Linux Firewall

Linux workshop #2

Summary

- Introduction to firewalls
- Introduction to the linux firewall
- Basic rules
- Advanced rules
- Scripting
- Redundancy
- Extensions
- Distributions
- Links

Introduction to firewalls

What is a firewall ?

- A firewall is a device that acheives network security features. Generally it keeps an internal network secured by filtering, analyzing and blocking undesirable traffic.

Where is a firewall placed ?

- A firewall is placed between two or more networks, that have different purposes, levels of security, and access rules.

Stateless, stateful and application

- A stateless firewall is a simple firewall that evaluates packets against defined rules. It takes packets one by one. Can be bypassed.
- A stateful firewall monitors connections' state and is able to take decisions based on it.
- Application firewalls provides advanced features to examine payloads (DPI, IPS…)

Introduction to linux firewall

- **Linux Firewall :**
- **Netfilter:** packet filtering framework for linux kernel (> 2.4)
- **ip(6)tables:** userspace CLI tool used to configure filtering rulesets.

- **Other related tools**
- **arptables:** CLI tool used for arp packet filtering
- **ebtables:** ethernet bridging table firewall tool

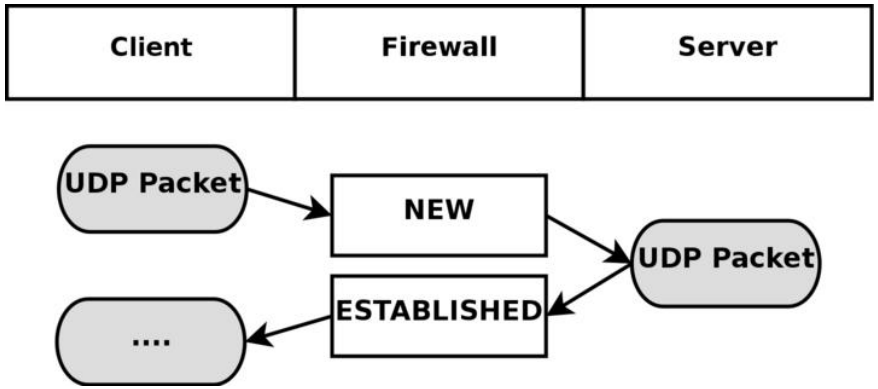
- http://www.netfilter.org/
- http://ebtables.sourceforge.net/

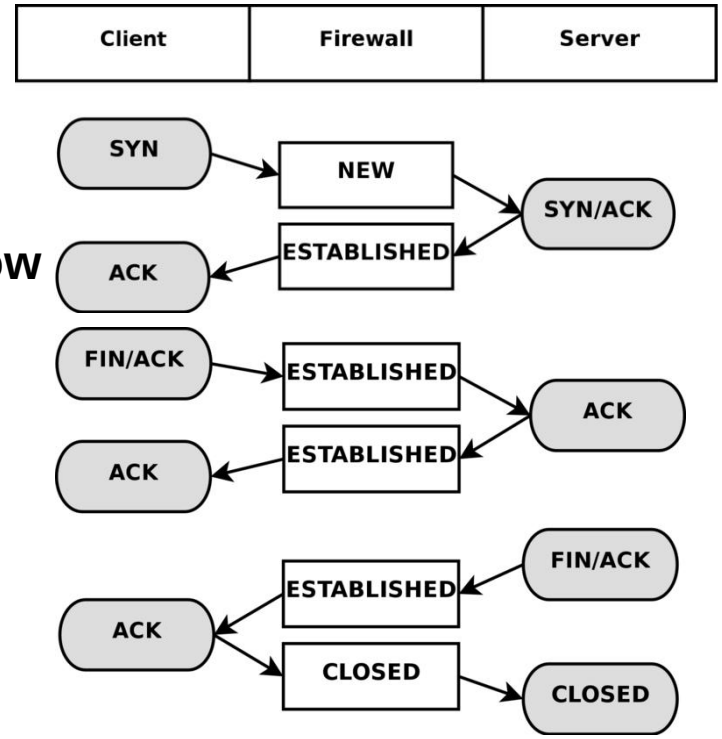
Introduction to linux firewall

<table>
<tr><th>OSI Layers</th><th>TCP/IP model</th><th>Linux</th><th>Actions</th></tr>
<tr><td>Physical</td><td rowspan="2">Network interface</td><td>Link + NIC</td><td>Check the data integrity, pass the information to the datalink layer</td></tr>
<tr><td>Datalink</td><td>Driver</td><td>Check if the frame is intended to this host with the MAC address</td></tr>
<tr><td>Network</td><td>Internet</td><td rowspan="2">Kernel TCP/IP stack (netfilter…)</td><td>Based on source/destination IP address, the packet is either routed or passed to the next layer</td></tr>
<tr><td>Transport</td><td>Transport</td><td>Based on the port the data are delivered to the right application</td></tr>
<tr><td>Session</td><td rowspan="3">Application</td><td rowspan="3">Applications</td><td rowspan="3">Applications</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Application</td></tr>
</table>

Introduction to linux firewall

- **TCP** connection tracking based on **states**
- Achieve with **conntrack** module.
- **UDP** connection tracking based on **time window**





- *Images iptables.info*

Introduction to linux firewall

Chains are categories:

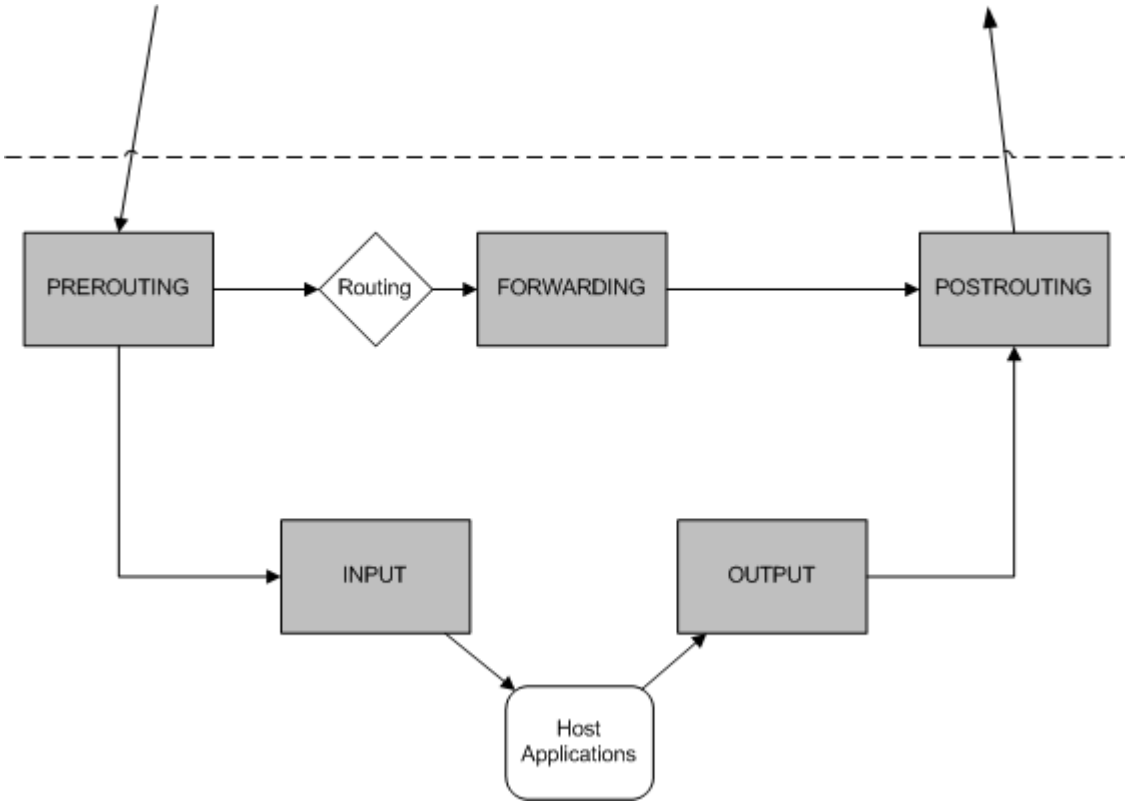
- **INPUT:** packet received and intended to the local host
- **OUTPUT:** packet sent by the host
- **PREROUTING:** packet received
- **FORWARD:** routing, forwarding packet from a network to another
- **POSTROUTING:** apply rules after the routing/forwarding decision

- `iptables –P INPUT DROP`
- `iptables –A INPUT –p tcp --dport 22 –j ACCEPT`

- It is possible to create **custom chains:**
- `iptables –N custom_chain`

Introduction to linux firewall

- **Chains** continued



Introduction to linux firewall

- Netfilter provide **connection tracking system** (conntrack, stateful firewalling)

- **States:**
- **NEW:** new connection, new session
- **ESTABLISHED:** established transport session (successfull SYN-SYN/ACK-ACK for TCP)
- **RELATED:** the session is related to another (e.g.: FTP)
- **INVALID:** session is invalid and does not match any of the previous cases.

- Other **TCP states**:
- SYN_SENT, SYN_RECV, FIN_WAIT, CLOSE_WAIT, LAST_ACK, TIME_WAIT, CLOSE

- `iptables –A INPUT –m state --state RELATED,ESTABLISHED –j ACCEPT`
- `iptables –A OUTPUT –m state --state RELATED,ESTABLISHED –j ACCEPT`
- `iptables –A FORWARD –m state --state RELATED,ESTABLISHED –j ACCEPT`

Introduction to linux firewall

- iptables store its information in… **tables** !

- Each table is dedicated to a specific use.
- Each of them contain can use a set of chains, and a set of targets.

- **FILTER:** filtering operations, the most common table.
- **NAT:** network address translation purposes. Only concerned by NEW state.
- **MANGLE:** advanced packet alteration operations
- **RAW:** used to prevent connection tracking

- `iptables –t filter –L -n`

Introduction to linux firewall

- In the netfilter terminology, actions are called TARGETS:
- There are terminating and non-terminating targets.

- **ACCEPT:** accept the packet
- **DROP:** drop the packet without notifying the source
- **REJECT:** drop the packet and notify the source with TCP RST (--reject-with-tcp-rst)
- **LOG:** event logging
- **DNAT:** used to change the destination IP/port (NAT)
- **SNAT:** used to change the source IP/port (NAT)
- **MASQUERADE:** used on gateways to setup NAT overloading

- Actions continued: TOS, TTL, RETURN, MARK, QUEUE/NFQUEUE, ULOG/NFLOG, MIRROR, REDIRECT

Introduction to linux firewall

- In a chain the **order of the statements is important**.
- The first to match will be taken in account
- Consequently, be sure to set the **most precise statements first.**
- SSH connection accepted:
- `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`
- `iptables -A INPUT -p tcp -j DROP`
- SSH connection denied
- `iptables -A INPUT -p tcp -j DROP`
- `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`

Introduction to linux firewall

- Delete a rule
- `iptables -D INPUT –p tcp –s 1.2.3.4 --dport 22 –j ACCEPT`
- `iptables –D INPUT 1`

- Flush all chains / a chain
- `iptables –F`
- `iptables –t INPUT –F`

- Delete a chain
- `iptables –t INPUT –X`

Basic Rules

- **Define policy actions**
- `iptables -P INPUT DROP`
- `iptables -P OUTPUT DROP`
- `iptables -P FORWARD DROP`

- **Open a port**
- `iptables -A INPUT -p tcp -s 1.2.3.4 --dport 22 -j ACCEPT`
- `iptables -A OUTPUT -p tcp -d 1.2.3.4 --dport 22 -j ACCEPT`

- **Accept ESTABLISHED and RELATED sessions**
- `iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT`
- `iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT`

Advanced rules

- **Rate limit**
- `iptables -A INPUT –p TCP --syn -m limit --limit 5/second -j ACCEPT`
- `iptables -A INPUT -s 1.2.3.4 -m limit --limit 1/minute –j LOG`

- **Logging**
- `iptables -N LOGCHAIN`
- `iptables -A LOGCHAIN -j LOG --log-prefix "fwlog:"`
- `iptables -A LOGCHAIN -j DROP`

- **Blacklist**
- `iptables -N blacklist`
- `iptables -A blacklist -s 10.0.0.0/8 -j DROP`
- `iptables -A INPUT -j blacklist`
- `iptables -A OUTPUT -j blacklist`
- `iptables -A FORWARD -j blacklist`

Advanced rules cont'd

- **Dynamic NAT overload** (eth0 external)
- `iptables -t NAT -A POSTROUTING -o eth0 -j MASQUERADE`

- **IPv6 filtering**
- `ip6tables –P INPUT –j DROP`
- `ip6tables –P OUTPUT –j DROP`
- `ip6tables –P FORWARD –j DROP`
- `ip6tables –A INPUT –p icmpv6 --icmpv6-type 136/0 –j DROP`
- `ip6tables –A OUTPUT –p icmpv6 --icmpv6-type 136/0 –j DROP`

- **Quality of Service**
- `iptables -t MANGLE -A PREROUTING -p tcp -m tcp --sport 3389 -j MARK --set-mark 0xe`
- `iptables -t MANGLE -A PREROUTING -p tcp -m tcp --sport 3389 -j RETURN`
- `iptables -t MANGLE -A PREROUTING -j MARK --set-mark 0x6`

Troubleshooting commands

- Show all current rules
- `iptables –L –n`
- `iptables –L`

- Show all current rules in the CLI format
- `iptables --list-rules`

- Netfiler loaded module
- `lsmod | grep nf`

- Connection information (conntrack package)
- `conntrack –L`
- `conntrack -E`

Scripting

- Necessity to script iptables to be **reboot persistent**
- Bash script (Bourne again shell)
- Start / Stop actions
- **LSB tags**
- Placed in /etc/init.d/
- `touch /etc/init.d/firewall.sh`
- `chmod a+x /etc/init.d/firewall.sh`

Scripting

- Write down all your iptables rules
- `# Clear everything`
- `iptables -t filter -F`
- `# Deny all`
- `iptables -t filter -P INPUT DROP`
- `iptables -t filter -P FORWARD DROP`
- `iptables -t filter -P OUTPUT DROP`
- `# Allow ICMP`
- `iptables -t filter -A INPUT -p icmp -j ACCEPT`
- `iptables -t filter -A OUTPUT -p icmp -j ACCEPT`
- `# Allow SSH`
- `iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT`
- `iptables -t filter -A OUTPUT -p tcp --dport 22 -j ACCEPT`
- `# Connections`
- `iptables –A INPUT –m state --state RELATED,ESTABLISHED –j ACCEPT`
- `iptables –A OUTPUT –m state --state RELATED,ESTABLISHED –j ACCEPT`

Scripting cont'd

- Add some code to implement **actions**

```
case $1 in
start)
## PUT RULES HERE##
;;
stop)
# Clear everything and allow all
iptables -t filter -F
iptables -t filter -P INPUT ACCEPT
iptables -t filter -P FORWARD ACCEPT
iptables -t filter -P OUTPUT ACCEPT
;;
esac
```

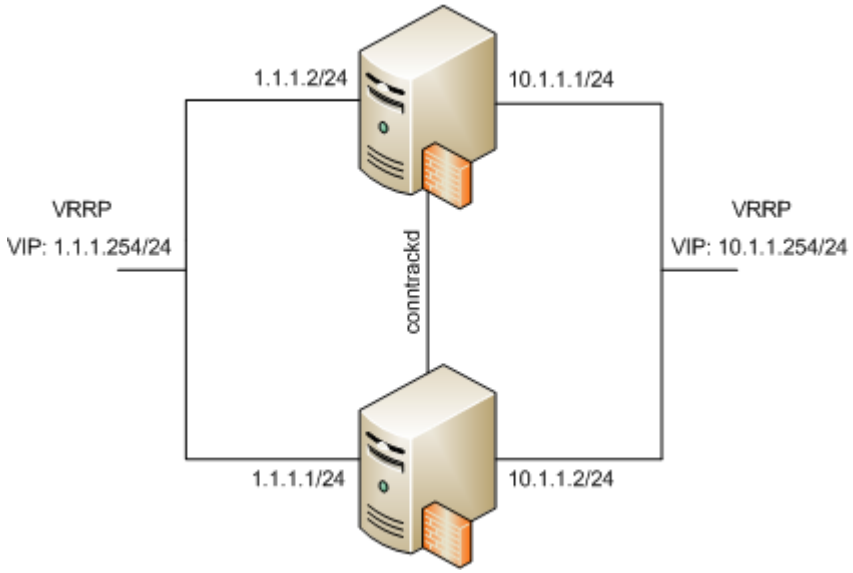
Scripting cont'd

- Install the script to start during the OS boot sequence
- `#!/bin/sh`
- `### BEGIN INIT INFO`
- `# Provides: firewall.sh`
- `# Required-Start:`
- `# X-Start-Before:`
- `# Default-Start: 2 3 4 5`
- `# Required-Stop:`
- `# Default-Stop: 0 1 6`
- `# Short-Description: Start the ip(6)tables firewall.`
- `# Description: Start the ip(6)tables firewall.`
- `### END INIT INFO`

- `update-rc.d firewall.sh remove`
- `update-rc.d firewall.sh defaults`

Redundancy

- Two things needed :
- A **redundancy mechanism** (VRRP, keepalive)
- A **state table synchronization** system (conntrackd)



Extensions

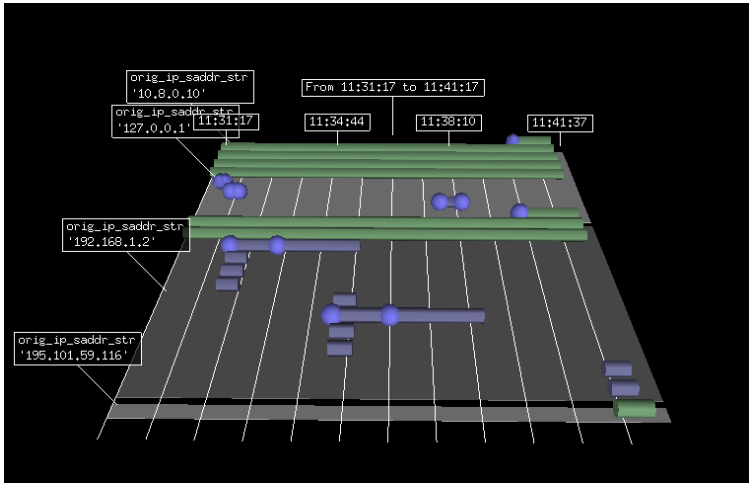
- Advanced logging with Ulogd2 + PostgreSQL + nf3d
- http://2009.rmll.info/IMG/pdf/ulogd2-2.pdf

- Nulog web interface

- NuFW identity based firewall

- L7 filter enables application level firewall
- http://l7-filter.sourceforge.net/

- Advanced manipulations with Nfqueue libraries



Firewall oriented distributions

Software and physical appliances:

- IPcop
- Astaro security (acquired by Sophos)
- Shorewall
- NuFW
- EdenWall
- Exosec
- …

Questions

?

Linux firewall experts

- No more afraid of iptables
- No more afraid of a large number of rules
- No more afraid of redundancy
- **Just more pratical works before becoming linux firewall experts!**

Links

Netfilter/ IPtables:

- http://www.netfilter.org/
- http://ipset.netfilter.org/iptables.man.html
- http://doc.ubuntu-fr.org/iptables
- https://help.ubuntu.com/community/IptablesHowTo
- http://centoshelp.org/networking/iptables-advanced/
- http://linuxgazette.net/108/odonovan.html
- http://www.techrepublic.com/article/utilizing-the-advanced-firewall-techniques-in-iptables/1031075
- https://home.regit.org/ (Eric Leblond)
- http://2008.rmll.info/IMG/pdf/rmll-2008.pdf (Pablo Neira Ayuso)
- http://www.lartc.org/howto/

Thank you