Secure VPN with Cisco Devices – Creating a High-Availability Setup

OpenCA

Workshop 2005

Munich – October 18th

T · · Systems ·

Secure VPN with Cisco Devices – Creating a High-Availability Setup

Overview

- Basic requirement
- Server Architecture
- Network Architecture
- OpenCA implementation
- Certificate usage

Secure VPN with Cisco Devices – Creating a High-Availability Setup

Basic Requirements

- Scalable PKI Environment
- Structured environment
- Redundant hardware and software
- Distributed Application Management :
  - Clear definition of authority
  - Cost effective platform

Secure VPN with Cisco Devices – Creating a High-Availability Setup

Basic Requirements

- Manageability
- SCEP for Cisco equipment
- User certificates on USB Tokens and PKCS#12 files
- Server certificates via Basic Request and PKCS#10 requests

Secure VPN with Cisco Devices – Creating a High-Availability Setup

Server Architecture

Hardware Components

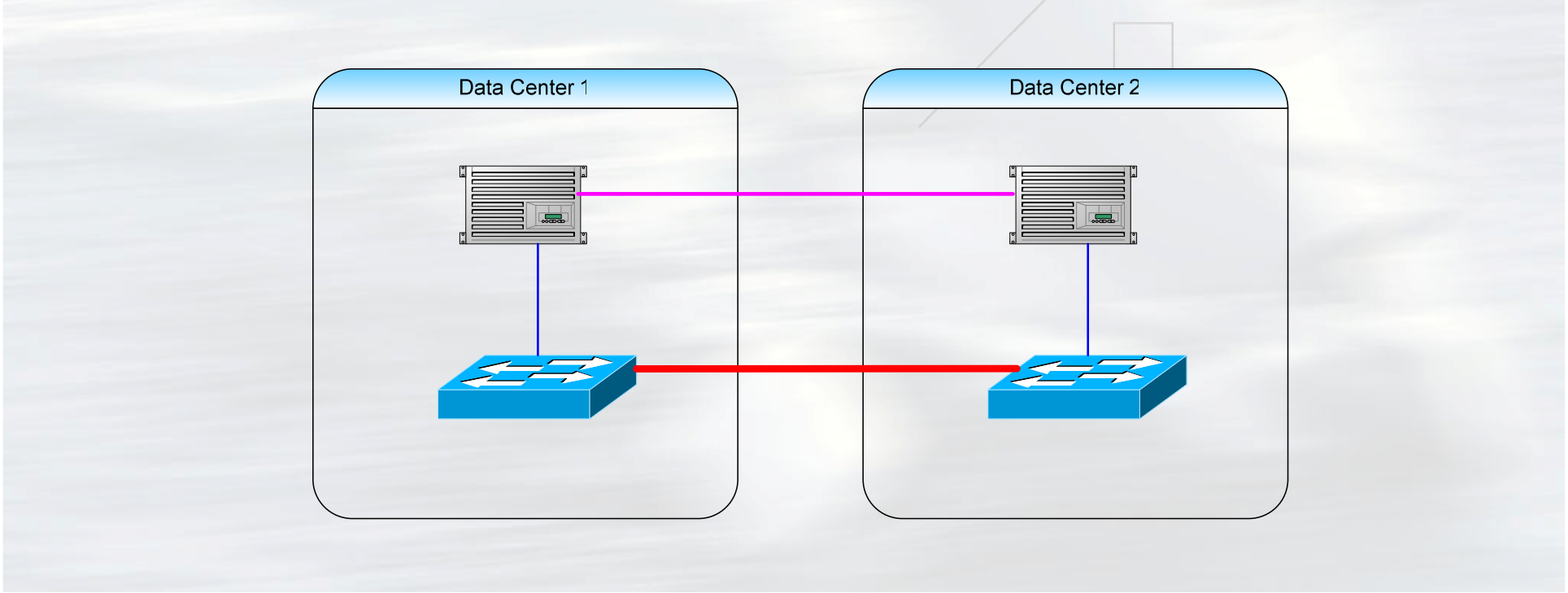
- 2 x Sun V20z
  - Dual AMD64 Opteron
  - 1GByte RAM
  - 2 x 36 GByte HDD (Hardware RAID-1)

Key Software components

- SuSE 9.2 - V-Server
- DRBD – Network Raid-1 Block Device
- OpenCA 0.9.2
- 10-15 Possible Virtual Servers

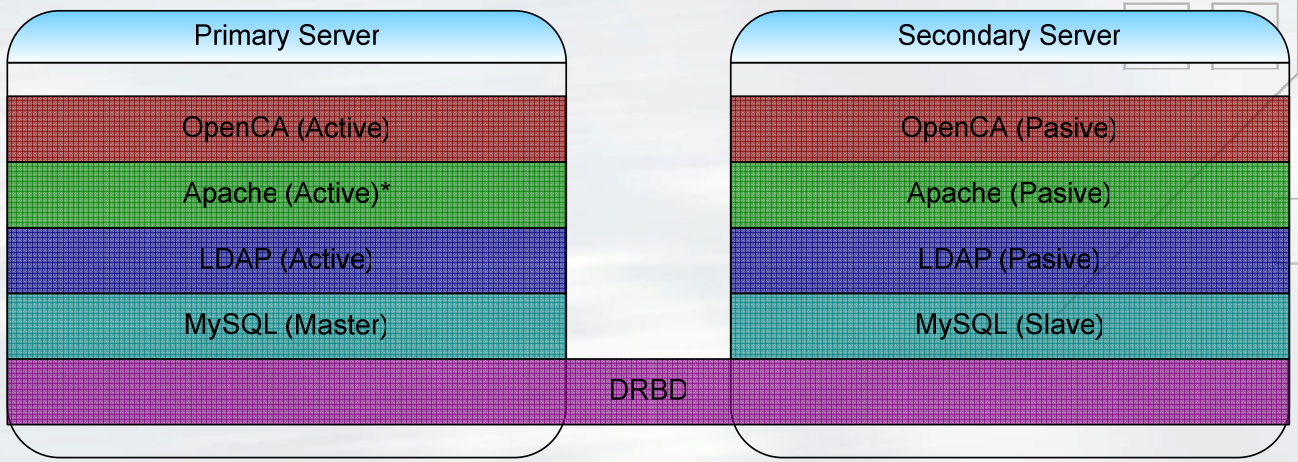
Secure VPN with Cisco Devices – Creating a High-Availability Setup

Server Architecture



Secure VPN with Cisco Devices – Creating a High-Availability Setup

Server Architecture

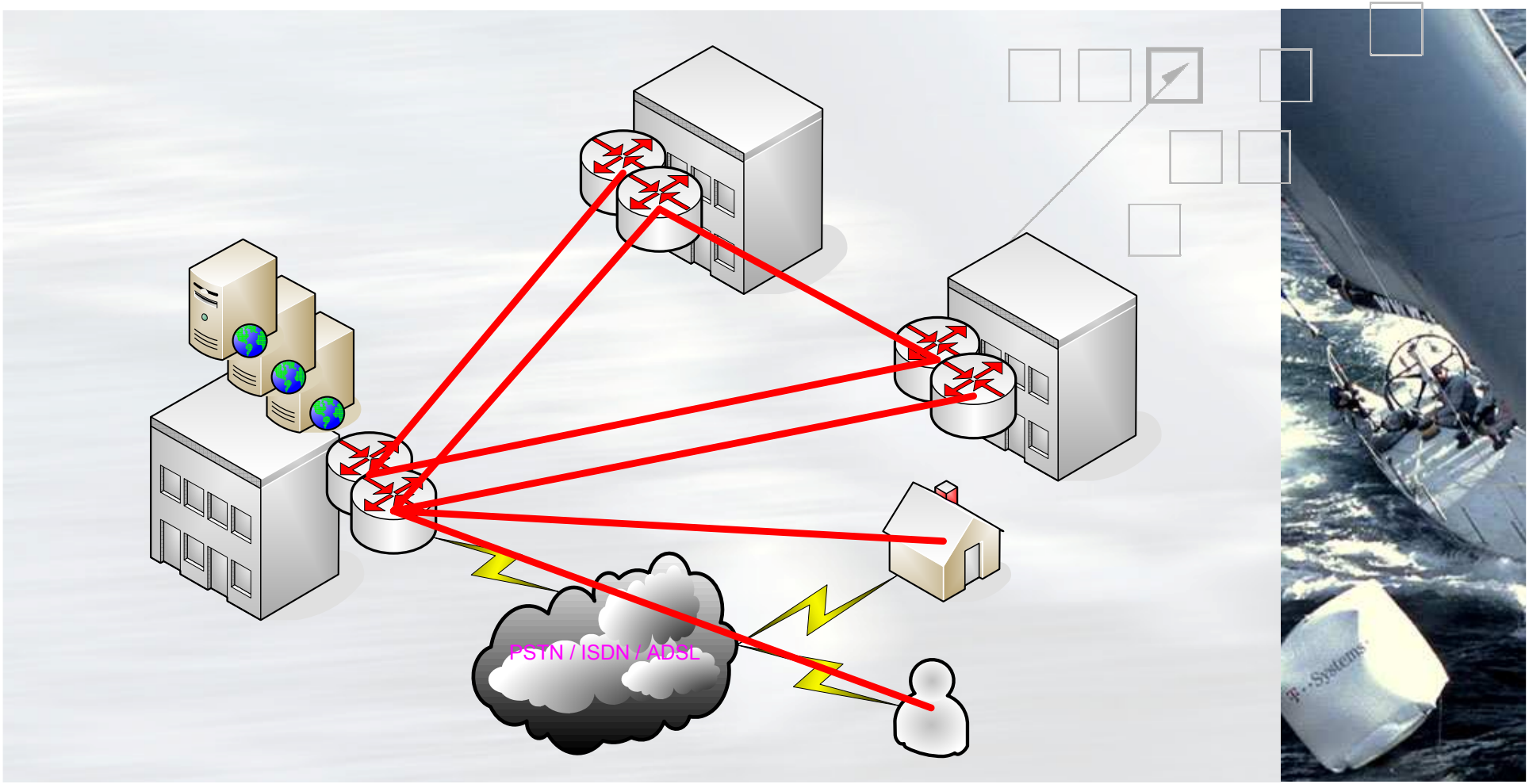


- Primary Server has active OpenCA, Apache and LDAP Servers
- Secondary Server only runs MySQL and DRBD as active processes
- Controlled manual switch over process

* Used for CRL and Root CA certificate distribution

Secure VPN with Cisco Devices – Creating a High-Availability Setup

Simplified Network Architecture



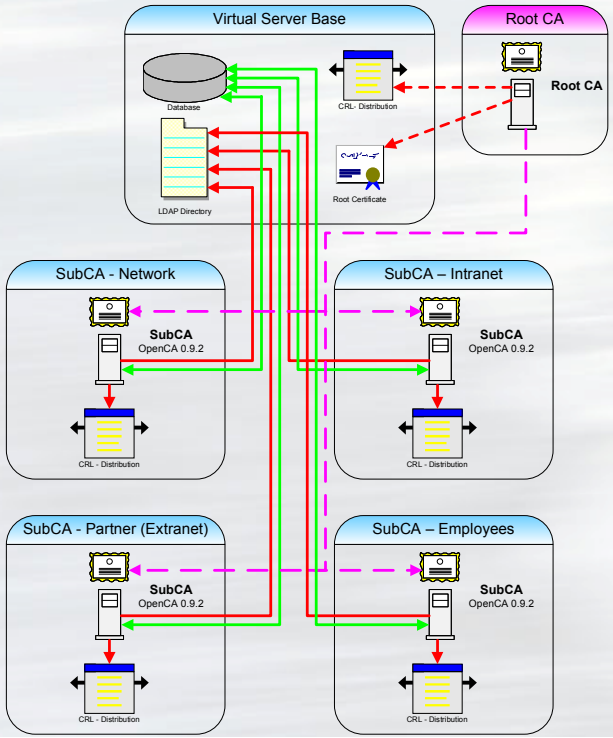
Secure VPN with Cisco Devices – Creating a High-Availability Setup

Simplified Network Architecture

- More than 300 sites connected
- Cisco VPN Technology
- Various connection technologies
  - Leased lines (X.21, ATM)
  - ISDN and Analogue dialup
  - Mobile GSM and UMTS
  - Internet and DSL
- SCEP Certificate enrolment and CRL updates

Secure VPN with Cisco Devices – Creating a High-Availability Setup

OpenCA Implementation

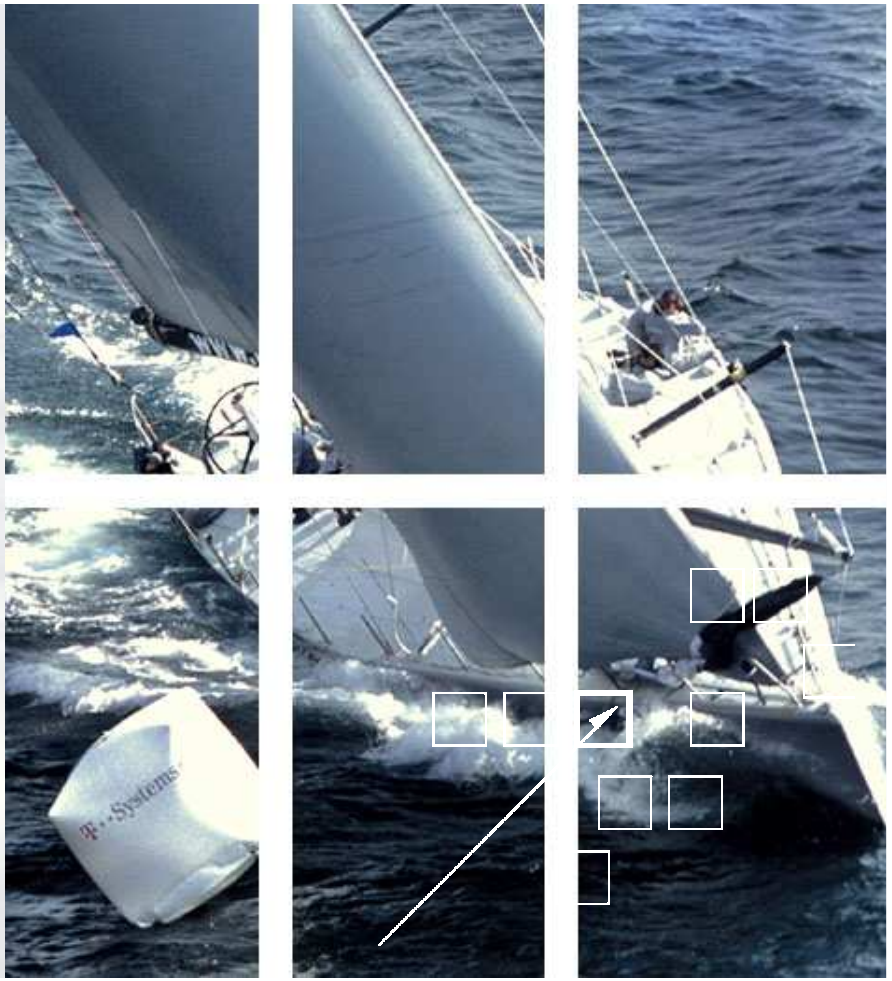


- Offline Root CA
  - Live CD
  - USB Stick with custom CA
- Online SubCAs
- OpenCA 0.9.2
  - SuSE 9.2 Virtual Machines

Secure VPN with Cisco Devices – Creating a High-Availability Setup

OpenCA Implementation

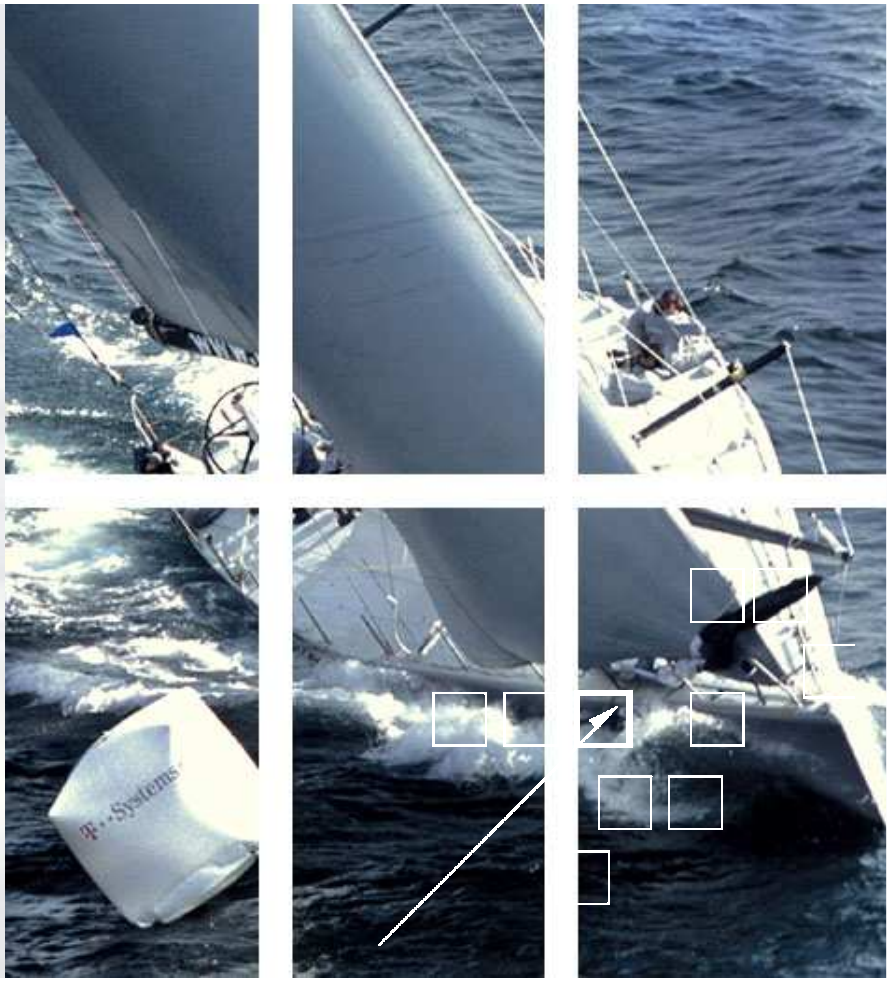
- A separate SubCA for each business area
- Each SubCA can be administered by the responsible unit
- One MySQL Database server and LDAP server used by all SubCAs
- Backup of V-Server Base system includes all SubCAs



Secure VPN with Cisco Devices – Creating a High-Availability Setup

OpenCA Implementation

- Easier security management as all SubCAs only have Apache and OpenCA processes.
- Access to RA, CA, LDAP and NODE interfaces controlled by Operator Certificates



Questions?

Max Schmid
T-Systems International GmbH
Dachauerstraße 651
80995 Munich
Germany
+49 89 1011 4722
max.schmid@t-systems.com

T · · Systems