Configuring a Linux Firewall

Courtney Hagen

W0263284

ISEC2700

Table of Contents

[Introduction 3](#_Toc5186476)

[Task 1 – Creating iptables rules manually 3](#_Toc5186477)

[Initial Iptables Output 3](#_Toc5186478)

[Iptables Output after Settings Changes 3](#_Toc5186479)

[Task 2 – Uncomplicated Firewall (UFW) 4](#_Toc5186480)

[Iptables Output before UFW 4](#_Toc5186481)

[Iptables Output after UFW 4](#_Toc5186482)

[Iptables Output after Services 8](#_Toc5186483)

[Question 5 12](#_Toc5186484)

[References 13](#_Toc5186485)

# Introduction

The purpose of this document is to demonstrate my knowledge with configuring Linux firewalls using iptables.

# Task 1 – Creating iptables rules manually

## Initial Iptables Output

# Generated by iptables-save v1.6.1 on Tue Apr 2 21:37:56 2019

\*filter

:INPUT DROP [4:304]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [4:304]

COMMIT

# Completed on Tue Apr 2 21:37:56 2019

## Iptables Output after Settings Changes

# Generated by iptables-save v1.6.1 on Tue Apr 2 21:53:38 2019

\*filter

:INPUT DROP [8:736]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [8:736]

-A INPUT -i eth0 -p tcp -m tcp --dport 110 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A INPUT -i eth0 -p tcp -m tcp --dport 143 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A OUTPUT -o eth0 -p tcp -m tcp --sport 143 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

-A OUTPUT -o eth0 -p tcp -m tcp --sport 110 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT

COMMIT

# Completed on Tue Apr 2 21:53:38 2019

# Task 2 – Uncomplicated Firewall (UFW)

## Iptables Output before UFW

# Generated by iptables-save v1.6.1 on Wed Apr 3 07:57:16 2019

\*filter

:INPUT DROP [68:5855]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [56:5004]

COMMIT

# Completed on Wed Apr 3 07:57:16 2019

## Iptables Output after UFW

# Generated by iptables-save v1.6.1 on Wed Apr 3 08:05:48 2019

\*filter

:INPUT DROP [0:0]

:FORWARD DROP [0:0]

:OUTPUT ACCEPT [0:0]

:ufw-after-forward - [0:0]

:ufw-after-input - [0:0]

:ufw-after-logging-forward - [0:0]

:ufw-after-logging-input - [0:0]

:ufw-after-logging-output - [0:0]

:ufw-after-output - [0:0]

:ufw-before-forward - [0:0]

:ufw-before-input - [0:0]

:ufw-before-logging-forward - [0:0]

:ufw-before-logging-input - [0:0]

:ufw-before-logging-output - [0:0]

:ufw-before-output - [0:0]

:ufw-logging-allow - [0:0]

:ufw-logging-deny - [0:0]

:ufw-not-local - [0:0]

:ufw-reject-forward - [0:0]

:ufw-reject-input - [0:0]

:ufw-reject-output - [0:0]

:ufw-skip-to-policy-forward - [0:0]

:ufw-skip-to-policy-input - [0:0]

:ufw-skip-to-policy-output - [0:0]

:ufw-track-forward - [0:0]

:ufw-track-input - [0:0]

:ufw-track-output - [0:0]

:ufw-user-forward - [0:0]

:ufw-user-input - [0:0]

:ufw-user-limit - [0:0]

:ufw-user-limit-accept - [0:0]

:ufw-user-logging-forward - [0:0]

:ufw-user-logging-input - [0:0]

:ufw-user-logging-output - [0:0]

:ufw-user-output - [0:0]

-A INPUT -j ufw-before-logging-input

-A INPUT -j ufw-before-input

-A INPUT -j ufw-after-input

-A INPUT -j ufw-after-logging-input

-A INPUT -j ufw-reject-input

-A INPUT -j ufw-track-input

-A FORWARD -j ufw-before-logging-forward

-A FORWARD -j ufw-before-forward

-A FORWARD -j ufw-after-forward

-A FORWARD -j ufw-after-logging-forward

-A FORWARD -j ufw-reject-forward

-A FORWARD -j ufw-track-forward

-A OUTPUT -j ufw-before-logging-output

-A OUTPUT -j ufw-before-output

-A OUTPUT -j ufw-after-output

-A OUTPUT -j ufw-after-logging-output

-A OUTPUT -j ufw-reject-output

-A OUTPUT -j ufw-track-output

-A ufw-after-input -p udp -m udp --dport 137 -j ufw-skip-to-policy-input

-A ufw-after-input -p udp -m udp --dport 138 -j ufw-skip-to-policy-input

-A ufw-after-input -p tcp -m tcp --dport 139 -j ufw-skip-to-policy-input

-A ufw-after-input -p tcp -m tcp --dport 445 -j ufw-skip-to-policy-input

-A ufw-after-input -p udp -m udp --dport 67 -j ufw-skip-to-policy-input

-A ufw-after-input -p udp -m udp --dport 68 -j ufw-skip-to-policy-input

-A ufw-after-input -m addrtype --dst-type BROADCAST -j ufw-skip-to-policy-input

-A ufw-after-logging-forward -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK] "

-A ufw-after-logging-input -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK] "

-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 3 -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 4 -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 11 -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 12 -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 8 -j ACCEPT

-A ufw-before-forward -j ufw-user-forward

-A ufw-before-input -i lo -j ACCEPT

-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny

-A ufw-before-input -m conntrack --ctstate INVALID -j DROP

-A ufw-before-input -p icmp -m icmp --icmp-type 3 -j ACCEPT

-A ufw-before-input -p icmp -m icmp --icmp-type 4 -j ACCEPT

-A ufw-before-input -p icmp -m icmp --icmp-type 11 -j ACCEPT

-A ufw-before-input -p icmp -m icmp --icmp-type 12 -j ACCEPT

-A ufw-before-input -p icmp -m icmp --icmp-type 8 -j ACCEPT

-A ufw-before-input -p udp -m udp --sport 67 --dport 68 -j ACCEPT

-A ufw-before-input -j ufw-not-local

-A ufw-before-input -d 224.0.0.251/32 -p udp -m udp --dport 5353 -j ACCEPT

-A ufw-before-input -d 239.255.255.250/32 -p udp -m udp --dport 1900 -j ACCEPT

-A ufw-before-input -j ufw-user-input

-A ufw-before-output -o lo -j ACCEPT

-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

-A ufw-before-output -j ufw-user-output

-A ufw-logging-allow -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW ALLOW] "

-A ufw-logging-deny -m conntrack --ctstate INVALID -m limit --limit 3/min --limit-burst 10 -j RETURN

-A ufw-logging-deny -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK] "

-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN

-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN

-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN

-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny

-A ufw-not-local -j DROP

-A ufw-skip-to-policy-forward -j DROP

-A ufw-skip-to-policy-input -j DROP

-A ufw-skip-to-policy-output -j ACCEPT

-A ufw-track-output -p tcp -m conntrack --ctstate NEW -j ACCEPT

-A ufw-track-output -p udp -m conntrack --ctstate NEW -j ACCEPT

-A ufw-user-limit -m limit --limit 3/min -j LOG --log-prefix "[UFW LIMIT BLOCK] "

-A ufw-user-limit -j REJECT --reject-with icmp-port-unreachable

-A ufw-user-limit-accept -j ACCEPT

COMMIT

# Completed on Wed Apr 3 08:05:48 2019

## Iptables Output after Services

# Generated by iptables-save v1.6.1 on Wed Apr 3 08:04:05 2019

\*filter

:INPUT DROP [0:0]

:FORWARD DROP [0:0]

:OUTPUT ACCEPT [0:0]

:ufw-after-forward - [0:0]

:ufw-after-input - [0:0]

:ufw-after-logging-forward - [0:0]

:ufw-after-logging-input - [0:0]

:ufw-after-logging-output - [0:0]

:ufw-after-output - [0:0]

:ufw-before-forward - [0:0]

:ufw-before-input - [0:0]

:ufw-before-logging-forward - [0:0]

:ufw-before-logging-input - [0:0]

:ufw-before-logging-output - [0:0]

:ufw-before-output - [0:0]

:ufw-logging-allow - [0:0]

:ufw-logging-deny - [0:0]

:ufw-not-local - [0:0]

:ufw-reject-forward - [0:0]

:ufw-reject-input - [0:0]

:ufw-reject-output - [0:0]

:ufw-skip-to-policy-forward - [0:0]

:ufw-skip-to-policy-input - [0:0]

:ufw-skip-to-policy-output - [0:0]

:ufw-track-forward - [0:0]

:ufw-track-input - [0:0]

:ufw-track-output - [0:0]

:ufw-user-forward - [0:0]

:ufw-user-input - [0:0]

:ufw-user-limit - [0:0]

:ufw-user-limit-accept - [0:0]

:ufw-user-logging-forward - [0:0]

:ufw-user-logging-input - [0:0]

:ufw-user-logging-output - [0:0]

:ufw-user-output - [0:0]

-A INPUT -j ufw-before-logging-input

-A INPUT -j ufw-before-input

-A INPUT -j ufw-after-input

-A INPUT -j ufw-after-logging-input

-A INPUT -j ufw-reject-input

-A INPUT -j ufw-track-input

-A FORWARD -j ufw-before-logging-forward

-A FORWARD -j ufw-before-forward

-A FORWARD -j ufw-after-forward

-A FORWARD -j ufw-after-logging-forward

-A FORWARD -j ufw-reject-forward

-A FORWARD -j ufw-track-forward

-A OUTPUT -j ufw-before-logging-output

-A OUTPUT -j ufw-before-output

-A OUTPUT -j ufw-after-output

-A OUTPUT -j ufw-after-logging-output

-A OUTPUT -j ufw-reject-output

-A OUTPUT -j ufw-track-output

-A ufw-after-input -p udp -m udp --dport 137 -j ufw-skip-to-policy-input

-A ufw-after-input -p udp -m udp --dport 138 -j ufw-skip-to-policy-input

-A ufw-after-input -p tcp -m tcp --dport 139 -j ufw-skip-to-policy-input

-A ufw-after-input -p tcp -m tcp --dport 445 -j ufw-skip-to-policy-input

-A ufw-after-input -p udp -m udp --dport 67 -j ufw-skip-to-policy-input

-A ufw-after-input -p udp -m udp --dport 68 -j ufw-skip-to-policy-input

-A ufw-after-input -m addrtype --dst-type BROADCAST -j ufw-skip-to-policy-input

-A ufw-after-logging-forward -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK] "

-A ufw-after-logging-input -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK] "

-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 3 -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 4 -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 11 -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 12 -j ACCEPT

-A ufw-before-forward -p icmp -m icmp --icmp-type 8 -j ACCEPT

-A ufw-before-forward -j ufw-user-forward

-A ufw-before-input -i lo -j ACCEPT

-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny

-A ufw-before-input -m conntrack --ctstate INVALID -j DROP

-A ufw-before-input -p icmp -m icmp --icmp-type 3 -j ACCEPT

-A ufw-before-input -p icmp -m icmp --icmp-type 4 -j ACCEPT

-A ufw-before-input -p icmp -m icmp --icmp-type 11 -j ACCEPT

-A ufw-before-input -p icmp -m icmp --icmp-type 12 -j ACCEPT

-A ufw-before-input -p icmp -m icmp --icmp-type 8 -j ACCEPT

-A ufw-before-input -p udp -m udp --sport 67 --dport 68 -j ACCEPT

-A ufw-before-input -j ufw-not-local

-A ufw-before-input -d 224.0.0.251/32 -p udp -m udp --dport 5353 -j ACCEPT

-A ufw-before-input -d 239.255.255.250/32 -p udp -m udp --dport 1900 -j ACCEPT

-A ufw-before-input -j ufw-user-input

-A ufw-before-output -o lo -j ACCEPT

-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

-A ufw-before-output -j ufw-user-output

-A ufw-logging-allow -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW ALLOW] "

-A ufw-logging-deny -m conntrack --ctstate INVALID -m limit --limit 3/min --limit-burst 10 -j RETURN

-A ufw-logging-deny -m limit --limit 3/min --limit-burst 10 -j LOG --log-prefix "[UFW BLOCK] "

-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN

-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN

-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN

-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny

-A ufw-not-local -j DROP

-A ufw-skip-to-policy-forward -j DROP

-A ufw-skip-to-policy-input -j DROP

-A ufw-skip-to-policy-output -j ACCEPT

-A ufw-track-output -p tcp -m conntrack --ctstate NEW -j ACCEPT

-A ufw-track-output -p udp -m conntrack --ctstate NEW -j ACCEPT

-A ufw-user-input -p tcp -m tcp --dport 110 -j ACCEPT

-A ufw-user-input -p udp -m udp --dport 110 -j ACCEPT

-A ufw-user-input -p tcp -m tcp --dport 993 -j ACCEPT

-A ufw-user-input -p udp -m udp --dport 993 -j ACCEPT

-A ufw-user-limit -m limit --limit 3/min -j LOG --log-prefix "[UFW LIMIT BLOCK] "

-A ufw-user-limit -j REJECT --reject-with icmp-port-unreachable

-A ufw-user-limit-accept -j ACCEPT

COMMIT

# Completed on Wed Apr 3 08:04:05 2019

## Question 5

UFW holds the relationship between services and their rules in the /etc/services folder. That way, you could theoretically just type in the service and it would know what to do in terms of allowing or denying this service. (An Introduction to Uncomplicated Firewall (UFW), 2015)

# References

An Introduction to Uncomplicated Firewall (UFW). (2015, October 30). Retrieved April 3, 2019, from https://www.linux.com/learn/introduction-uncomplicated-firewall-ufw