

# Security Issues related to Cloud Computing and Virtualisation

Philippe Massonet  
([philippe.massonet@cetic.be](mailto:philippe.massonet@cetic.be))

The research leading to these results has been partially funded by the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 215605.

## Definition of Cloud Computing

- Cloud is IT as a service, delivered by virtualized resources that are independent of location
- Cloud computing is a deployment model in which IP-based connectivity provides services delivered from a logical resource rather than a hard-wired/physical one.
- Different levels: IaaS, PaaS, SaaS
- At the confluence of grid computing, virtualization, utility computing, hosting and software as a service.

## The Reservoir Vision - Positioning

- RESERVOIR is an aggressive research attempt to meet the emerging needs of the service-based economy sponsored by the EU
- There are many other solutions out there
  - Amazon EC2 (Elastic Compute Cloud),
  - S3 (Simple Storage Solution),
  - Google and IBM cooperative effort
- So what's new in RESERVOIR ?

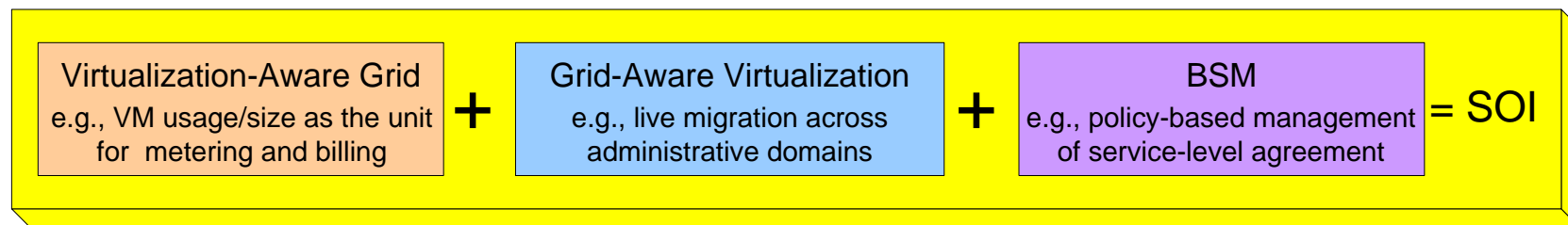
# Motivation for RESERVOIR

- Service-oriented economy is at our door
- Services over the internet are winning in the market
  - Consumers use YouTube, eBay, Amazon, Second Life...
  - SMEs use hosted Microsoft Exchange, Salesforce.com
  - Enterprises routinely rely on remote IT outsourcing
- Services reduce complexity and cost

Service-Oriented Economy  
requires  
Service-Oriented Infrastructure (SOI)

# Approach


- Focus on technologies that enable to build cooperating computing clouds
- Integration of virtualization technologies with grid computing driven by new techniques for business service management  $\Rightarrow$  The Service Oriented Infrastructure (SOI) equation:



- Building on this equation we will architect and implement a platform for supporting complex services, which
  - Enables dynamic deployment of complex multi-tier services across heterogeneous administration domains
  - Take a inclusive look at virtualization of servers, network and storage
    - Enable migration “without borders”
  - Supports service definition, SLA management, accounting and billing

# Scenario – Service Definition

## Web site service

1. The Olympic committee uses client tools to generate the service definition. 

### Includes:

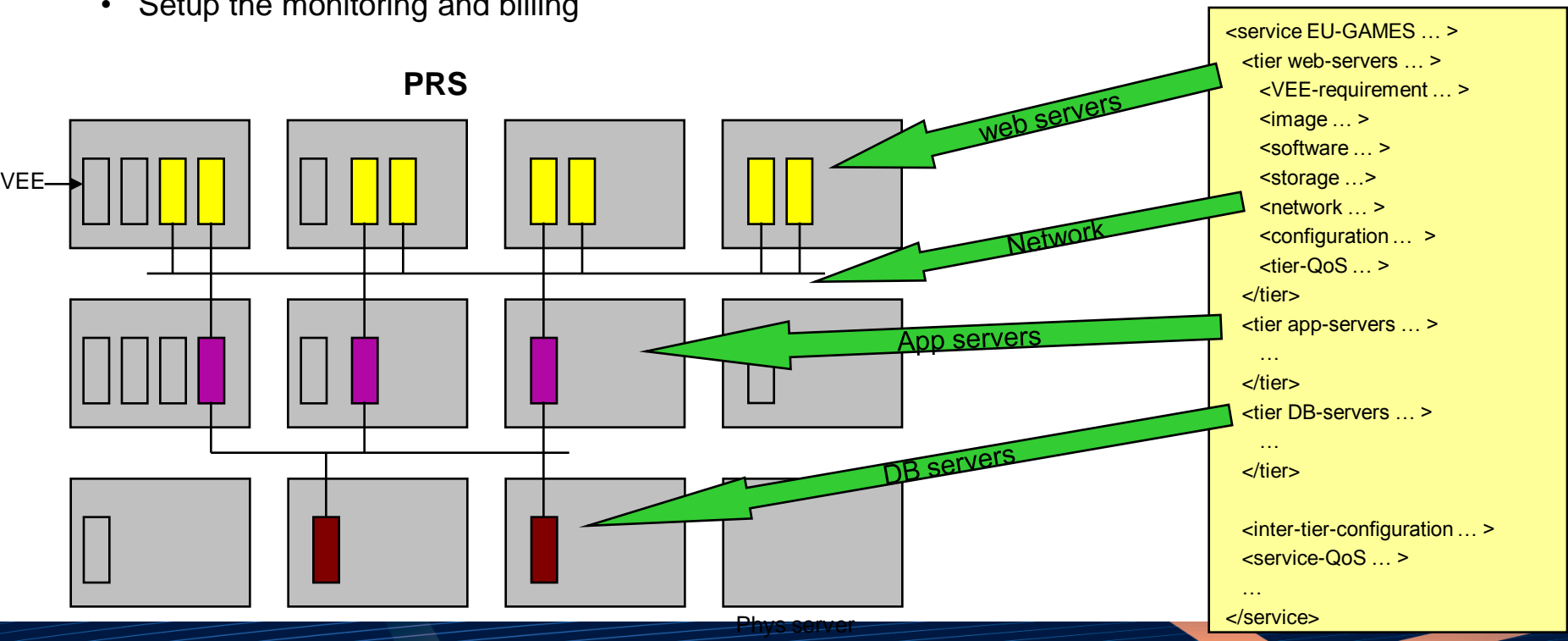
- Tier definition (web servers, application servers, databases)
- Required Virtual Execution Environments (VEEs)
- Software
- Images
- Storage
- Network
- Required configuration
- Inter-tier relations
- **Required QoS.**

```
<service EU-GAMES ... >
  <tier web-servers ... >
    <VEE-requirement ... >
    <image ... >
    <software ... >
    <storage ...>
    <network ... >
    <configuration ... >
    <tier-QoS ... >
  </tier>
  <tier app-servers ... >
    ...
  </tier>
  <tier DB-servers ... >
    ...
  </tier>

  <inter-tier-configuration ... >
  <service-QoS ... >
    ...
</service>
```

# Scenario – Service Deployment

2. The committee negotiates and ships the service definition to a primary RESERVOIR site (PRS)
3. The PRS automatically deploys the complex service on its own site:
  - Configure required storage & network, creates VEEs selecting proper physical resources to meet QoS
  - Install required images, software according the service definition
  - Apply the required configuration
  - Setup the monitoring and billing

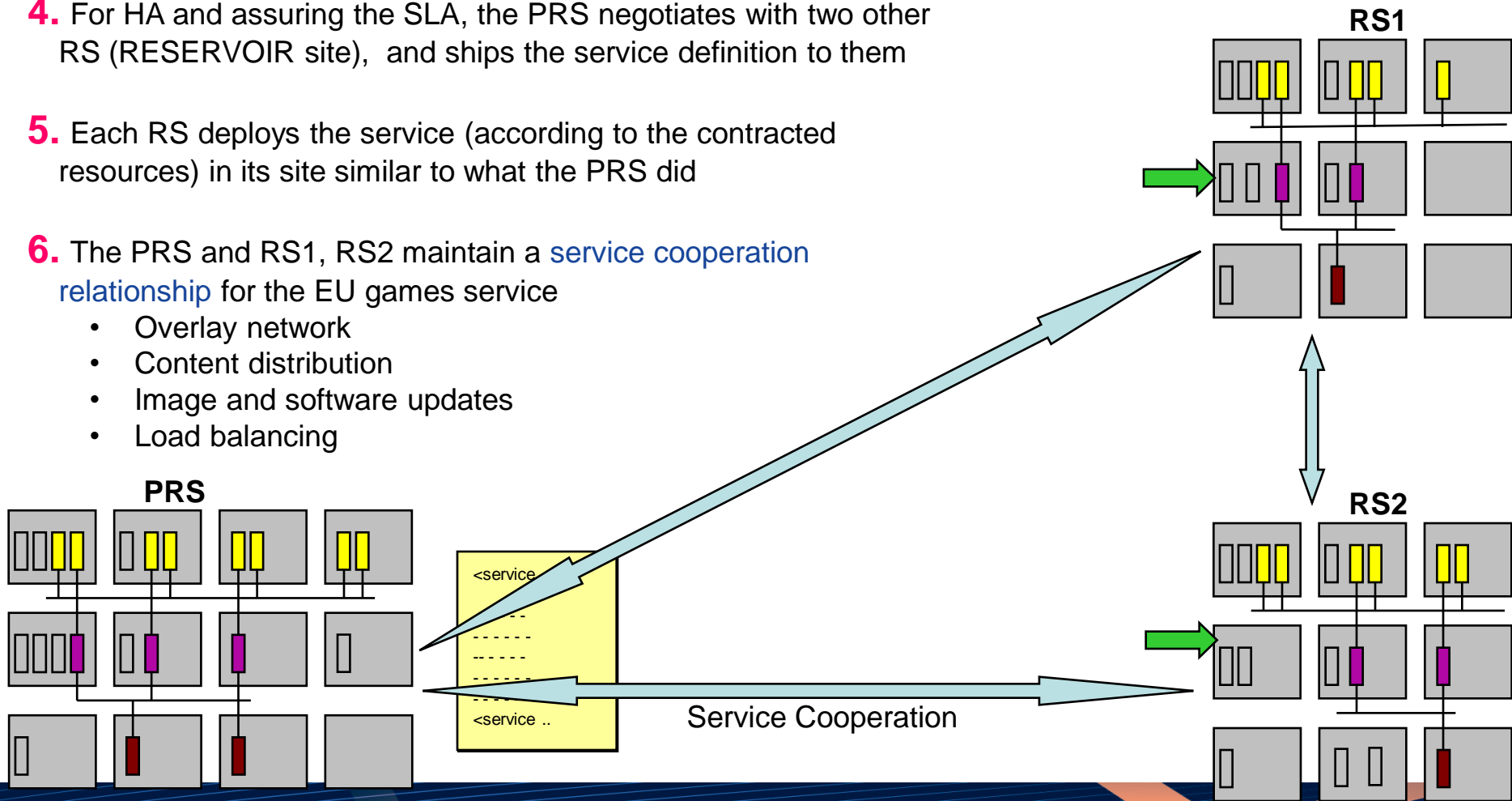


## **RESERVOIR Differentiator:**

Service definition language enabling automatic deployment of complex services over virtual infrastructure

# Scenario – Service Cooperation

4. For HA and assuring the SLA, the PRS negotiates with two other RS (RESERVOIR site), and ships the service definition to them
5. Each RS deploys the service (according to the contracted resources) in its site similar to what the PRS did
6. The PRS and RS1, RS2 maintain a **service cooperation relationship** for the EU games service
  - Overlay network
  - Content distribution
  - Image and software updates
  - Load balancing

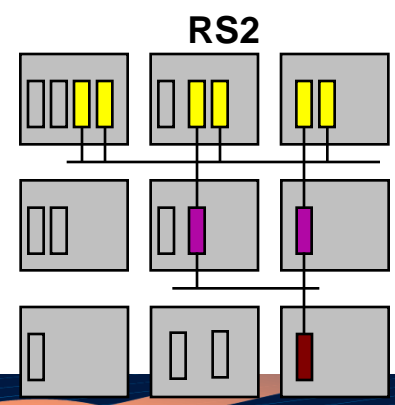
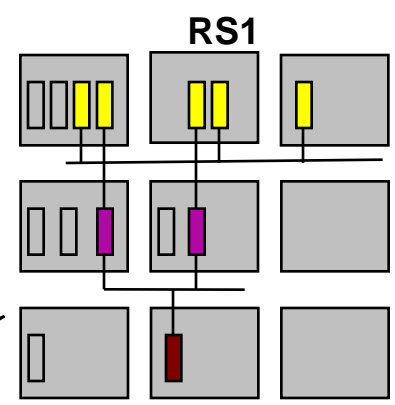
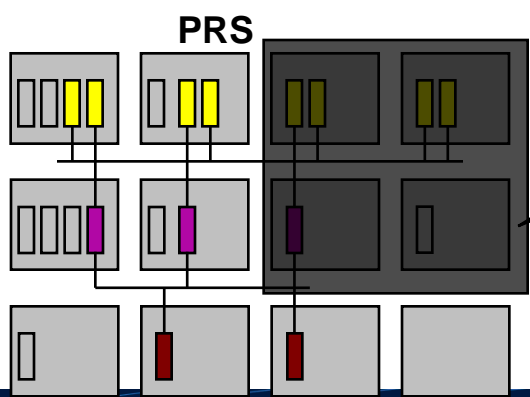


## **RESERVOIR Differentiator:**

Inter-domain management site protocols that enable multiple management sites to cooperate in providing a single service, where the cooperation is automatically driven from a service definition document.

# HA with Live VM Migration

- 7. PRS site suffers electricity problems and needs to power off physical servers.
- 8. PRS negotiates for additional resources at RS1 employing the RS-RS protocol
- 9. PRS *evacuates* the VEEs on the servers to be powered off, migrating them to RS1
  - Live migration to maintain application servers' states and client connections



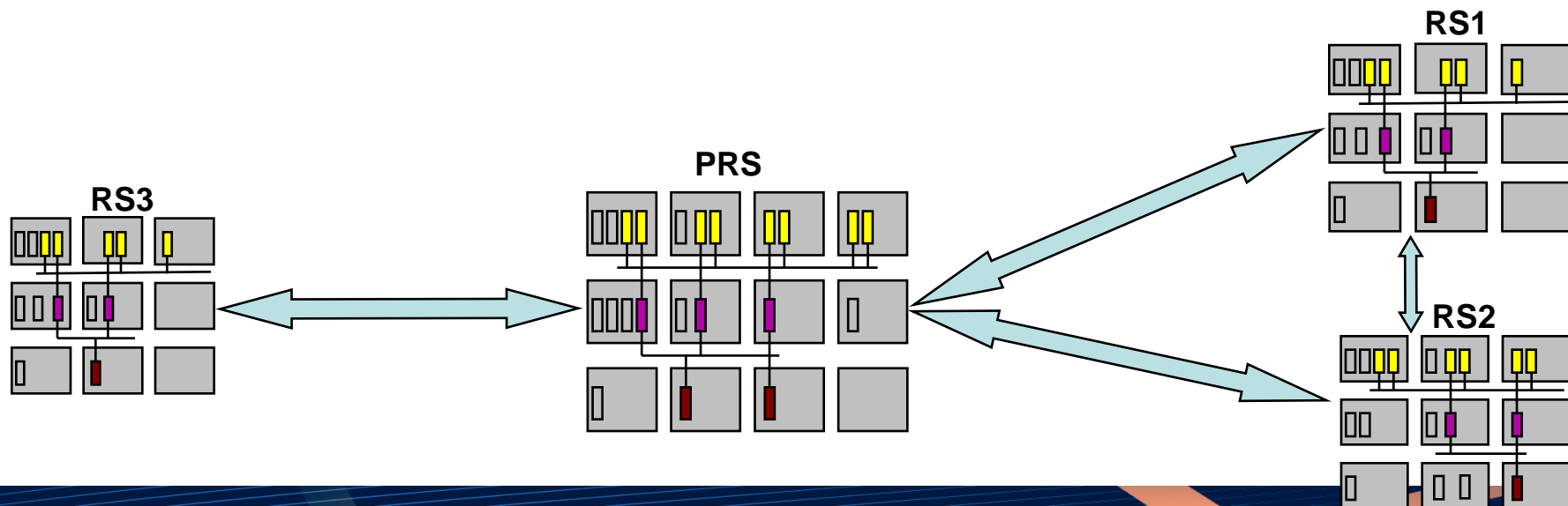
## **RESERVOIR Differentiator:**

Live migration without borders:

Cross geographical, network and management domains

# Scenario – On Demand Service Expansion

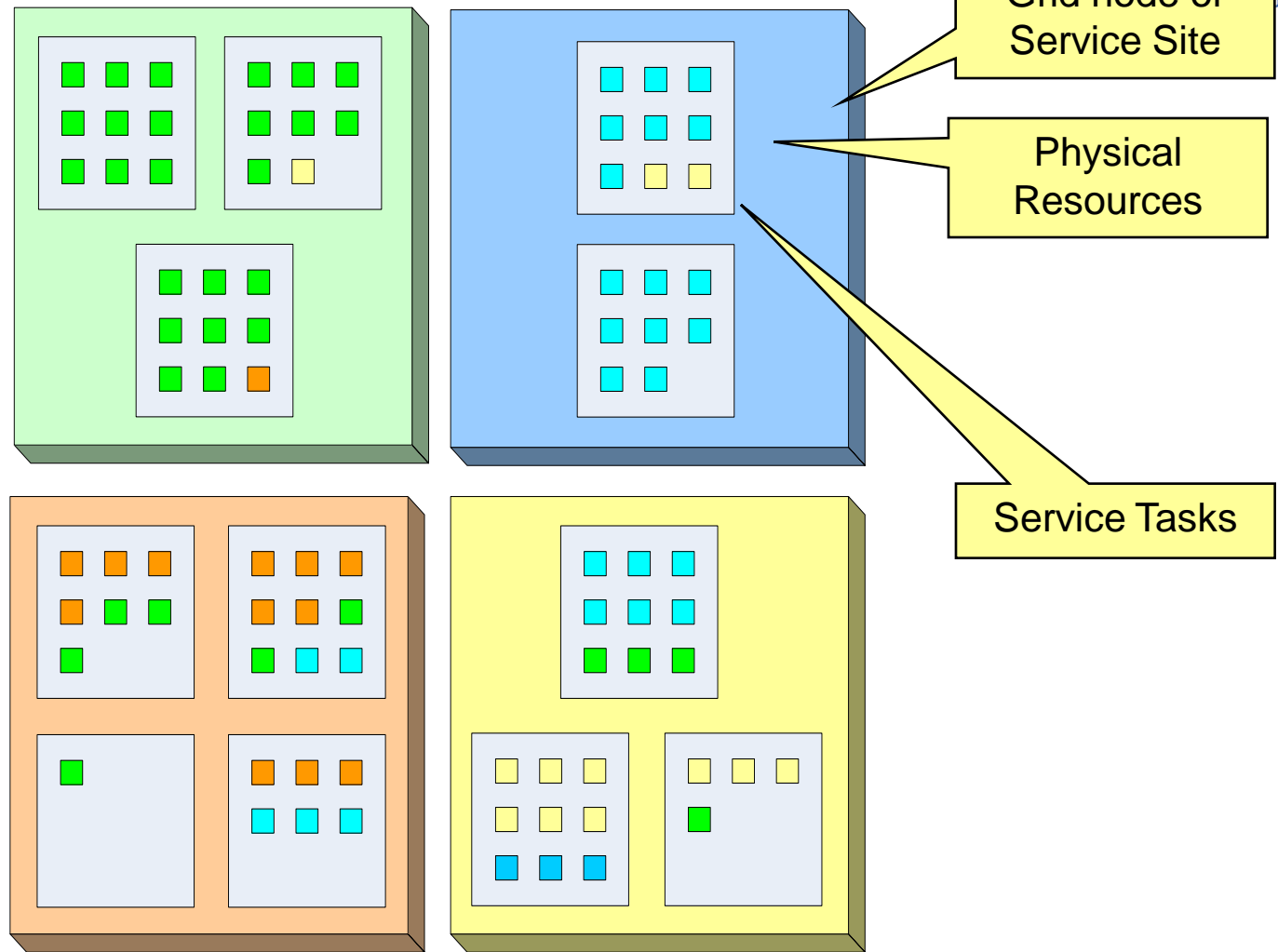
10. Load increases and PRS realizes that the available resources at the 3 sites are not enough
11. PRS negotiates with additional RS3, and ships it the service definition
12. RS3 deploys the service (according to the contracted resources), and **dynamically joins** the **service cooperation relationship** for the EU Olympics service



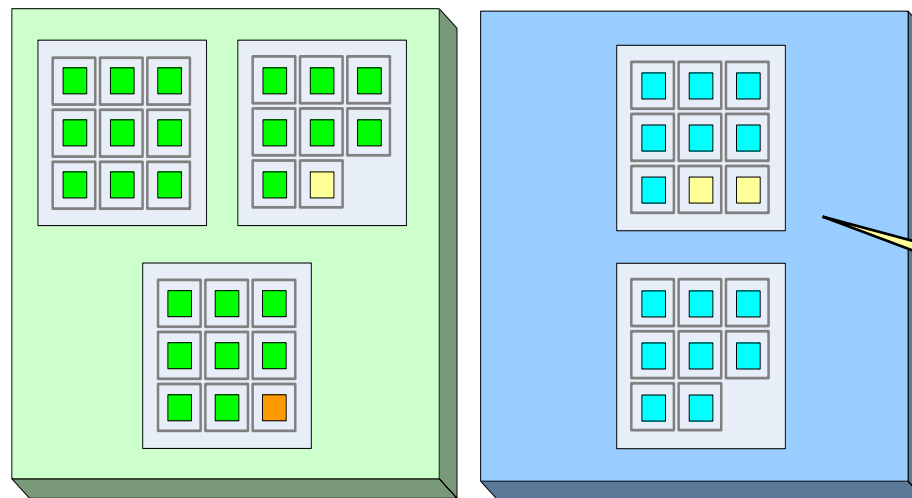
## **RESERVOIR Differentiator:**

The ability to dynamically hire additional 'service power' from a new management site, fully automated, using the service definition language and the inter-domain site protocols

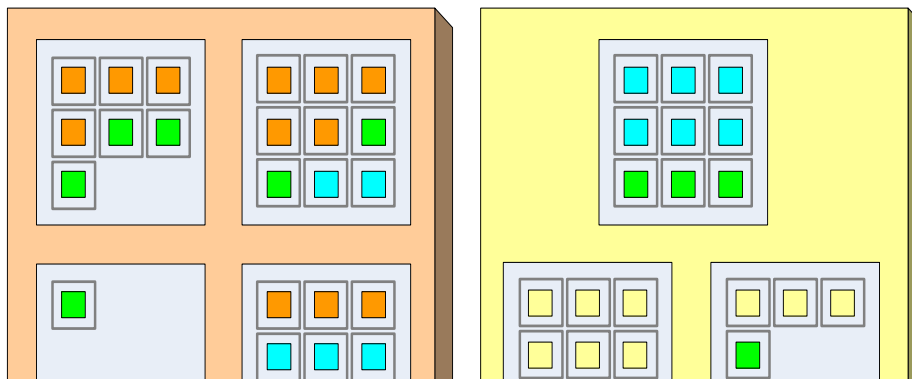
# SOI: Grid Computing



# SOI: Grid Computing + Virtualization

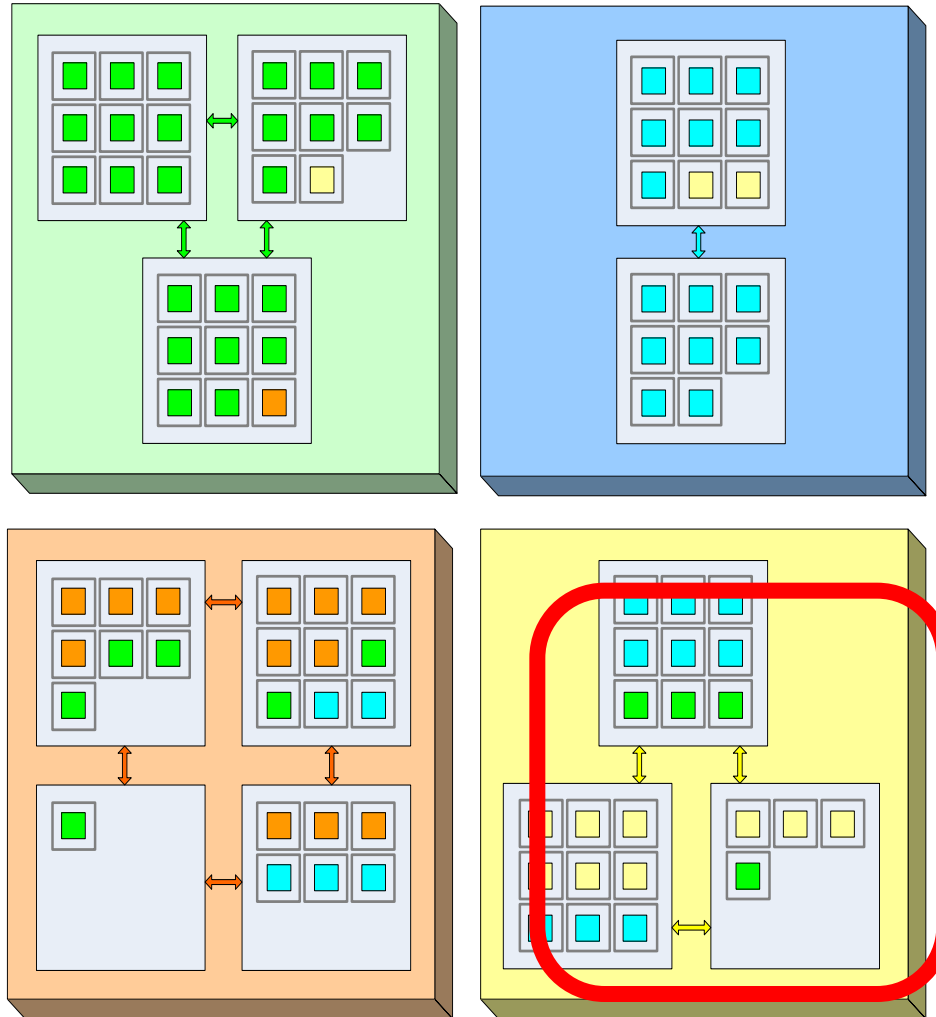


Virtual Execution Environment (VEE)



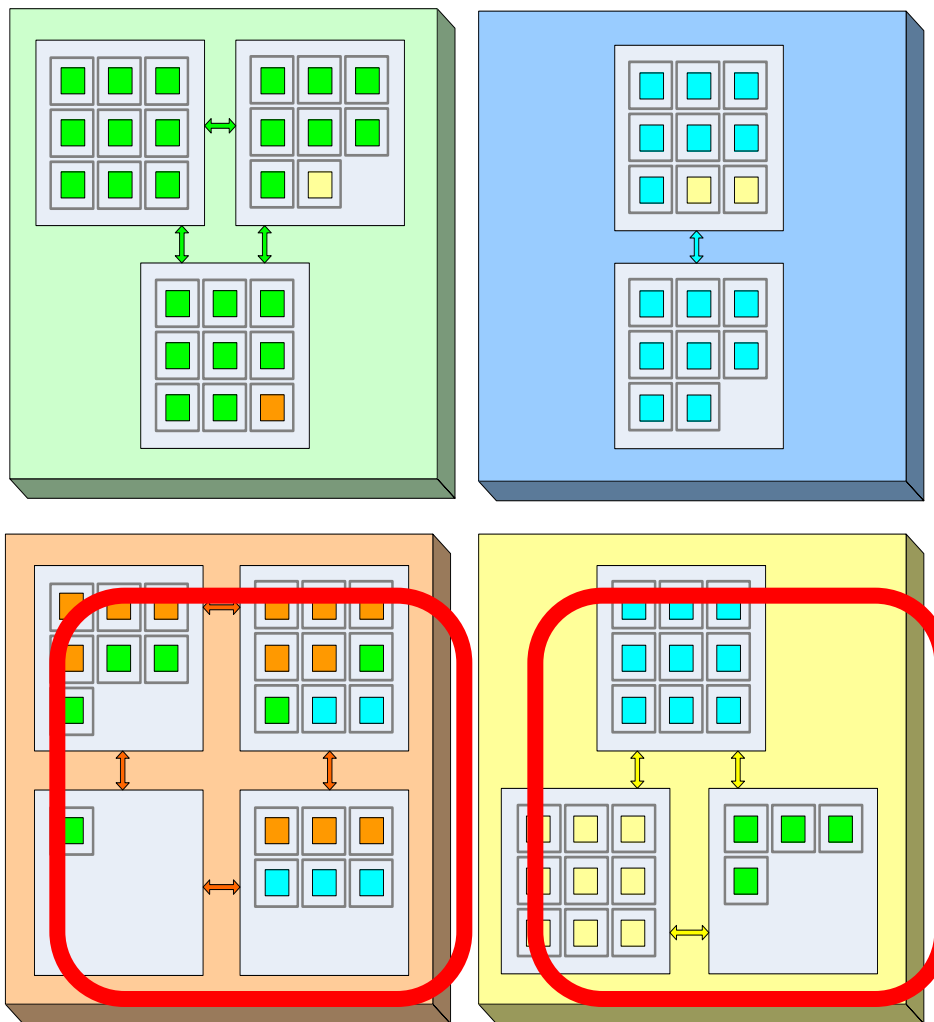
Improved isolation, Relax dependencies, Well defined billing units

# SOI: Grid Computing + Virtualization + BSM



Policy 1:  
 If possible keep  
 VEEs from  
 the same  
 organization in  
 the  
 same physical  
 box

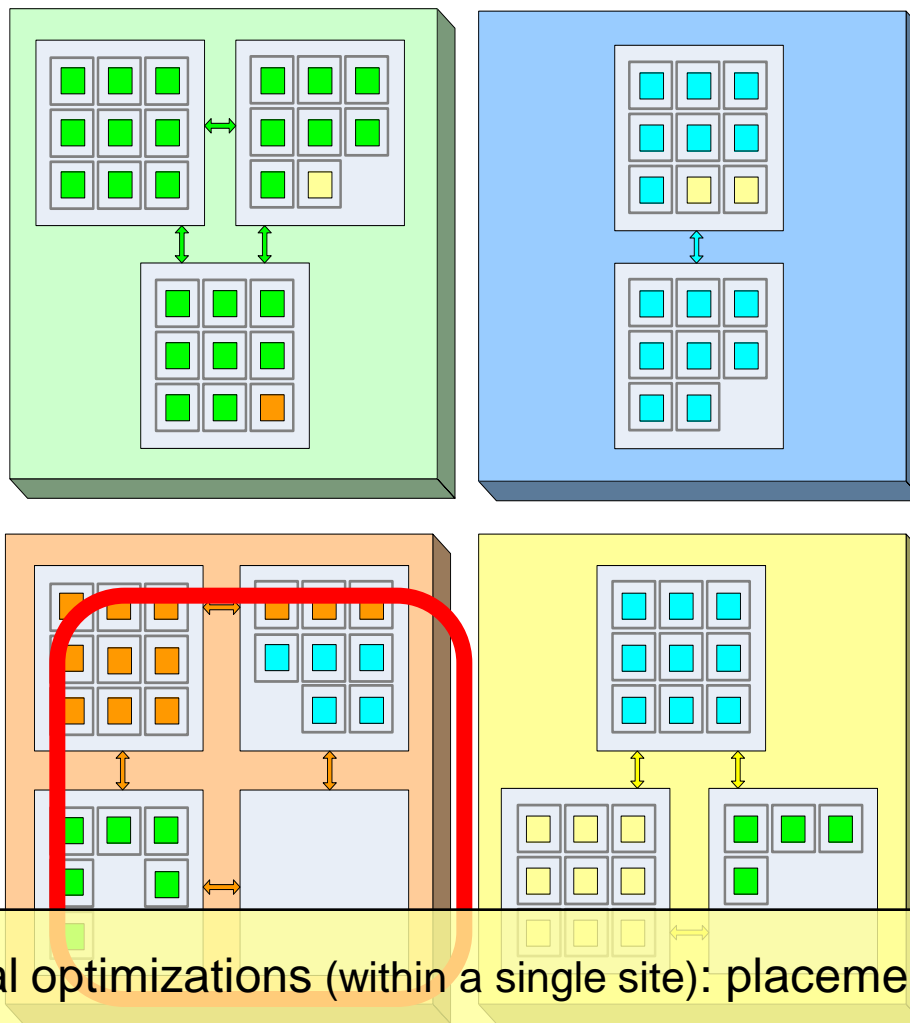
# SOI: Grid Computing + Virtualization + BSM



Policy 1:  
If possible keep VEEs from the same organization in the same physical box

Policy 2:  
Turn off underutilized physical boxes

# SOI: Grid Computing + Virtualization + BSM

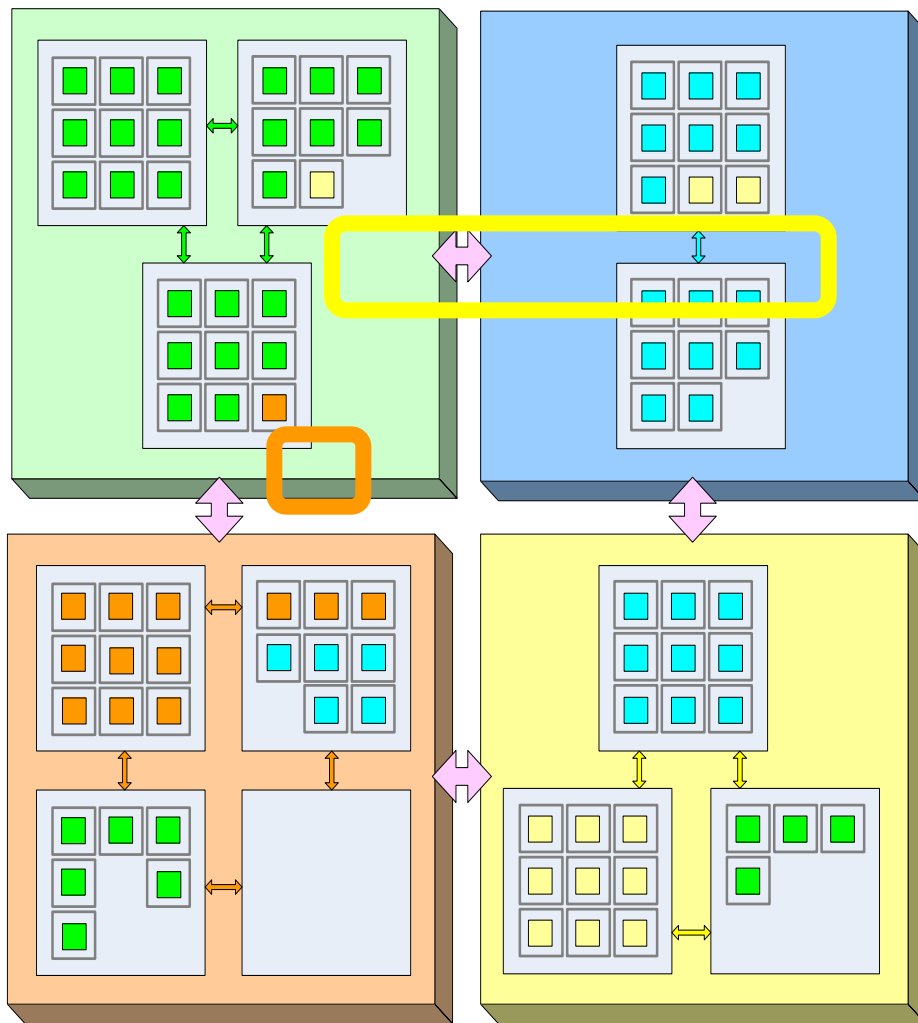


**Policy 1:**  
 If possible keep VEEs from the same organization in the same physical box

**Policy 2:**  
 Turn off underutilized physical boxes

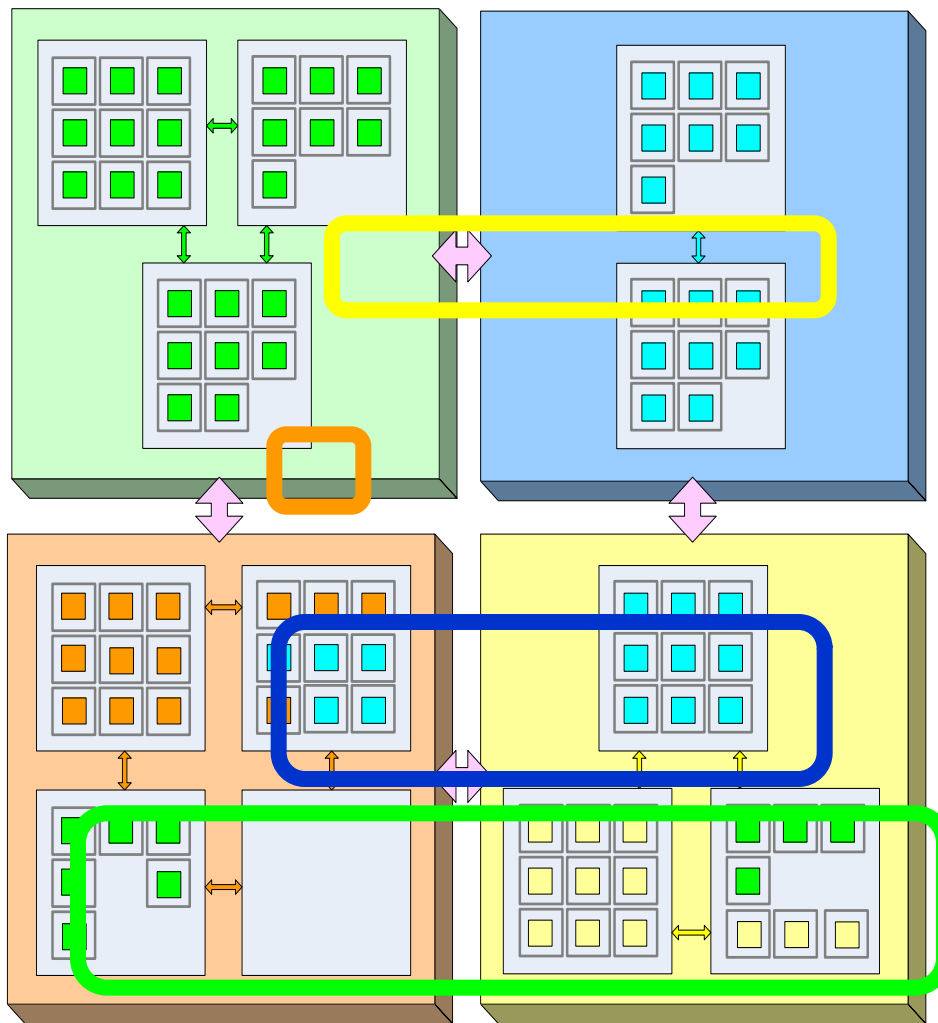
Local optimizations (within a single site): placement, power, etc.

# SOI: Grid Computing + Virtualization + BSM – Boundaries



Policy 3:  
If possible keep  
VEEs in "owning"  
organization

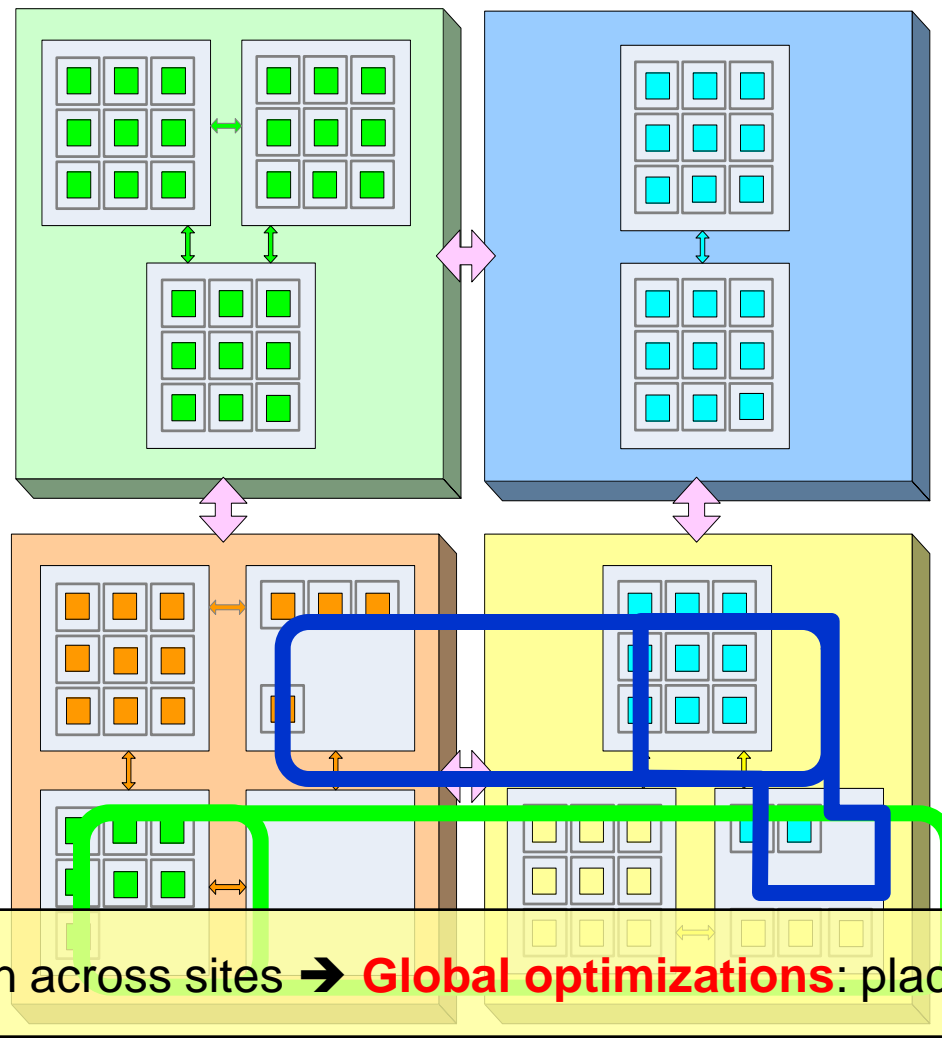
# SOI: Grid Computing + Virtualization + BSM – Boundaries



Policy 3:  
If possible keep VEEs in “owning” organization

Policy 4:  
If possible keep VEEs in least number of external organizations

# SOI: Grid Computing + Virtualization + BSM – Boundaries

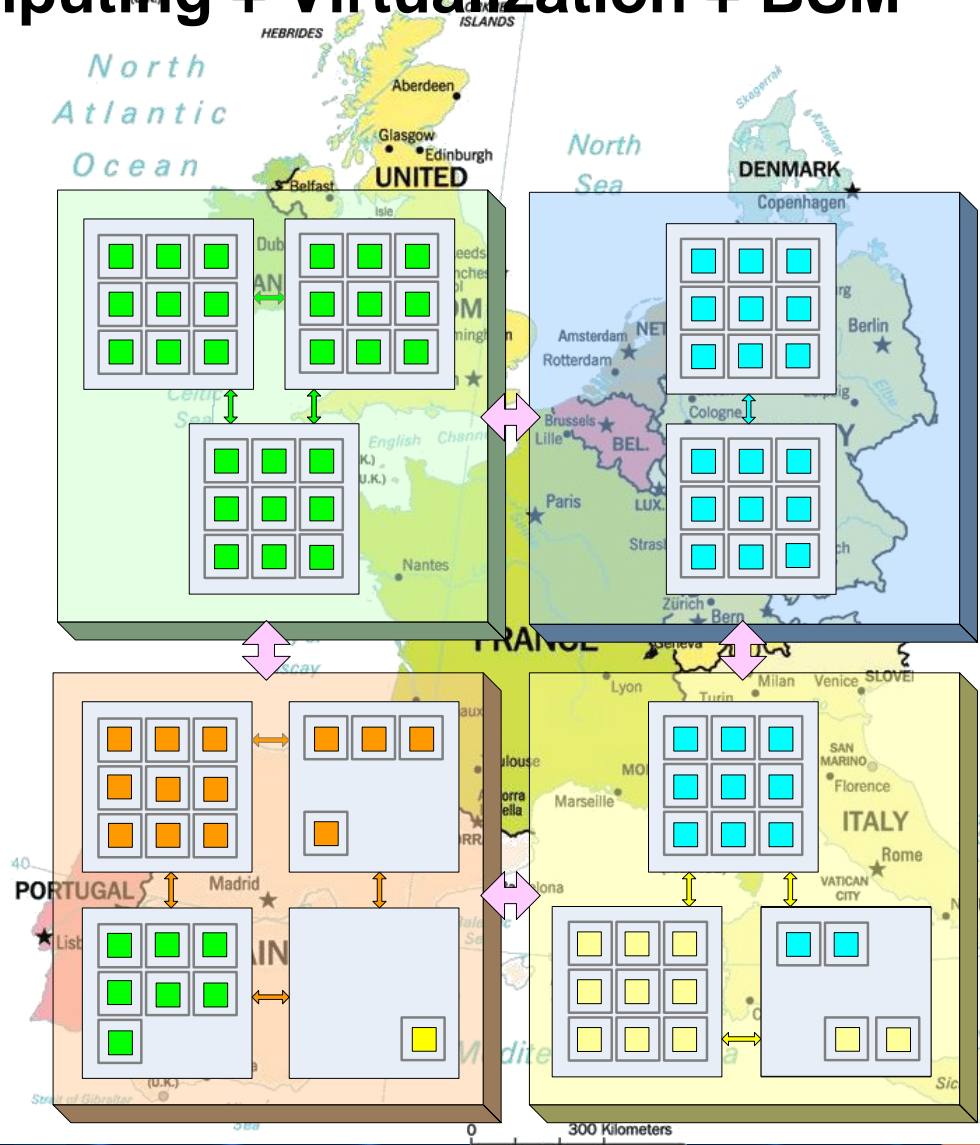


Policy 3:  
If possible keep VEEs in “owning” organization

Policy 4:  
If possible keep VEEs in least number of external organizations

Migration across sites → **Global optimizations**: placement, cost, etc.

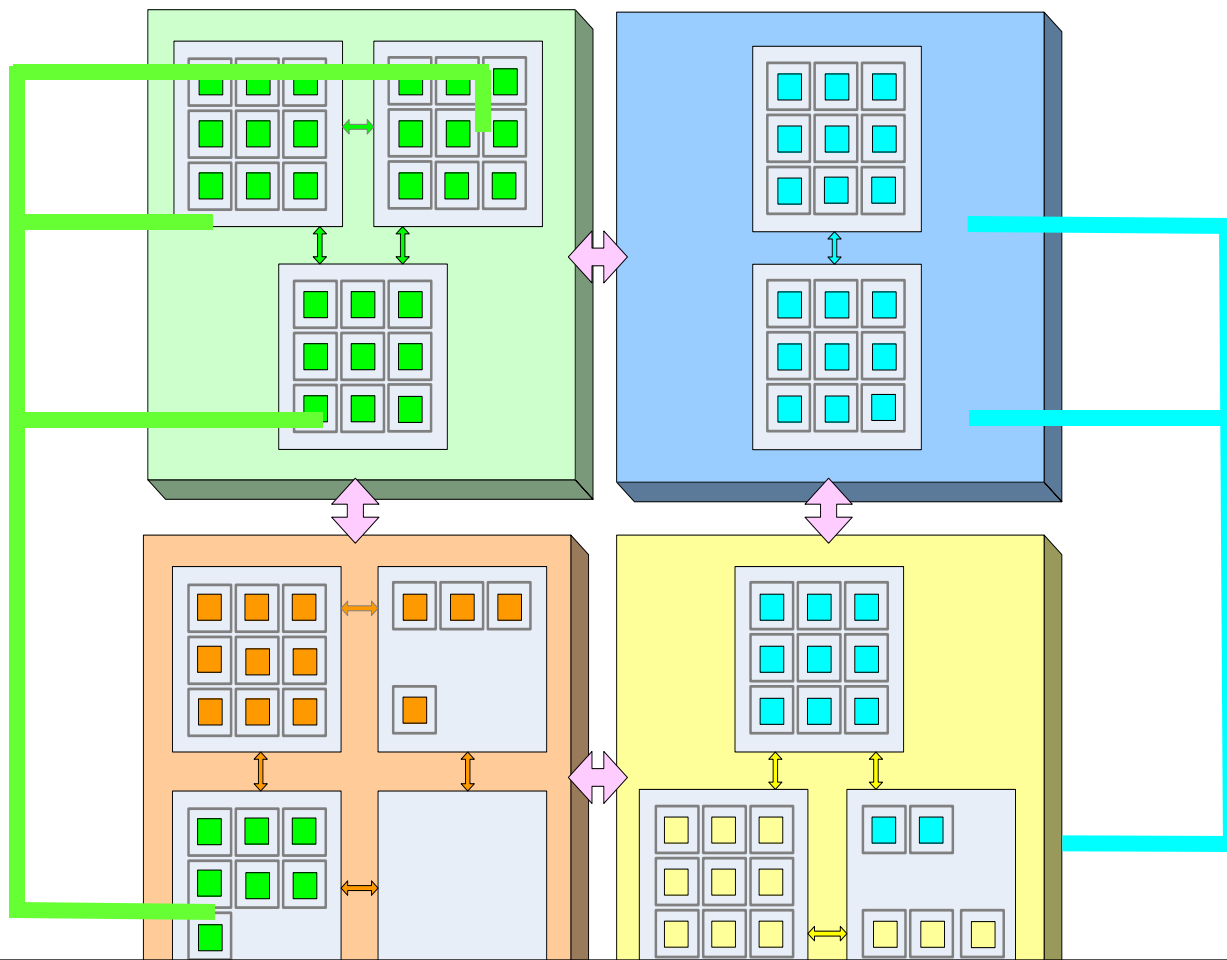
# SOI: Grid Computing + Virtualization + BSM - Boundaries



Policy 5:  
"Follow" your customer

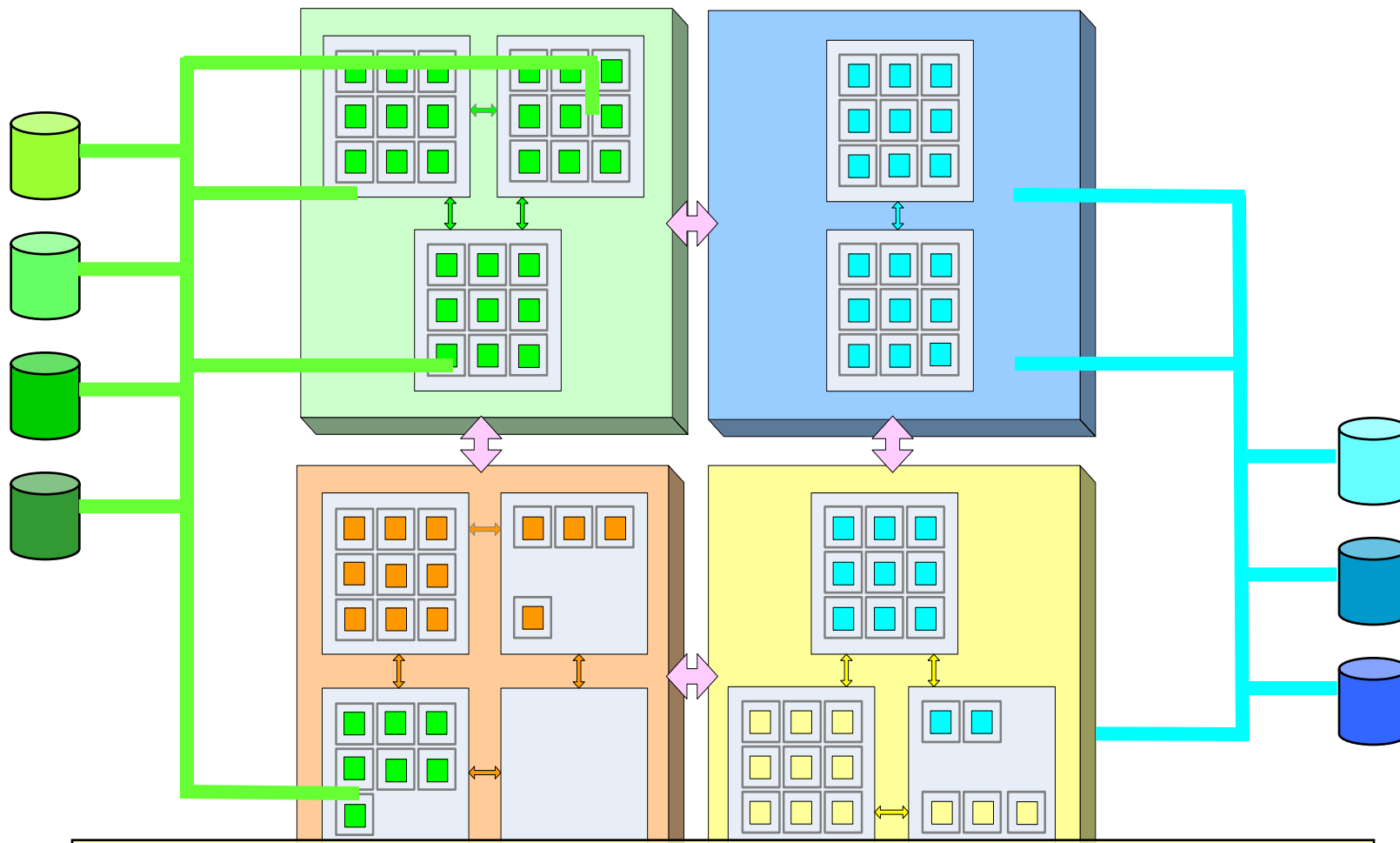


**– Boundaries → Virtualize the Network ...**



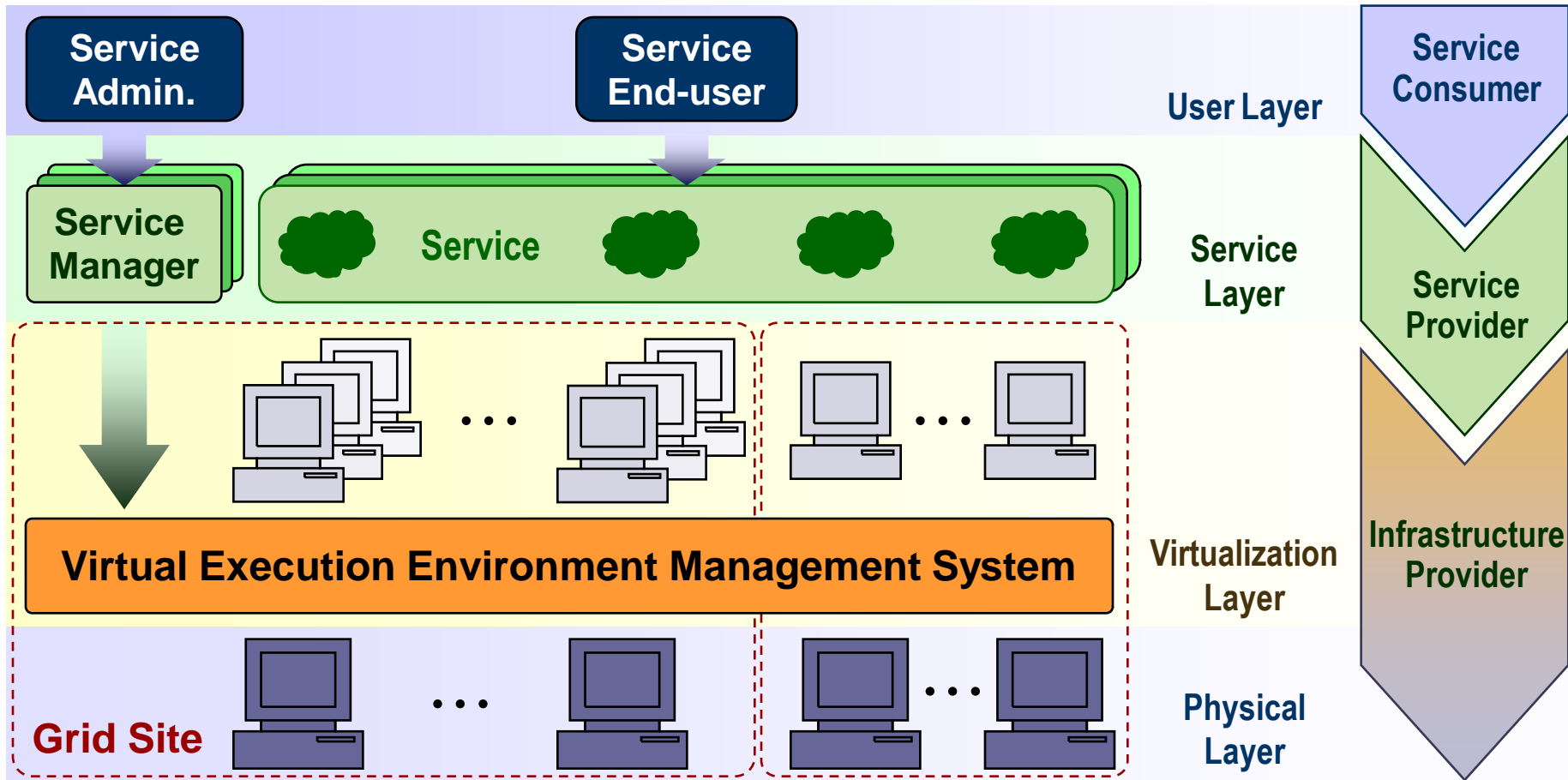
Create virtual networks connecting VEEs regardless of physical server location

# - Boundaries → ... and the Storage

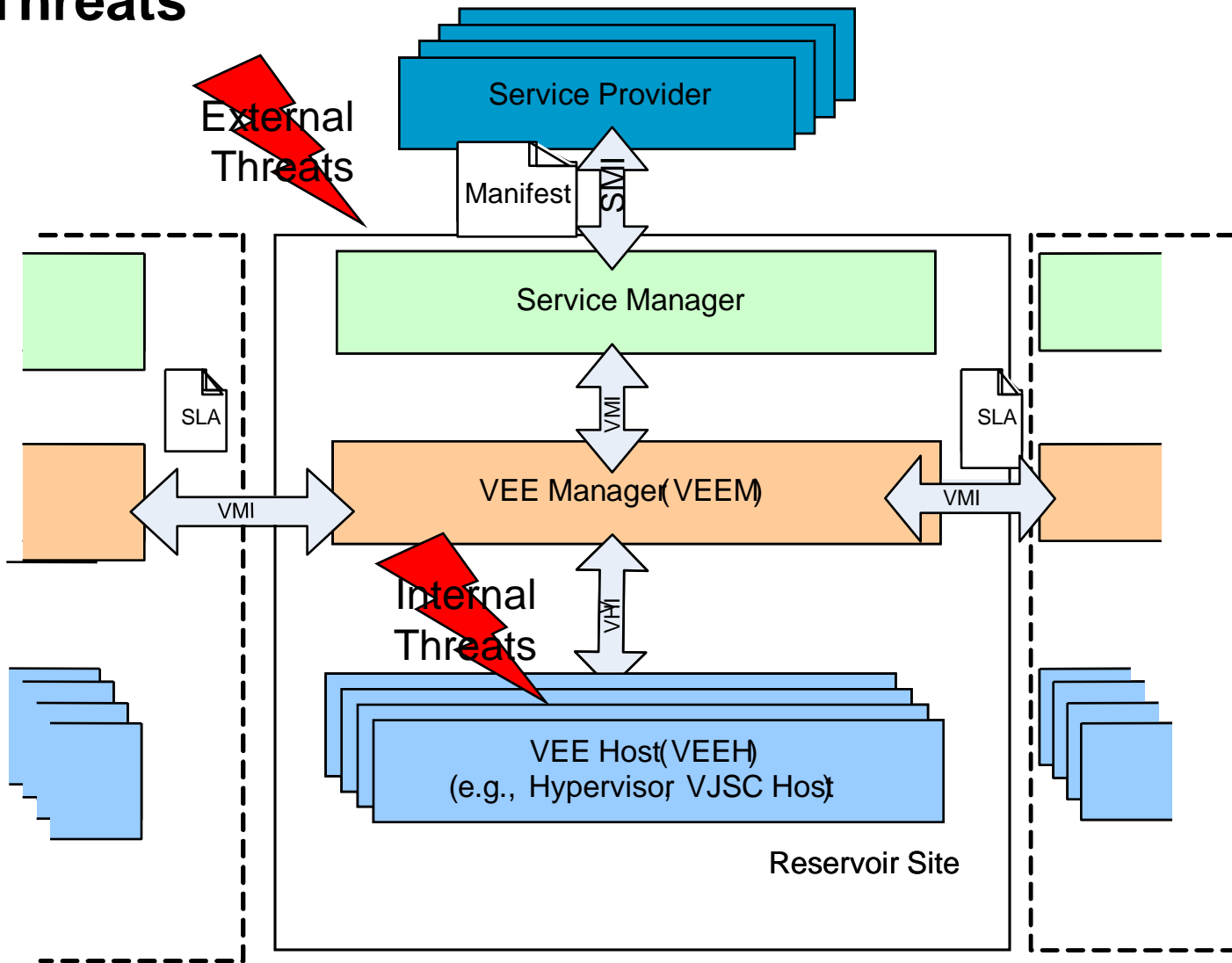


Enable secure access to relevant data regardless of storage location

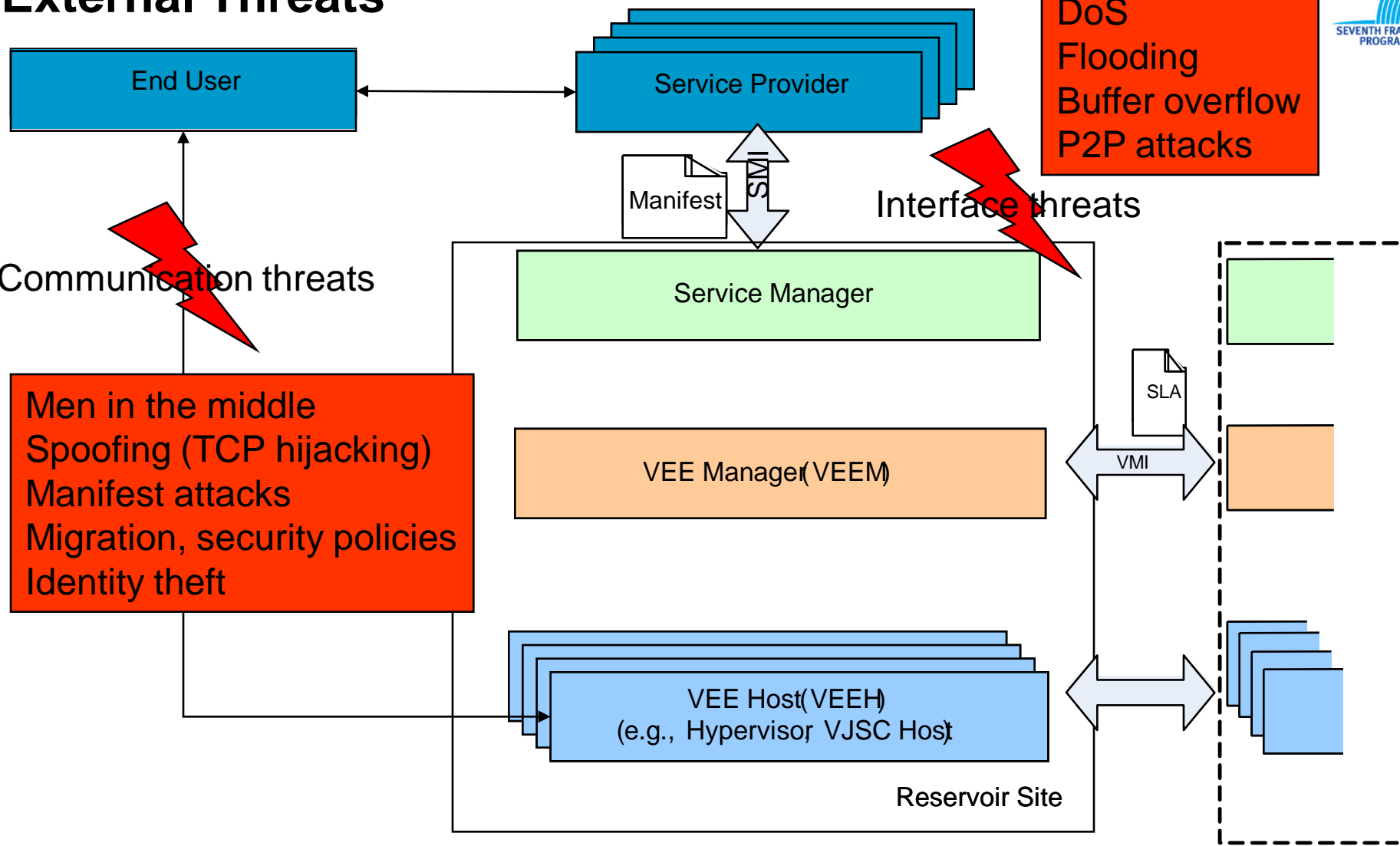
# RESERVOIR from 10000 feet



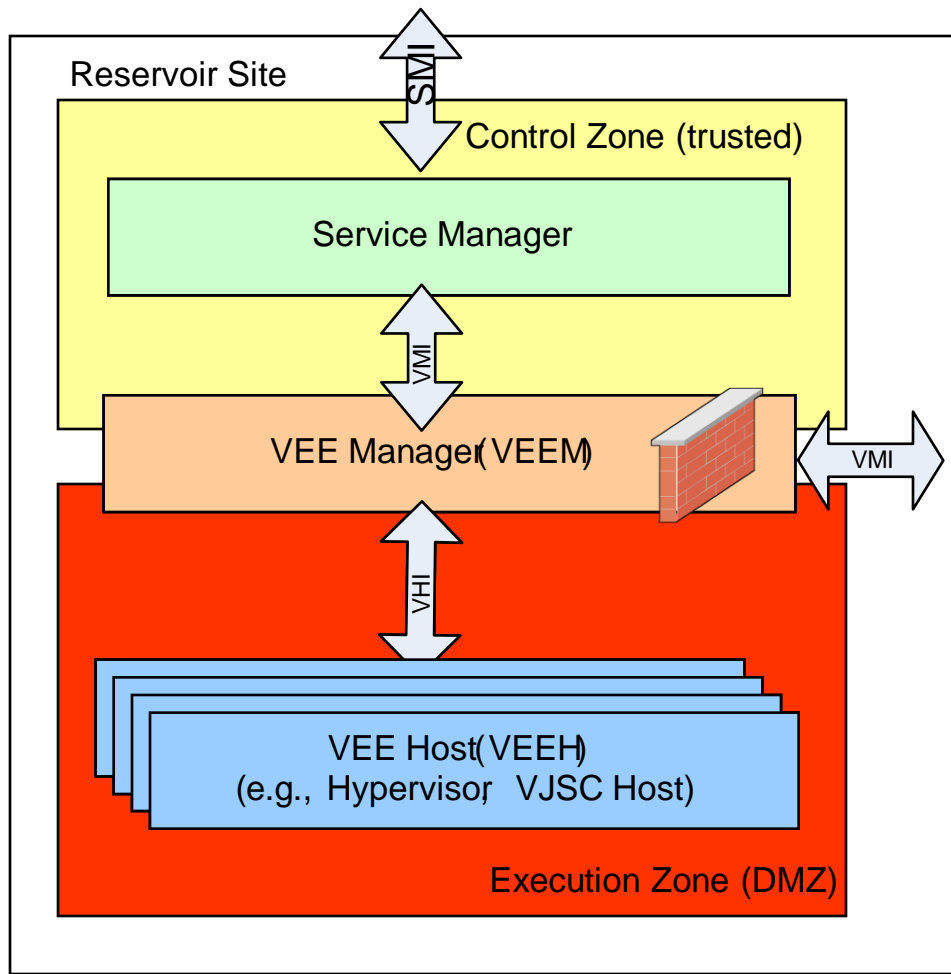
# Security Threats



# External Threats



# Internal Threats



**VEEH Process:**

- Downloads IM from SP
- Stores IM in NAS
- Performs setup
- Boots the VM

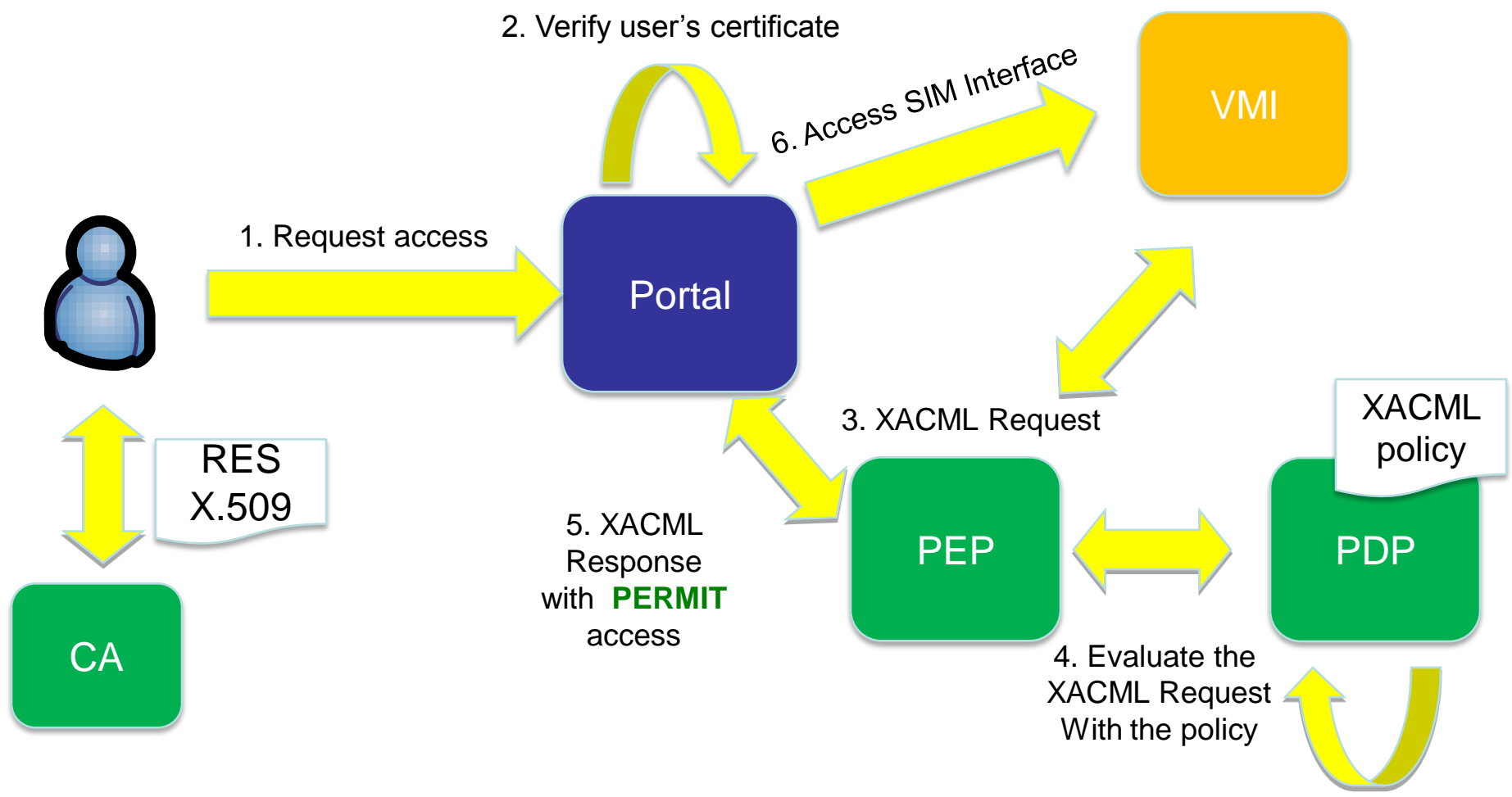


- Auth/comm with SP and sites
- SM to VEEM misbehaviour
- Data export
- Fake VEE placement
- Storage data compromised (fake image)
- Hypervisor and underlying OS
- VEE data partitioning

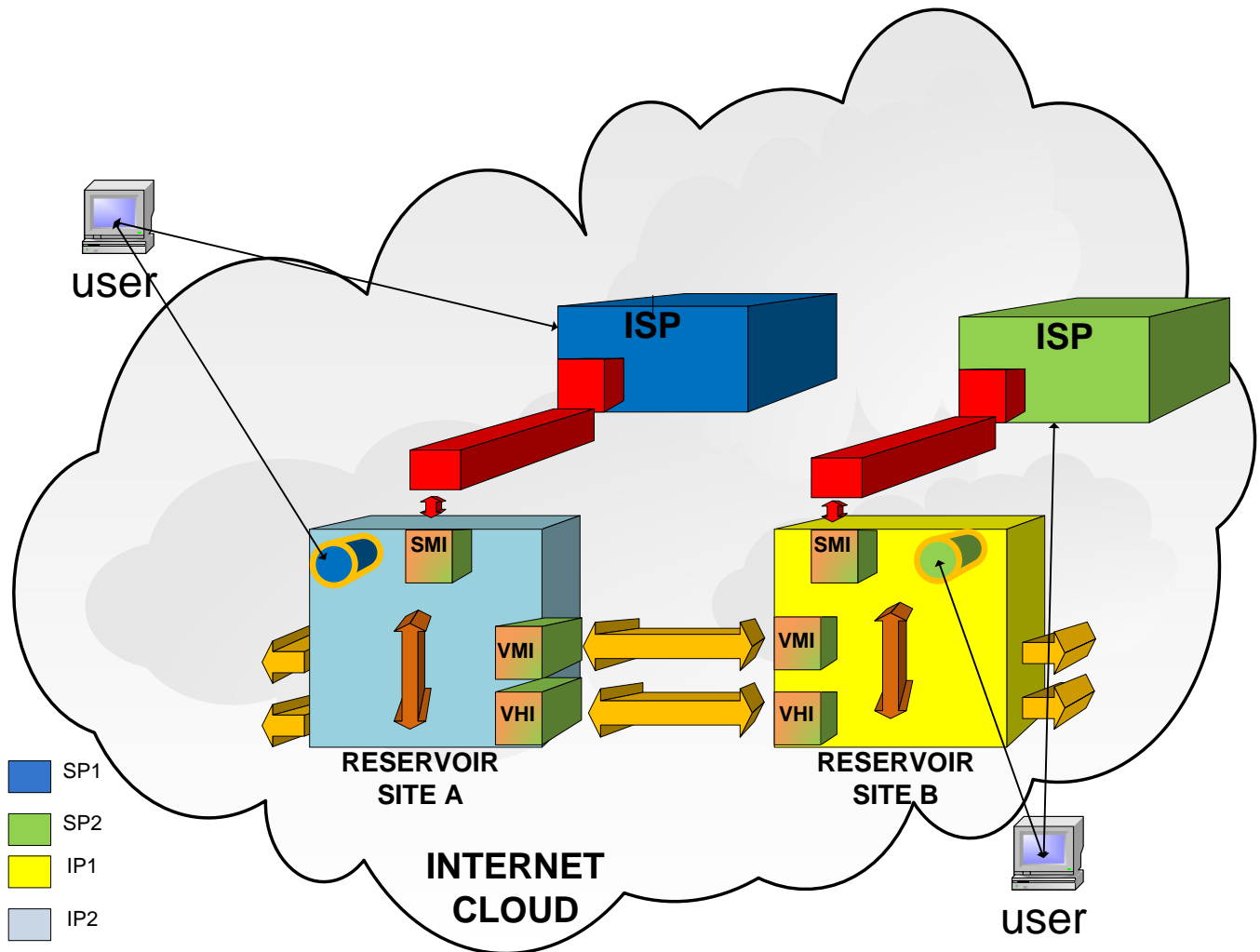
# Authentication and Access Control

- Authentication:
  - SP + users
  - Sites + administrators
  - VEEM?
  - VEE?
  - Hypervisor?
- Access control at different levels:
  - Portal
  - SMI
  - VMI
  - VHI
  - VEEM administration
  - Application
  - ...

# Authentication and Access Control – first version

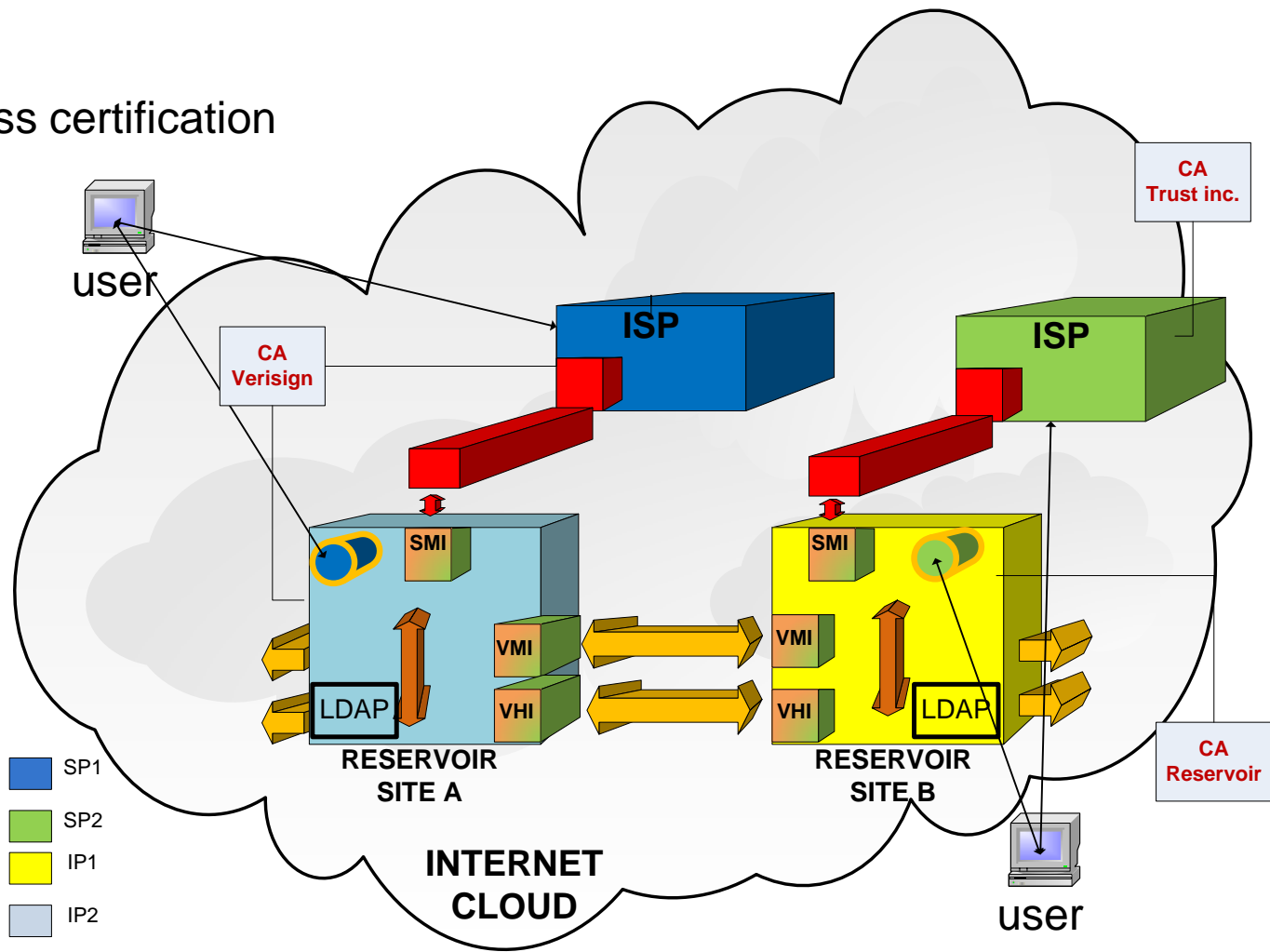


# Authentication and Access Control – Federation



# Authentication and Access Control – Federation (Ctd)

Cross certification

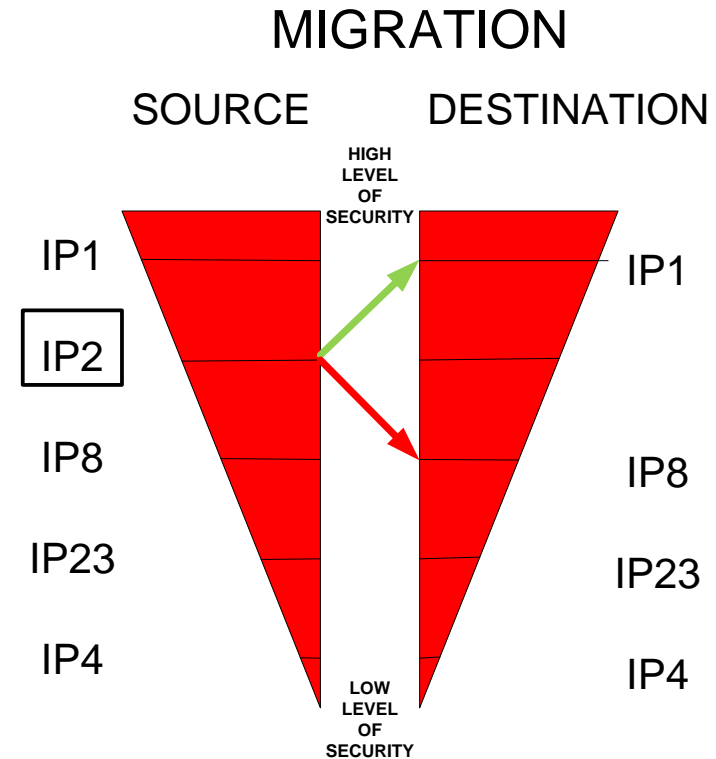
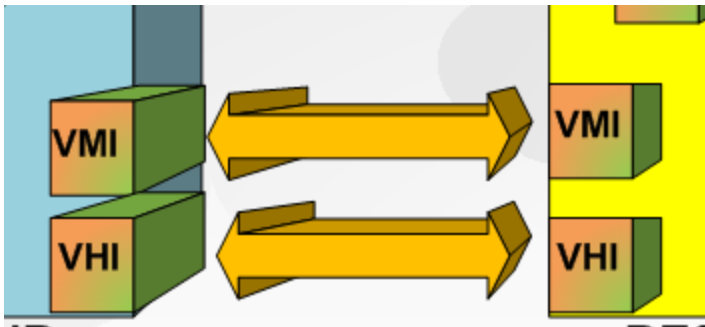


- SP1
- SP2
- IP1
- IP2


# Securing Migration

- Confidentiality of VEE
  - Encryption
- Integrity of VEE
  - Sign the migrated VEE

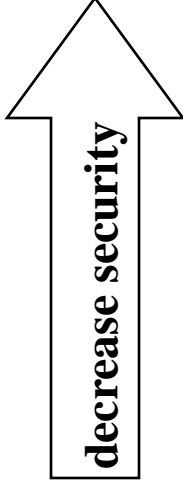
# Securing Migration - Infrastructure Security Profiling



# Securing Migration - Infrastructure Security Profiling



|           | https | Firewall | Crypto File System | VPN tunnel | VLAN |
|-----------|-------|----------|--------------------|------------|------|
| Profile 0 | X     |          |                    | X          |      |
| Profile 1 | X     | X        |                    | X          | x    |
| .....     |       |          |                    |            |      |
| Profile n | X     | X        | x                  | X          | x    |

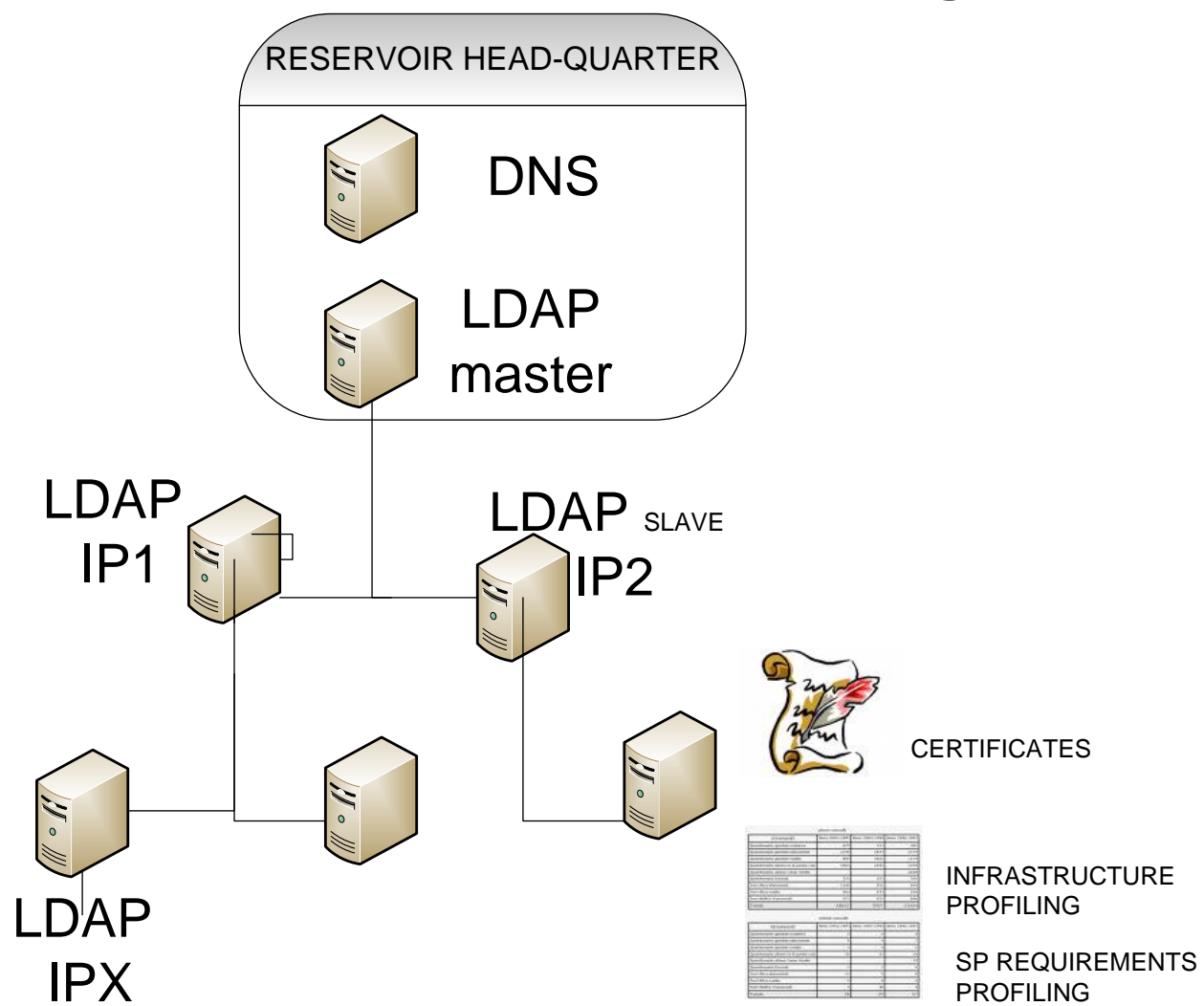


# Matching with SP security requirements - User Request Profiling



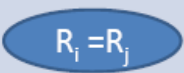




|            | https Access | Firewall | Crypto File System | IDS | Network Isolated |
|------------|--------------|----------|--------------------|-----|------------------|
| ProfileU 0 | X            |          |                    | X   |                  |
| ProfileU 1 | X            | X        |                    | X   | x                |
| .....      |              |          |                    |     |                  |
| ProfileU n | X            | X        | X                  | X   | x                |

# LDAP architecture: Master and Slave configuration



# A step further: Policy matching based Access Control

- Issues:
  - How do we find sites that we want to work with?
  - Do we know they are secure?
- Secure broker Service
  - It implements all the authorisation logic needed
  - Performing policy matching (XACML policies) between
    - User (SP) sec policy and primary site sec policy
    - Source site sec policy and target site sec policy
    - Global federation sec policy and site sec policy

| Rule similarity type  | Authorized request set  |
|-----------------------|---|
| $R_i$ Converges $R_j$ |  |
| $R_i$ Diverges $R_j$  |  |
| $R_i$ Restricts $R_j$ |  |
| $R_i$ Extends $R_j$   |  |
| $R_i$ Shuffles $R_j$  |  |

## A Step even Further: Trusted Computing

- TC: Hardware based security for identification and integrity
- How to use it in RESERVOIR?
  - VEEH
  - VEEM security functions, e.g. signing of migrating VEE (integrity)
  - Signing VEEM logs (integrity) so the can be audited by SP
- How to integrate it in RESERVOIR
  - Hypervisor
  - Network
  - CA
  - Access control

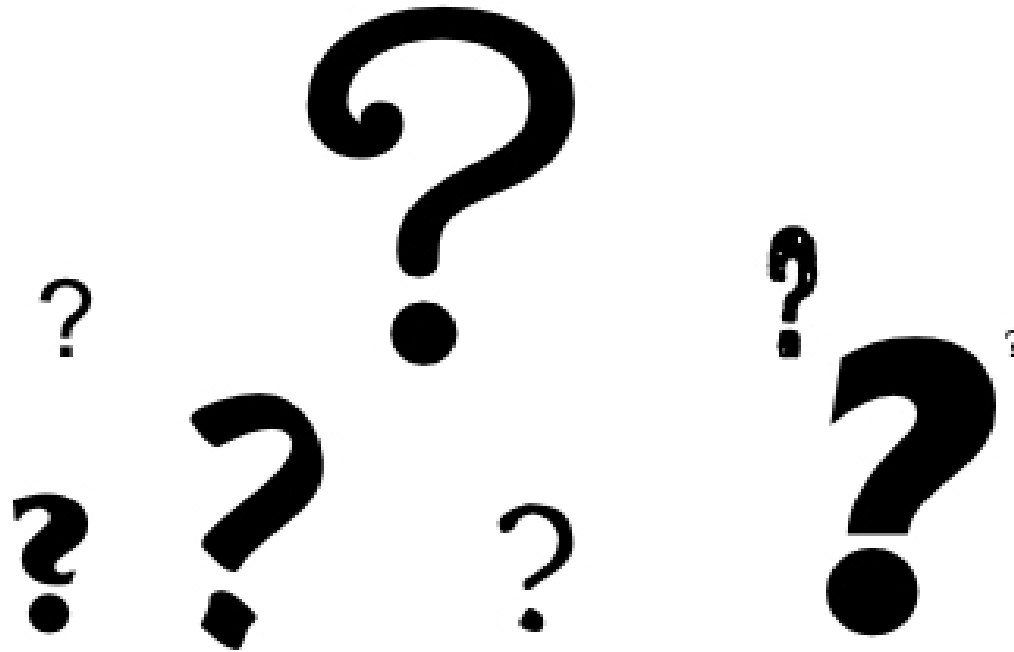
# Securing the Administration Interfaces

- Need to secure Administration
- We need input on who is developing this and how it is being developed
  - If it is a web based interface, then we can provide authentication and access control.
- Which administration logs are available?
  - Do we want to guarantee integrity?

## Isolation

- Service isolation: Protecting a Service from Other Services Running in the Same VEE
- VEE isolation: Protecting a VEE from other VEEs Running in the Same Compute Node

Any Question...



**THANK YOU**