

Agorà Mobile

or:

How I Learned to Stop Worrying
and Put our Intranet on the Internet

Guglielmo Bondioni
Manager of ICT Security
Fastweb S.p.A.

Milan, 2015-03-11

Fastweb 2015

Customer Base **2.1 Mln** wireline customers EoY 2014

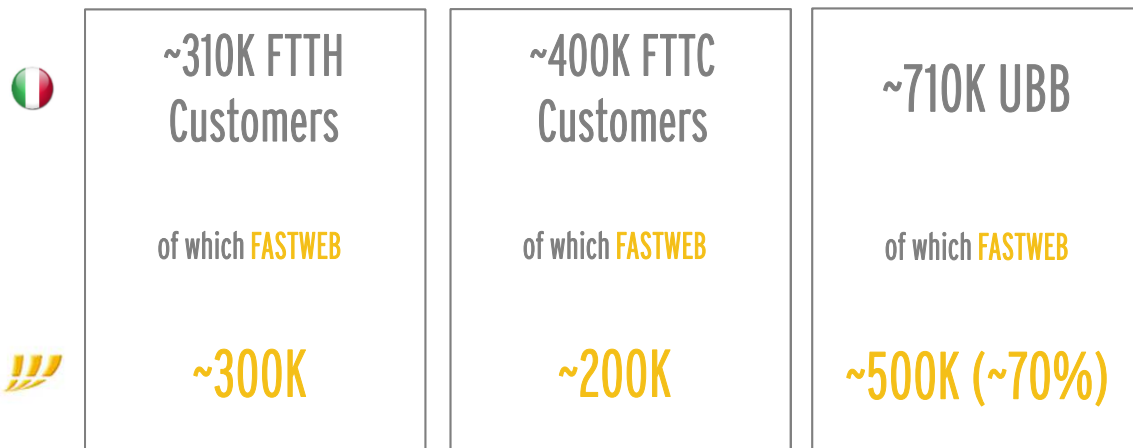
Leader in broadband **FASTWEB**

un passo avanti

Main competitor of the incumbent in Corporate/PA segment **~30%** Market Share Corporate

The only operator with sales and margins growing YoY **+3%** Revenue in 2014

Leading the ultra-broadband market



With 500k customers connected at speed up to 100 Mbps, FASTWEB has a 70% share of the UBB market

Arricchire la vita e il lavoro attraverso Internet

Enrich life and work
through the Internet

CUSTOMER FIRST

TRUST

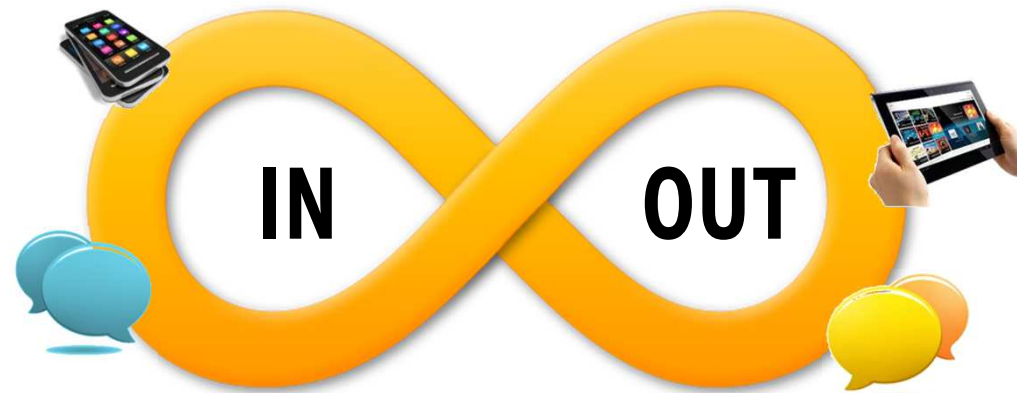
INNOVATION 360°

INITIATIVE

AGILITY

PG. 4

So, let's take our intranet to the Internet!



**Create a digital work environment
to foster communication, cooperation and interaction within the company
anywhere, at any time and with any device.**

Security's typical response:

NO.

... not an option.

Enrich life and work
through the Internet

CUSTOMER FIRST

TRUST

INNOVATION 360°

INITIATIVE

AGILITY

PG. 7

Dilemma

How do we take
sensitive internal web sites
to the Internet, *safely*?

?

The image shows a screenshot of the Learning Hub website interface. At the top, there is a yellow banner with a large white question mark. Below this, the website header includes the 'Learning Hub' logo, navigation links like 'help' and 'contatta la redazione', and a search bar. The main content area features a central article about 'FASTWEB' and 'HUAWEI' with a photo of a man speaking. To the right, there are sidebars for 'Un "come fare per" al giorno' and 'Ultimi annunci in Bacheca'. At the bottom left, there is a list of recent news items dated 'oggi, 4 Novembre 2014'. The interface is decorated with various icons like a headset, a clock, and a Wi-Fi symbol. The bottom of the page has a colorful bar with pink, purple, green, orange, and teal segments.

... we don't.

Not *that* sensitive.

Web sites in highest demand

- Intranet home page (news, help pages)
- Help Desk & Facilities request forms
- Training portal
- Approvals
- Desk/room reservations
- Videoconferencing reservations



Not too sensitive

No customer data
Only public information
Only general convenience tools

Still, we want to do it safely

**Security chose to act as enabler,
driving the change
instead of enduring it.**

So we took action

- **We sat down with HR and IT and wrote the requirements**
- **We found there wasn't a solution available within our IT ecosystem**
- **So we made a tender**

Note that if you run the latest* version of some of the major identity and access solutions you can leverage those

*** 2014**

Partner with a systems integrator

Working alongside us



- High Level skills in Information Security
- Analysis of Fastweb issues thanks to Advisory expertises
- Technology Mapping about Fastweb's Requirements
- A quick & successful POC
- Extremely fast roll out

our choice was SINERGY

A platform for reducing risk

Achieve a uniform base level of security...

... and do it **once and for all**

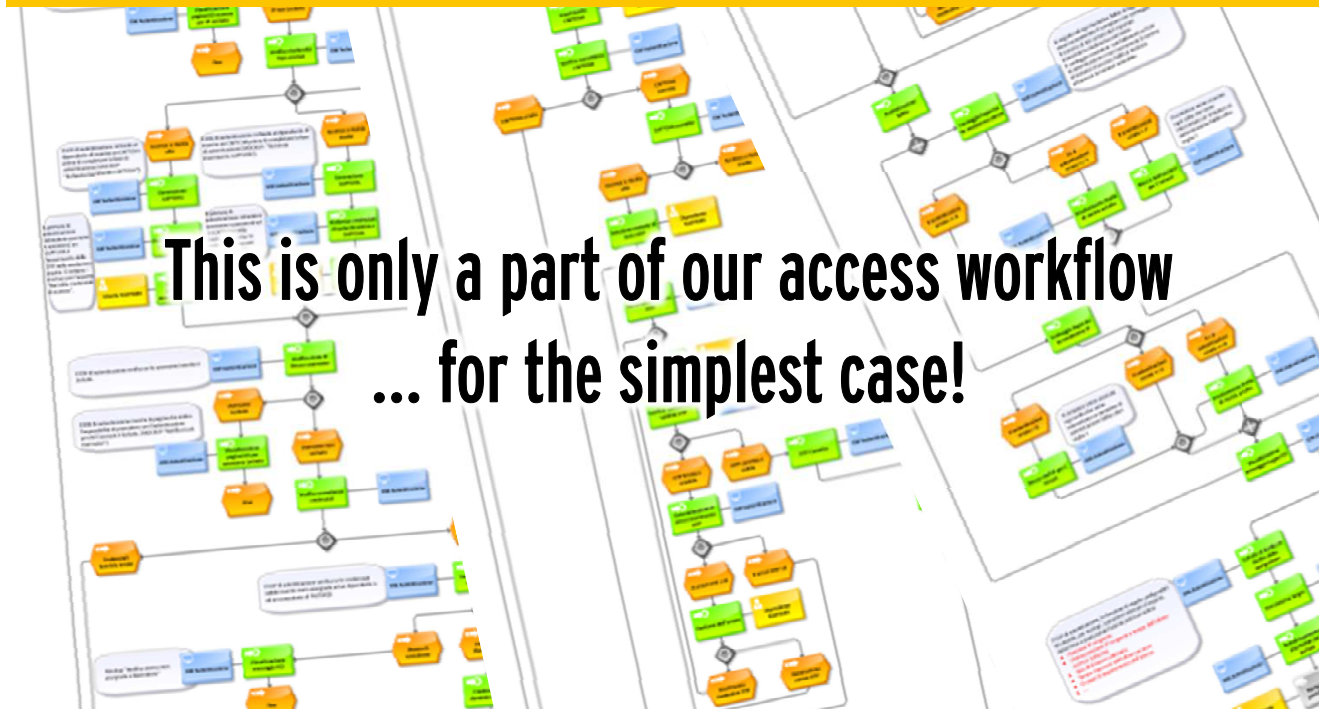
- User / pw + OTP, CAPTCHA when needed
- *Not those pesky VPN hardware tokens?*
- Nope. OTP without HW, over multiple channels like SMS or email
- Sensible lock-out policy
- Geo-IP, reputation from various sources + internal feed
- HTTPS everywhere
- Session risk evaluation

our choice was F5 Big-IP APM



Use cases and workflow

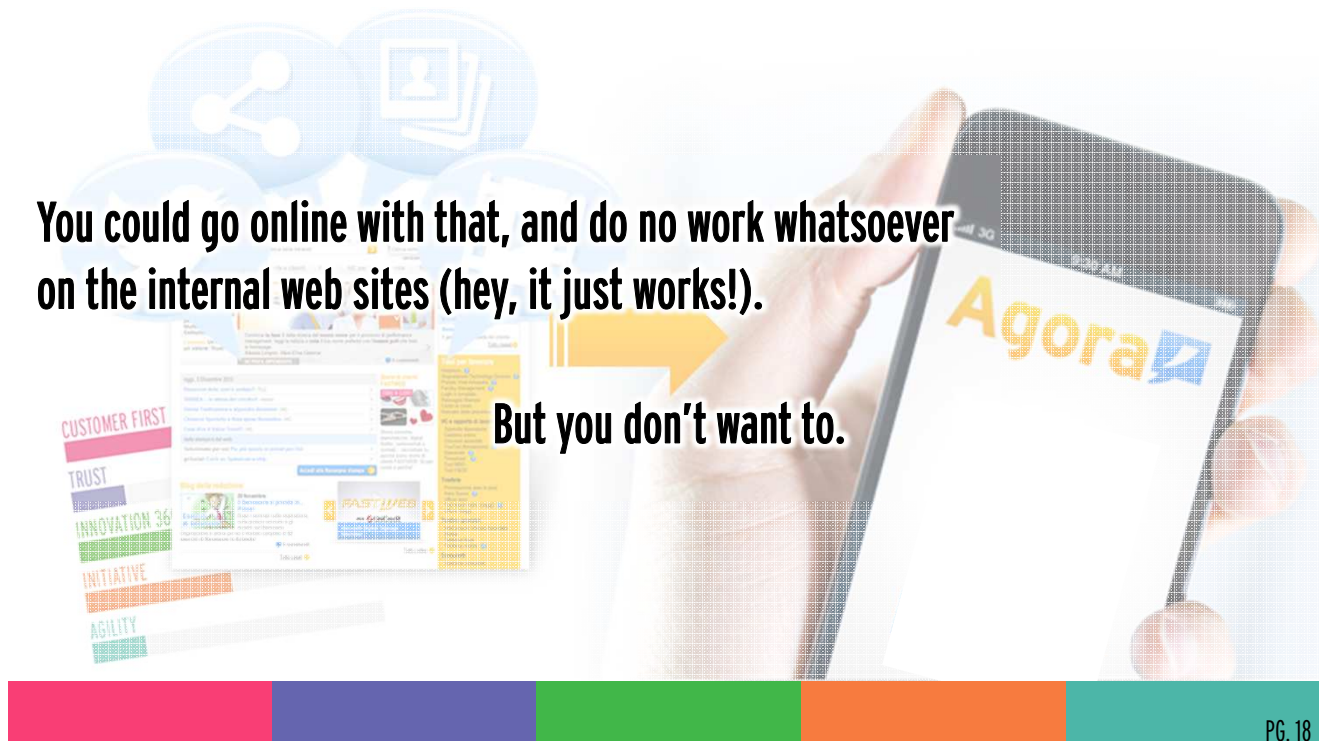
**This is only a part of our access workflow
... for the simplest case!**



Is that it?

You could go online with that, and do no work whatsoever on the internal web sites (hey, it just works!).

But you don't want to.



Estimating risk

Risk / benefit evaluation for each site or tool

- **Joint committee: HR, Security, IT**
- **Map all the pages and navigation**
- **Identify contents, exclude sensitive / admin pages**
- **Formal approval**



Updating internal web sites

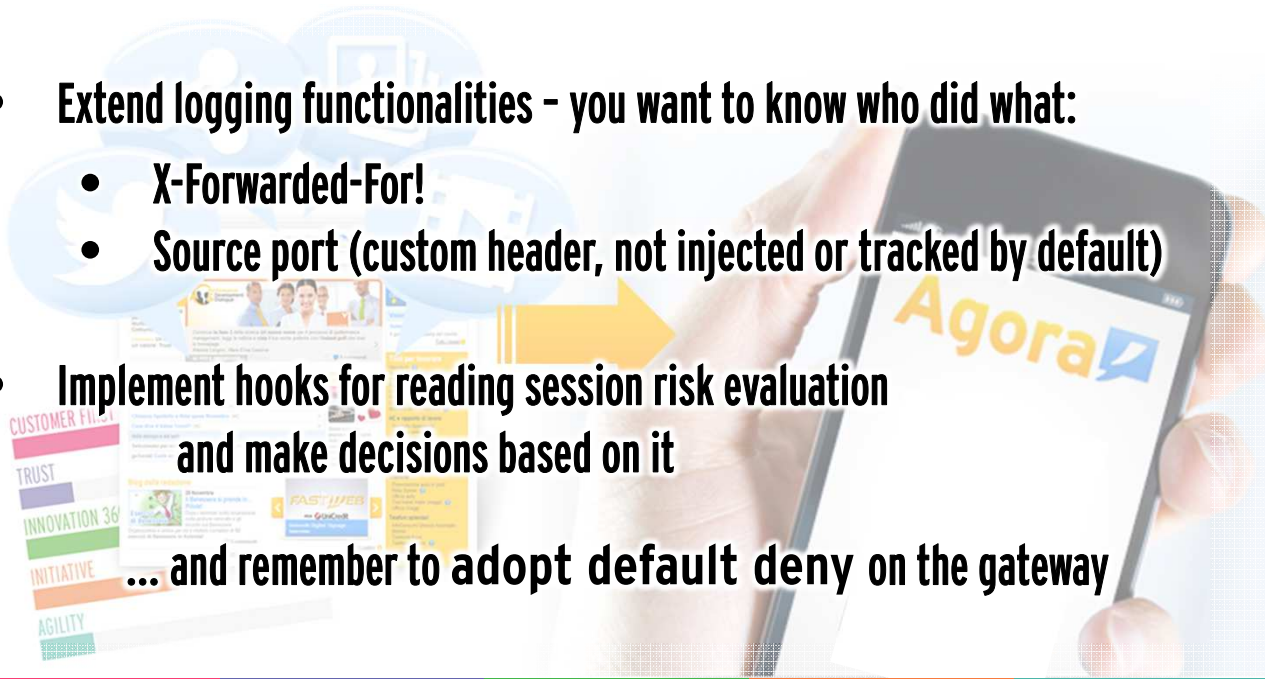
Run PTs for each tool or page

- Is it broken? Can it be fixed?
 - No -> sorry, it won't go on the Internet
 - Yes -> Fix what's broken, update security 😊

But of course, adopt default deny on the gateway

Enhancing internal web sites

- **Extend logging functionalities - you want to know who did what:**
 - **X-Forwarded-For!**
 - **Source port (custom header, not injected or tracked by default)**
- **Implement hooks for reading session risk evaluation and make decisions based on it**
... and remember to adopt default deny on the gateway



Finally, let people use it



FEEDBACK

ciao, da terminale iphone 3, acceso il telefono per mandare un sms o fare una chiamata. Ho scaricato l'App AgoraMobile, la decontestualizzata. Riaccedendo vengo indirizzata sulla pagina di RIESCO a vedere bene il video. Ho visto un PAR. Scusate, ma nel menù del Tool Sale Riunioni, che trovo utilissimo!



... but keep an eye on it.



No technology keeps you safe on its own

- Logs from the gateway and web sites go to the SOC
- Establish alarm conditions beforehand
- Agree on reaction policy:

“Since the sites aren’t mission or business critical,
if we see something funny,
we shut the whole thing down”

Q&A





Thank you for your attention.

Guglielmo Bondioni
Manager of ICT Security
Fastweb S.p.A.

with

