High Security Laboratory (LHS)

Inria
INVENTEURS DU MONDE NUMÉRIQUE

Loria
Laboratoire lorrain de recherche en informatique et ses applications

cnrs

UNIVERSITÉ DE LORRAINE

What is the HSL ?

- **Highlights**
  - ~ 800K€ (FEDER – Conseil Régional Lorraine - Communauté Urbaine du Grand Nancy- DRRT – Inria)
  - A physical place (« bulletproof »)
  - A dedicated network – RIPE – routing
  - A full enclosure infrastructure (autonomous infra)
  - A specific IT Team (~ 2 ETP)

High Security Laboratory (LHS)

An academic infrastructure for ...

- **Research in security**
  - Virology – Malware analysis
    - Packer analysis
    - Flow control graph ,dynamic execution in sandboxing
  - Malware capture & Darknet - Internet comprehension
    - Honeypots networks (servers and evolution to LIHC)
    - Darknet real-time and analysis
  - Android security
    - OVAL for android
    - APISense
  - ...

Research in security ⇒ Sensitive data

High Security Laboratory (LHS)

High Security Laboratory (LHS)

...Question about confidentiality...

- **What is the confidentiality level ?**
  - *Of my data ? Of our code ? Of our results ?*
  - *Of the code given by company ? (NDA → what kind of security engagement) ?*
  - *Legal issues ? (CNIL, medical, ...)*
- **Security vs Usability ?**
  - *Share with others ? (always)… mail ?*
  - *Asynchronous work on my laptop ?*
  - *Applications links ...*

High Security Laboratory (LHS)

...Answer about confidentiality...

- **Absolute security doesn't exist**
  - *A question of money, time, usability*
  - *Confidentiality vs availability,*

- **How to set the correct level ?**
  - *Risk management (EBIOS, …)*
    - *Method,*
    - *DIY*
  - *A question of TRUST*

High Security Laboratory (LHS)

High Security Laboratory (LHS)

LHS : A secured physical place

How to build the Trust

Partitionning, physicals protections

- A dedicated closed physical area
- 3 zones
  - Office / Computer room / Red room
  - Differents individual authorization
- A almost dedicated power supplie
- A isolated authentication system
- Strong authentication (2 factors).
  - Biometric & badge
- Armored glass
- ...

LHS : A specific network

How to build the Trust

Network and Host security, technical, architectural and setup

- A dedicated network, dedicated equipments.
- 2 (differents) firewalls with stricts rules, even between internal networks
- NAT
- LAN prefered to VLAN, same kind of Vhosts on the same physical host.
- Full centralized administration.
- Log centralisation
- Bastion & dedicated VPN ... or not (safes).
- Centralized account ... or not (safes).
- Proxy outgoing... or not (safes).
- ...

Come and see by yourself...

LHS : Sensitive data hosting

Supply – Level 1

Virtual server

- A virtual server (debian)
- On the DMZ if services access from the outside.
- Admin account.
- Access by ssh via bastion or openvpn.
- Local files (databases, ...) or on the LHS-NAS
- Puppet management
  - Apache/nginx, git/gitlab, wordpress/mediawiki, ssh, mysql, postfix, apt, ldap, icinga, rsyslog, ...
- ...

LHS : Sensitive data hosting

Price :

1 server minimum.
Please ask us for the setup.

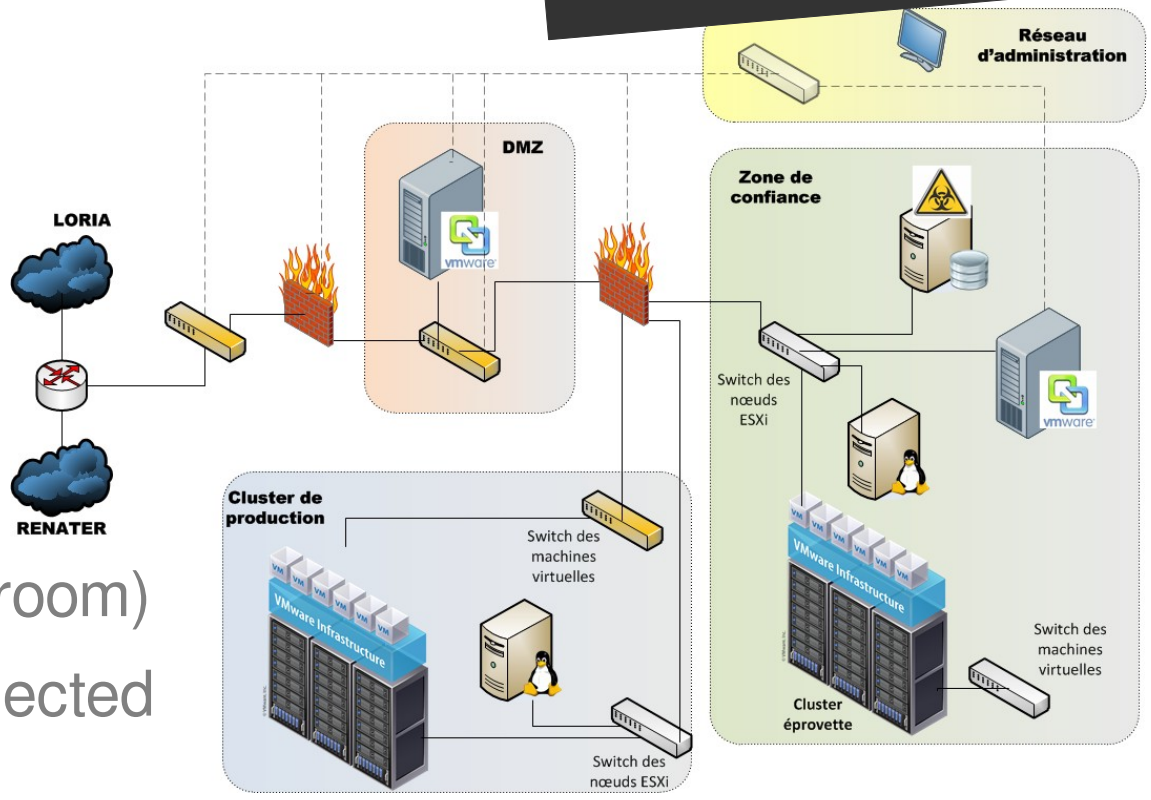
Supply – Level 2

A dedicated private LAN

- A dedicated LAN
- A physical server & vhosts (level 1)

A « disconnected » Server

- A physical server (Red room) connected directly connected to a another.
- vhosts (level 1)



LHS : Sensitive data hosting

Supply – Level 3

Safes

- Provide a secured distant workspace to a team
  - Data must be in this workspace
  - Data usage must be done in this workspace
- Different teams must be mutually isolated
- Supplier administrators must not be able to access data
  - Physical access to hardware must not allow to access data

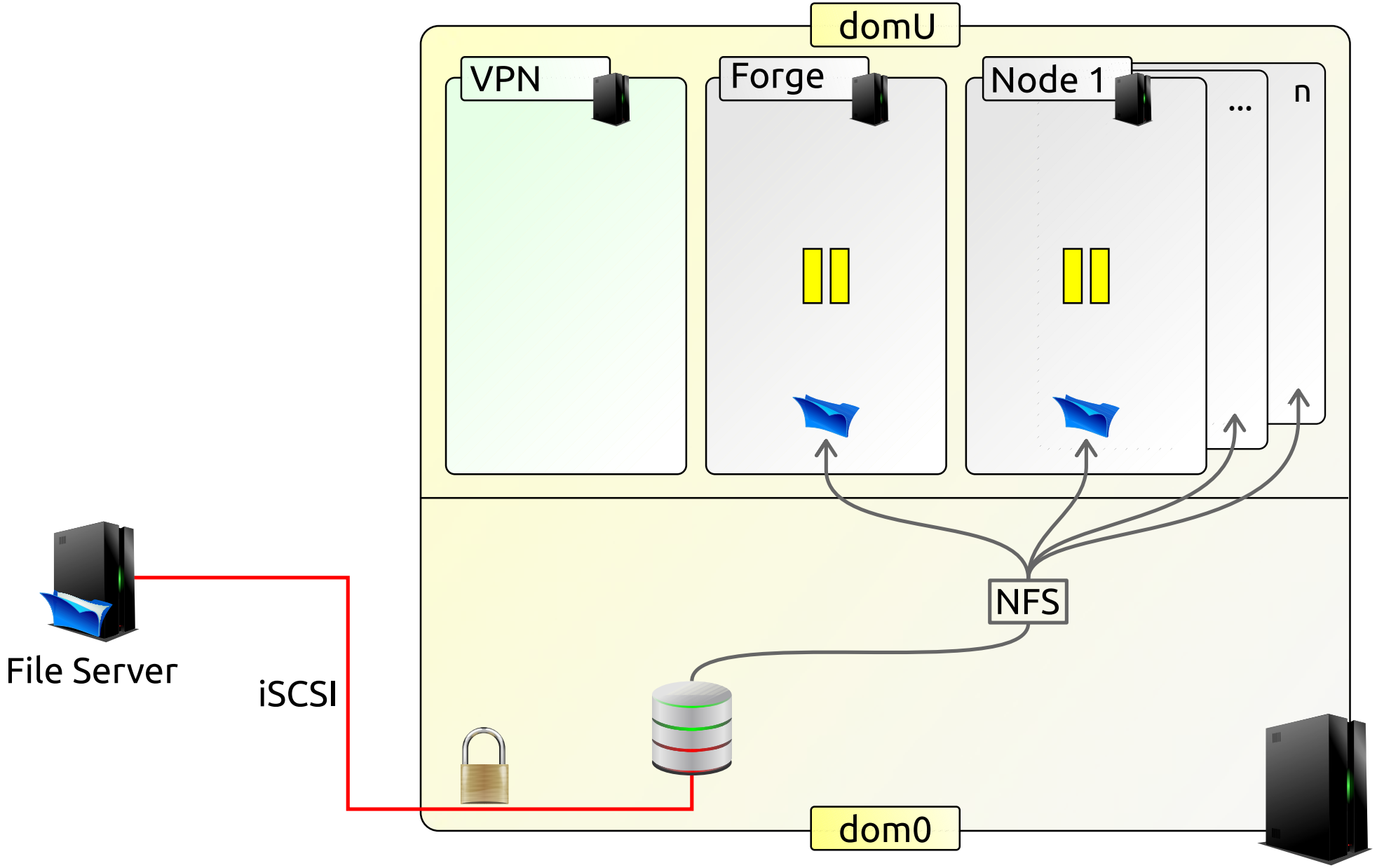
LHS : Sensitive data hosting

Supply – Level 3

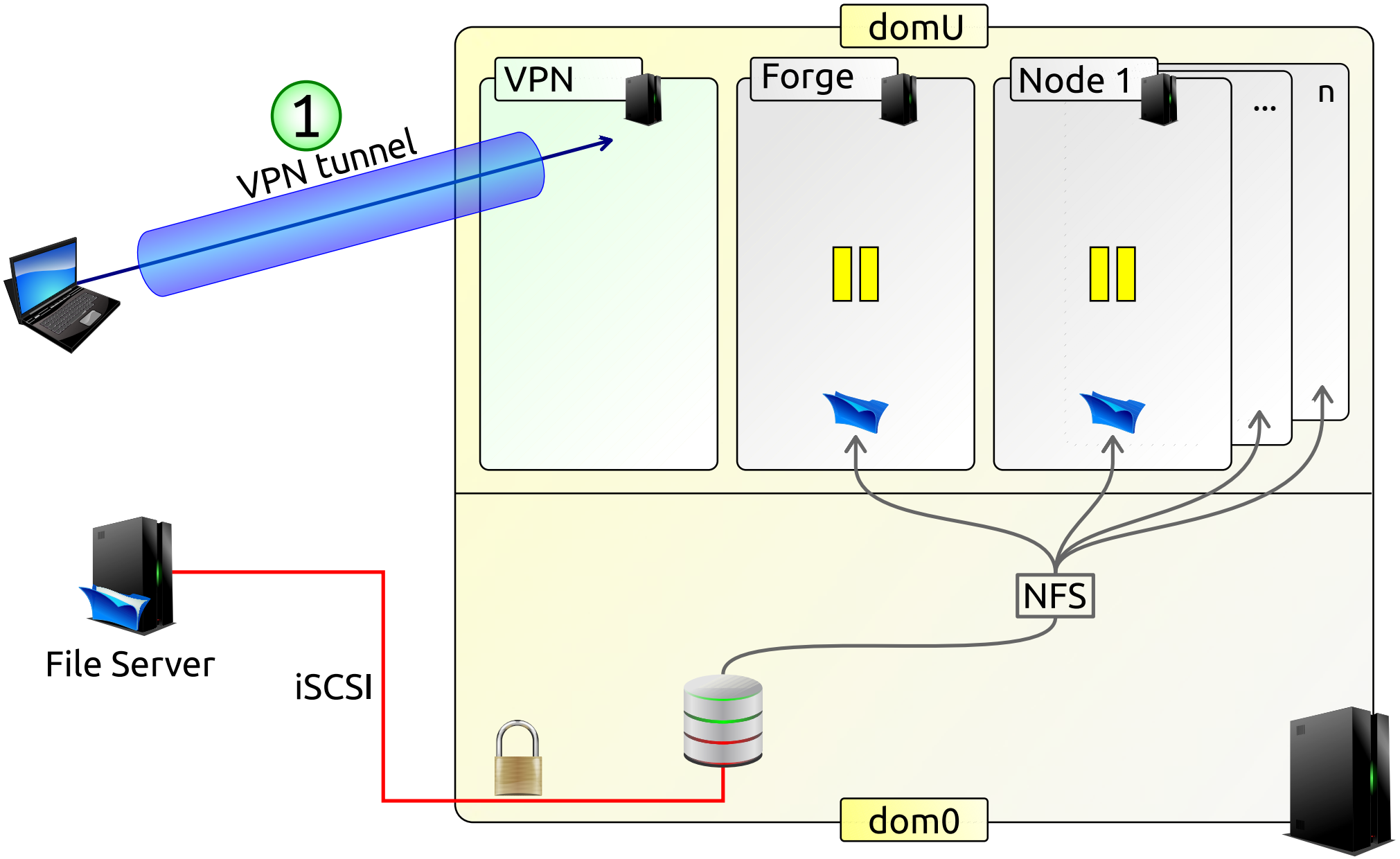
Safes

- Data confidentiality/privacy oriented
- Work directly in the safe, data don't need to go out for use
- When nobody is logged, unencrypted data are not available
- Safe is closed when the last user disconnects
- Isolated and secure network and storage
- Stack of basic services
- Scalable computing and services nodes
- Protected against the administrators of the supplier

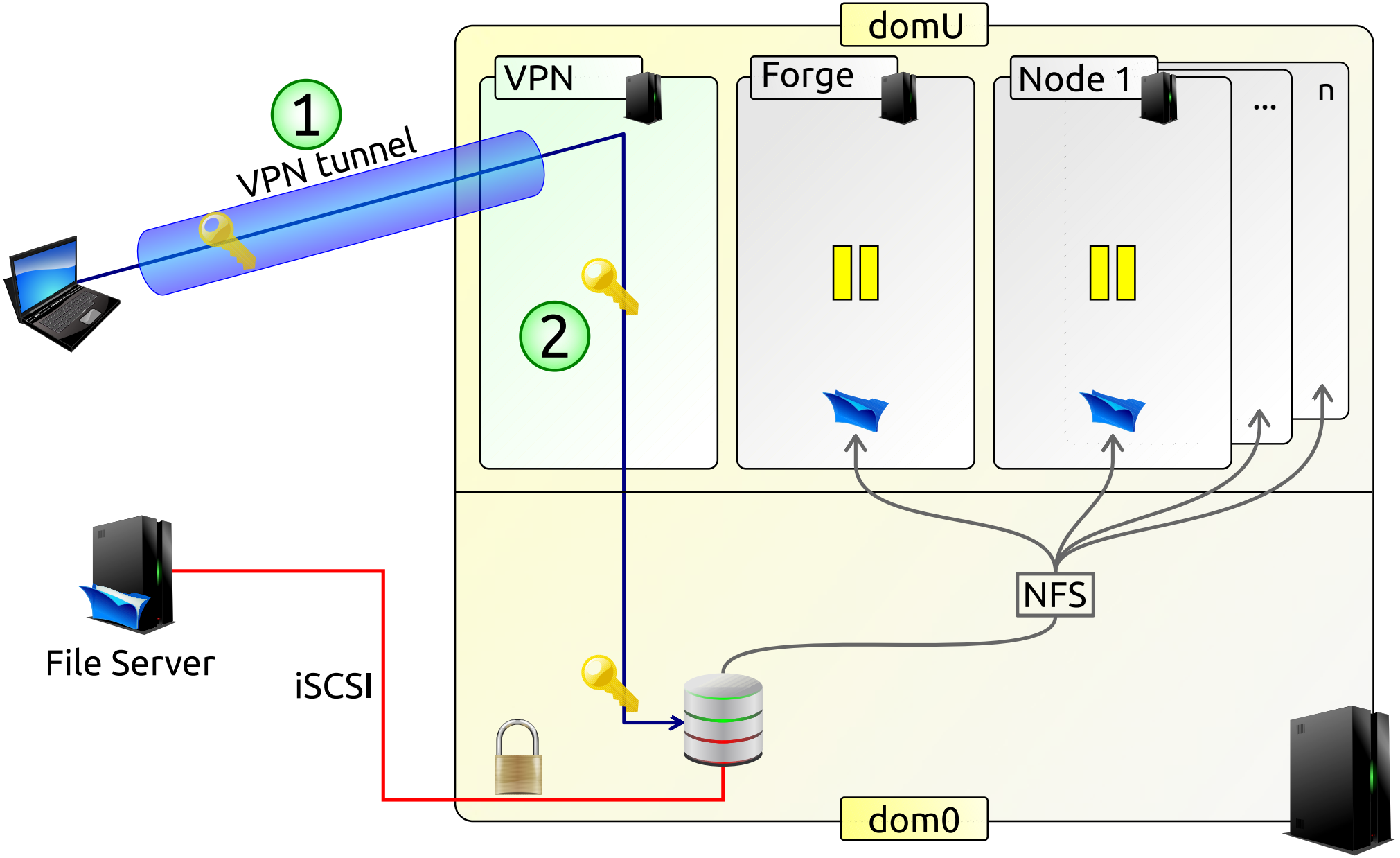
LHS : Focus on Safes – State 0 : safe closed.



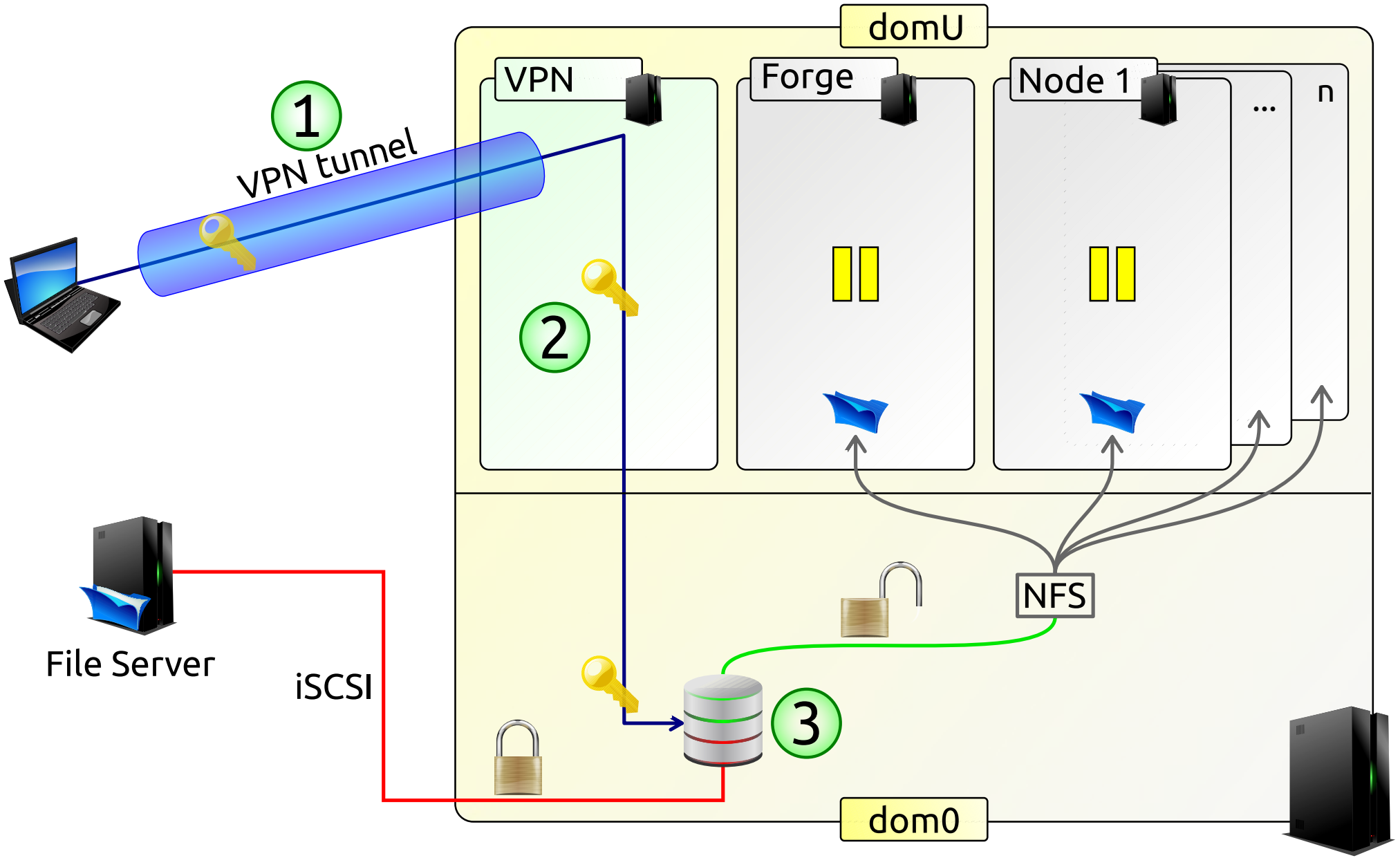
LHS : Focus on Safes – State 1 : First user connection.



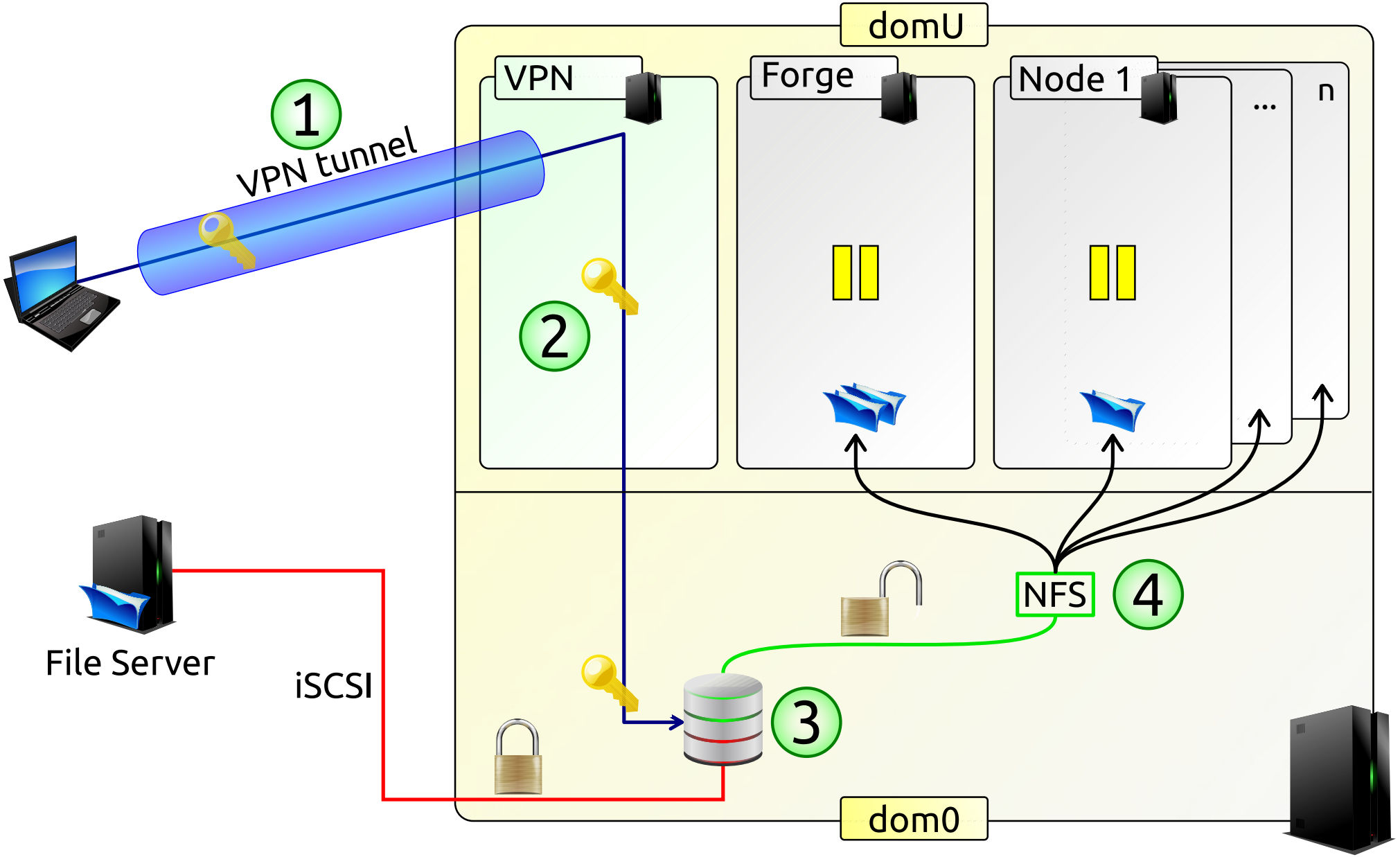
LHS : Focus on Safes – State 2 : Decyphering.



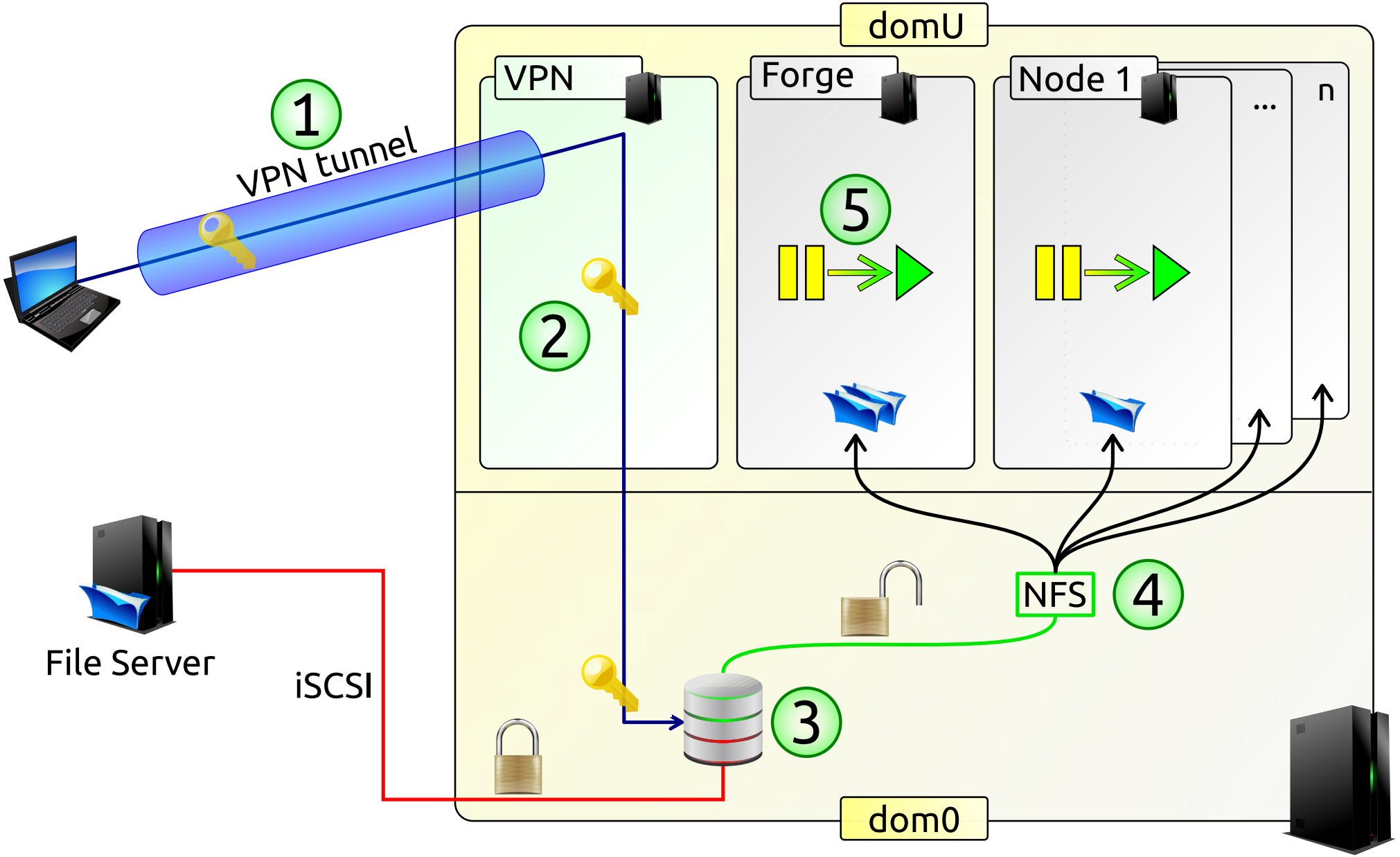
LHS : Focus on Safes – State 3 : Exporting clear data.



LHS : Focus on Safes – State 4 : Sharing data for VM.



LHS : Focus on Safes – State 5 : Waking up VMs.



LHS : questions