LESSONS FOR WHEN YOUR SAAS PROVIDER GOES OUT OF BUSINESS

Chris
Senior Security Engineer
Web Security Team

Raphi
Principal Systems Engineer
Crisis Lead

…and many more!

A ROUTINE THURSDAY MORNING…

2023-02-02T09:15:43+01:00

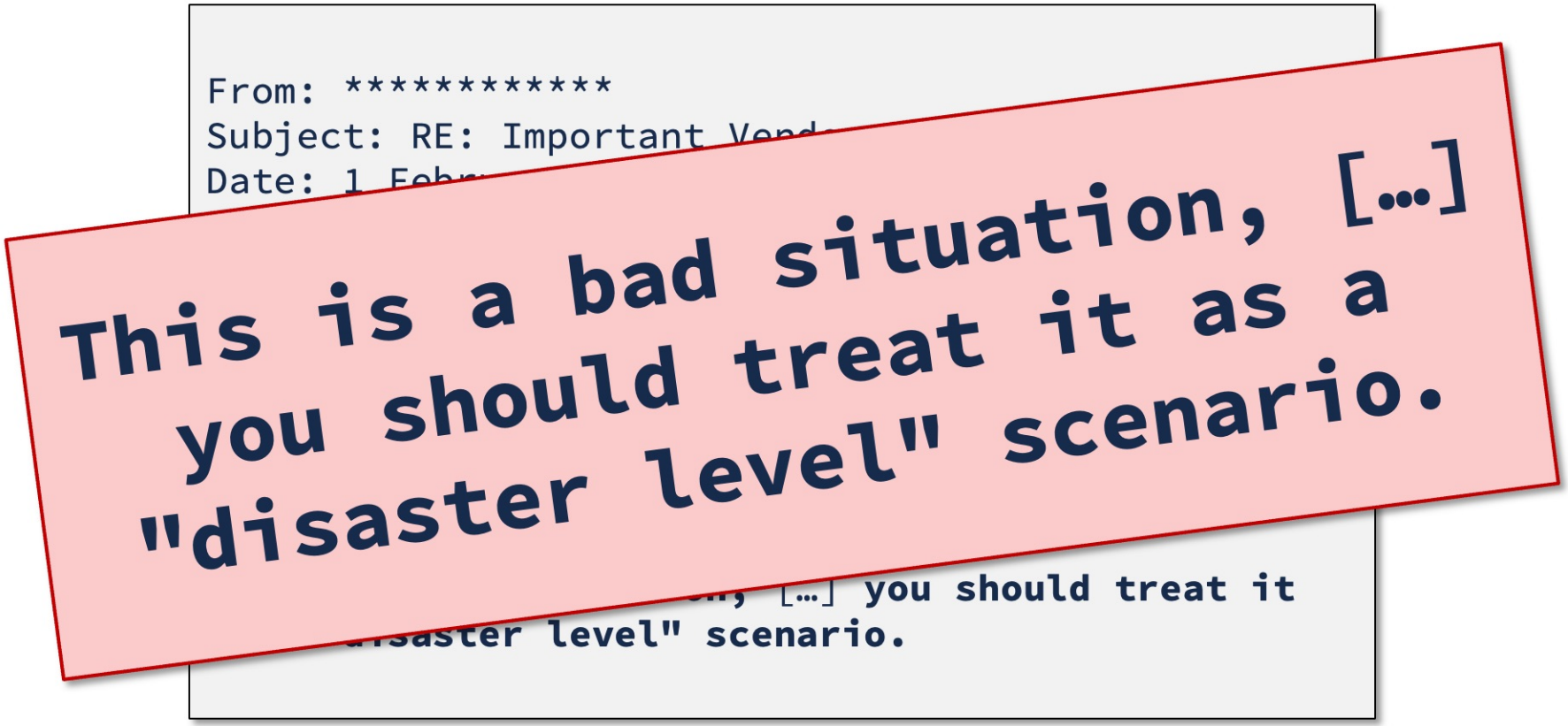
Hi Raphi,
I/we need an Incident Manager.
Don't disclose this yet.
HUGE disaster.

Product Manager

From: **********
Subject: RE: **Important Vendor Company Update**
Date: 1 February 2023 at 17:45:43 CET

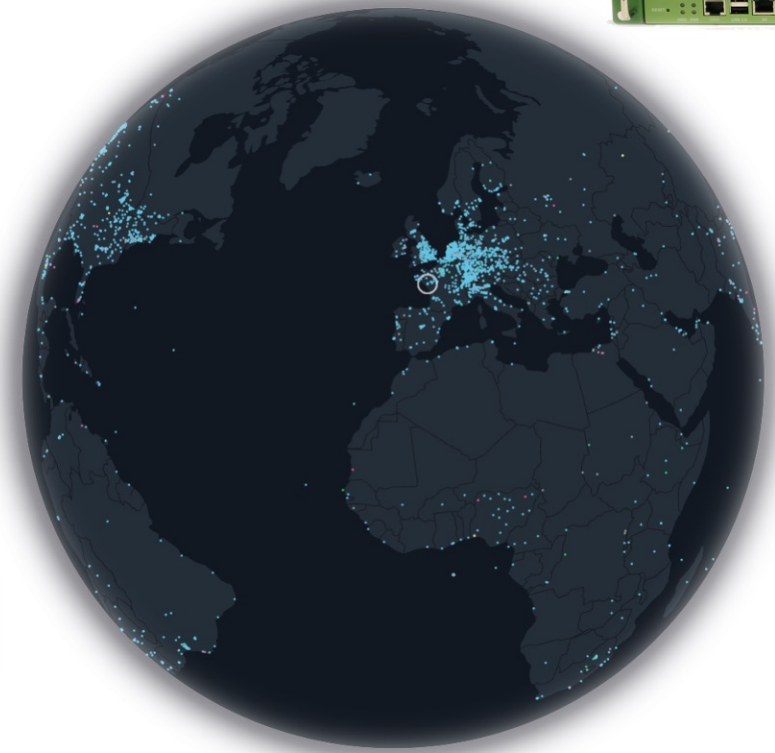
From the technical perspective, it means that the systems will continue working automatically, however there is **no personnel left** to attend to them if there is an issue. There is also no FP/FN processing or any other work that requires people. Effectively, we are running on borrowed time now.

This is a bad situation, […] **you should treat it as a "disaster level" scenario.**



OPEN SYSTEMS IN A NUTSHELL

1990
Open Systems founded in 🇨🇭

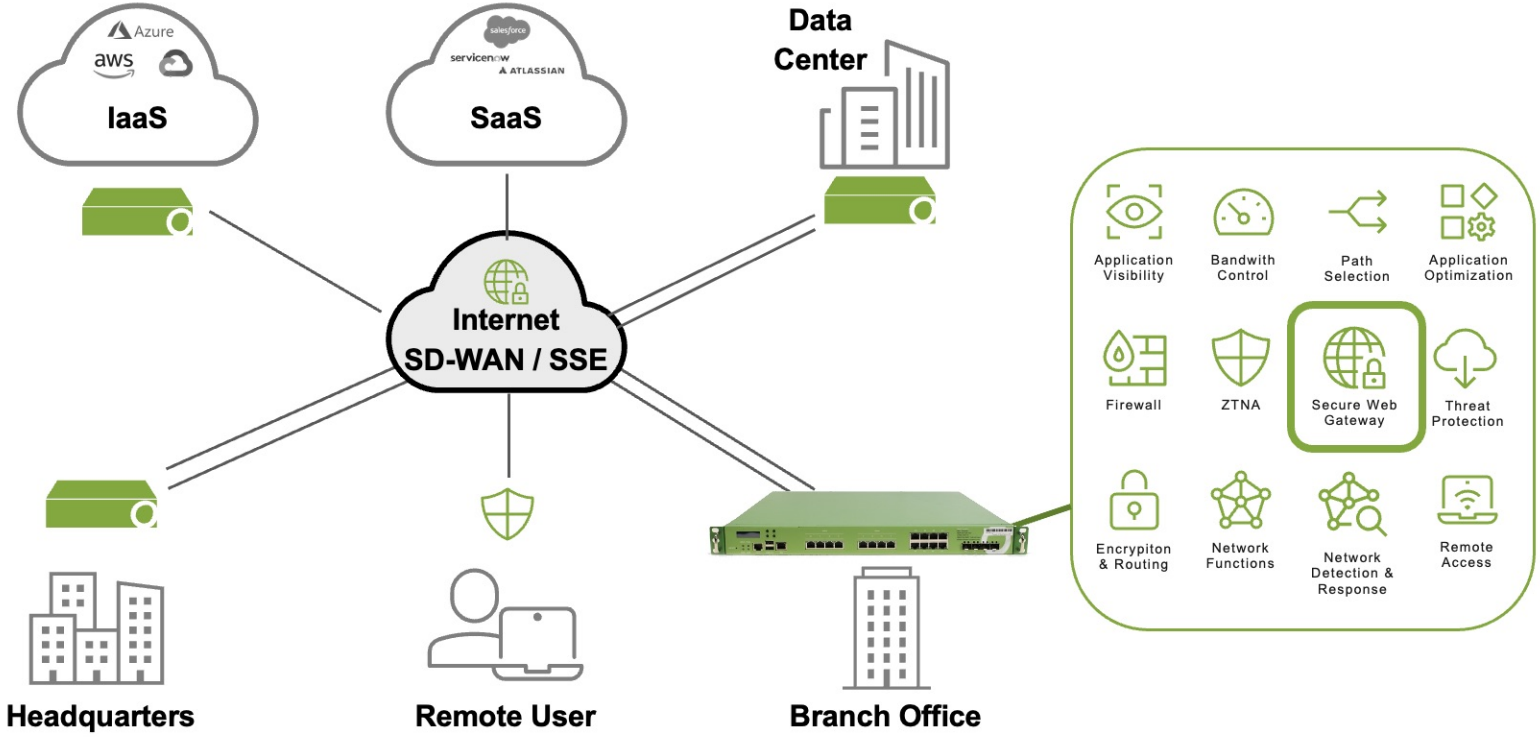


10K
Edge platforms

~250
Employees

180+
Countries

OPEN SYSTEMS CONNECTS AND SECURES USERS OF HYBRID ENVIRONMENTS, SEAMLESSLY, SIMPLY AND EFFICIENTLY, WHILE PROTECTING THEM FROM THREATS. 24x7. AROUND THE GLOBE.



MISSION CONTROL – 24x7 OPERATIONS

All engineers contributing part time!

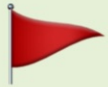
Get out of that
chaos phase!

BOOTSTRAP A COORDINATED WELL-LED RESPONSE

Self



Collaboration



Schedule 1st sitrep



Comprehend the problem & assess the situation

1. SUSTAIN OPERATIONS

1. COMMUNICATION

2. NEW SOLUTION

… AND ACTION – FIRST SITUATION REPORT

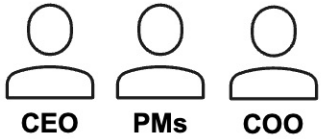
2023-02-02T11:30:00+01:00 - CONFIDENTIAL

tl;dr vendor is bankrupt

Please cancel any other meetings.
MANDATORY pre-read: https://***

Goal:
- Share new knowledge & align on the current situation
- Plan for the next 6h defined

Agenda:
1. **PM**, 5min, **Retro & Current situation**
2. IC, 5min, First problem analysis
3. **IC**, 5min, **Draft Plan for the next 6h**
    1. Tasks for subproblems
    2. Immediate measures
4. Misc & Questions
5. Next situation report

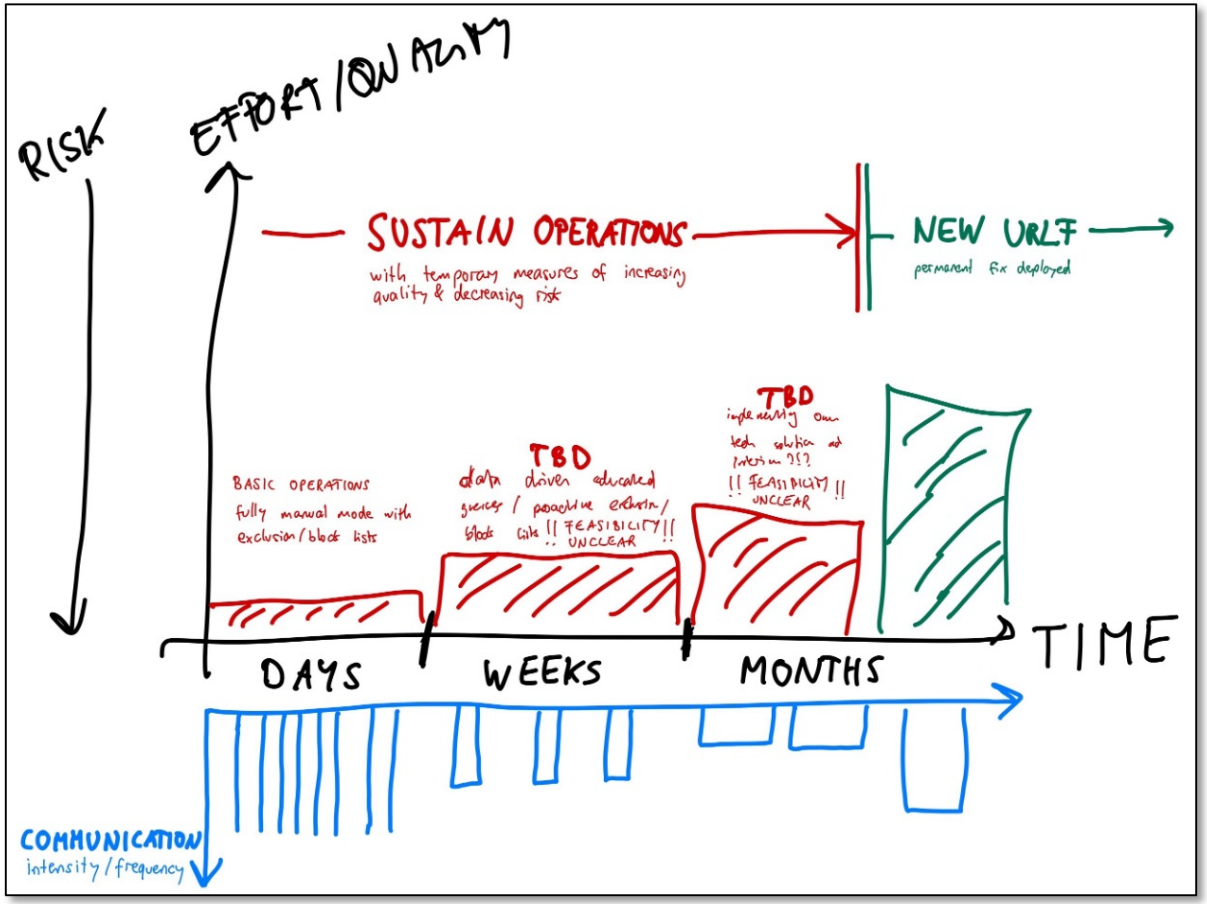


1. SUSTAIN OPERATIONS — **Product Owner, Head of Mission Control**

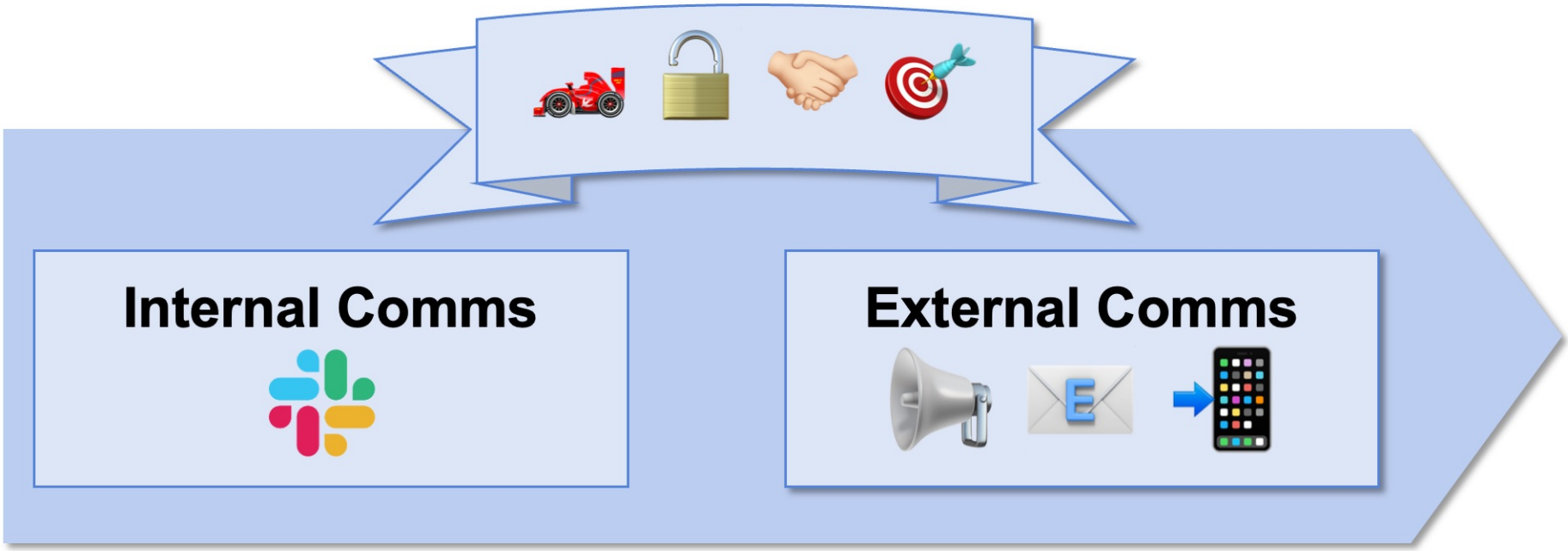
1. COMMUNICATION — **Technical Account Management Lead**

2. NEW SOLUTION — **Product Manager**

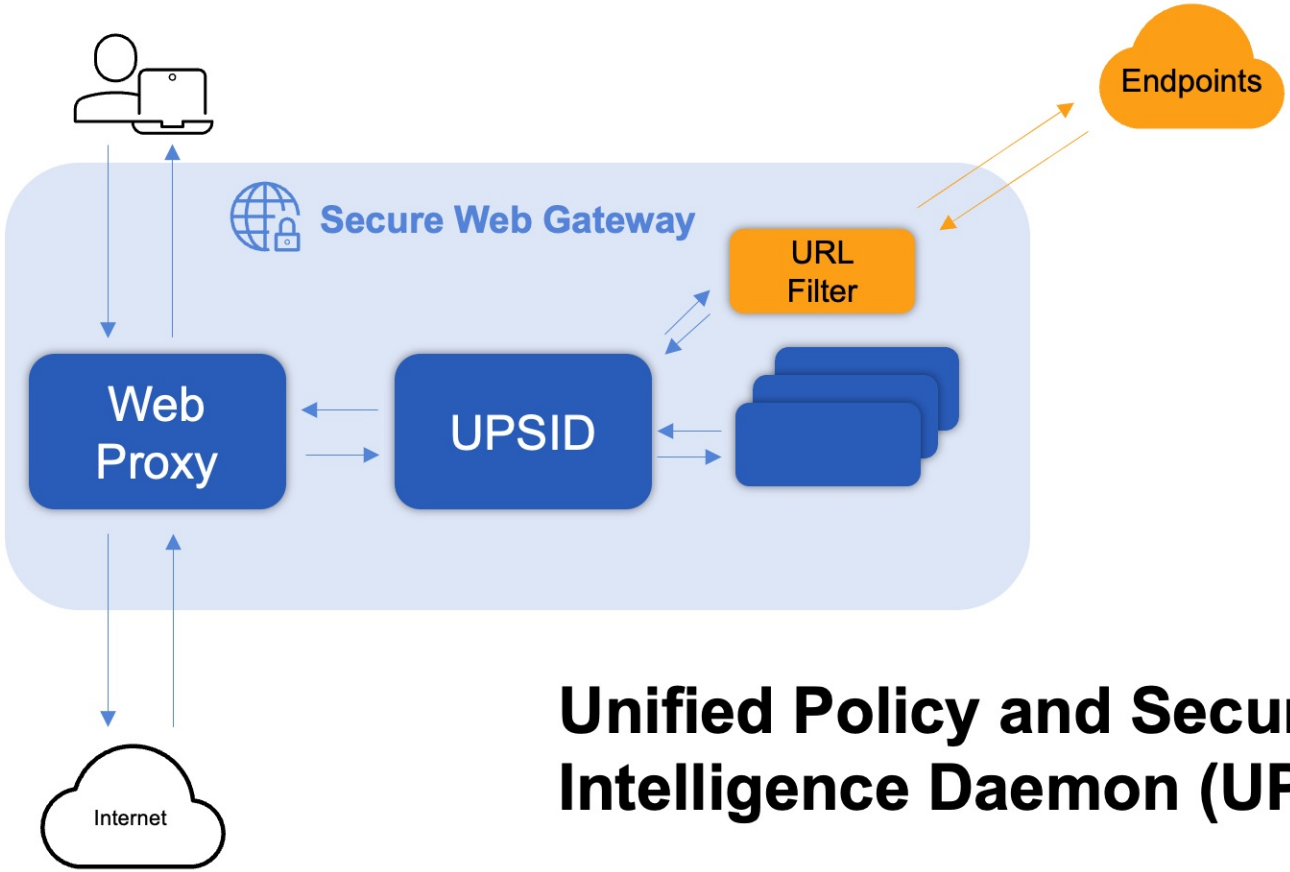
FIRST DAY – THE COMMANDER'S INTENT



FIRST DAY – ESTABLISHING COMMUNICATIONS

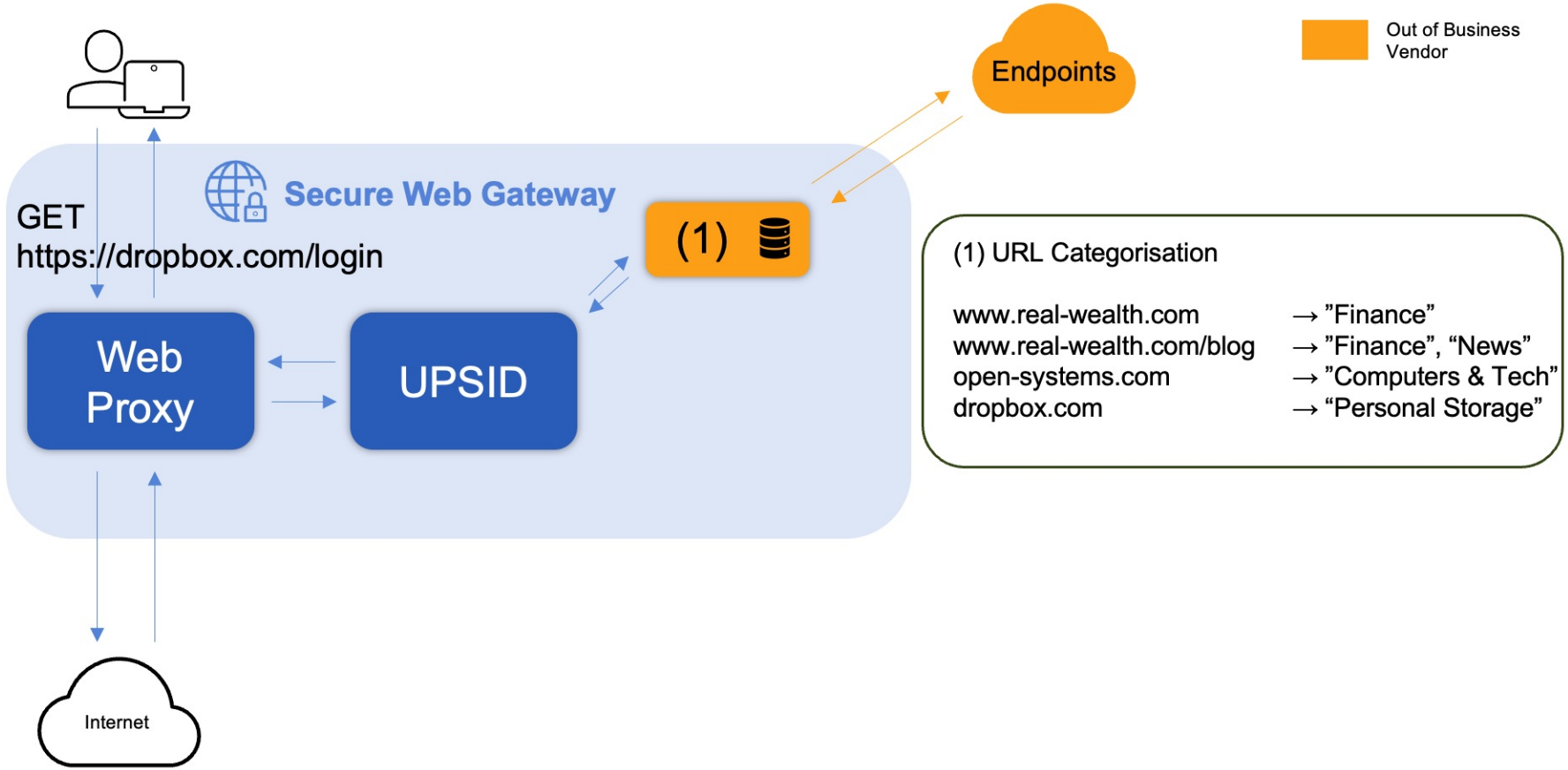


FIRST DAY – HOW DOES THE URL FILTER WORK?

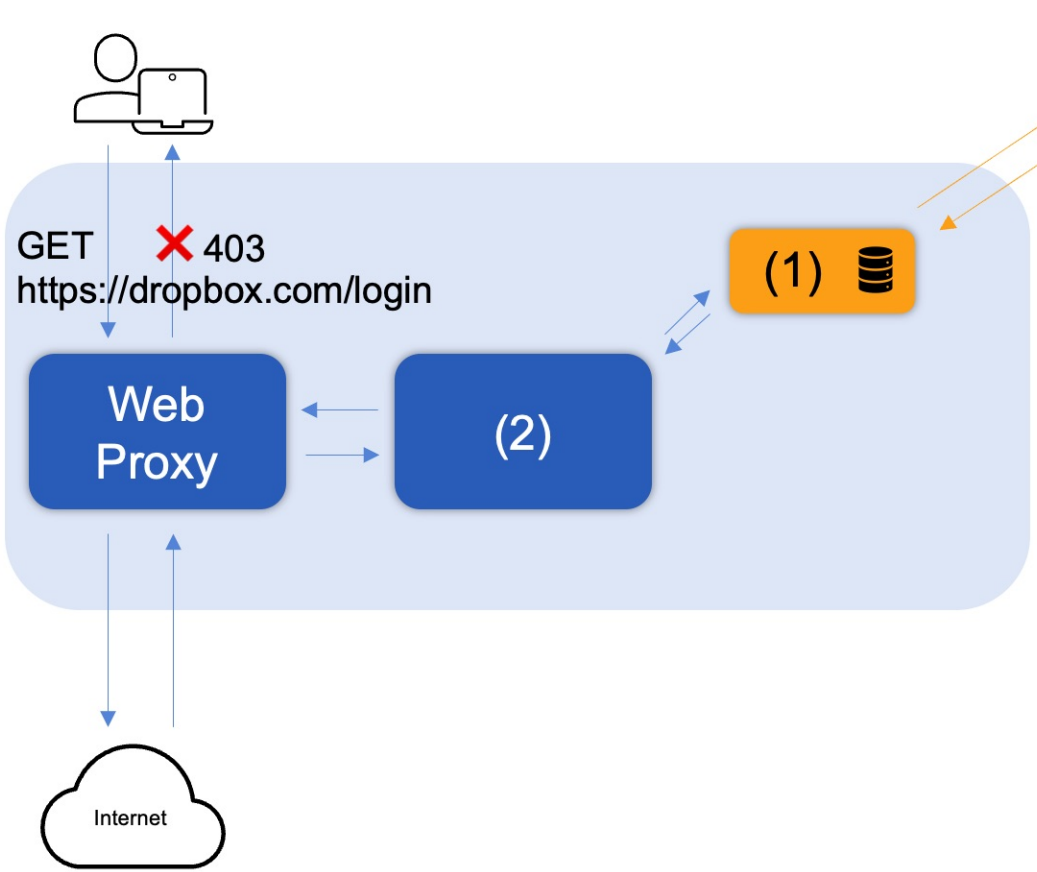


Unified Policy and Security Intelligence Daemon (UPSID)

FIRST DAY – HOW DOES THE URL FILTER WORK?



FIRST DAY – HOW DOES THE URL FILTER WORK?



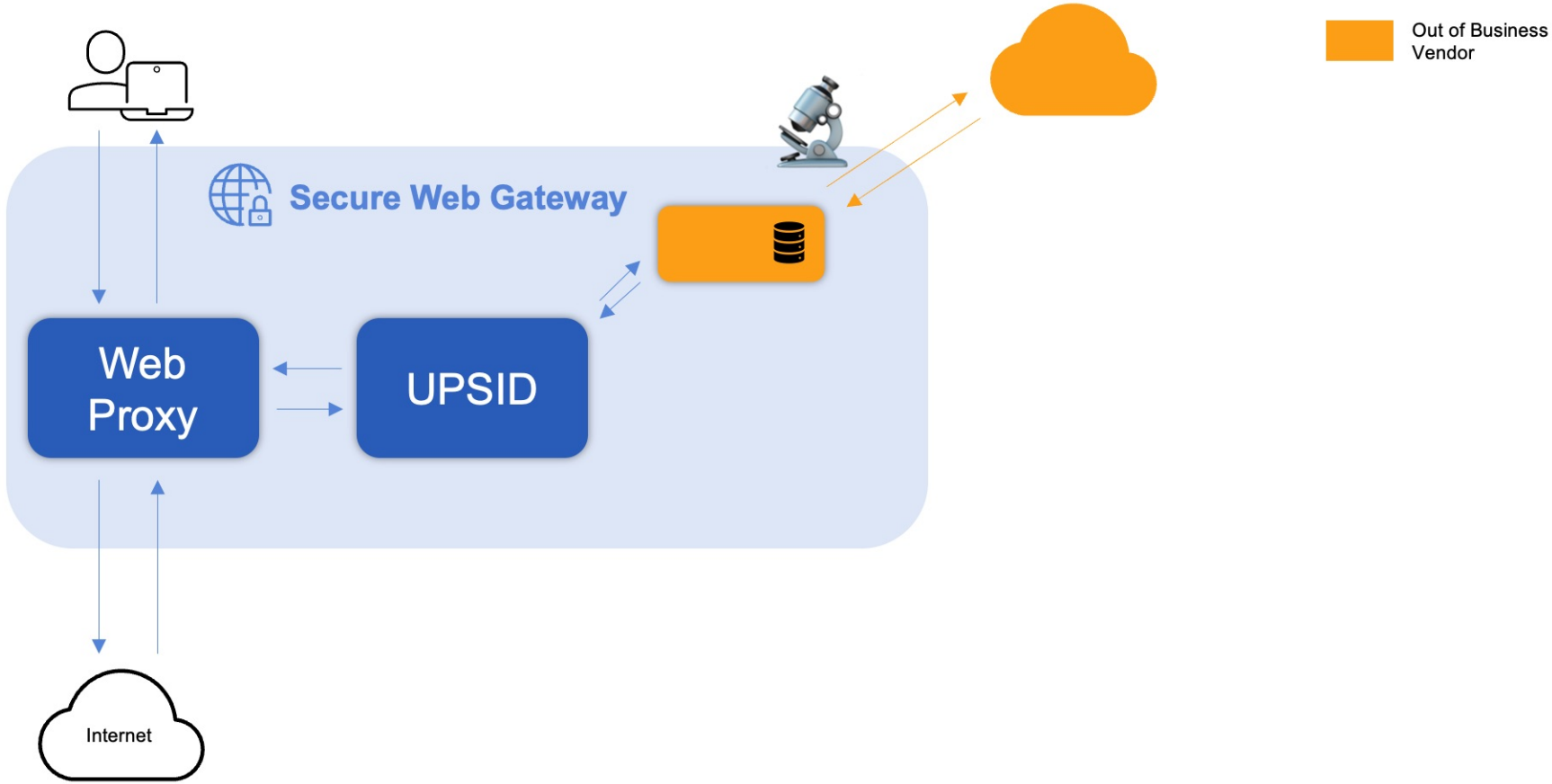
(1) URL Categorisation

www.real-wealth.com	→ ”Finance”
www.real-wealth.com/blog	→ ”Finance”, “News”
open-systems.com	→ ”Computers & Tech”
dropbox.com/login	→ “Personal Storage”

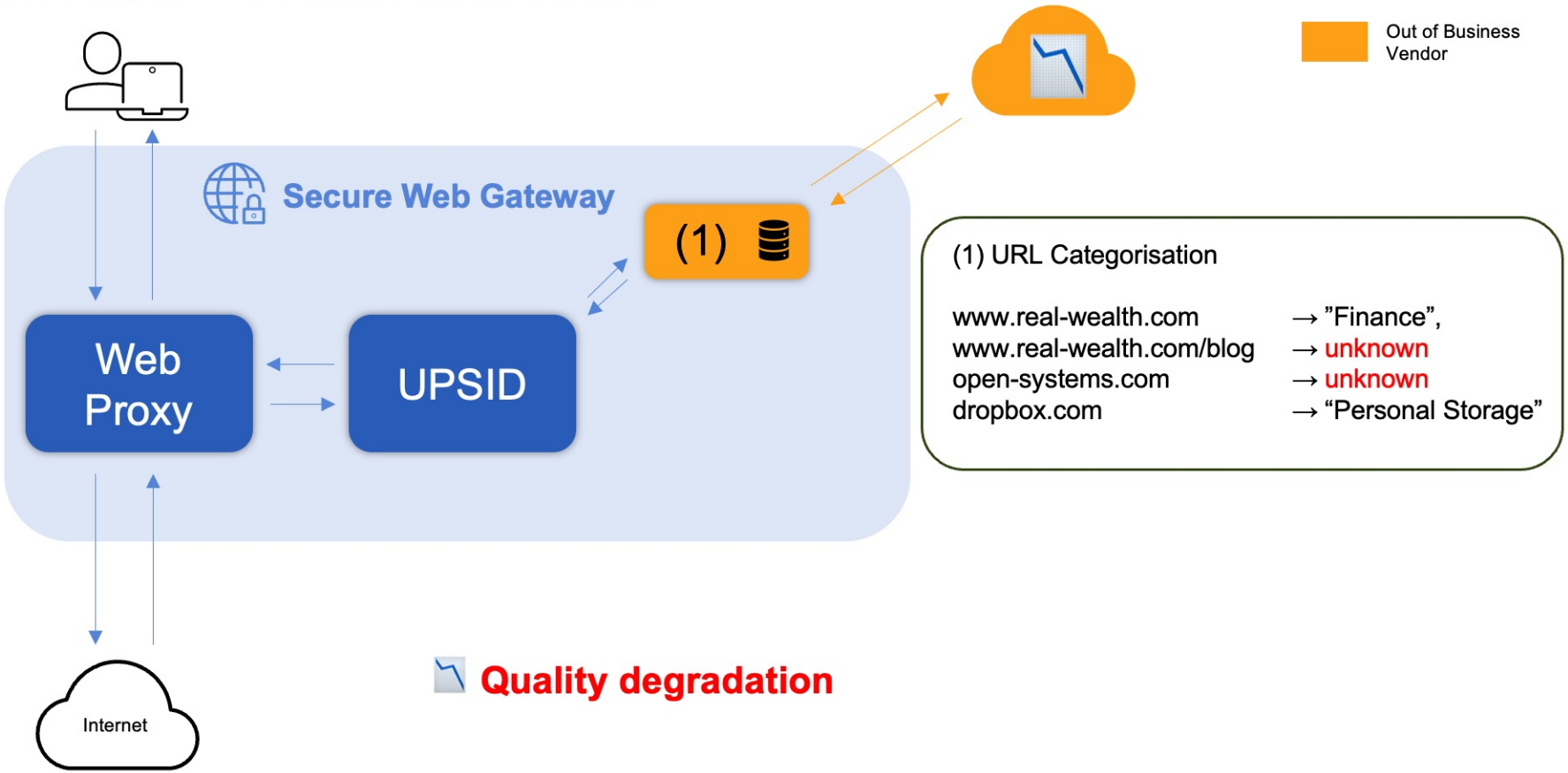
(2) Customer Policy

“Finance"	→	✅
“News”	→	✅
“Personal Storage”	→	❌
“Social Media”	→	❌

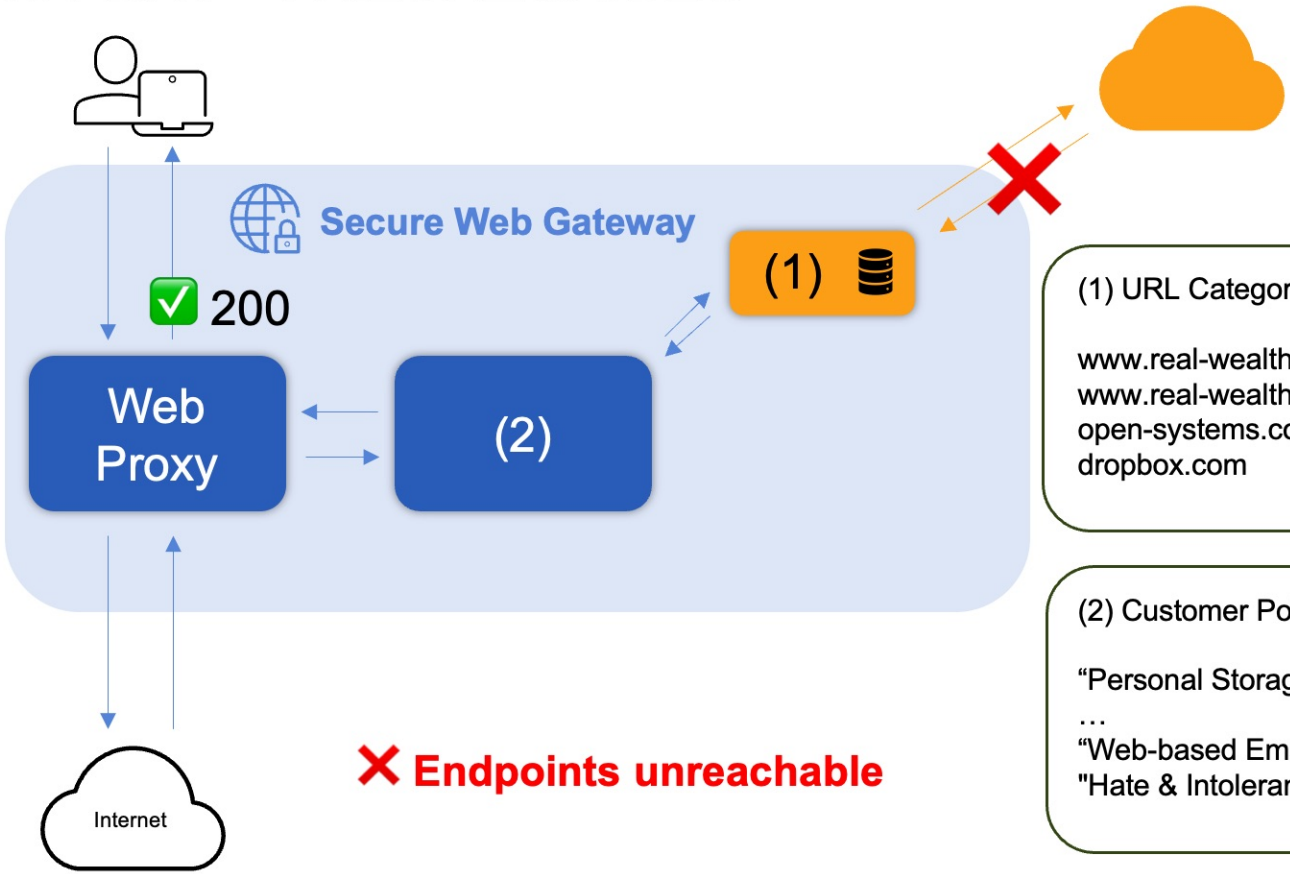
FIRST DAY – FAILURE MODES



FIRST DAY – FAILURE MODES



FIRST DAY – FAILURE MODES



(1) URL Categorisation

www.real-wealth.com	→	Timeout
www.real-wealth.com/blog	→	Timeout
open-systems.com	→	Timeout
dropbox.com	→	Timeout

(2) Customer Policy

“Personal Storage "	→	✅ (fail-open)
…	→	✅
“Web-based Email”	→	✅
"Hate & Intolerance“	→	✅

FIRST DAY – OPERATIONS IN MISSION CONTROL

2023-02-02 [redacted] Crisis Response

Created by [redacted], last modified by Raphael Seebacher on 07.10.2024

INTERNAL USE ONLY
Do not share any of the information below externally

SHTF

SHTF Runbook - [redacted] goes down

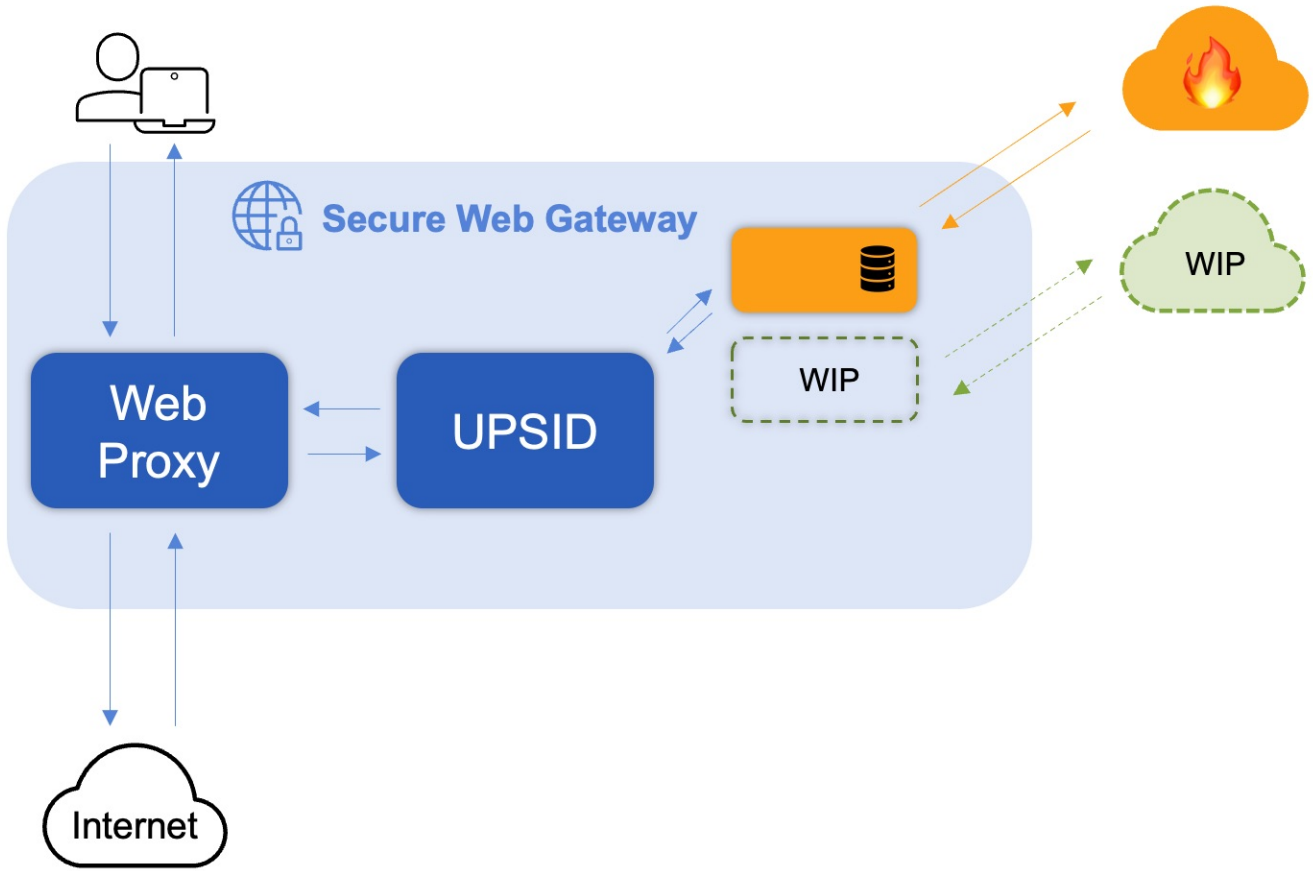
Table of Contents

- Incident Response Overview & Status
- Action Log

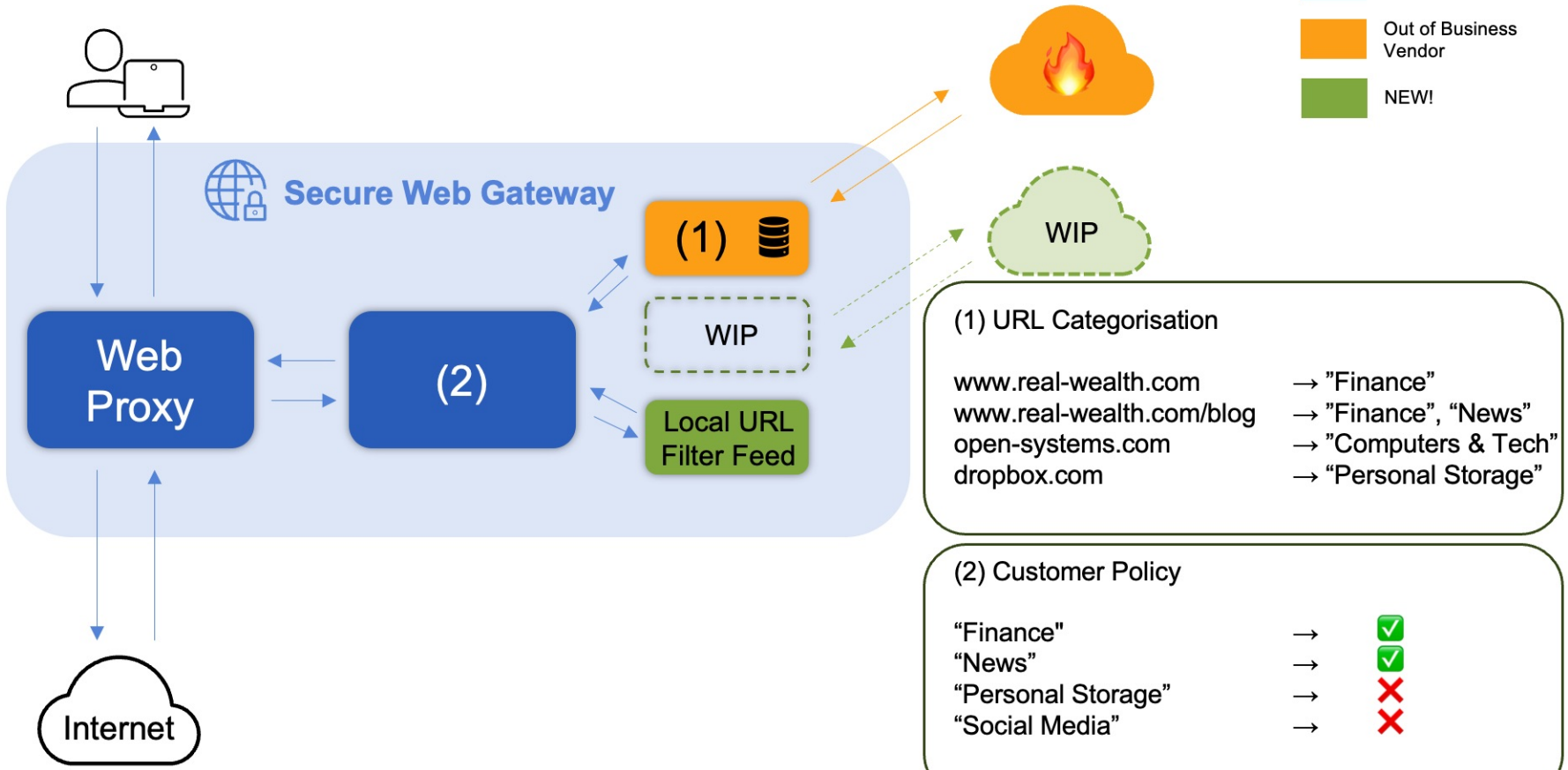
RoB (Rules of Behaviour)

1. Speak up, raise conc
2. Document what you
3. Keep ALL communica
4. NO side actions
5. NO panic - stick to th
6. Significant change of

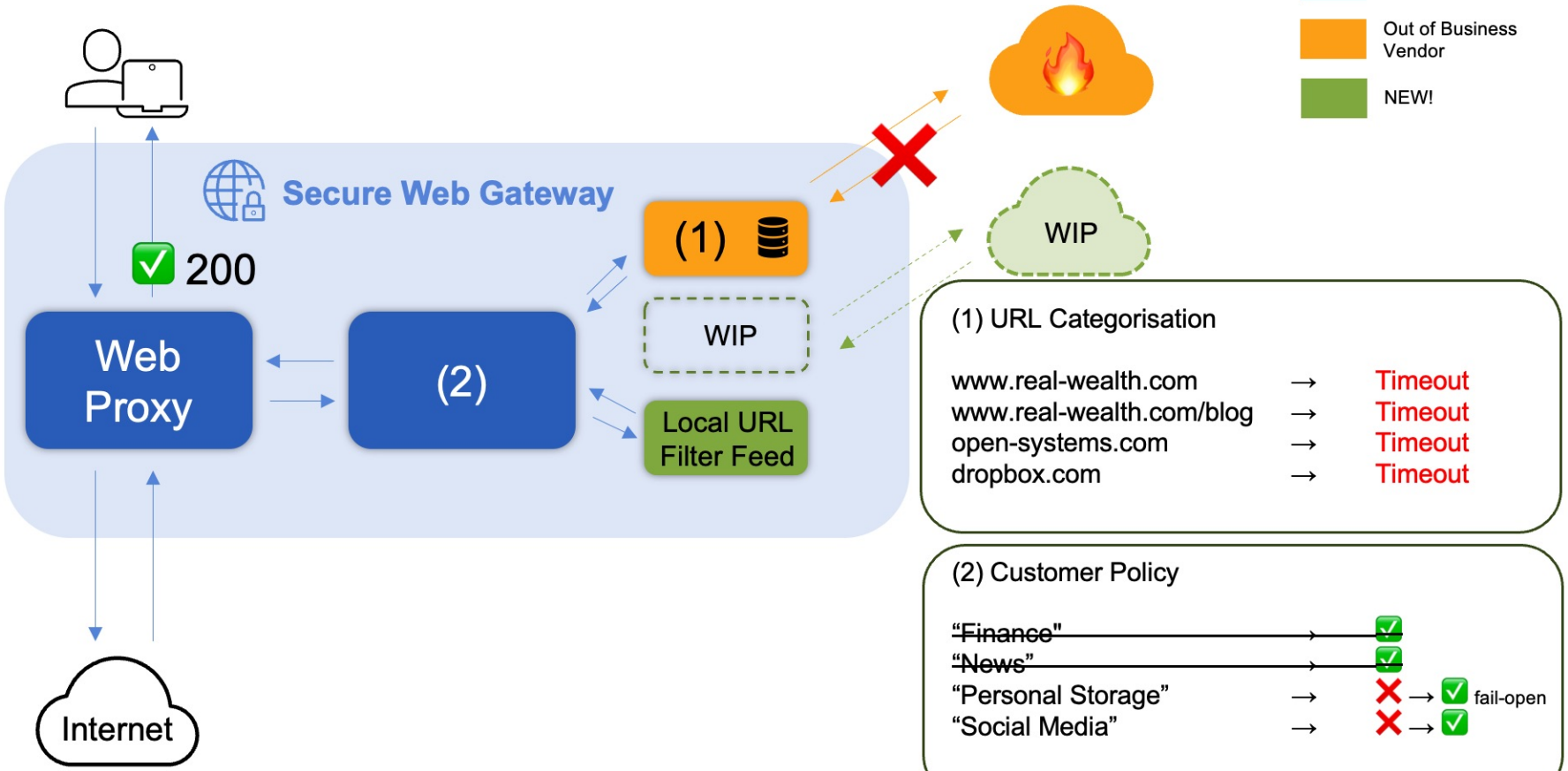
FIRST WEEK - TECH / OPS



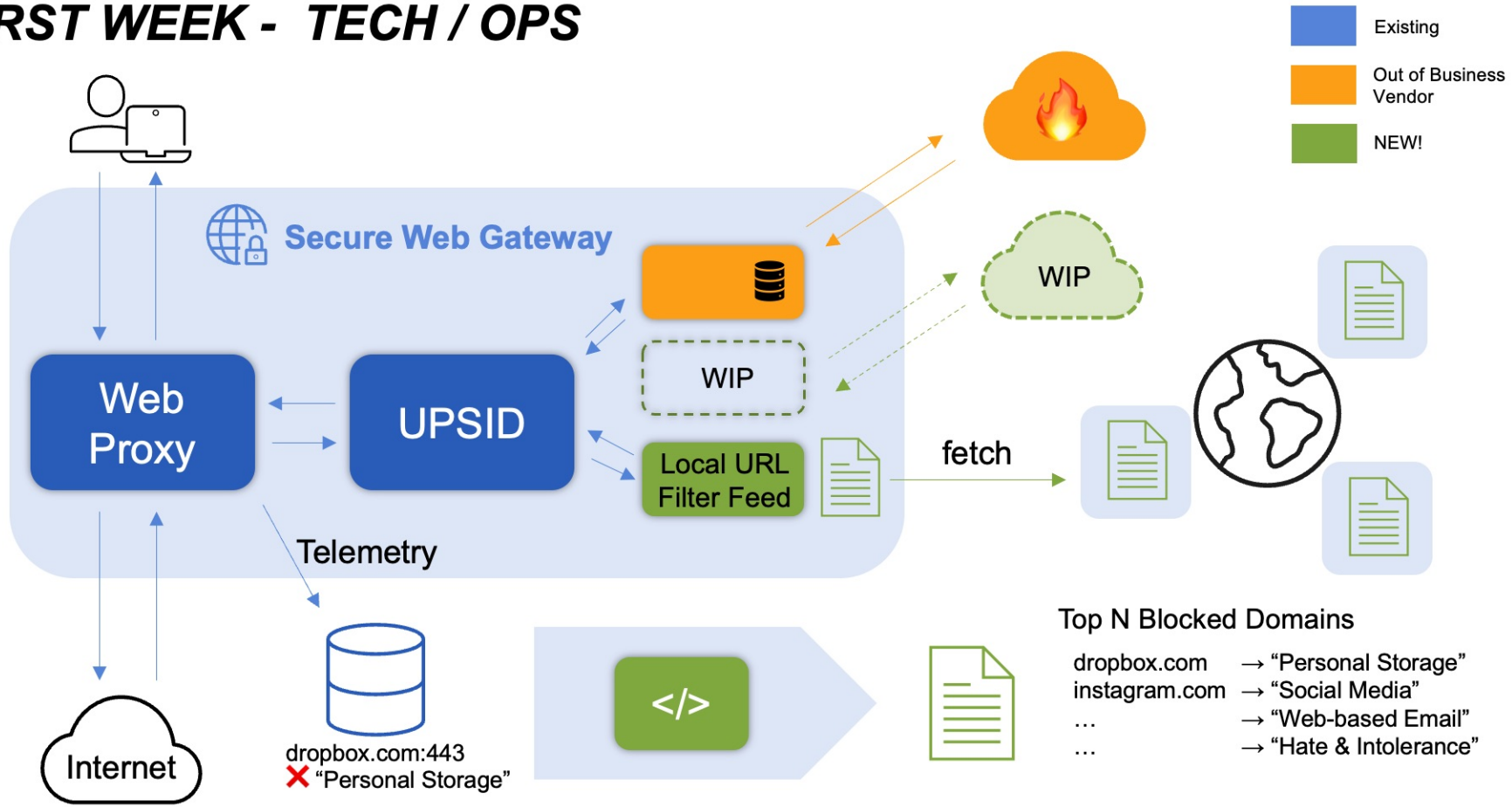
FIRST WEEK - TECH / OPS



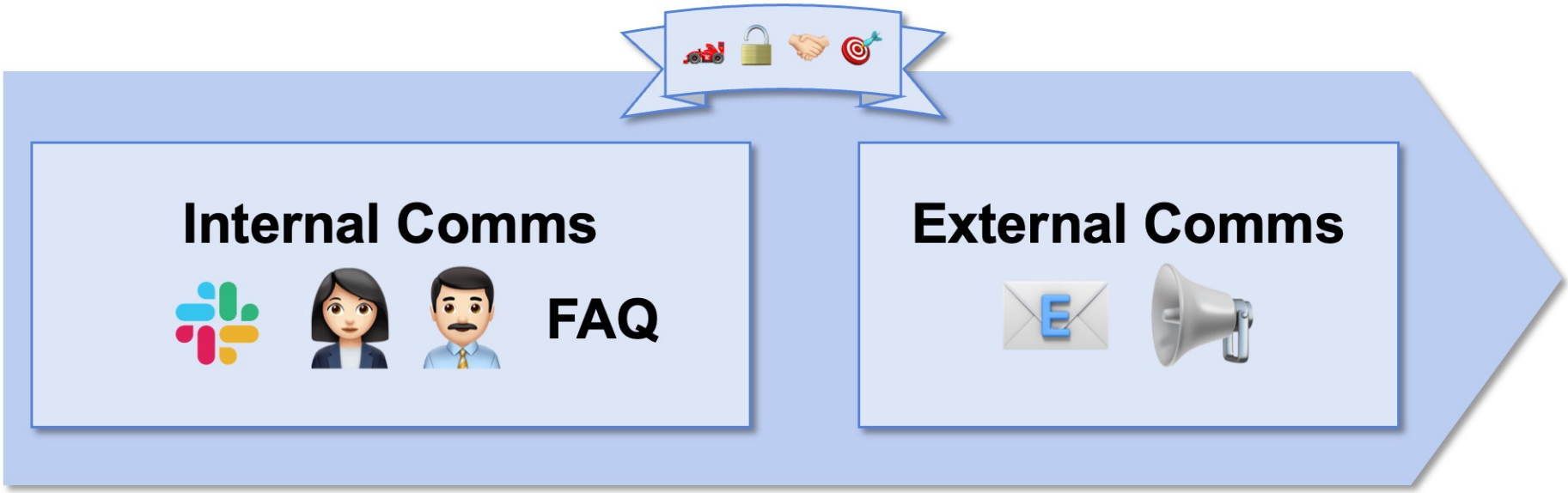
FIRST WEEK - TECH / OPS



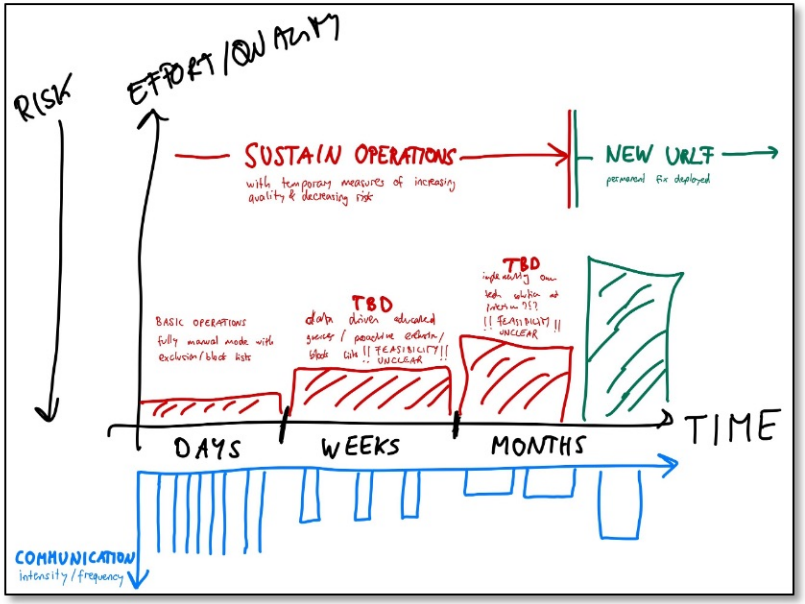
FIRST WEEK - TECH / OPS



FIRST WEEK – COMMUNICATIONS



FIRST WEEK – GETTING INTO THE RHYTHM



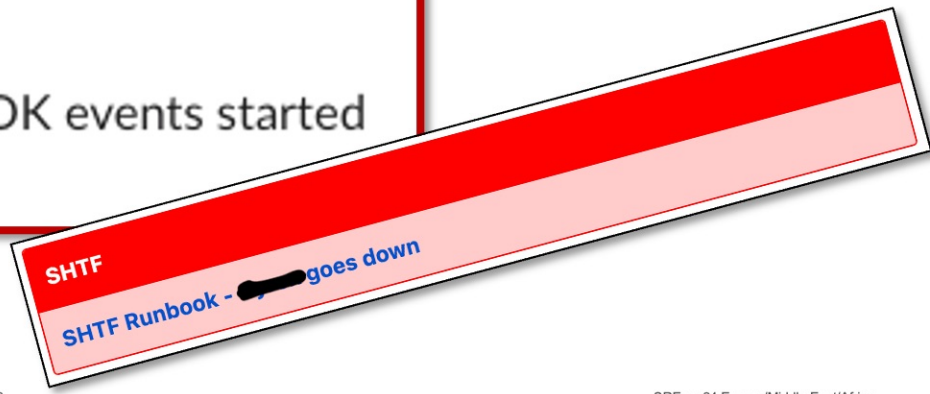
FIRST WEEK – RESPONSE WELL UNDER CONTROL…

vendor endpoints unreachable for 15m

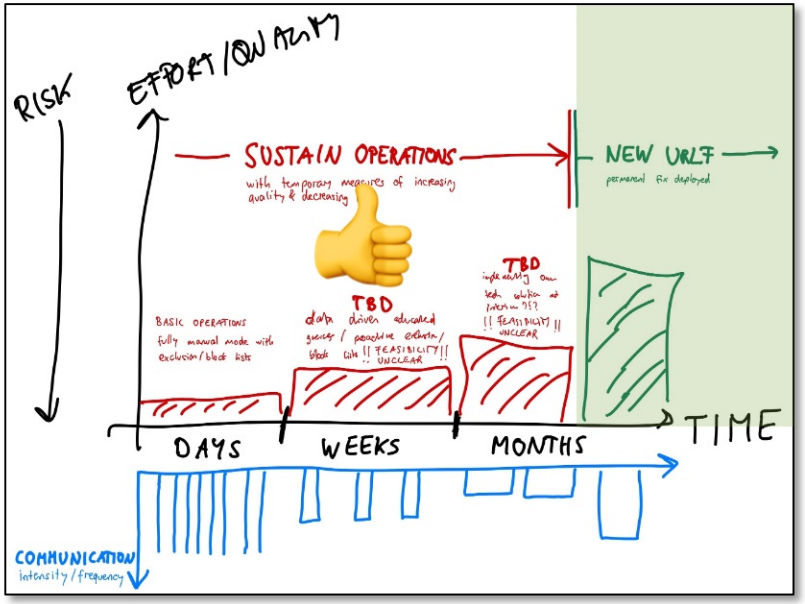
mma Feb 8th, 2023 at 03:03

~~false alert~~ outage at 02:43 CET

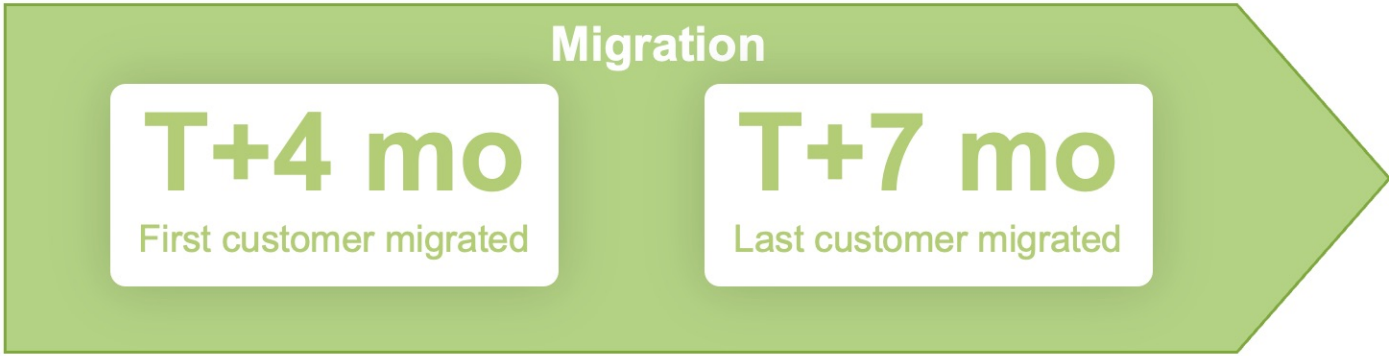
- `NURSE:URLFILTER:CATEGORIZATION:ERROR` got quarantined (~90 events)
- `upsic -lookup alohasalads.com` returned no categories for ~15 mins
- then everything back to normal, OK events started coming in



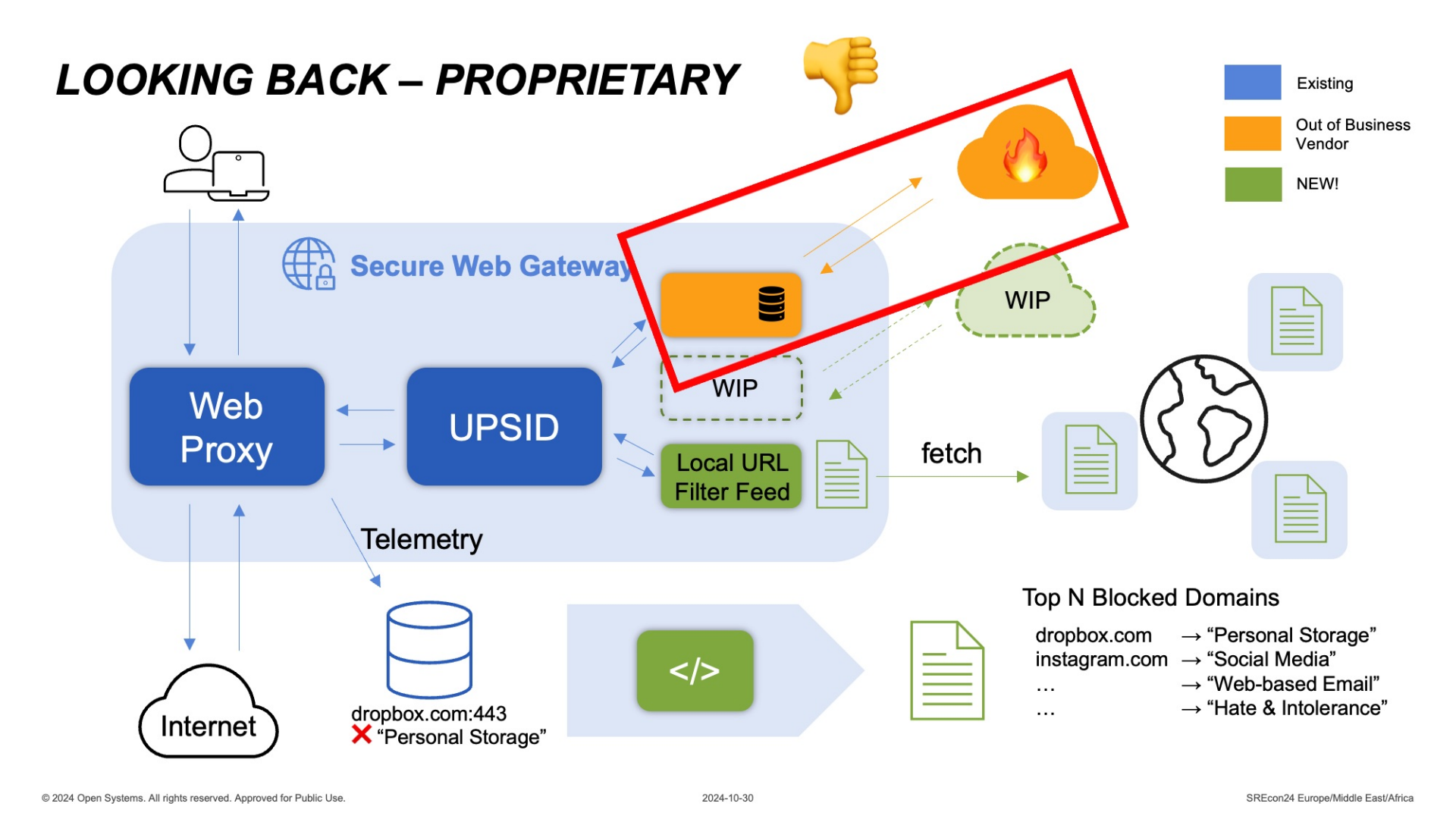
FIRST MONTH(S) – KEEP GOING DESPITE THE ROUTINE



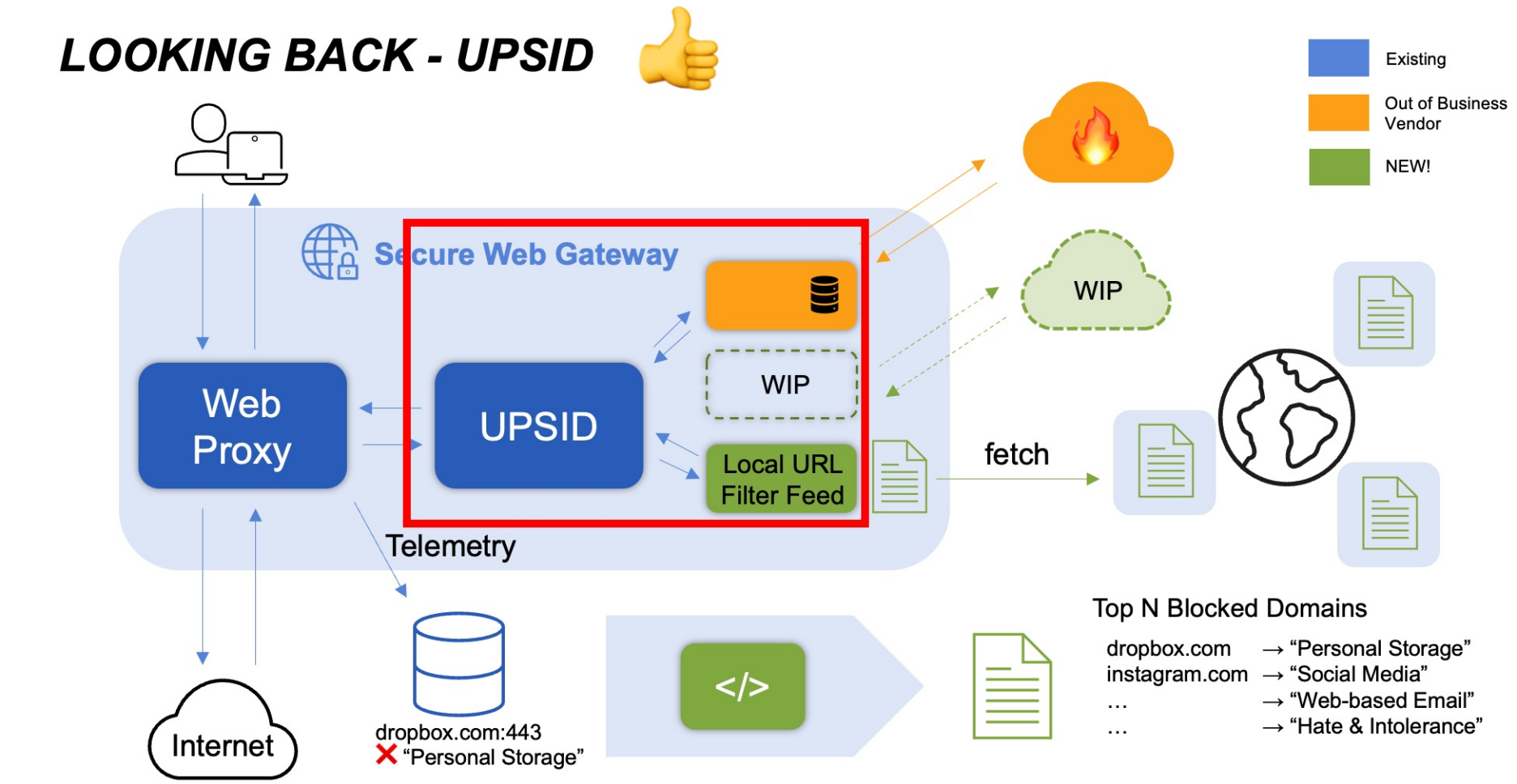
FIRST MONTH(S) - NEW URL FILTER



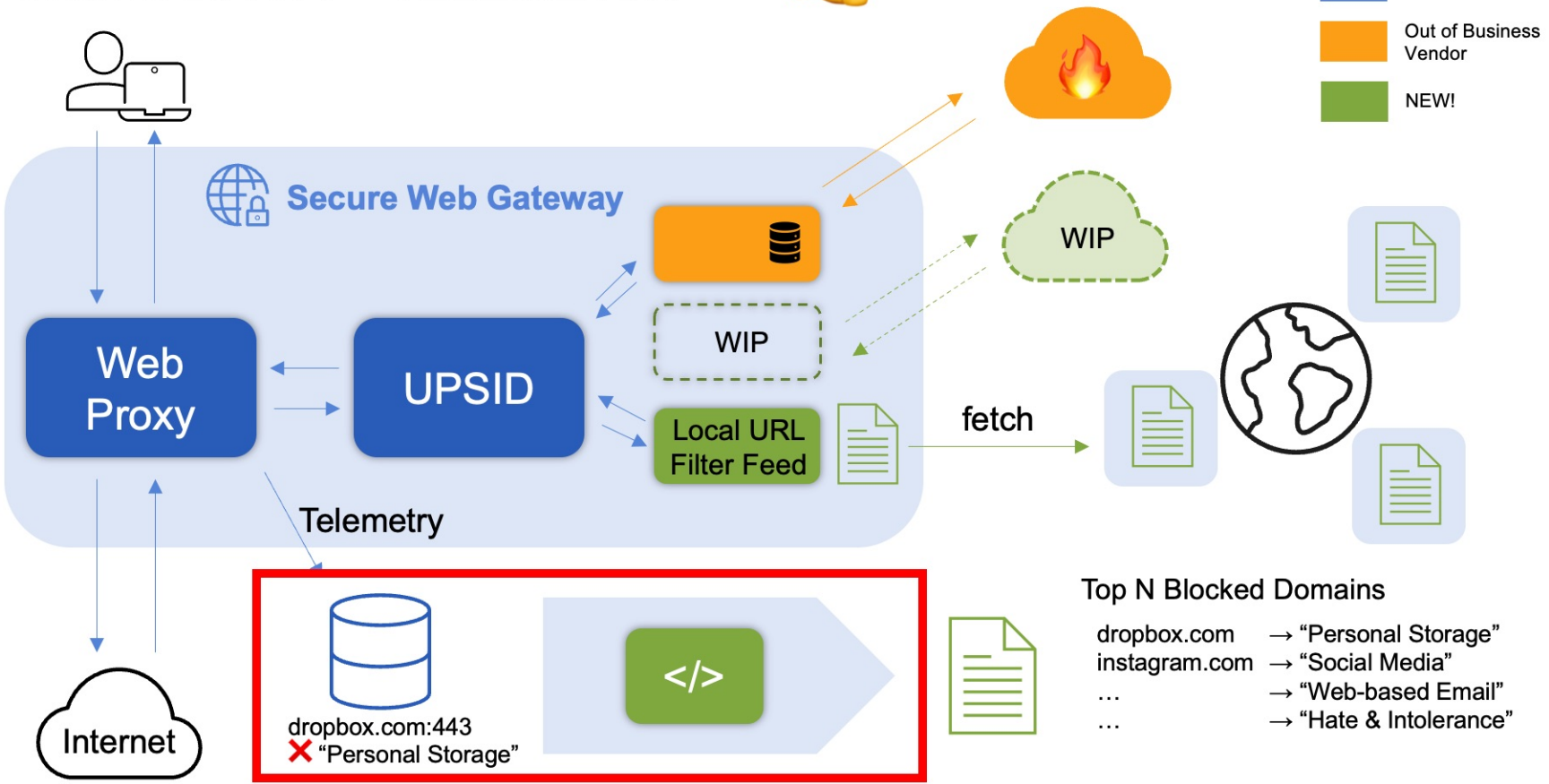
LOOKING BACK – PROPRIETARY



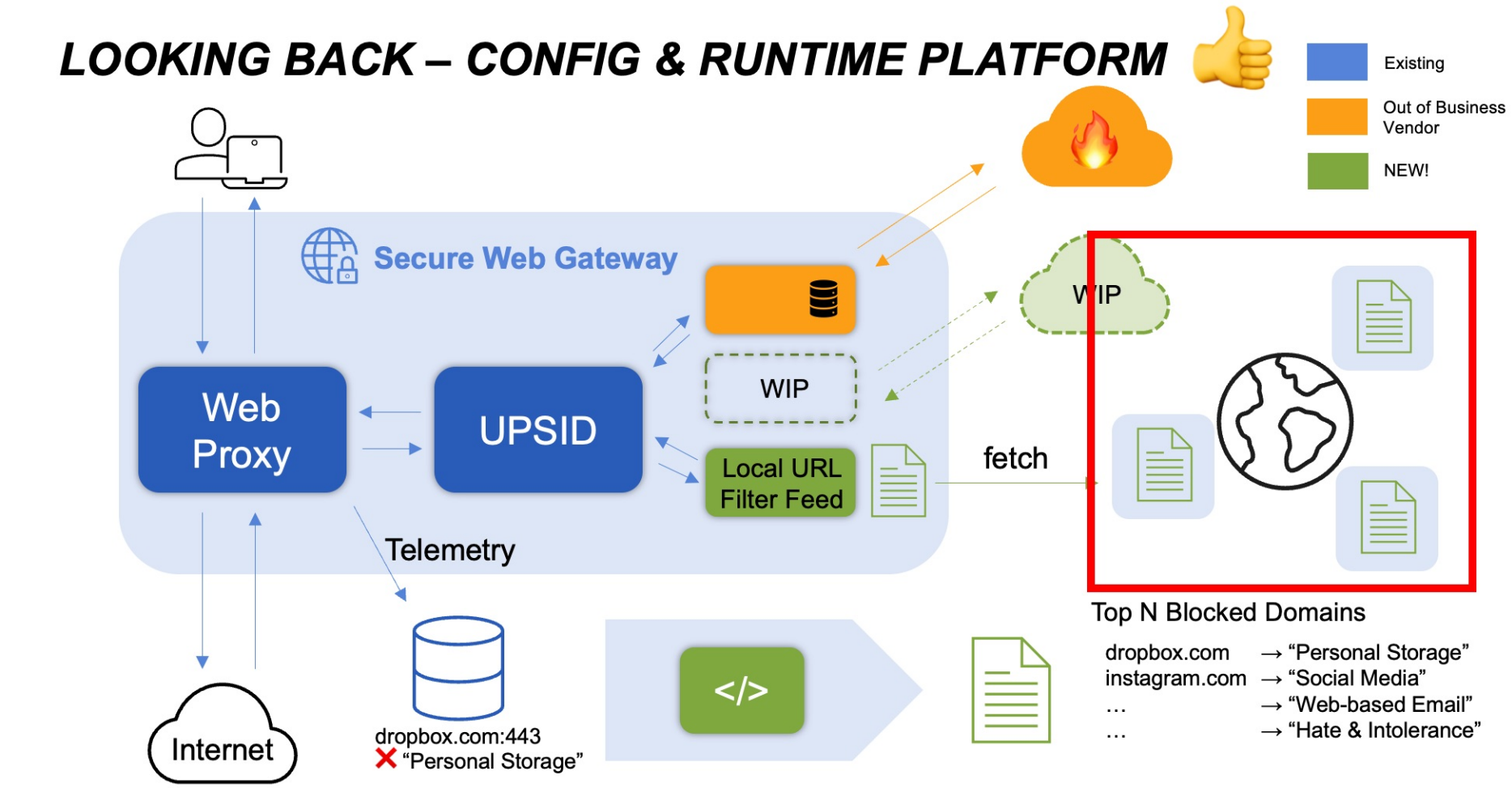
LOOKING BACK - UPSID



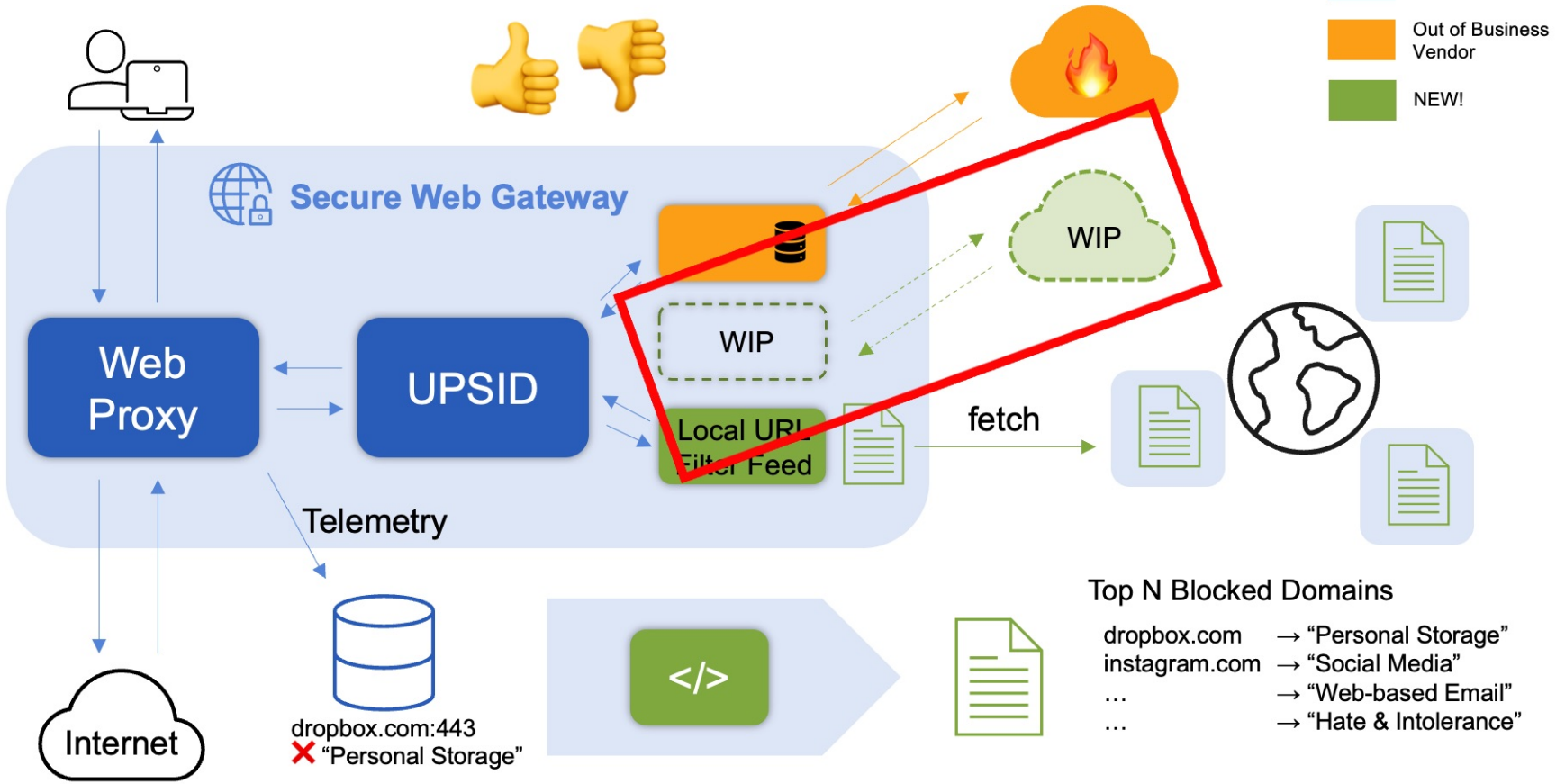
LOOKING BACK – TELEMETRY



LOOKING BACK – CONFIG & RUNTIME PLATFORM



LOOKING BACK – VENDOR REPLACEMENT



LOOKING BACK - THE GOOD & THE BAD

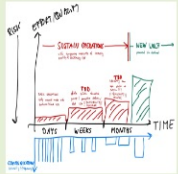
Crisis preparedness

Communication

Hope for the best, plan for the worst

KISS

keep it simple, stupid



Trust “your” people