November 27th 2019 – Realdolmen

What’s all about?

horse feed manufacturer

- A hacker is targeting a small fast-growing company as easy prey.

- The hacker will go through the company’s defense and compromise CEO laptop

- The CSO enables protection using Fortinet Solutions and observe results

- The hacker will try again

Workshop flow

- Five use cases

Hacking >>>>> Protection >>>>> Hacking

- We explain and do each use case, then you will do it yourself
- First use case
  - Is a three step exercise
  - We will guide you through, step by step

- Other use cases
  - You will do the three steps on your own

Cast and Roles

?

Who will be Who

Karen

Bill Hacker
THE HACKER

Yasmine

John Boss
THE CEO OF THE COMPANY:
“TheCompany”

Stijn

Peter Geek
THE CSO OF THE COMPANY

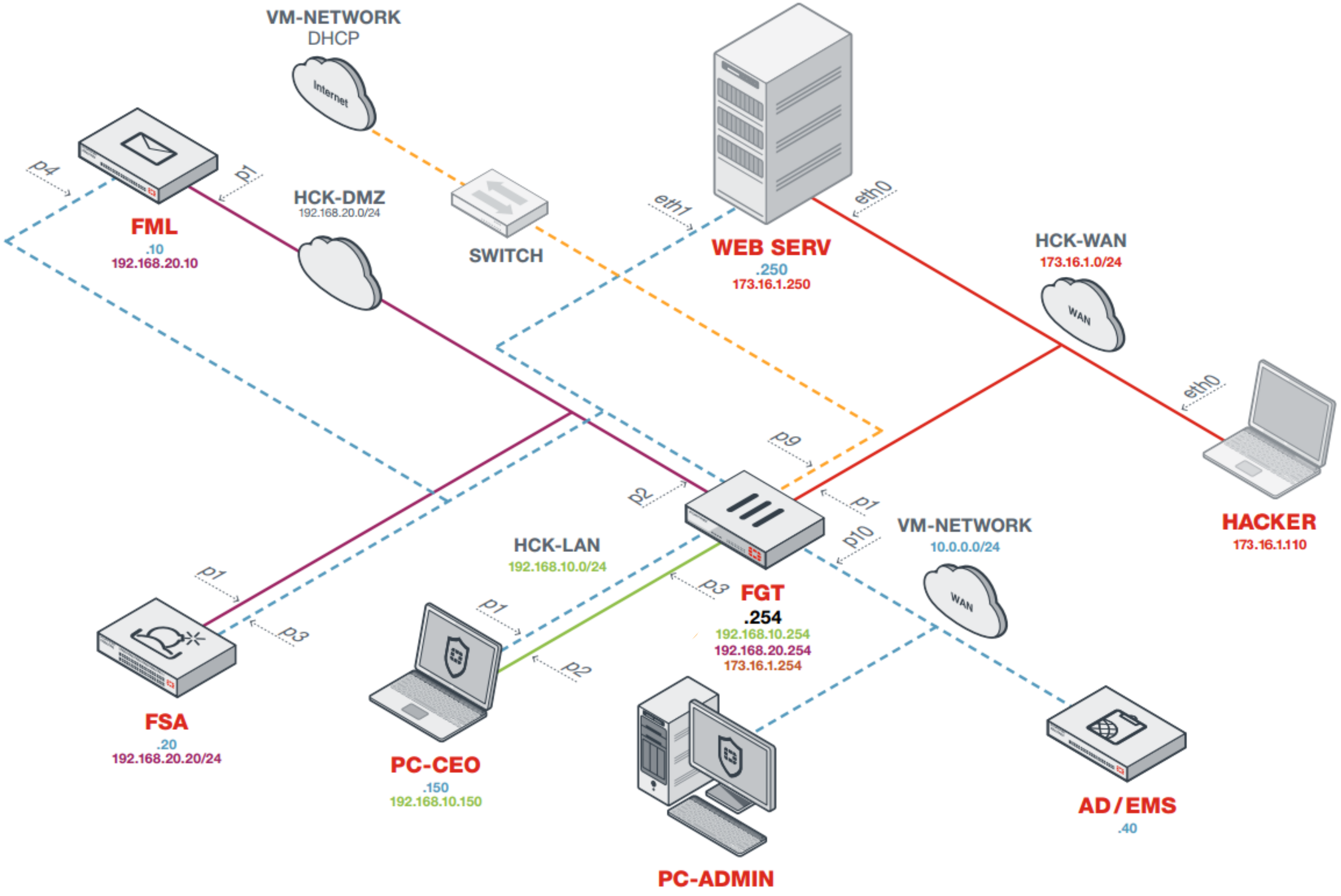
Peter

SPEAKER

Sam WebDesign
THE WEB DESIGNER

Roger Friend
A FRIEND OF THE CEO

Architecture



Connect to the Lab

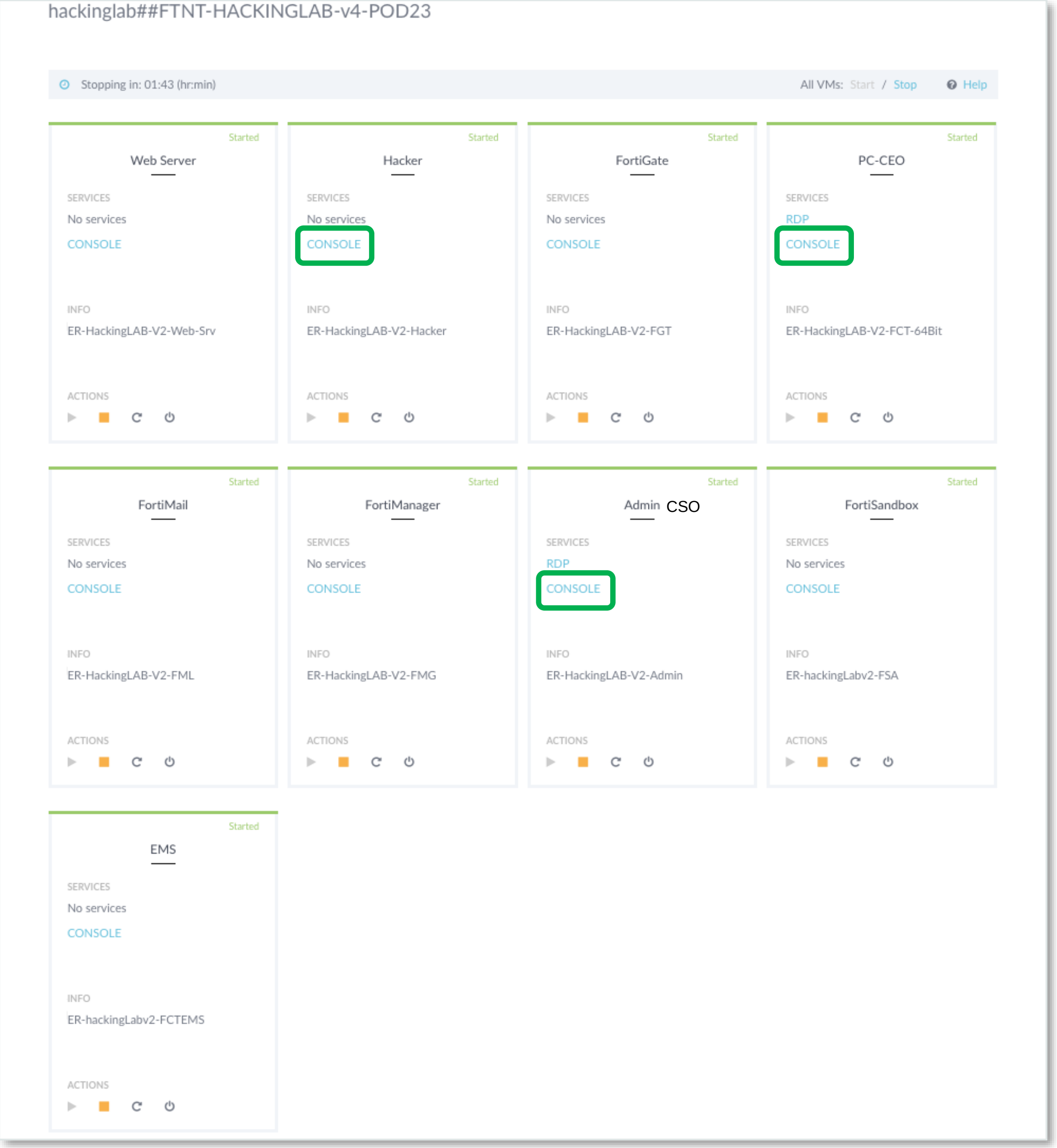
- Connect to GUEST

- URLs:
  - » http://tinyurl.com/......

- Wait for us when you are connected

- We will guide you step by step

Ravello Landing Page



hackinglab##FTNT-HACKINGLAB-v4-POD23

Stopping in: 01:43 (hr:min)

All VMs: Start / Stop

Help

Web Server (Started)

SERVICES
No services
CONSOLE

INFO
ER-HackingLAB-V2-Web-Srv

ACTIONS

Hacker (Started)

SERVICES
No services
CONSOLE

INFO
ER-HackingLAB-V2-Hacker

ACTIONS

FortiGate (Started)

SERVICES
No services
CONSOLE

INFO
ER-HackingLAB-V2-FGT

ACTIONS

PC-CEO (Started)

SERVICES
RDP
CONSOLE

INFO
ER-HackingLAB-V2-FCT-64Bit

ACTIONS

FortiMail (Started)

SERVICES
No services
CONSOLE

INFO
ER-HackingLAB-V2-FML

ACTIONS

FortiManager (Started)

SERVICES
No services
CONSOLE

INFO
ER-HackingLAB-V2-FMG

ACTIONS

Admin CSO (Started)

SERVICES
RDP
CONSOLE

INFO
ER-HackingLAB-V2-Admin

ACTIONS

FortiSandbox (Started)

SERVICES
No services
CONSOLE

INFO
ER-hackingLabv2-FSA

ACTIONS

EMS (Started)

SERVICES
No services
CONSOLE

INFO
ER-hackingLabv2-FCTEMS

ACTIONS

Usernames and Passwords

John Boss
THE CEO OF THE COMPANY:
“TheCompany”

Laptop: Boss / fortinet

Peter Geek
THE CSO OF THE COMPANY

FortiMail: admin / fortinet
FortiGate: admin / fortinet
EMS (10.0.0.10): admin / fortinet
FSA: admin / fortinet
Administrator / fortinet

Bill Hacker
THE HACKER

Laptop: root / fortinet
Web servers: fortinet / fortinet

Handout - Script instructions

- Step by step guide

Very important task

CSO glasses **on** > Busy with your exercise

CSO glasses **off** > Finished with your exercise

Use case 1

Protection with FortiGate

Chapter 1 – Hacking

- Hacker
  - Copy the website “Thecompany.com” to “Thecompany.net”
  - Fake the domain name from “Equi-declic” to “Equideclic”
  - Craft and send, as the Web developer, an email with the malicious link to “Thecompany.net” that will download a PDF and exploit an adobe vulnerability, download a virus giving access to the CEO’s laptop
- CEO
  - Receive the email, Clicks on the link

WAIT

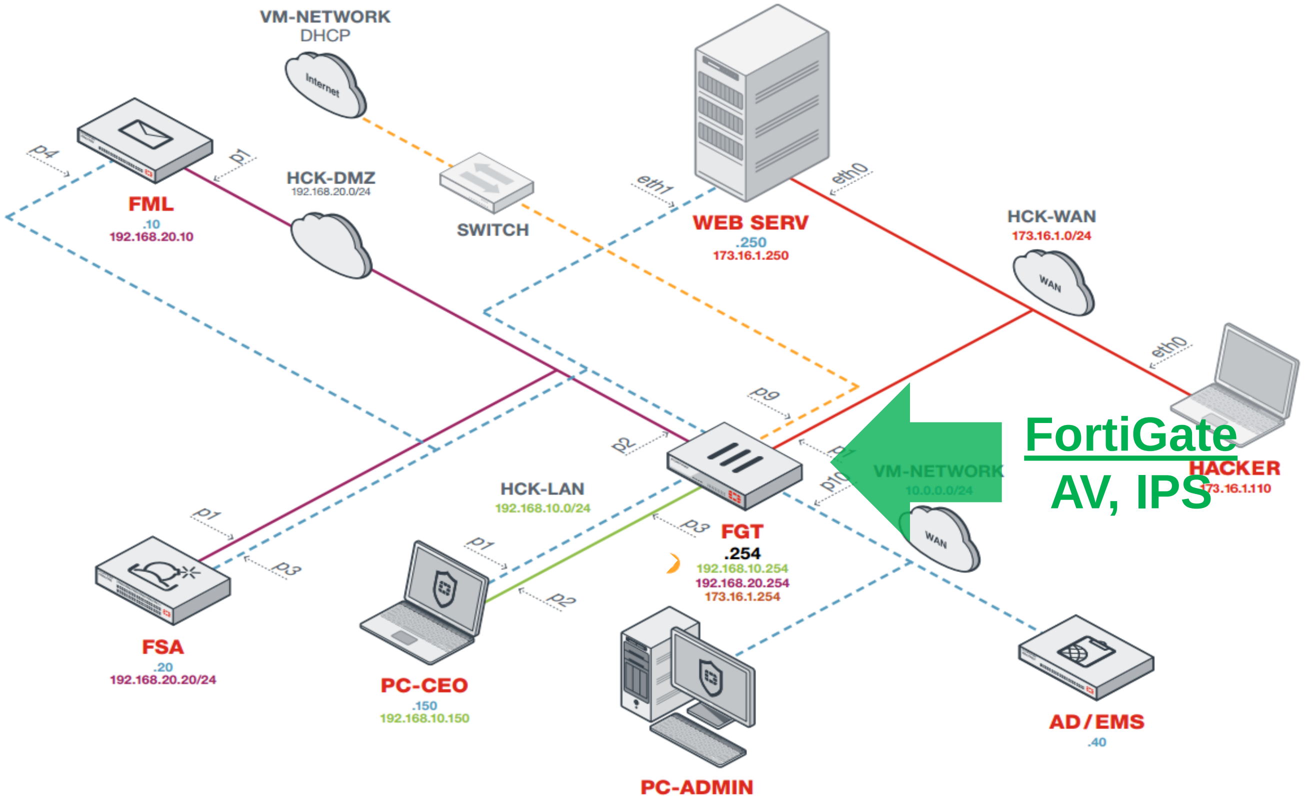
Chapter 2 – Hacking

- Hacker
  - » Can access CEO’s laptop
  - » Can do different tasks
  - » Installs a keylogger and collect login / password
  - » Access to the real website
  - » Reboots CEO’s laptop
- Result
  - » Full control of CEO’s laptop and website

Chapter 3 – Protection with Fortigate

- CSO
  - » Incident logs for IPS en AV
  - » IPS en AV protection using FortiGate

Solution



FortiGate
AV, IPS

WAIT

Chapter 4 – Protection with FortiGate

- Hacker
  - Send email again
- CEO
  - Read email
  - Click the link
- CSO
  - Analyze AV and IPS logs

From now on

- We will show the complete use case in one go

Never shutdown your systems

Use case 2

Protection with FortiMail

Chapter 5 - Hacking

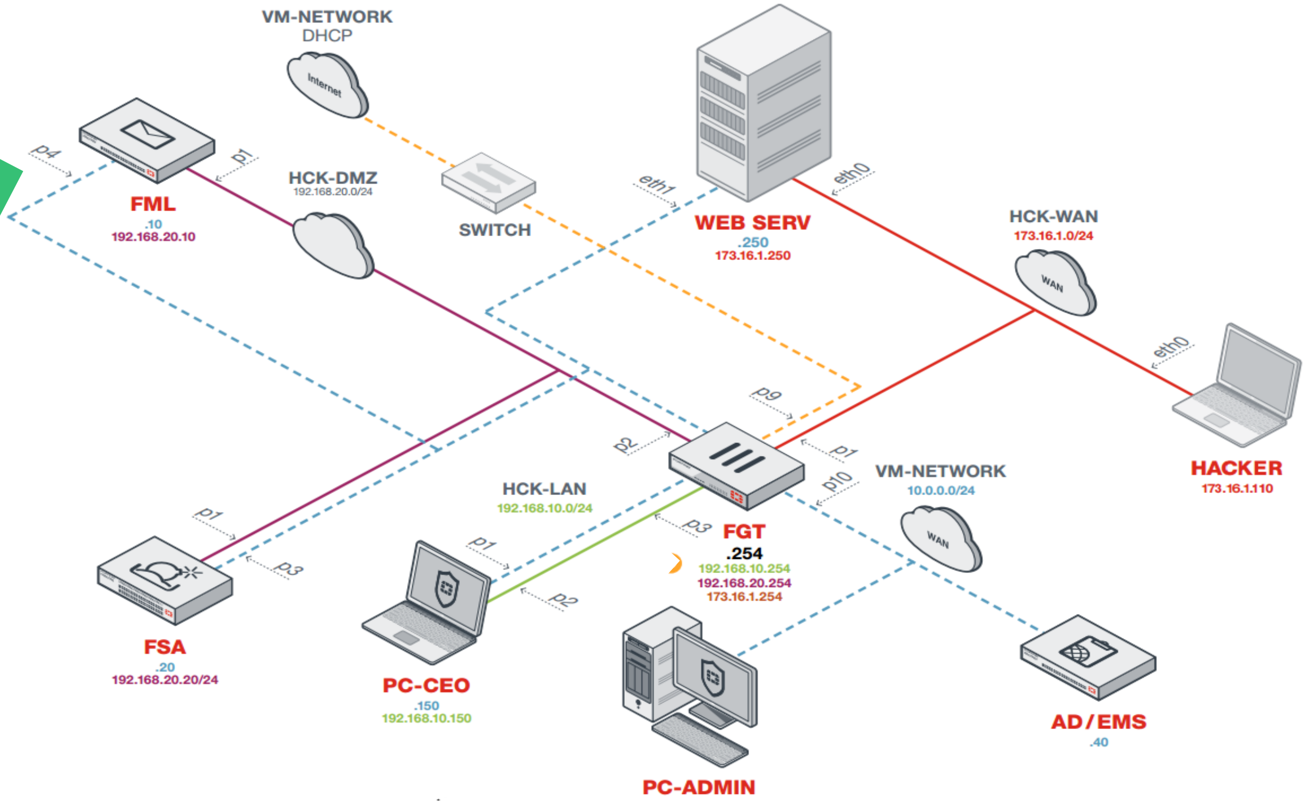
- Hacker
  - Discovers that some security is in place, but maybe not for encrypted traffic
  - Craft and send, acting as the Web developer, an encrypted email with an infected word document
  - Has again access to the CEO’s laptop via an encrypted communication link
- CEO
  - Read email, opens word document
  - Angry because reboot
- CSO
  - HTTPS and SMTPS connection logs with no inside details

Chapter 6 – Protection with Fortimail

- CSO
  - » Fortimail is the endpoint of the SMTPS session
  - » Enable AV profile on inbound traffic

Solution

FortiMail
AV, SMTPS



Chapter 7 – Protection with FortiMail

- Hacker
  - » Send again mail with word document again
- CEO
  - » Received email from web designer
  - » Attachment removed (on Fortimail)
- CSO
  - » Analyze the attack logs

Break

Use case 3

Protection with FortiMail and FortiSandbox

Chapter 8 - Hacking

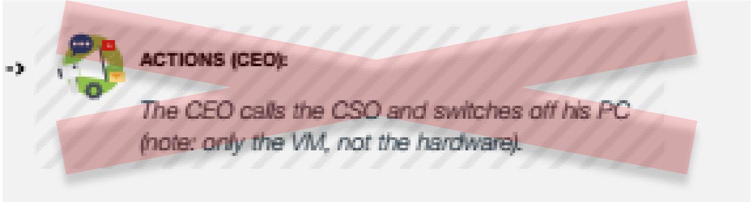
- Hacker
  - Modifies the 0 day JigSaw ransomware
  - Send this using email, simulating he is ‘Peter Geek’ asking the CEO to update his laptop
- CEO
  - Receives email from ‘Peter’
  - Again angry
  - Starts the update
  - Checks his pictures and they are locked
  - Locked out from his desktop
- CSO
  - No logs on FortiMail and FortiGate
  - Enable FortiSandbox integration FortiMail

Solution

Chapter 8 - Hacking

- Hacker
  - Modifies the 0 day JigSaw ransomware
  - Send this using email, simulating he is ‘Peter Geek’ asking the CEO to update his laptop
- CEO
  - Receives email from ‘Peter’
  - Again angry
  - Starts the update
  - Checks his pictures and they are locked
  - Locked out from his desktop
- CSO
  - No logs on FortiMail and FortiGate
  - Enable FortiSandbox integration FortiMail

DO NOT SHUTDOWN OR REBOOT THE CEO LAPTOP



~~ACTIONS (CEO):~~

~~The CEO calls the CSO and switches off his PC (note: only the VM, not the hardware).~~

Solution

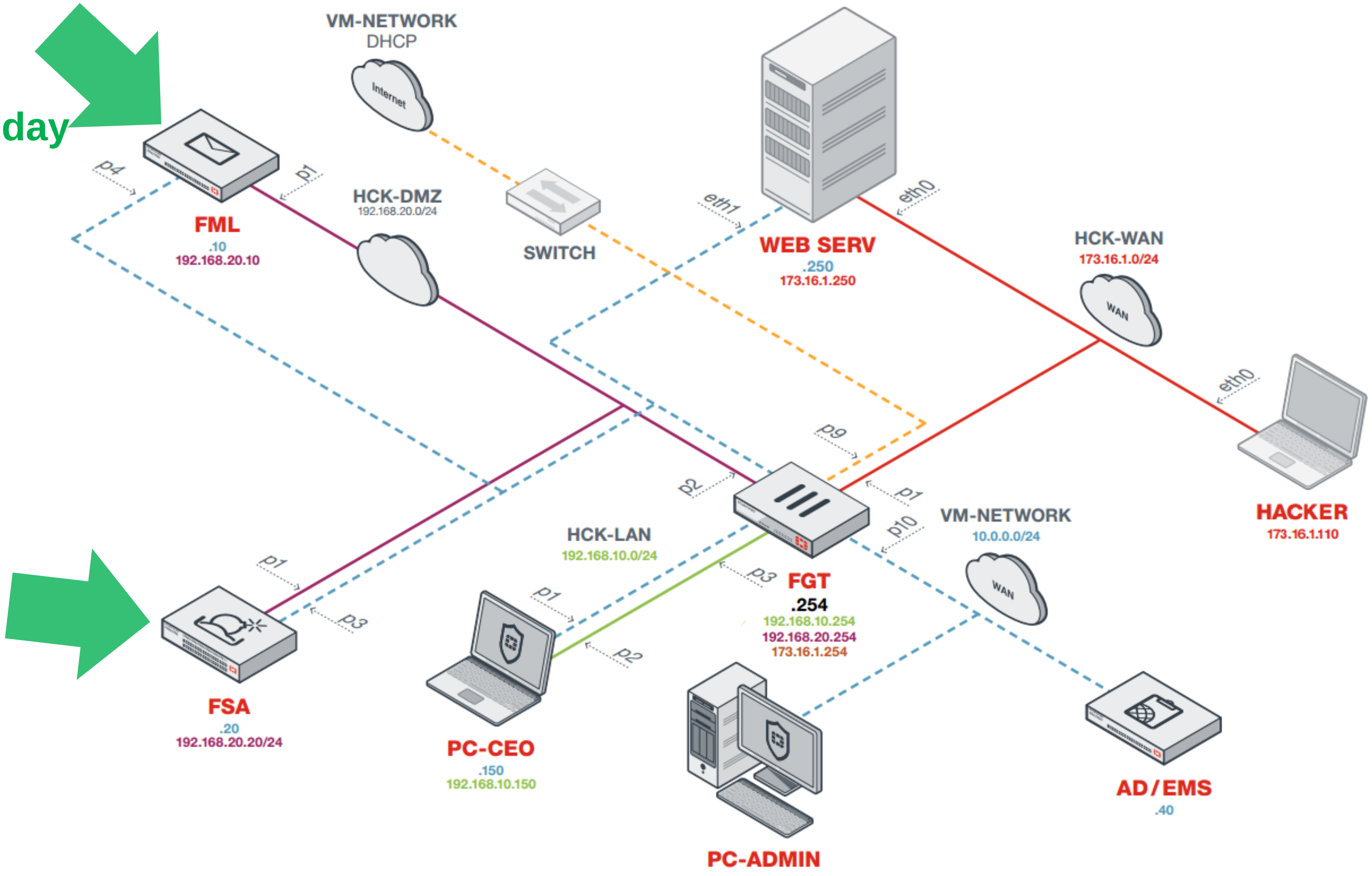
Start this exercise and wait when finished

WAIT

Security Fabric components

FortiMail
AV, SMTPS, 0day

FortiSandbox
0day



Chapter 9 – Protection with FortiMail and FortiSandbox

- Hacker
  - » Send mail again
- CSO
  - » Looks at events and queue in FortiMail
  - » He connects to the FortiSandbox and analyze the file scan results
- CEO
  - » Receive mail from ‘Peter Geek’ with a removed attachment

CEO needs to click again on Ravello link

WAIT

Chapter 9 – Protection with FortiMail and FortiSandbox

- Hacker
  - » Send mail again
- CSO
  - » Looks at events and queue in FortiMail
  - » He connects to the FortiSandbox and analyze the file scan results
- CEO
  - » Receive mail from ‘Peter Geek’ with a removed attachment

Use case 4

Protection with FortiClient

Chapter 10 - Hacking via personal email

- Hacker
  - Social networking activity
  - Friend is Roger Friend; sailing
  - Send a crafted game to the CEO personal email from ‘Roger Friend’
- CEO
  - Read mail
  - Saves attachment and execute it
- Hacker
  - Full control of CEO’s laptop
  - Reboot CEO’s laptop

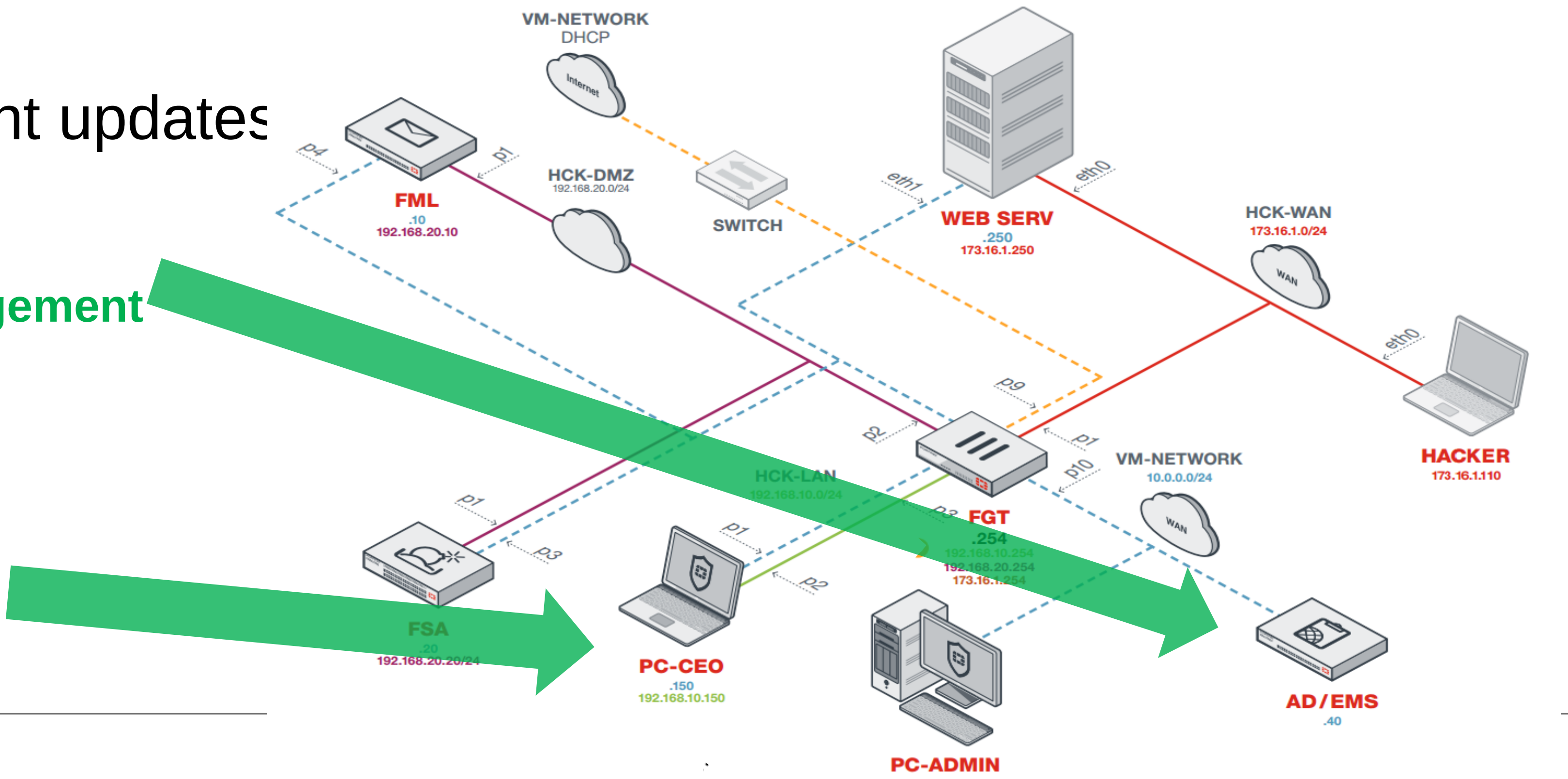
Chapter 11 - Protection with FortiClient

- CSO
  - » FortiGate IMAP session logs from private email
  - » Local law issue?
  - » Enable AV and FortiSandbox integration on FortiClient using EMS
- CEO
  - » Receives the FortiClient updates

Solution

EMS
FortiCient management

FortiClient
AV



Chapter 12 - Protection with FortiClient

- Hacker
  - » Send again the last email
- CEO
  - » Receives the email
  - » Blocked to virus detection by FortiClient
- CSO
  - » Alerts on FortiClient

WAIT

Chapter 12 - Protection with FortiClient

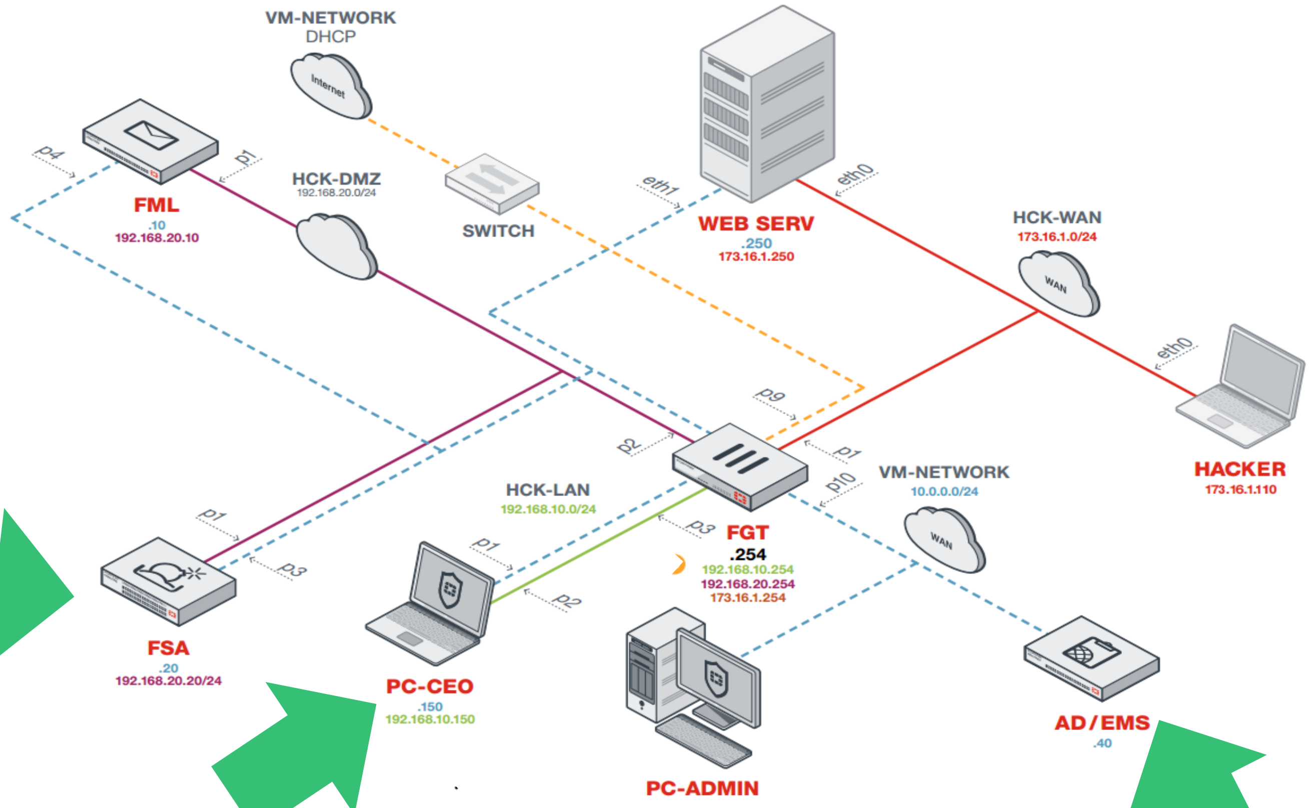
- Hacker
  - Send again the last email
- CEO
  - Receives the email
  - Blocked to virus detection by FortiClient
- CSO
  - Alerts on FortiClient

Use case 5

Protection with FortiClient and FortiSandbox

Chapter 13 - Protection with FortiClient and FortiSandbox

- Hacker
  - » Tries again with a 0 day virus using an email to the CEO personal email
- CEO
  - » Receives the email
  - » FortiClient detects the 0 day
- CSO
  - » Alert on FortiClient



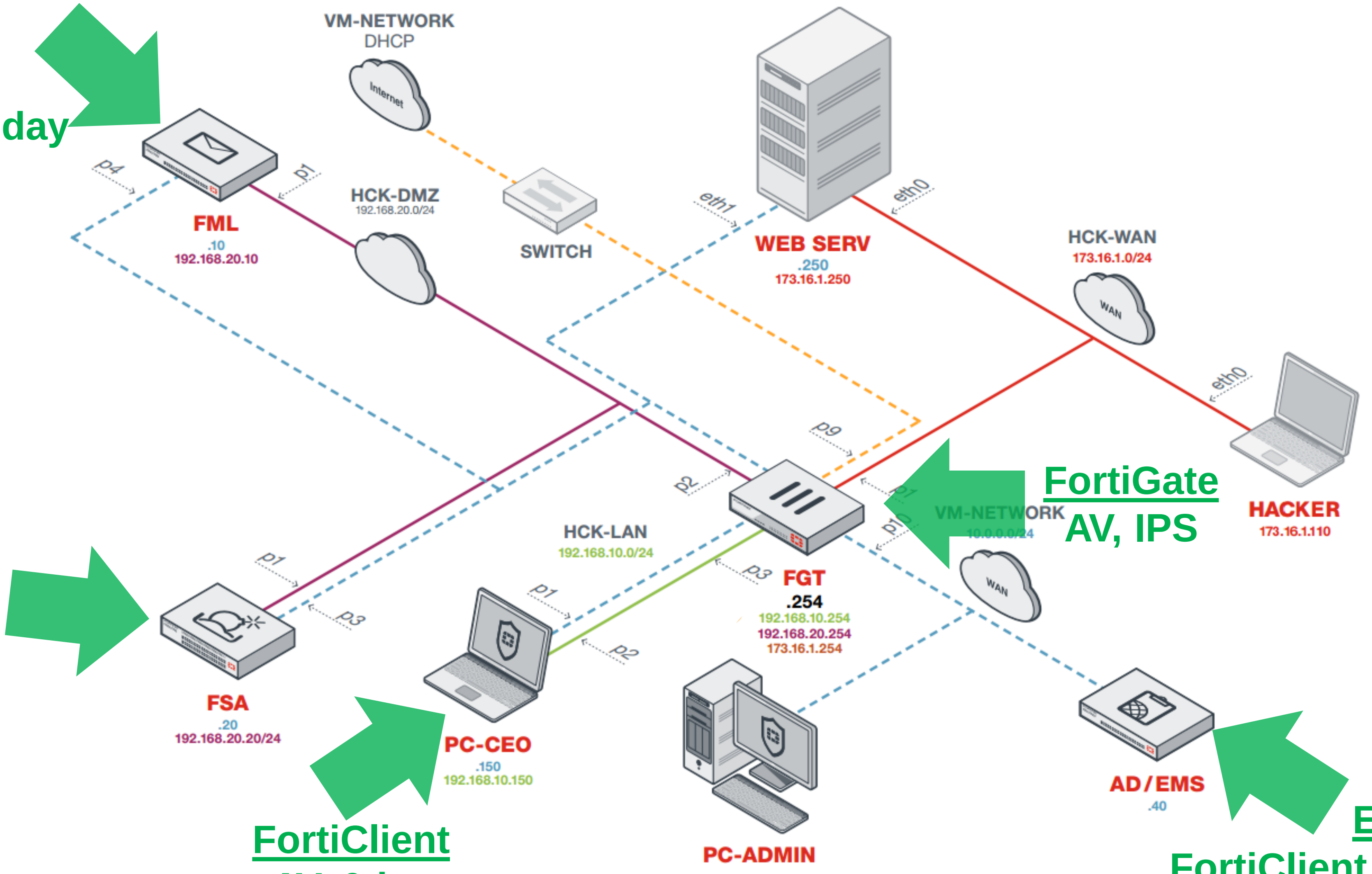
FortiSandbox
0day

FortiClient
AV, 0day

EMS
FortiClient management

WAIT

Security Fabric components



FortiMail
AV, SMTPS, 0day

FortiGate
AV, IPS

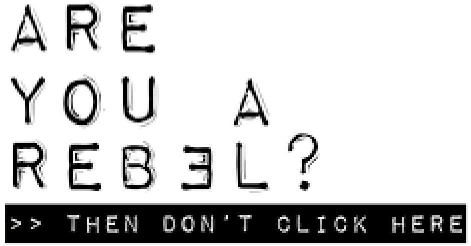
FortiSandbox
0day

FortiClient
AV, 0day

EMS
FortiClient management

What have we learned today?

- Hacker
  - » Frustrated hackers exist
  - » Blocked due to well protected company
- CEO
  - » Don’t click on everything
  - » User awareness
  - » Reserve budget
- CSO
  - » Learned that Fortinet has outstanding protection solutions



FORTINET
HACKING
LAB
DISCOVER
THE FORTINET SECURITY
FABRIC IN ACTION
You are invited!

Thank You