Cybersecurity Software

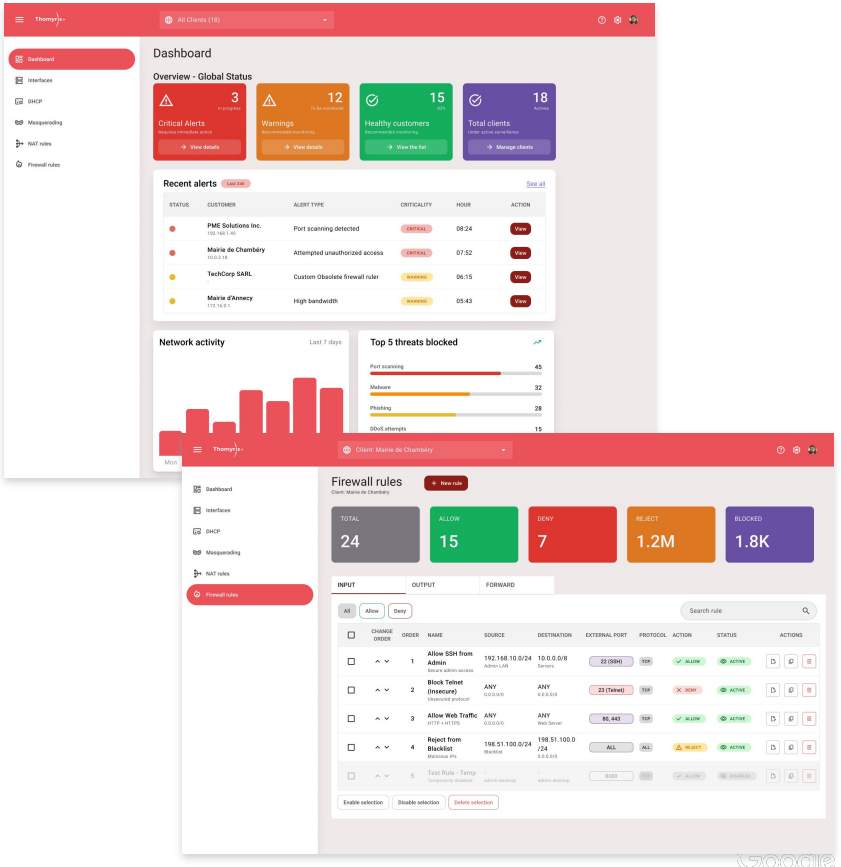
Project overview

The product:

A cybersecurity software that is user-friendly and tailored to the specific needs of system and network administrators.

Project duration:

8 months



Project overview

The problem:

The costly dependence on a third-party cybersecurity solution and the inability to capitalize on the SME and local government market with a proprietary offering.

The goal:

Develop a marketable proprietary solution that meets the needs of system administrators

Project overview

My role:

This project allowed me to plan and direct each step of the design thinking process as a junior UX designer with UI design experience.

Responsibilities:

- Conduct user research
- Define the problem and provided insights to inform the ideation phase
- Define personas, user journeys, empathy maps and user flows
- Visual design of low-fi and high-fi wireframes, prototypes, and user testing

Understanding the user

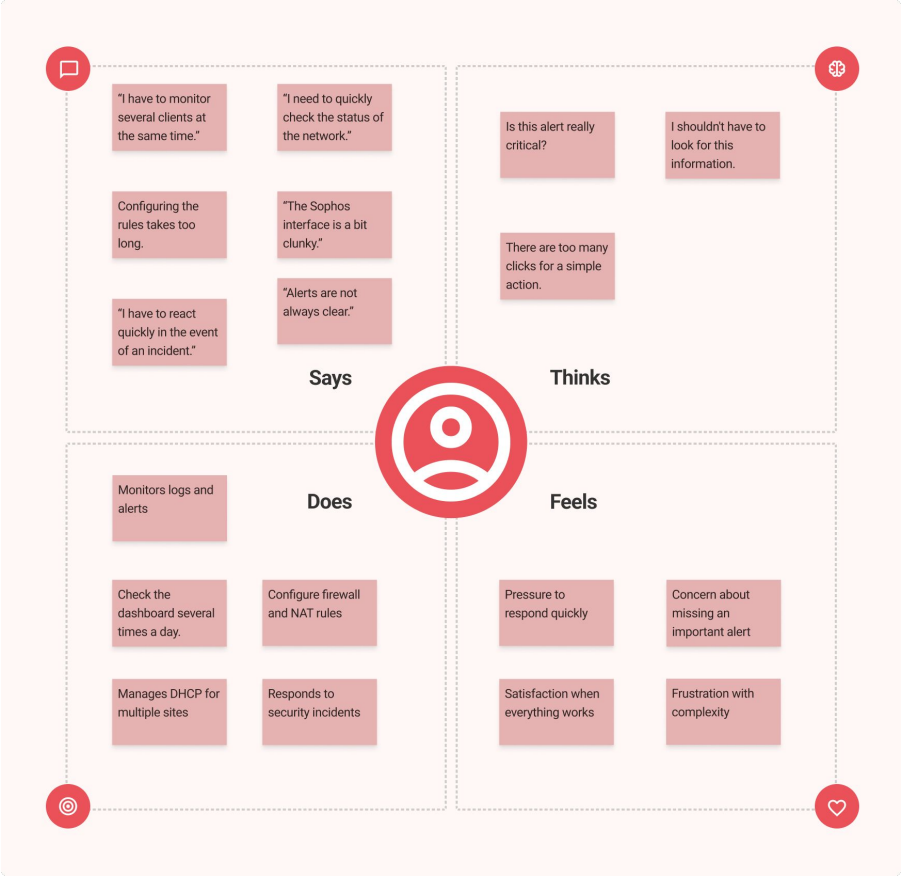
- User research
- Personas
- Problem statements
- User journey maps
- User flows

User research: summary

My work focused on implementing a user-centered design approach. I began by conducting user interviews and auditing the existing solution in order to build an accurate picture of administrators' needs, frustrations, and workflows (formalized using Personas and User Journey Maps).

Empathy map

For this technical B2B project, the empathy map is essential to ensure that the ergonomics are not only functional, but also reassuring, effective, and respectful of the administrator's pressure and work context.



User research: pain points

1

Pain point

Creating firewall, NAT, or DHCP rules requires numerous clicks through deep, unintuitive menus.

2

Pain point

Some features are not used by users, making the interface too cluttered.

3

Pain point

The lack of clear prioritization of alerts and notifications led to cognitive overload.

4

Pain point

The current software dashboard does not allow you to view the overall security status.

Persona: **Marc**

Problem statement:

Marc is a Senior System and Network Administrator who needs simplified configuration workflows and direct access to essential features such as NAT and Firewall rules because the current tool forces him to navigate through deep, unintuitive menus, turning simple tasks into time-consuming and frustrating processes.

Marc Favre

AGE	35
WORK	Senior System & Network Administrator
LOCATION	Chambéry, France
TECH LITERATE	High
STATUS	Married, 2 children

> I need a tool that allows me to see the status of all my customers at a glance and act quickly without wasting time in complex menus.

Bio

Marc has been working for seven years at an IT company specializing in managed services. He manages network security and infrastructure for 18 clients, mainly SMEs (20-150 employees) and town halls.

A typical day

- 8:30 a.m. Check the overall dashboard - review alerts from overnight
- 9:00 a.m. Configuring a new firewall for an SME client
- 11:00 a.m. Incident: resolving a NAT rule issue blocking a service
- 2:00 p.m. Adding DHCP rules for a new town hall client
- 4:00 p.m. Monitoring and adjustments for several clients
- 5:30 p.m. Generating weekly reports for three clients

Core needs

- Effectively monitor the security status of all your customers in real time
- Quickly configure firewall and NAT rules without errors
- Identify and resolve incidents in less than 15 minutes
- Automate recurring tasks (DHCP, standard rules)
- Generate reports for customers quickly

Frustrations

- Complex interface: Too many clicks for simple actions in the current software
- Cumbersome multi-client management: Must reconnect for each client
- Poorly prioritized alerts: Difficult to distinguish between critical and informational alerts
- Scattered documentation: Non-centralized configurations

Motivations

- Ensure optimal security for all customers
- Save time on repetitive tasks
- Respond quickly to critical incidents
- Stay up to date on best practices
- Maintain a work-life balance

User journey map

The investigation phase generates the most frustration with an interface that is not optimized for quick information retrieval.

By optimizing phases 2 and 4, resolution time could be reduced from 45-60 minutes to 20-25 minutes (a 50% gain).

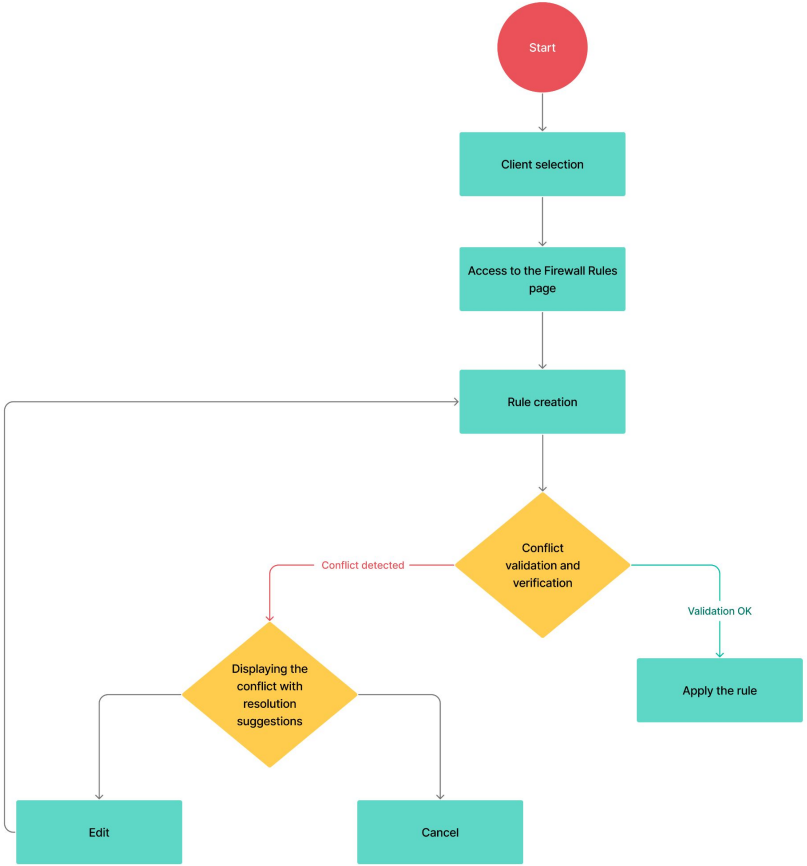
PHASES	PHASE 1	PHASE 2	PHASE 3	PHASE 4	PHASE 5
ACTIVITY	Detection	Investigation	Diagnosis	Resolution	Validation
ACTIONS	• Receives an email alert • Logins to the IT software • Checks the dashboard	• Search for related logs • Navigate between multiple tabs • Check the rule history • Compare with other clients	• Analyze firewall rules • Identify the problematic rule • Check dependencies • Document the problem	• Modify the firewall rule • Wait for propagation • Test the affected service • Check the metrics	• Monitor alerts • Contact the end user • Check logs • Close the ticket
THOUGHTS	• "Is this critical?" • "Which customer is affected?" • "Do I need to take action now?"	• "What caused this?" • "Is there a pattern?" • "Where is the information I'm looking for?"	• "This rule is definitely the problem." • "Who created this configuration?" • "Will it affect other services?"	• "Have I considered everything?" • "How long will it take to apply?" • "It should work now"	• "Everything is back to normal" • "The customer is satisfied" • "How long did it take me?"
PAIN POINTS	• Lack of detail in email alerts • No immediate context • Must guess the criticality	• Information scattered throughout the interface • Too many clicks to access logs • No automatic correlation • Interface slow to load	• Difficult to visualize the impact of a rule • No history of changes • Lack of validation before change	• Long modification process (7-10 clicks) • No immediate feedback • Uncertainty about propagation • Risk of configuration error	• Must manually check multiple sources • No automatic confirmation • Resolution time difficult to track
EMOTIONS	Anxious	Frustrated	Focus	Stressed	Relieved
OPPORTUNITIES	• Opportunities • Contextualized alerts with criticality level • Push notification with details • Direct access to the affected customer	• Consolidated view of relevant logs • Automatic cause suggestions • Visual timeline of events • Quick multi-client comparison	• Visualization of the impact of rules • Complete history with author • Simulation before modification • Auto-generated documentation	• Modification in 2-3 clicks • Real-time feedback • Easy rollback in case of error • Configuration templates	• Automatic confirmation of resolution • Notification to the customer • Auto-generated incident report • Performance metrics

User Flow

Scenario: Creating a firewall rule to block a port

Objective: Marc must create a firewall rule to block port 23 (Telnet) on an SME client's network following a security request.

Optimized process: New solution (3-4 steps) vs. old software (8-10 steps)

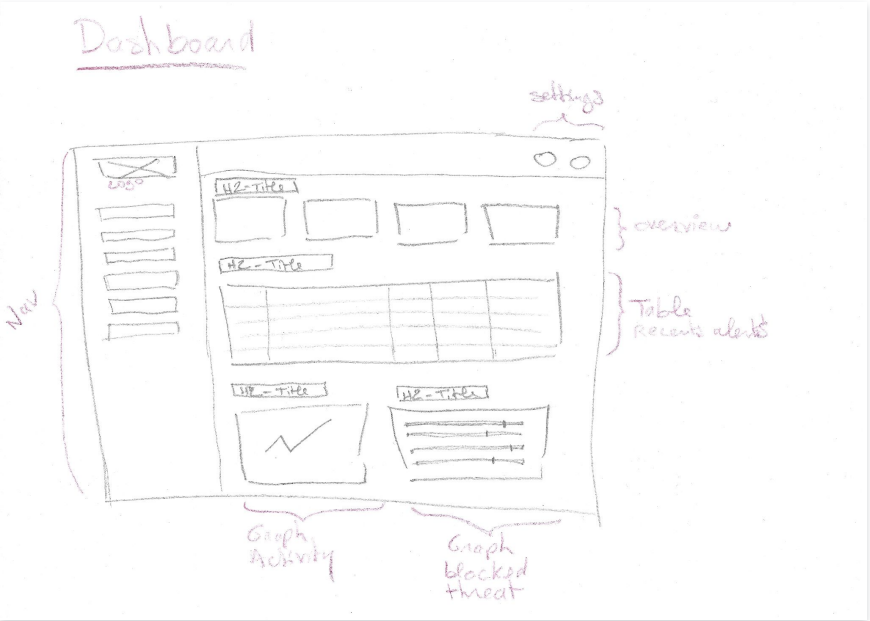


Starting the design

- Paper wireframes
- Low-fidelity prototype
- Usability studies

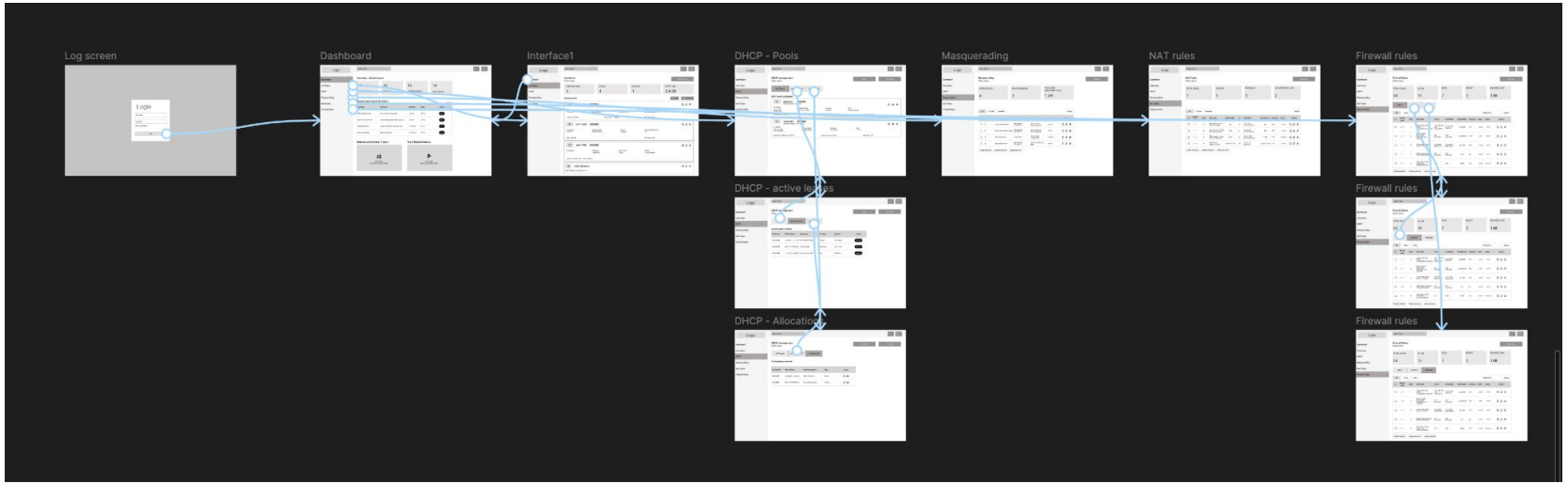
Paper wireframes

Focusing on the core features identified during user research, I sketched the first wireframes using pen and paper.
By setting aside aesthetic considerations (colors, fonts) to focus exclusively on the hierarchy of features and user journeys, paper facilitates direct, uncomplicated collaboration between designers and stakeholders before high-fidelity production begins.



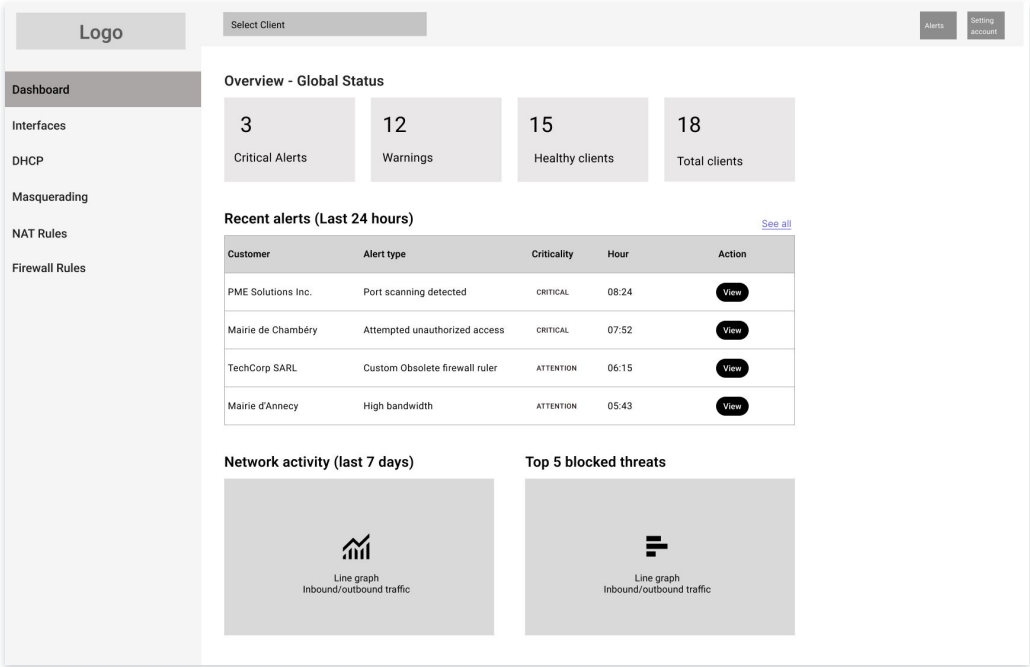
Low-fidelity prototype

Low-fidelity wireframes were a crucial step in the design of the cybersecurity software, allowing us to quickly validate the information structure and user journeys before investing in the visual design.



Low-fidelity prototype

I created wireframes for all key pages in the system: Dashboard, Interfaces, NAT Rules, Firewall Rules, Masquerading, and DHCP. This low-fidelity approach allowed me to focus on information architecture, content hierarchy, and feature organization without being distracted by aesthetic choices.

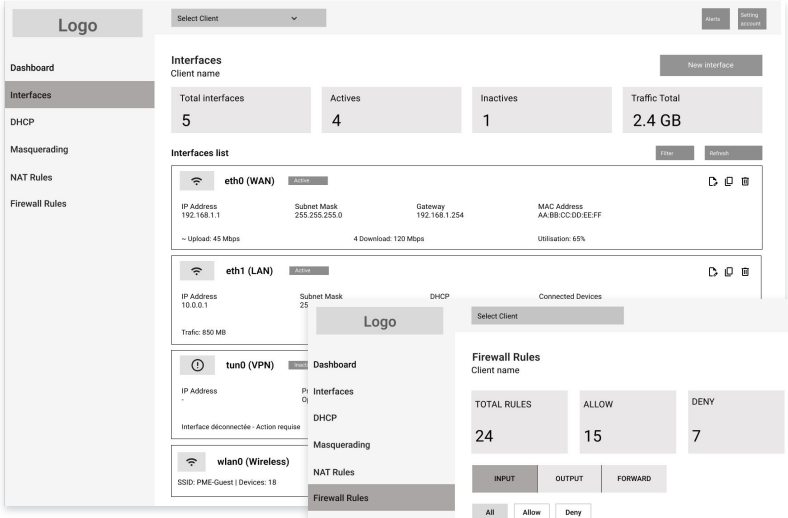


Dashboard page

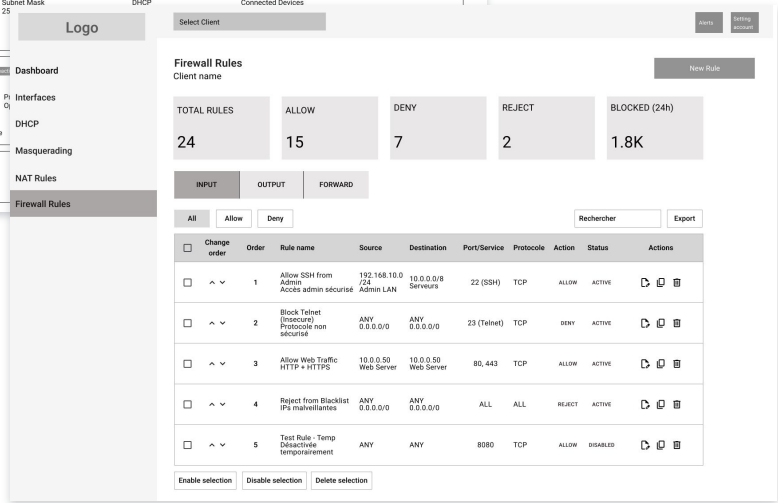
Low-fidelity prototype

Les wireframes ont mis en évidence des solutions innovantes comme le sélecteur de clients persistant dans le header, les tableaux avec actions en ligne pour réduire les clics, et l'organisation par onglets ou cards selon le contexte. Cette phase de wireframing a permis d'obtenir des retours précoces de Marc (le persona principal) et d'itérer rapidement sur les concepts avant de passer à la haute fidélité, économisant ainsi un temps précieux et réduisant les coûts de modifications ultérieures.

Interfaces page



Firewall rules page



Usability study: findings

Now that I have the key insights from the usability study, let's look at the findings and define the actual problems that a designer can solve.

Finding 1

Rules Management Table: The vertical order of security rules is not intuitively understood as the actual execution priority, despite the presence of a numbering column.
Detail missing: There is a disconnect between the static display of the list and the dynamic logic of "Top-Down" processing. Without visual affordances for reordering users lack the confidence that the rule position directly dictates the filtering outcome.

Finding 2

Global Header: Users failed to perceive the client selector as a persistent global navigation element, leading to redundant navigation patterns.
Detail missing: The UI lacks a clear visual "anchor" that confirms the selected context remains active across different modules. Users defaulted to their legacy mental model (based on Sophos), where changing a client requires returning to a central dashboard.

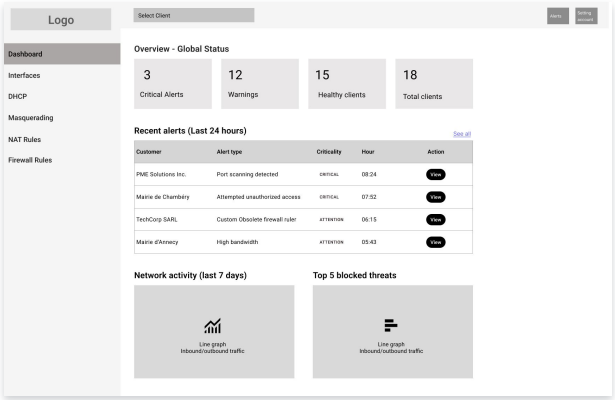
Refining the design

- High-fidelity prototype
- Accessibility

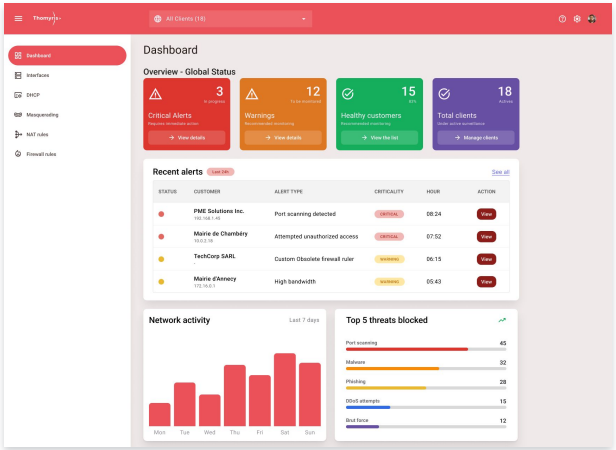
Mockups

By synthesizing the usability test findings, I evolved the low-fidelity wireframes into high-fidelity mockups. This transition focused on mitigating user anxiety through explicit confirmation loops, securing the configuration flow, and improving the signal-to-noise ratio with a high-contrast visual hierarchy for critical alerts.

Before usability study

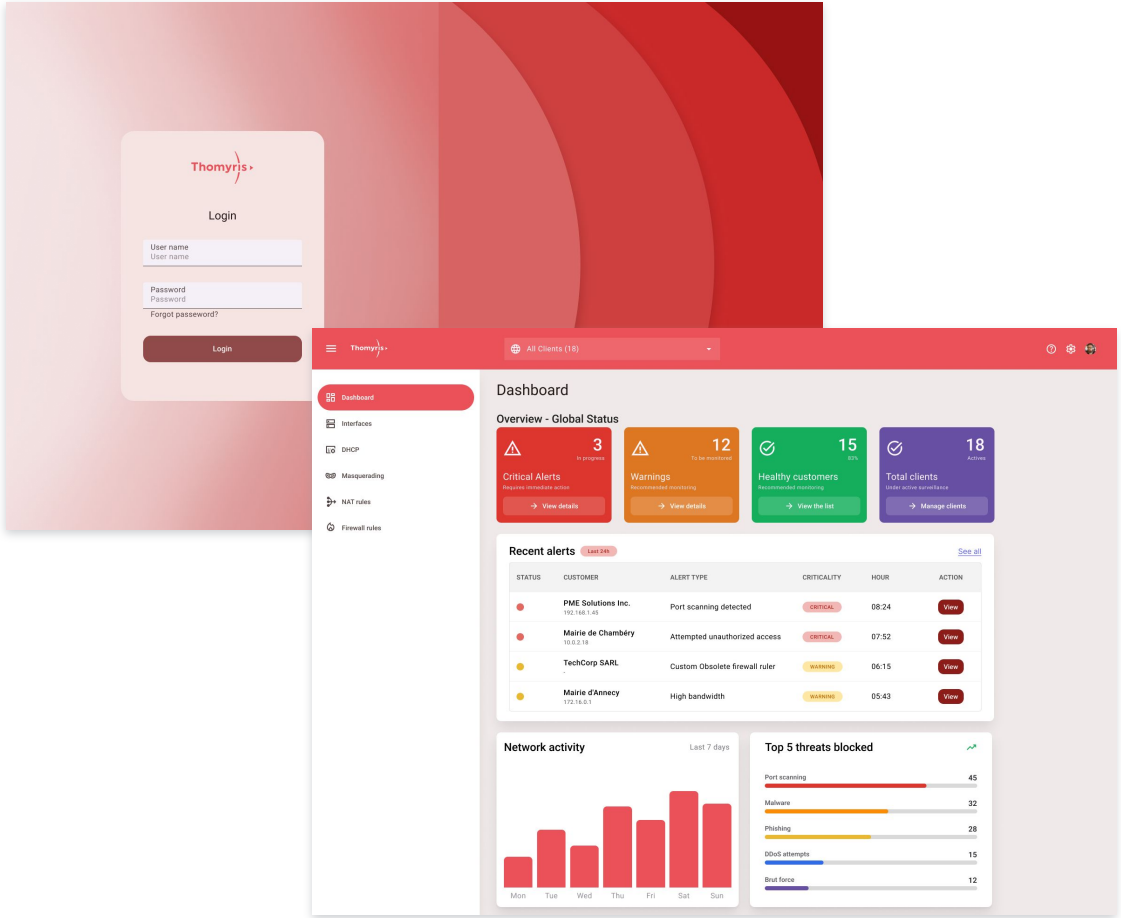


After usability study



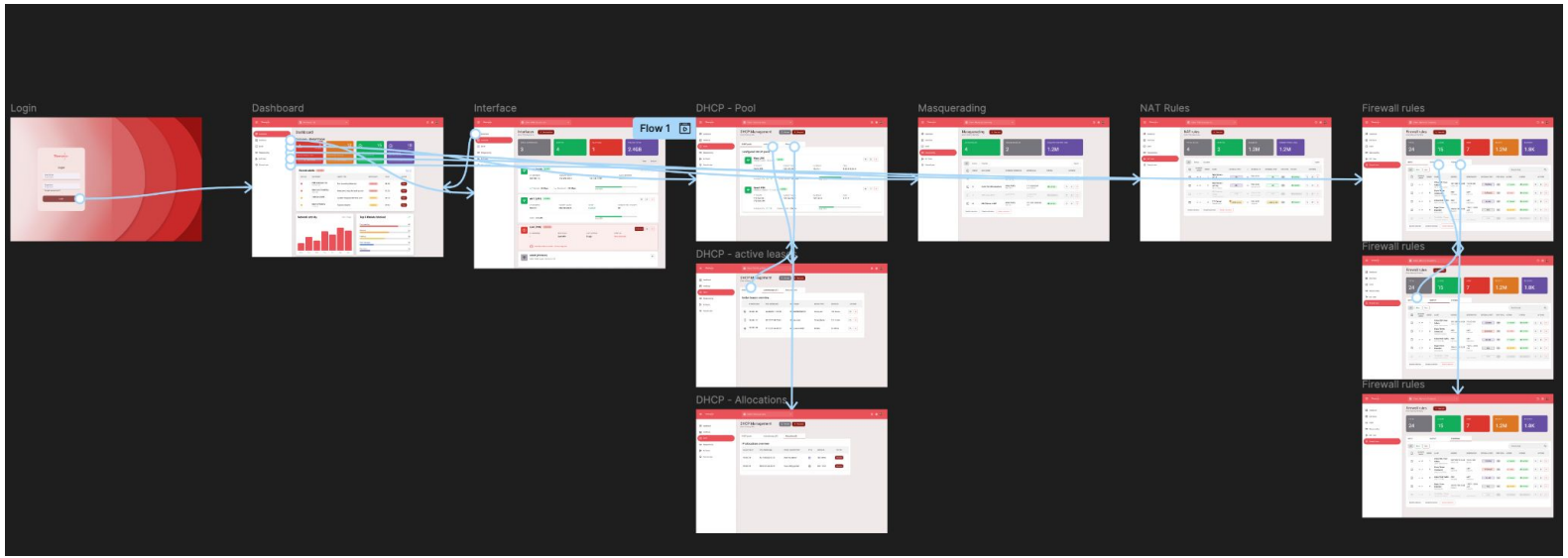
High-fidelity prototype

Thomyris' visual design is based on a rigorous adaptation of Material Design, optimized for information density. To resolve the conflict between brand identity (red) and security codes, we introduced a deep burgundy for interactions, reserving bright red exclusively for critical alerts. This color hierarchy, coupled with a modular structure, ensures maximum user responsiveness to threats.

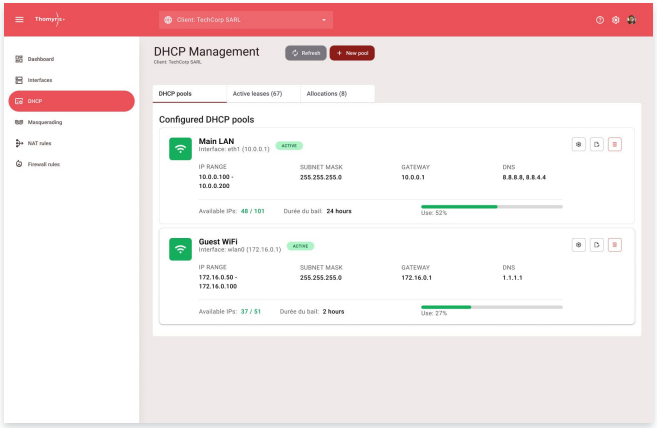


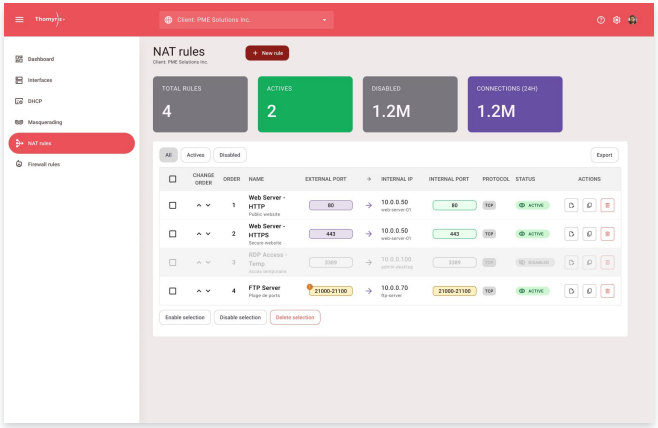
High-fidelity prototype

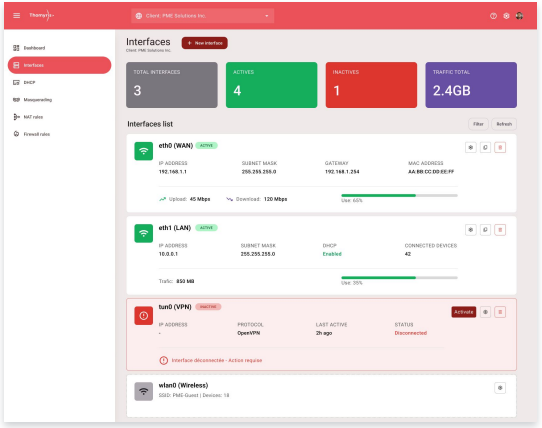
Thomyris' navigation has been optimized for crisis management. By combining a global context selector (Header) and a static functional menu (Sidebar), we eliminate multi-client handling errors.

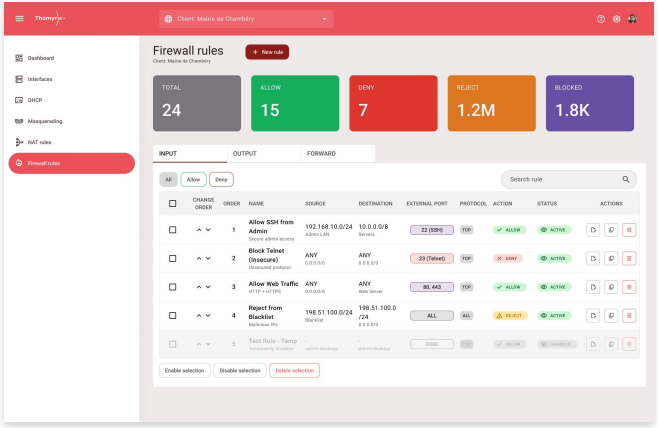


High-fidelity prototype









Outcomes

Maximized Productivity & Profitability

The transition to instant multi-client and simplified workflows **would reduce configuration time by 80%**, freeing up to **15 hours per week** per administrator.
The solution would eliminate the need for third-party licenses, generating direct savings of several thousand euros per customer.

Enhanced Security & Quality of Service

The introduction of automatic validations **would reduce configuration errors by 70%**, further securing customer infrastructures.
Visual prioritization would enable threats to be identified three times faster, drastically reducing the window of exposure to risks.

Employee Experience & Engagement

Reducing cognitive load and stress related to destructive actions **would significantly improve job satisfaction** (target NPS: 8.5/10).
Thanks to the intuitive interface, training time for new experts would be **reduced by 60%**, facilitating team growth.

Going forward

- Takeaways

Takeaways

Impact:

The deployment of the software would mark a strategic turning point for the company by resolving the major issue of costly dependence on third-party solutions. By developing a proprietary platform, the company would not only eliminate annual licensing fees amounting to several thousand euros per customer; it would open the doors to an untapped market of SMEs and local authorities. Thanks to a design optimized for mass management and an intuitive interface, the company could now offer a sovereign, agile solution perfectly suited to the budgets and specific needs of local players, transforming a cost center into a new high value-added revenue channel.

What I learned:

As a UX UI designer working on a cybersecurity software, I have gained valuable insights and knowledge through the design process. Some of the key things I have learned include:

- Understanding user needs
- Importance of simplicity
- Accessibility considerations
- User feedback
- Manage information to not overwhelm the user

Let’s connect!

Email

lossouarn.armelle@gmail.com

Website

www.armelle-lossouarn.com

LinkedIn

@armelle-lossouarn

Behance

@armellelossoua