

## Secure network provisioning on demand

Providing secured Community of Interest based virtual networks based on the user (or his role) that logs on

LSEC - Future Internet (Security) Architecture Seminar  
10 Septembre 2010  
Luc Leysen

## Agenda

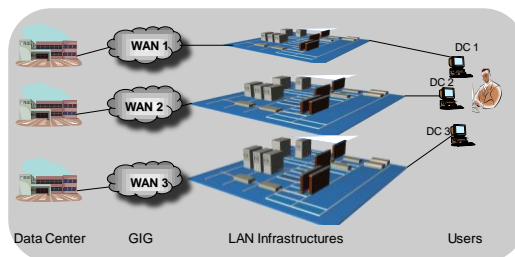
- Introduction
- Current network challenges
- Future network vision
- Upcoming solution to the challenges
- Advantages of COI based networking
- Unisys Stealth solution
- Questions / Answers

# Agenda

- Introduction
- **Current network challenges**
- Future network vision
- Upcoming solution to the challenges
- Advantages of COI based networking
- Unisys Stealth solution
- Questions / Answers

## Current networking challenges Design

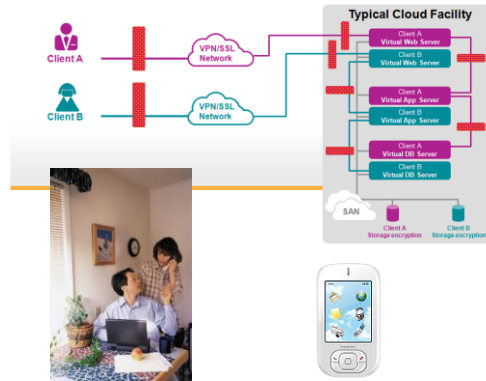
- Availability and capacity
- Security has high impact
  - segmentation
    - E.g. separate administration networks
  - Case high security:
    - E.g. Military, government
    - Multiple networks
- More difficult/costly to maintain scalability & redundancy
- Different equipment for different networks



# Current networking challenges

## Fading network frontiers

- Reasons
  - Homeworking growth / office-space reduction
  - 3rd party local access (Internet, their Company network)
  - Projects involving customers, partners,...
  - Outsourcing, Cloud
  - IT Consumerization
- Consequences
  - Secure network design requires fast updating while complexity increases
  - More external access to Internal network  
Unencrypted Internal network => higher risk



# Current networking challenges

## Security

- Edge protection : mature but complex
  - Internal network protection => often limited
    - ACL, less frequently Firewalls
    - NAC/NAP
      - Often not yet in place
      - Current Implementations: 802.1X 2001,2004
        - Vulnerabilities
          - MITM, MAC Spoofing, EAPOL Logoff attacks
          - Waiting for 802.1X 2010: MACSec IEEE 802.1AE => encryption
        - Certificates => PKI => complex
      - No encryption/ barely segmented
- => Vulnerable to attacks



## Current networking challenges

### New connection needs

- Various Reasons
  - Partner connection
  - Visitor : Internet access
    - Separate wireless network
  - Internal move : different access
  - Reorganization: building/organization
  - New servers: projects,...
- Extra equipment may be required
  - Extra network equipment
  - Extra end-user equipment
    - If different security level
  - Extra wiring /space/power/HVAC



**UNISYS**  
imagine it. done.

Page 7

## Current networking challenges

### New connection needs

- Extra effort: Involvement of both
  - Network team(s)
  - Security team(s)
- Extra physical access controls
- Time to setup
  - Response to urgent needs ? E.g. projects
  - Too often leads to:
    - No answer to business need
    - Business finds workarounds
      - => Non-compliant with policies
    - IT provides shortcut solution
      - => Not in line with requirements and/or policy
- Needs of the few?
  - e.g. Financial results exchange between CxO
  - High setup cost per person



**UNISYS**  
imagine it. done.

Page 8

# Current networking challenges

## Machine based

- Other user => same network access
- Location restrictions
  - Specific port / specific location
  - Physical access controls required to limit unauthorized access
- User Role change => New/changed connection needs
- Insufficient Time restrictions
  - Often not enforced
  - Procedures periodic review device network access requirements ?

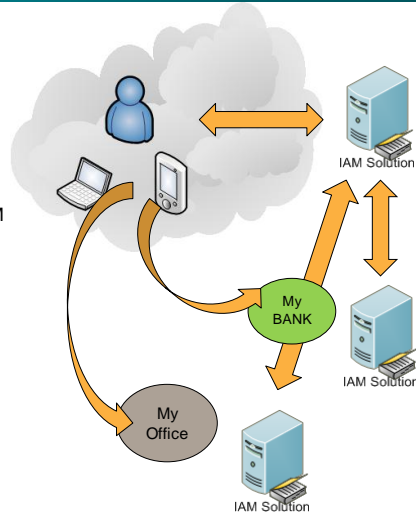


## Agenda

- Introduction
- Current network challenges
- **Future network vision**
- Upcoming solution to the challenges
- Advantages of COI based networking
- Unisys Stealth solution
- Questions / Answers

## Future networking Vision

- Your logon Identity will determine which other devices you see:
  - Wherever they are and you are
  - Encryption will be used practically all the time
- Identity & access management systems determine the scope of what you “see” on the network of your end device
- Trust relationships such as Federation between IAM systems will control the network access to 3rd party systems.
- Communities Of Interests (COI) will form instantly based on connection needs.
  - Future?
  - Today : Unisys Stealth is pretty close
  - ⇒ COI Based networking
- NAC type of policy checking will occur before allowing access, checking endpoint security, possibly also location

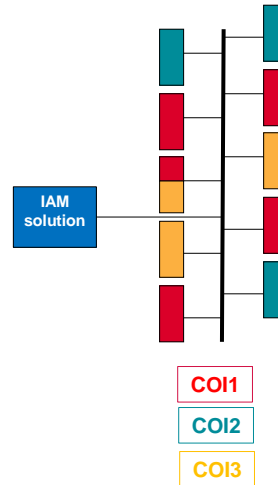


## Agenda

- Introduction
- Current network challenges
- Future network vision
- **Upcoming solution to the challenges**
- Advantages of COI based networking
- Unisys Stealth solution
- Questions / Answers

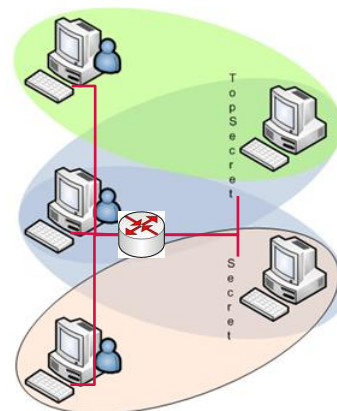
## Upcoming solution to the challenges Community of Interest based networking

- Physical Network design simplified  
=>Management & Cost reduction
- User Identity determines COI access  
through role assignments
- Encryption + Data dispersal  
mechanism guarantees military  
grade isolation of COI => Increased  
security
- Allows dynamic creation of secure  
Virtual Networks => Huge flexibility
- Role provisioning = Network  
provisioning => Business in control



## Upcoming solution to the challenges Community of Interest based networking

- Integration in the network  
without changes to routers or  
applications
- Hence transparent to  
protocols such as DHCP,  
RIP, OSPF...

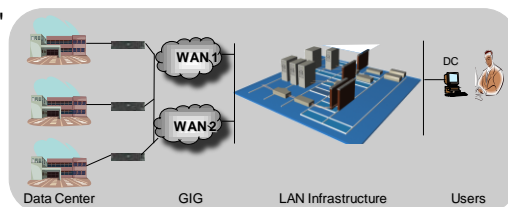


# Agenda

- Introduction
- Current network challenges
- Future network vision
- Upcoming solution to the challenges
- **Advantages of COI based networking**
- Unisys Stealth solution
- Questions / Answers

# Advantages of COI based networking Network design

- Availability and capacity
  - Consolidated, more "flat" networks
  - only 1 network to maintain
    - optimal scalability & redundancy
    - Improved overall SLA
    - More focused standardization
    - Easier management
  - Simplified design

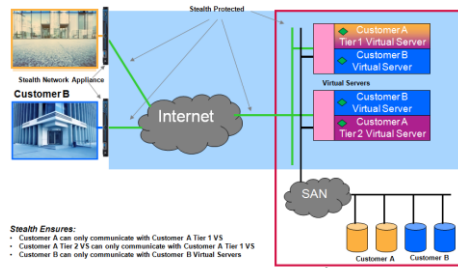


- Security
  - Confidentiality and integrity guaranteed by COI
  - Edge security between uncontrolled and controlled network

# Advantages of COI based networking

## No more Fading network frontiers

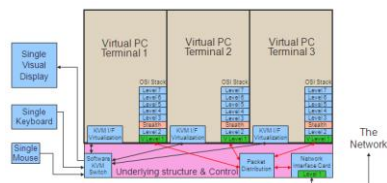
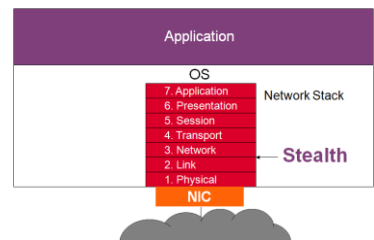
- Network frontiers are implicit per COI
- Can go beyond traditional network frontiers
  - Over 3rd party/untrusted physical networks
- Physical access to network infrastructure doesn't mean access to the "networks" anymore



# Advantages of COI based networking

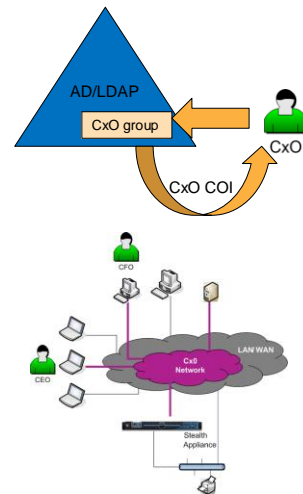
## New connection need

- Controlled by Identity
- Connectivity limited to explicitly required scope
  - Also at network layer
  - No attack possible on transport/session/application layers outside assigned COI
- Most cases : No extra equipment need
  - Extra VM if different security level
  - More GREEN solution



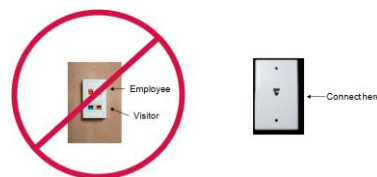
## Advantages of COI based networking New connection need

- Limited management effort
  - Definition of a COI mapped to an AD group:
    - Only when a new COI is needed
  - Add user to AD/LDAP group
  - Can be automated through IAM workflow
  - Delegation to business possible
  - Hence very quick
  - Easy to fulfil urgent needs (e.g. Project) or the needs of the few (e.g. CxO) without extra cost



## Advantages of COI based networking User based

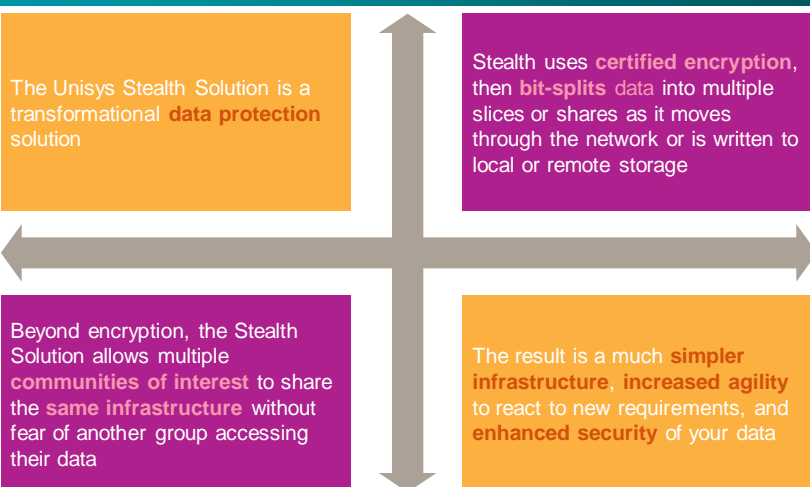
- Other user logs on => Different connectivity
- No location Restrictions
  - Any socket anywhere
- Time restrictions imposed easily
  - Logon restrictions for end user
- Automatic deprovisioning of user through IAM at end of assignment
  - Automatic removal of accessible "networks"



# Agenda

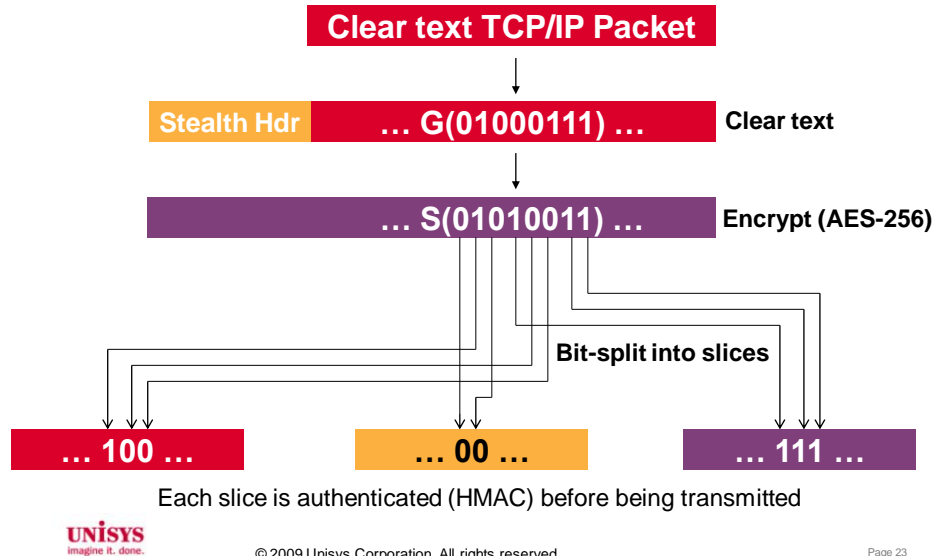
- Introduction
- Current network challenges
- Future network vision
- Upcoming solution to the challenges
- Advantages of COI based networking
- **Unisys Stealth solution**
- Questions / Answers

# Unisys Stealth solution What is it?



## Unisys Stealth solution

How does it work?



## Unisys Stealth solution

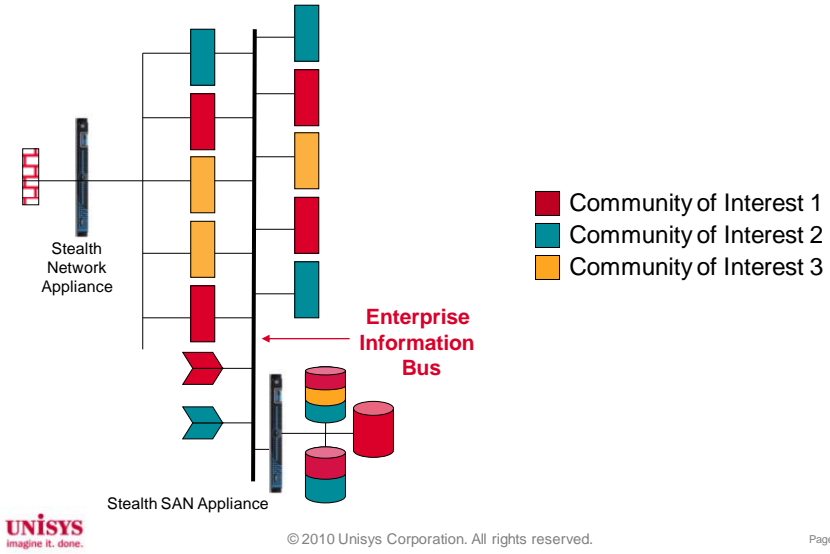
Standard ++ security mechanisms

- Cryptographic module
  - FIPS 140-2 certified
  - AES-256 cryptographic algorithm
  - Unique patent pending bit-level splitting solution
- Integrity control with hash code
- Optional resilience mechanism
- EAL 4+ Certification in progress (Oct 2010)
- Session keys automatic management
  - Entirely invisible for users
- No end-user certificates required => no PKI



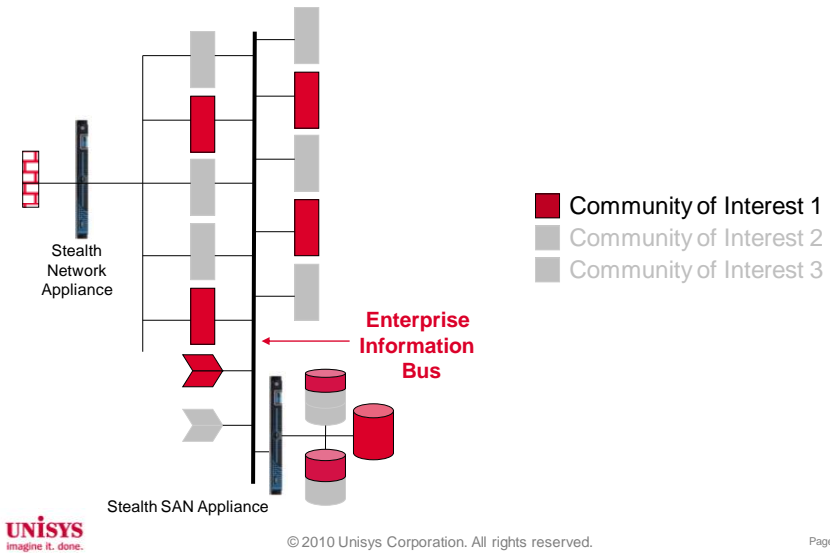
# Unisys Stealth solution

## Data access by COI

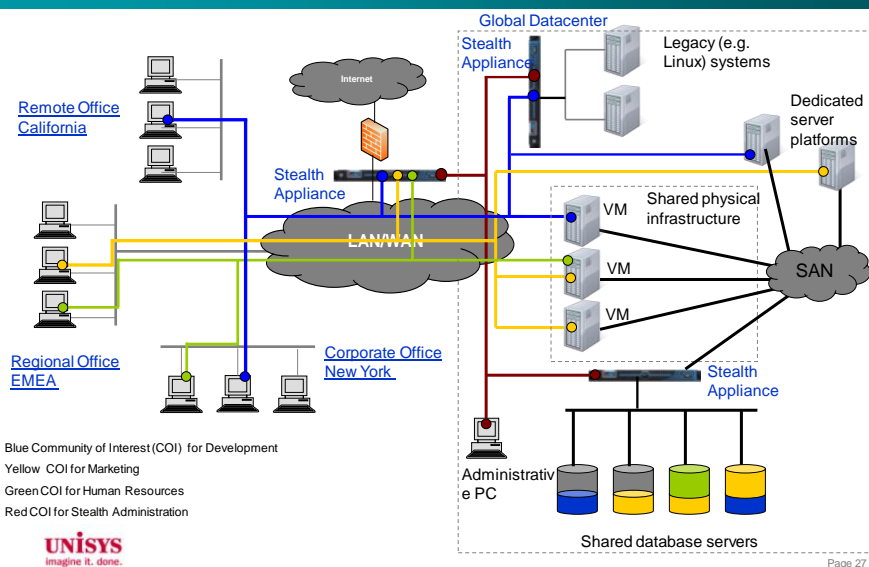


# Unisys Stealth solution

## The rest remain cloaked : Stealth



## Unisys Stealth solution Possible architecture



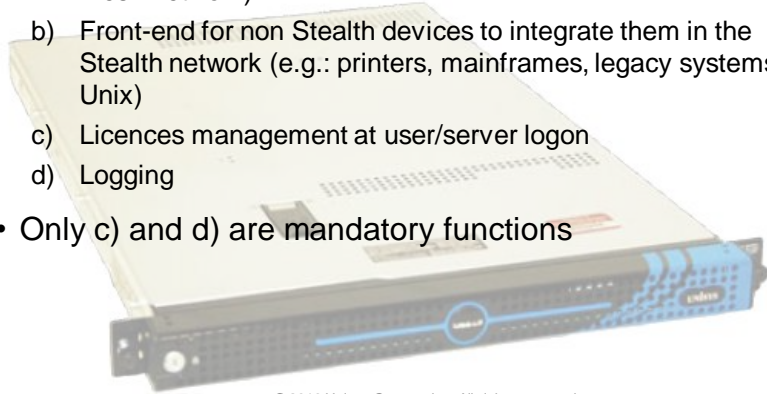
## Unisys Stealth solution Supported operating systems

- Currently supported systems
  - Windows XP
  - Windows Server 2003
  - Windows 7
  - Windows Server 2008
  - Linux Red Hat
- On-demand supported systems
  - Vista
  - Other Linux editions
- All other systems are supported by Stealth appliances

## Unisys Stealth solution

### Stealth appliances functions

- Stealth appliances play four distinct roles :
  - a) Gateway to and from a non Stealth Network (ex: Internet, Mesh network)
  - b) Front-end for non Stealth devices to integrate them in the Stealth network (e.g.: printers, mainframes, legacy systems, Unix)
  - c) Licences management at user/server logon
  - d) Logging
- Only c) and d) are mandatory functions



© 2010 Unisys Corporation. All rights reserved.

Page 29



Thank you for your attention

## QUESTIONS & ANSWERS