Cấu hình

Directories

- firewalld hỗ trợ 2 config direc

Default and Fallback Configuration

- direc /usr/lib/firewalld chứa các default và fallback config được cung cấp bởi firewalld cho icmptypes, services, zones.

- các file cung cấp bởi firewalld package ko được thay đổi, chúng sẽ tự quay lại mặc định khi khi update firewalld

- Ngoài icmptype, service và zones có thể được cung cấp bởi các package hoặc bằng cách tạo các file

System Specific Configuration

- system or user config được lưu trong /etc/firewalld được tạo bởi sysad, các cusstom hoặc = tay

- Để thay đổi các setting hoặc pre defined icmptype, zones, service, copy file từ default configuration directory tới các direc liên kết

- Nếu ko có /etc/firewalld direc hoặc ko có các config tại đây, firewalld sẽ sử dụng default config và default setting cho firewalld.conf

Runtime versus Permanent

- Các cấu hình được chia ra thành runtime và permanent config

Runtime config

- runtime config là các config có hiệu lực, chúng được đưa xuống firewalld trong kernel. - Khi firewall service bắt đầu chạy, các permanent config sẽ chuyển thành các runtime config. Việc thay đổi runtime config ko được tự động lưu lại tại permanent config.

- runtim config sẽ mất khi firewalld service stop, firewalld reload sẽ chạy lại các permanent config. Changed zone cũng reload lại các perman config

Permanent Configuration

- Perman config được lưu tại config file và sẽ được load lại, chúng sẽ trở thành các runtime config khi service restart, reboot, boot..

Runtime to Permanent

- runtime environment có thể sử dụng để tạo các firewall setup phù hợp với các thời điểm. Khi các cấu hình đã phù hợp với yêu cầu, có thể đưa các cấu hình runtime xuống perman = cmd: firewall-cmd --runtime-to-permanent

firewalld.conf

- firewall.conf trong “/etc/firewalld” được cung cấp các config cơ bản cho firewalld. Nếu file ko tồn tại, firewall internal mặc định sẽ được sử dụng

Default Zone

- Default zone được sử dụng mặc định. Các ràng buộc không rõ ràng tại các zone khác sẽ được xử lý mặc định bằng default zone

DefaultZone=public

Minimal Mark

-Marks up to this minimum are free for use for example in the direct interface. If more free marks are needed, increase the minimum.

MinimalMark=100

Clean Up on exit

- Nếu được set = no, các config firewall sẽ ko được làm sạch khi thoát hoặc dừng firewalld

CleanupOnExit=yes

Lockdown

- If set to enabled, firewall changes with the D-Bus interface will be limited to applications that are listed in the lockdown whitelist. The lockdown whitelist file is lockdown-whitelist.xml.

Lockdown=no

IPv6\_rpfilter

- Performs a reverse path filter test on a packet for IPv6. If a reply to the packet would be sent via the same interface that the packet arrived on, the packet will match and be accepted, otherwise dropped. The rp\_filter for IPv4 is controlled using sysctl.

IPv6\_rpfilter=yes

Individual Calls

- Do not use combined -restore calls, but individual calls. This increases the time that is needed to apply changes and to start the daemon, but is good for debugging.

IndividualCalls=no

Log Denied

- Add logging rules right before reject and drop rules in the INPUT, FORWARD and OUTPUT chains for the default rules and also final reject and drop rules in zones. Possible values are: all, unicast, broadcast, multicast and off.

LogDenied=off