디렉토리에 같은 이름의 파일이 생성된다. 이러한 방법으로 만약 영역을 기본 설정으로 리셋하려면, 그냥 해당 파일을 삭제하면 된다.

기본 영역의 설정을 변경, 또는 사용자 지정 영역(custom zones)을 만들려면 /etc/firewalld/zones 디렉토리에 만들어야 한다

Zone 설정 파일의 기본 구조

```
<?xml version="1.0" encoding="utf-8"?>
<zone [version="versionstring"] [target="ACCEPT|%%REJECT%%|DROP"]>
  [ <short>short description</short> ]
  [ <description>description</description> ]
  [ <interface name="string"/> ]
  [ <source address="address[/mask]"|mac="MAC"|ipset="ipset"/> ]
  [ <service name="string"/> ]
  [ <port port="portid[-portid]" protocol="tcp|udp|sctp|dccp"/> ]
  [ <protcol value="protocol"/> ]
  [ <icmp-block name="string"/> ]
  [ <icmp-block-inversion/> ]
  [ <masquerade/> ]
  [ <forward-port port="portid[-portid]" protocol="tcp|udp|sctp|dccp" [to-port="portid[-portid]"] [to-addr="ipv4address"]/> ]
  [ <source-port port="portid[-portid]" protocol="tcp|udp|sctp|dccp"/> ]
  [
    <rule [family="ipv4|ipv6"]>
    [ <source address="address[/mask]"|mac="MAC"|ipset="ipset" [invert="True"]/> ]
    [ <destination address="address[/mask]" [invert="True"]/> ]
    [
      <service name="string"/> |
      <port port="portid[-portid]" protocol="tcp|udp|sctp|dccp"/> |
      <protocol value="protocol"/> |
      <icmp-block name="icmptype"/> |
      <icmp-type name="icmptype"/> |
      <masquerade/> |
      <forward-port port="portid[-portid]" protocol="tcp|udp|sctp|dccp" [to-port="portid[-portid]"] [to-addr="address"]/>
    ]
    [ <log [prefix="prefixtext"] [level="emerg|alert|crit|err|warn|notice|info|debug"]> [<limit value="rate/duration"/>] </log> ]
    [ <audit> [<limit value="rate/duration"/>] </audit> ]
    [
      <accept> [<limit value="rate/duration"/>] </accept> |
      <reject [type="rejecttype"]> [<limit value="rate/duration"/>] </reject> |
      <drop> [<limit value="rate/duration"/>] </drop> |
      <mark set="mark[/mask]"> [<limit value="rate/duration"/>] </mark>
    ]
    </rule>
  ]
</zone>
```

4. 서비스(Service)

Firewalld 서비스는 방화벽에서 들어오고 나가는 트래픽으로 정확히 무엇을 허용해야 하는지 지정한다.
여기에는 일반적으로 열어야하는 포트(ports)와 로드해야하는 커널 모듈이 포함된다.
각 서비스별 정의된 프로토콜, 포트, 모듈, 목적지에 대해 정의가 된 서비스이다.
여기서 서비스는 /etc/service에 명시된 내용과 다르다.

서비스를 사용하면 모든 것을 차례대로 설정하는 대신 포트 열기(opening ports), 프로토콜 정의(defining protocols), 패킷 전달 활성화(enabling packet forwarding) 등과 같은 여러 작업을 한 단계로 수행할 수 잇으므로 사용자 시간이 절약된다.

서비스는 service-name.xml 형식으로 명명된 개별 XML구성 파일을 통해 지정된다.
그래픽 지원되는 firewall-config, firewall-cmd, firewall-offline-cmd 등을 사용해 서비스를 추가/제거 할 수 있다.

다른 방법으로, /etc/firewalld/services/ 디렉토리에서 XML 파일들을 수정할 수 있다.
각 서비스는 XML구성 파일이 있다. 기본 저장 경로는 /usr/lib/firewalld/services 이다.
사용자 정의 XML 파일은 /etc/firewalld/services 디렉토리에 추가할 수 있다.
사용자가 서비스를 추가하거나 변경하지 않은 경우 /etc/firewalld/services/에서 해당 XML 파일을 찾을 수 없다.
서비스를 추가하거나 변경하려면 /usr/lib/firewalld/services/ 디렉토리의 파일을 템플릿으로 사용할 수 있다.

서비스 XML 파일 생성하기

서버에 Oracle 데이터베이스를 설치한다고 가정해보자. 1521 포트가 열려 있어야 하며 TCP 유형이어야 한다.
다음과 같은 내용으로 /etc/firewalld/services/oracledb.xml 파일을 만들어보자.

```
~]# cat /etc/firewalld/services/oracledb.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
    <short>OracleDB</short>
    <description>Oracle Database firewalld service. It allows connections to the Oracle Database service. You will need to deploy Oracle Database in this ma
    <port protocol="tcp" port="1521"/>
</service>
```

서비스 XML 파일 예시

```
<?xml version="1.0" encoding="utf-8"?>
<service>
 <short>FTP</short>
 <description>FTP is a protocol used for remote file transfer.
  If you plan to make your FTP server publicly available, enable this option.
  You need the vsftpd package installed for this option to be useful.
 </description>
 <port protocol="tcp" port="21"/>
 <module name="nf_conntrack_ftp"/>
</service>


<?xml version="1.0" encoding="utf-8"?>
<service>
 <short>IPsec</short>
 <description>Internet Protocol Security (IPsec) incorporates security for network transmissions directly into the Internet Protocol (IP).
  IPsec provides methods for both encrypting data and authentication for the host or network it sends to.
  If you plan to use a vpnc server or FreeS/WAN, do not disable this option.
 </description>
 <protocol value="ah"/>
 <protocol value="esp"/>
 <port protocol="udp" port="500"/>
 <port protocol="udp" port="4500"/>
</service>

<?xml version="1.0" encoding="utf-8"?>
<service>
 <short>Multicast DNS (mDNS)</short>
 <description>mDNS provides the ability to use DNS programming interfaces,
  packet formats and operating semantics in a small network without a conventional DNS server.
  If you plan to use Avahi, do not disable this option.
 </description>
 <port protocol="udp" port="5353"/>
 <destination ipv4="224.0.0.251" ipv6="ff02::fb"/>
</service>
```

5. 마스커레이딩(Masquerading)

IP 마스커레이딩은 한 대의 컴퓨터가 네트워크의 IP 게이트웨이 역할을 하는 프로세스이다.
마스커레이딩에 의해 게이트웨이는 인터페이스 밖으로 나가는 IP를 찾아서 패킷의 source address를 동적으로 이 주소로 바꾼다.
마스커레이딩의 일반적인 사용 사례는 라우터가 인터넷에서 라우팅되지 않는 사설 IP 주소를 라우터에서 나가는 인터페이스의 공용 동적 IP 주소로 대체하는 경우이다.

6. 포트 포워딩(Port Forwarding)

firewall을 사용하여 시스템의 특정 포트에 도달하는 모든 수신 트래픽이 선택한 다른 내부 포트나 다른 시스템의 외부 포트로 전달되도록 포트 리다이렉션을 설정할 수 있다.

7. 정책(Policy)

일부 예외(masquerade, forward-ports)를 제외하고 firewalld는 이전에 end-station 제한되었다.
즉, 가상 머신, 컨테이너 및 Zone 사이에서 흐르는 트래픽을 필터링하는 데 사용할 수 없다.
해당 기능의 일부는 직접 인터페이스(direct interface)를 하고 iptables의 rules을 작성하여 사용할 수 있었지만 사용자 경험이 좋지는 않았다.

필요한 것은 Zone 사이의 트래픽 흐름에 대한 정책을 적용하는 방법이다.
그런 다음 사용자는 firewalld의 기본 요소(services, ports, rich rules... 등등)를 정책(policy)에 연결할 수 있다.

---

firewalld-cmd 명령

firewall-cmd는 firewalld 데몬을 제어하는 도구이다.
런타임(runtime) 및 영구(permanent) 구성을 관리하기 위한 인터페이스를 제공한다.

General Options 은 설명 생략... (별로 안중요함)	
Status Options (상태 옵션)	
--state	*firewalld 데몬이 활성화된 상태인지 체크. 활성 상태이면 종료 코드 0을 반환*
--reload	*방화벽 규칙(rules)을 다시 로드하고 상태 정보를 유지한다. 현재 영구 구성(permanent configuration)은 새로운 런타임 구성(runtime configuration)이 된다. 즉, 다시 로드할 때까지 수행된 모든 런타임 전용 변경 사항은 영구 구성이 아닌 경우 다시 로드하면 손실된다.*
--complete-reload	*netfilter 커널 모듈을 포함하여 방화벽을 완전히 다시 로드한다. 상태 정보가 손실되기 때문에 활성화된 커넥션이 종료될 가능성이 크다. 이 옵션은 심각한 방화벽 문제가 있는 경우에만 사용해야 한다.*
--runtime-to-permanent	*런타임 구성(runtime configuration)을 저장하고 영구 구성(permanent configuration)을 덮어쓴다.*
--check-config	*영구 구성에 대한 검사를 한다. 여기에는 XML 유효성 및 의미를 포함한다.*
Log Denied Options (로그 거부 옵션)	
--get-log-denied	*로그 거부 설정을 출력한다.*
--set-log-denied=value	*기본 규칙(rules)에 대한 INPUT, FORWARD, OUTPUT 체인의 거부(reject) 및 삭제(drop) 규칙 직전에 로깅 규칙을 추가하고, 또한 구성된 링크 계층의 패킷 타입에 대한 영역(zones)의 최종 거부(reject) 및 삭제(drop) 규칙도 추가한다. 이 옵션에 지정 가능한 값은 all, unicast, broadcast, multicast and off(기본값 : 로깅 비활성화)*
Permanent Options (영구 옵션)	
--permanent	*이 옵션은 옵션을 영구적으로 설정하는 데 사용한다. 이러한 변경 사항은 즉시 적용되지 않으며 서비스를 restart/reload 또는 시스템 reboot 한 후에만 적용된다. --permanent 옵션이 없으면 변경 사항은 런타임 구성의 일부일 뿐이다.*
Automatic Helpers Options (자동 도우미 옵션)	
--get-automatic-helpers	*자동 도우미 설정을 출력한다.*
--set-automatic-helpers=값	*iptables 및 연결 추적 도우미(connection tracking helpers)를 안전하게 사용하려면 AutomaticHelpers를 끄는 것이 좋다. 그러나 이는 /proc/sys/net/netfilter/nf_conntrack_helper의 sysctl 설정이 변경되므로 netfilter helpers를 사용하는 다른 서비스에 부작용이 있을 수 있다. 시스템 설정을 사용하려면 커널 또는 sysctl로 설정된 기본값이 사용된다. 가능한 값은 yes 또는 no 이다. 기본값은 system 이다. 이 설정은 런타임 및 영구적인 변경이며 helpers를 사용할 수 있도록 방화벽을 reload 한다.*
Zone Options (영역 옵션)	
--get-default-zone	*연결 및 인터페이스에 대한 기본 영역(default zone)을 출력한다.*
--set-default-zone=zone	*zone이 선택되지 않은 연결 및 인터페이스에 대한 기본 zone을 설정한다. 기본 zone을 설정하면 기본 zone을 사용하는 연결 또는 인터페이스의 zone이 변경된다.*
--get-active-zones	*zone에서 사용되는 interfaces 및 source와 함께 현재 활성 zone을 인쇄한다. 활성 zone은 interface 또는 source에 대한 바인딩이 있는 zone이다. 출력 포맷은 다음과 같다.*

	zone1
	  interfaces: interface1 interface2 ..
	  sources: source1 ..
	zone2
	  interfaces: interface3 ..
	zone3
	  sources: source2 ..

--get-zones	미리 정의된 zones을 공백으로 구분하여 출력
--get-services	미리 정의된 services를 공백으로 구분하여 출력
--get-icmptypes	미리 정의된 icmptypes를 공백으로 구분하여 출력
--get-zone-of-interface=interface	interface가 바인딩 된 zone의 이름을 출력
--get-zone-of-source=source[/mask]|MAC|ipset:ipset	source가 바인딩 된 zone의 이름을 출력

--info-zone=zone	지정한 zone에 대한 정보를 출력
	
	zone
	interfaces: interface1 ...
	sources: source1 ...
	services: service1 ...
	ports: port1 ...
	protocols: protocol1 ...
	forward-ports:
	  forward-port1
	  ...
	source-ports: source-port1 ...
	icmp-blocks: icmp-type1 ...
	rich rules:
	  rich-rule1
	  ...

--list-all-zones	모든 zone에서 추가되거나 활성화된 항목을 출력
	
	zone1
	interfaces: interface1 ...
	sources: source1 ...
	services: service1 ...
	ports: port1 ...
	protocols: protocol1 ...
	forward-ports:
	  forward-port1
	  ...
	icmp-blocks: icmp-type1 ...
	rich rules:
	  rich-rule1
	  ...
	...

--permanent --new-zone=zone	새 zone을 추가
--permanent --new-zone-from-file=filename [--name=zone]	파일로부터 새 zone을 추가, --name 옵션으로 이름을 재정의 할 수 있다.
--permanent --delete-zone=zone	기존 zone을 삭제
--permanent --load-zone-defaults=zone	zone 기본 설정을 로드한다
--permanent --path-zone=zone	zone 설정 파일의 경로를 출력
Policy Options (정책 옵션)	
[--permanent] --get-policies	미리 정의된 policy 들을 공백으로 구분하여 출력
[--permanent] --info-policy=policy	지정한 policy에 대한 정보를 출력
[--permanent] --list-all-policies	모든 policy에서 추가되거나 활성화된 항목을 출력
--permanent --new-policy=policy	새로운 영구 policy를 추가
--permanent --new-policy-from-file=filename [--name=policy]	파일로부터 새 영구 policy를 추가, --name 옵션으로 이름을 재정의 할 수 있다.
--permanent --path-policy=policy	policy 설정 파일의 경로를 출력
--permanent --delete-policy=policy	기존 영구 policy를 삭제
--permanent --load-policy-defaults=policy	지정한 policy의 기본값 로드. firewalld와 함께 제공되는 policy에만 적용된다.(사용자 정의 policy는 지원안됨)
Options to Adapt and Query Zones and Policies (zone 및 policy를 조정하는 옵션) 이 섹션에 나오는 옵션은 하나의 특정 영역(zone) 또는 정책(policy)에만 영향을 미친다. --zone=zone 또는 --policy=policy 옵션과 함께 사용하면 지정된 zone 또는 policy에 영향을 미치고, 두 옵션 모두 생략하면 기본 영역(default zone)에 영향을 미친다.	
[--permanent] [--zone=zone] [--policy=policy] --list-all	추가되거나 활성화된 모든 항목 나열
--permanent [--zone=zone] [--policy=policy] --get-target	영구 zone의 target

--permanent [--zone=zone] [--policy=policy] --set-target=target	영구 zone에 지정한 target을 설정 zone을 위한 target은 default, ACCEPT, DROP, REJECT 중 하나이다. policy를 위한 target은 CONTINUE, ACCEPT, DROP, REJECT 중 하나이다. default는 REJECT와 유사하지만 암묵적으로 ICMP 패킷을 허용한다.
--permanent [--zone=zone] [--policy=policy] --set-description=description	설명을 설정한다.
--permanent [--zone=zone] [--policy=policy] --get-description	설명을 출력한다.
--permanent [--zone=zone] [--policy=policy] --set-short=description	짧은 설명을 설정한다.
--permanent [--zone=zone] [--policy=policy] --get-short	짧은 설명을 출력한다.
지금부터 나오는 옵션들은 옵션 앞에 [--permanent] [--zone=zone] [--permanent] [--policy=policy] 는 생략이 가능하다.	
--list-services	정의된 services를 공백으로 구분하여 출력
--add-service=service [--timeout=timeval]	service를 추가한다. 이 옵션은 여러번 지정할 수 있다. timeout을 지정하면 규칙(rule) 지정된 시간동안 활성화되고 나중에 자동으로 제거된다. (--timeout 옵션은 --permanent 옵션과 결합할 수 없다) timeval은 숫자(초)이거나 또는 문자 s(초), m(분), h(시간)중 하나가 뒤에 오는 숫자이다. 예) 20m, 1h 지정한 service는 firewalld에서 제공하는 service중 하나이다. (지원되는 service 목록을 보려면 위에 설명한 --get-services로 확인가능) 일부 service는 연결 추적 도우미(connection tracking helpers)를 정의한다. 클라이언트 모드에서 작동할 수 있는 도우미(helper)는 클라이언트에 대해 적용할 zone 대신에 outbound policy에 추가되어야 한다. 그렇지 않으면 도우미(helper)가 아웃바운드 트래픽에 적용되지 않는다. 반환 경로에서 연결 추적 도우미에 의해 정의된 관련 트래픽은 상태 저장 방화벽(stateful firewall) 규칙(rules)에 의해 허용된다.
--remove-service=service	service를 제거한다. 이 옵션은 여러번 지정할 수 있다.
--query-service=service	지정한 service의 추가 여부를 리턴한다. 참이면 0, 그렇지 않으면 1을 리턴 (Returns 0 if true, 1 otherwise.)
--list-ports	추가된 포트(port)를 공백으로 구분하여 출력 포트는 portid[-portid]/protocol 형식이며, 포트와 프로토콜 쌍이거나 프로토콜이 있는 포트 범위일 수 있다.
--add-port=portid[-portid]/protocol [--timeout=timeval]	port를 추가한다. 이 옵션은 여러번 지정할 수 있다. timeout을 지정하면 규칙(rule) 지정된 시간동안 활성화되고 나중에 자동으로 제거된다. (--timeout 옵션은 --permanent 옵션과 결합할 수 없다) port는 싱글 포트 번호이거나 포트 범위 portid-portid일 수 있다. 프로토콜은 tcp 또는 udp일 수 있다.
--remove-port=portid[-portid]/protocol	port를 제거한다. 이 옵션은 여러번 지정할 수 있다.
--query-port=portid[-portid]/protocol	지정한 port의 추가 여부를 리턴한다. 참이면 0, 그렇지 않으면 1을 리턴
--list-protocols	추가된 프로토콜을 공백으로 구분하여 출력
--add-protocol=protocol [--timeout=timeval]	프로토콜을 추가한다. 이 옵션은 여러번 지정할 수 있다. timeout을 지정하면 규칙(rule) 지정된 시간동안 활성화되고 나중에 자동으로 제거된다. (--timeout 옵션은 --permanent 옵션과 결합할 수 없다) 프로토콜은 시스템에서 지원하는 모든 프로토콜이 가능하다. /etc/protocols 을 보면된다.
--remove-protocol=protocol	프로토콜을 제거한다. 이 옵션은 여러번 지정할 수 있다.
--query-protocol=protocol	지정한 프로토콜의 추가 여부를 리턴한다. 참이면 0, 그렇지 않으면 1을 리턴
--list-source-ports	추가된 source ports를 공백으로 구분하여 출력 포트는 portid[-portid]/protocol 형식이다.
--add-source-port=portid[-portid]/protocol [--timeout=timeval]	source port를 추가한다. 이 옵션은 여러번 지정할 수 있다. timeout을 지정하면 규칙(rule) 지정된 시간동안 활성화되고 나중에 자동으로 제거된다. (--timeout 옵션은 --permanent 옵션과 결합할 수 없다) port는 싱글 포트 번호이거나 포트 범위 portid-portid일 수 있다. 프로토콜은 tcp 또는 udp일 수 있다.
--remove-source-port=portid[-portid]/protocol	source port를 제거한다. 이 옵션은 여러번 지정할 수 있다.
--query-source-port=portid[-portid]/protocol	source port의 추가 여부를 리턴한다. 참이면 0, 그렇지 않으면 1을 리턴
--list-icmp-blocks	추가된 ICMP(Internet Control Message Protocol) 타입의 block을 공백으로 구분하여 출력
--add-icmp-block=icmptype [--timeout=timeval]	icmptype에 대한 ICMP block을 추가한다. 이 옵션은 여러번 지정할 수 있다. timeout을 지정하면 규칙(rule) 지정된 시간동안 활성화되고 나중에 자동으로 제거된다. (--timeout 옵션은 --permanent 옵션과 결합할 수 없다) icmptype은 firewalld가 지원하는 icmp 타입중 하나이다. firewall-cmd --get-icmptypes (지원되는 icmptype을 확인)
--remove-icmp-block=icmptype	icmptype에 대한 ICMP block을 제거한다. 이 옵션은 여러번 지정할 수 있다.
--query-icmp-block=icmptype	지정한 icmptype에 대한 ICMP block이 추가되어있는지 여부를 리턴. 참이면 0, 그렇지 않으면 1을 리턴
--list-forward-ports	IPv4의 forward ports를 공백으로 구분하여 출력

--add-forward-port=port=portid[-portid]:proto=protocol[:toport=portid[-portid]] [:toaddr=address[/mask]] [--timeout=timeval]	IPv4의 forward port를 추가한다. 이 옵션은 여러번 지정할 수 있다. timeout을 지정하면 규칙(rule) 지정된 시간동안 활성화되고 나중에 자동으로 제거된다. (--timeout 옵션은 --permanent 옵션과 결합할 수 없다) port는 싱글 포트 번호이거나 포트 범위 portid-portid일 수 있다. protocol은 tcp 또는 udp일 수 있다. destination address는 단순 IP 주소이다. toaddr을 지정하면 암묵적으로 IP 포워딩이 가능하게 된다.
--remove-forward-port=port=portid[-portid]:proto=protocol[:toport=portid[-portid]] [:toaddr=address[/mask]]	IPv4의 forward port를 제거한다. 이 옵션은 여러번 지정할 수 있다.
--query-forward-port=port=portid[-portid]:proto=protocol[:toport=portid[-portid]] [:toaddr=address[/mask]]	IPv4의 forward port가 추가되어있는지 여부를 리턴. 참이면 0, 그렇지 않으면 1을 리턴
--add-masquerade [--timeout=timeval]	IPv4 마스커레이드를 활성화한다. timeout을 지정하면 마스커레이딩(masquerading)이 지정된 시간동안 활성화되고 나중에 자동으로 제거된다. (--timeout 옵션은 --permanent 옵션과 결합할 수 없다) 마스커레이딩은 만약 이 시스템이 라우터이고, 인터페이스 너머의 다른 zone의 시스템들과 연결되어있어 맨처음 커넥션이 이 시스템인 경우에 유용하다.
--remove-masquerade	IPv4 마스커레이드를 비활성화.
--query-masquerade	IPv4 마스커레이딩이 활성화되어있는지 여부를 리턴. 참이면 0, 그렇지 않으면 1을 리턴
--list-rich-rules	rich rule을 줄바꿈으로 구분하여 출력
--add-rich-rule='rule' [--timeout=timeval]	'rule' 이라는 rich rule을 추가한다. 이 옵션은 여러번 지정할 수 있다. timeout을 지정하면 규칙(rule) 지정된 시간동안 활성화되고 나중에 자동으로 제거된다. (--timeout 옵션은 --permanent 옵션과 결합할 수 없다)
--remove-rich-rule='rule'	'rule' 이라는 rich rule을 제거한다. 이 옵션은 여러번 지정할 수 있다.
--query-rich-rule='rule'	'rule' 이라는 rich rule이 추가되어있는지 여부를 리턴. 참이면 0, 그렇지 않으면 1을 리턴
Options to Adapt and Query Policies (policy를 조정하는 옵션) 이 섹션에 나오는 옵션은 하나의 특정 정책(policy)에만 영향을 미친다. 따라서 --policy 옵션은 반드시 같이 지정해야 한다.	
--permanent --policy=policy --get-priority	지정한 policy의 우선순위를 가져옴
--permanent --policy=policy --set-priority=priority	지정한 policy의 우선순위를 설정. 우선순위를 policy의 상대적 순서를 결정한다. 우선순위는 -32768에서 32767 사이의 정수 값이고, -1은 새로운 policy에 대한 기본값, 0은 내부용으로 예약되어있다. 우선순위가 0보다 작으면, 해당 policy의 rules이 모든 zone의 rules 보다 먼저 실행된다. 우선순위가 0보다 크면, 해당 policy의 rules이 모든 zone의 rules 보다 나중에 실행된다.
[--permanent] --policy=policy --list-ingress-zones	ingress zones(입구 영역? 수신 영역?) 목록을 공백으로 구분하여 출력
[--permanent] --policy=policy --add-ingress-zone=zone	지정한 ingress zone을 추가한다. 이 옵션은 여러번 지정할 수 있다. ingress zone은 firewalld에서 제공되는 zone 중 하나이거나 pseudo-zones(HOST, ANY) 중 하나이다. HOST : 호스트 시스템, 즉 firewalld를 실행하는 호스트 시스템에서 발생하는 트래픽에 사용된다. ANY : 호스트 시스템을 제외한 모든 zone에서 발생하는 트래픽에 사용된다.
[--permanent] --policy=policy --remove-ingress-zone=zone	지정한 ingress zone을 제거한다. 이 옵션은 여러번 지정할 수 있다.
[--permanent] --policy=policy --query-ingress-zone=zone	지정한 zone이 추가되어있는지 여부를 리턴. 참이면 0, 그렇지 않으면 1을 리턴
[--permanent] --policy=policy --list-egress-zones	egress zone을 공백으로 구분하여 출력
[--permanent] --policy=policy --add-egress-zone=zone	지정한 egress zone을 추가한다. 이 옵션은 여러번 지정할 수 있다.
[--permanent] --policy=policy --remove-egress-zone=zone	지정한 egress zone을 제거한다. 이 옵션은 여러번 지정할 수 있다.
[--permanent] --policy=policy --query-egress-zone=zone	지정한 zone이 추가되어있는지 여부를 리턴. 참이면 0, 그렇지 않으면 1을 리턴
Interfaces, Sources 바인딩 옵션 IPSet 옵션 Service 옵션 등등 너무 많아서 생략...	