nftables wiki

4-5 minutes

Welcome to the *nftables* HOWTO documentation page. Here you will find documentation on how to build, install, configure and use nftables.

If you have any suggestion to improve it, please send your comments to Netfilter users mailing list <netfilter@vger.kernel.org>.

News

Introduction

- What is nftables?
- How to obtain help/support

Reference

- man nft - netfilter website
- man nft - mankier.com
- Quick reference, nftables in 10 minutes
- Netfilter hooks and nftables integration with existing Netfilter components
- Understanding nftables families
- Data types
- Connection tracking system (conntrack), used for stateful firewalling and NAT
- Troubleshooting and FAQ
- Additional documentation

Installing nftables

- Using nftables from distributions
- Building and installing nftables from sources

Upgrading from xtables to nftables

- Legacy xtables tools
- Moving from iptables to nftables
- Moving from ipset to nftables

Basic operation

- Configuring tables
- Configuring chains
- Simple rule management
- Atomic rule replacement
- Error reporting from the command line
- Building rules through expressions
- Operations at ruleset level
- Monitoring ruleset updates

- Scripting
- Ruleset debug/tracing
- Ruleset debug/VM code analysis
- Output text modifiers

Expressions: Matching packets

- Matching packet metainformation
- Matching packet headers
- Matching connection tracking stateful metainformation
- Matching routing information
- Rate limiting matchings

Statements: Acting on packet matches

- Accepting and dropping packets
- Rejecting traffic
- Jumping to chain
- Counters
- Logging traffic
- Performing Network Address Translation (NAT)
- Setting packet metainformation
- Setting packet connection tracking metainformation
- Mangling packet headers (including stateless NAT)
- Duplicating packets
- Load balancing
- Queueing to userspace

Advanced data structures for performance packet classification

- Intervals
- Concatenations
- Math operations
- Stateful objects
  - Counters
  - Quotas
  - Limits
  - Connlimits (*ct count*)
- Other objects
  - Conntrack helpers (*ct helper*, Layer 7 ALG)
  - Conntrack timeout policies (*ct timeout*)
  - Conntrack expectations (*ct expectation*)
  - Synproxy
  - Secmarks
- Generic set infrastructure
  - Sets
  - Element timeouts
  - Updating sets from the packet path
  - Maps
  - Verdict maps
  - Metering (formerly known as flow tables before nftables 0.8.1)
- Flowtables (the fastpath network stack bypass)

Examples

- Simple ruleset for a workstation
- Simple ruleset for a server
- Simple ruleset for a home router
- Bridge filtering
- Multiple NATs using nftables maps
- Classic perimetral firewall example
- Port knocking example
- Classification to tc structure example
- Using configuration management systems (like puppet, ansible, etc)
- GeoIP matching

Development

Check Portal:DeveloperDocs - documentation for netfilter developers.

Some hints on the general development progress:

- List of updates since Linux kernel 3.13
- List of updates in the nft command line tool
- Supported features compared to {ip,ip6,eb,arp}tables
- List of available translations via iptables-translate tool

External links

Watch some videos:

- Watch Getting a grasp of nftables, thanks to NLUUG association for recording this.
- Watch The ultimate packet classifier for GNU/Linux, thanks to the FSFE for paying my trip to Barcelona and for recommending me as speaker to the KDE Spanish branch.
- Florian Westphal - Why nftables?
- Watch NLUUG - Goodbye iptables, Hello nftables

Watch videos to track updates:

- Watch Netdev 2.1 - Netfilter mini-workshop (2017)
- Watch Netdev 2.2 - Netfilter mini-workshop (2018)
- Watch Netdev 0x12 - Netfilter mini-workshop (2019)
- Watch Netdev 0x14 - Netfilter mini-Workshop (2020)

Additional documentations and articles:

- Tutorial Extending nftables by Xiang Gao
- Article New in Debian stable Stretch: nftables
- Article How to use nftables from python and git repository python-nftables-tutorial.git

Thanks

To the NLnet foundation for initial sponsorship of this HOWTO:

To Eric Leblond, for boostrapping the Nftables quick howto in 2013.