User Scenarios

Francisco Hernández

GMV – Soluciones Globales Internet (SGI)

DESEREC

Dependability Security by Enhanced Reconfigurability

Aim of DESEREC

Today's business rely more and more on ITC-based large infrastructures.

Due to this dependence, any failure or malfunction in IS / IT platform can lead to considerable money loss.

Aim of DESEREC:

- address those dependencies by "building a tool" that will allow us to manage efficiently issues like dependability, security and resilience of critical systems, using fast detection, response and reconfiguration.

Aim of User Scenarios

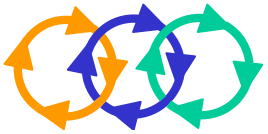
Analyse real world business cases which allow us to obtain useful information in order to design / build DESEREC.

- A User Scenario consist of:
  - A set of business services and detailed descriptions of them
  - Service maps: ITC infrastructure (HW & SW) supporting the services
  - Business, applications and systems dependences, constraints and requirements
  - Monitoring systems (sources of events)
  - A set of hypothetical hazards on ITC elements (HW/SW failures, attacks, …)
  - A list of possible reactions to the hazards
- This will help us to:
  - Identify functional, performance, security and other requirements for DESEREC

Aim of User Scenarios

Provide a test environment where DESEREC Demo can be checked.

- Test-Bed: Framework containing an “isolated” ITC infrastructure that emulates a production environment allowing to test the DESEREC Demo.
- Business cases defined within User Scenarios will be “executed” to check the properly functioning of DESEREC Demo. This way, we can obtain the following objectives:
  - Architecture validation
  - Functional requirements verification and validation



Our end-users

RENFE

RENFE is the national railway operator in Spain, providing the public service of passengers and trade goods transportation. Furthermore of this, RENFE is also an ISP (Internet Service Provider) in the spanish local market.

- Selected services for User Scenario:
  - Web Information
  - Internet Ticket Selling
  - Timetable querying

OTE (Hellenic Telecommunications Organization)

Telecom service provider in Greece and in the Balkan area. It´s a global telecom operator providing services of local, long and international distance calling, mobile telephony, Internet services, and high speed data communications (broadband network access)

- Selected services for User Scenario:
  - Fast Internet Access
  - IPTV Services: Video on Demand and Video Broadcasting

RENFE SCENARIO

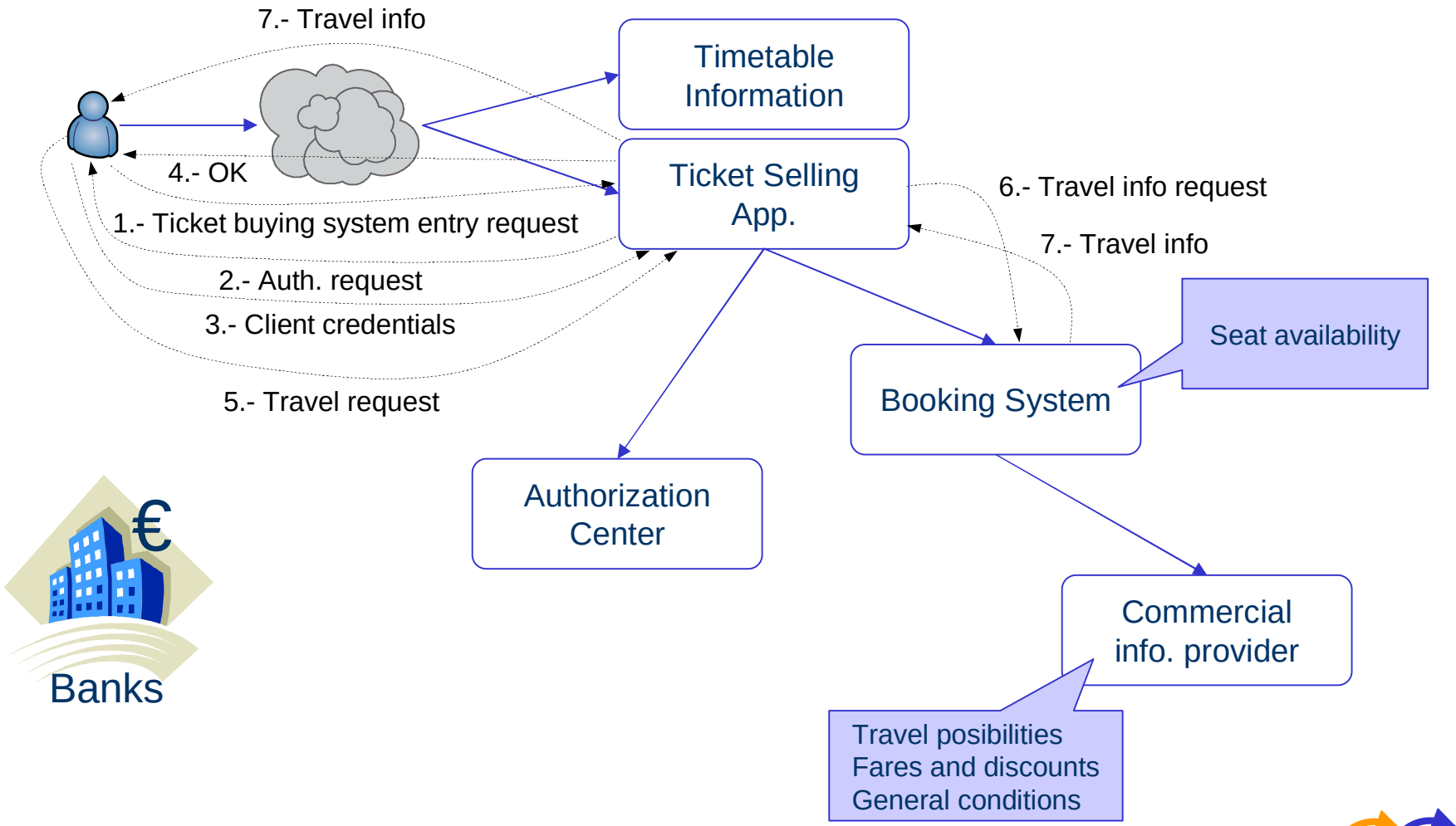
Business Services

- Web information: Public information available for all Internet users (general information about the company, relevant news, …) It´s the public area of the RENFE´s official website.

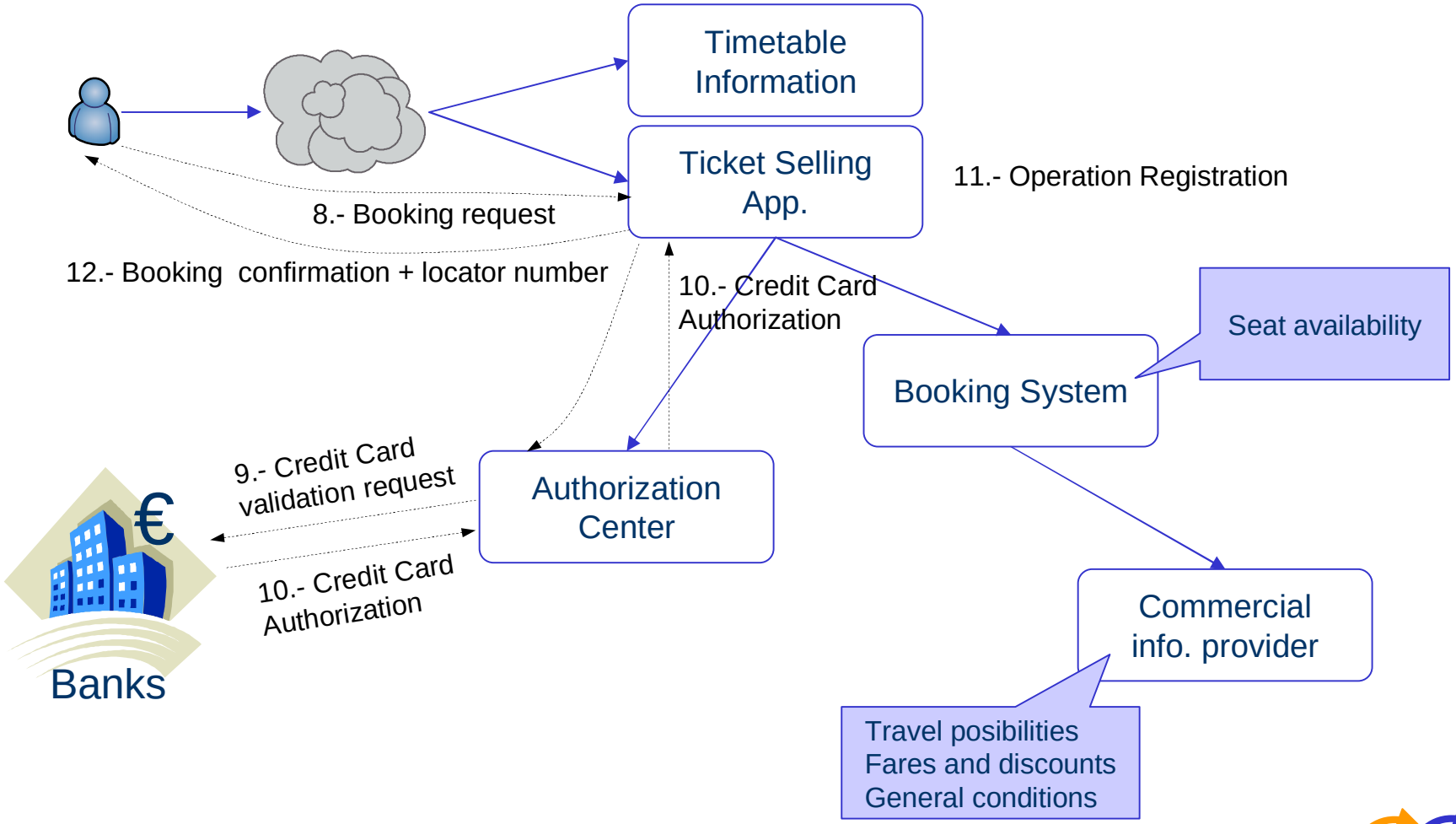
- TIKNET: Internet Purchase Ticketing service.

- Timetable information: Despite being considered as a part of the public information, it's quite related to TIKNET; both call to the same webservice to obtain the timetables.

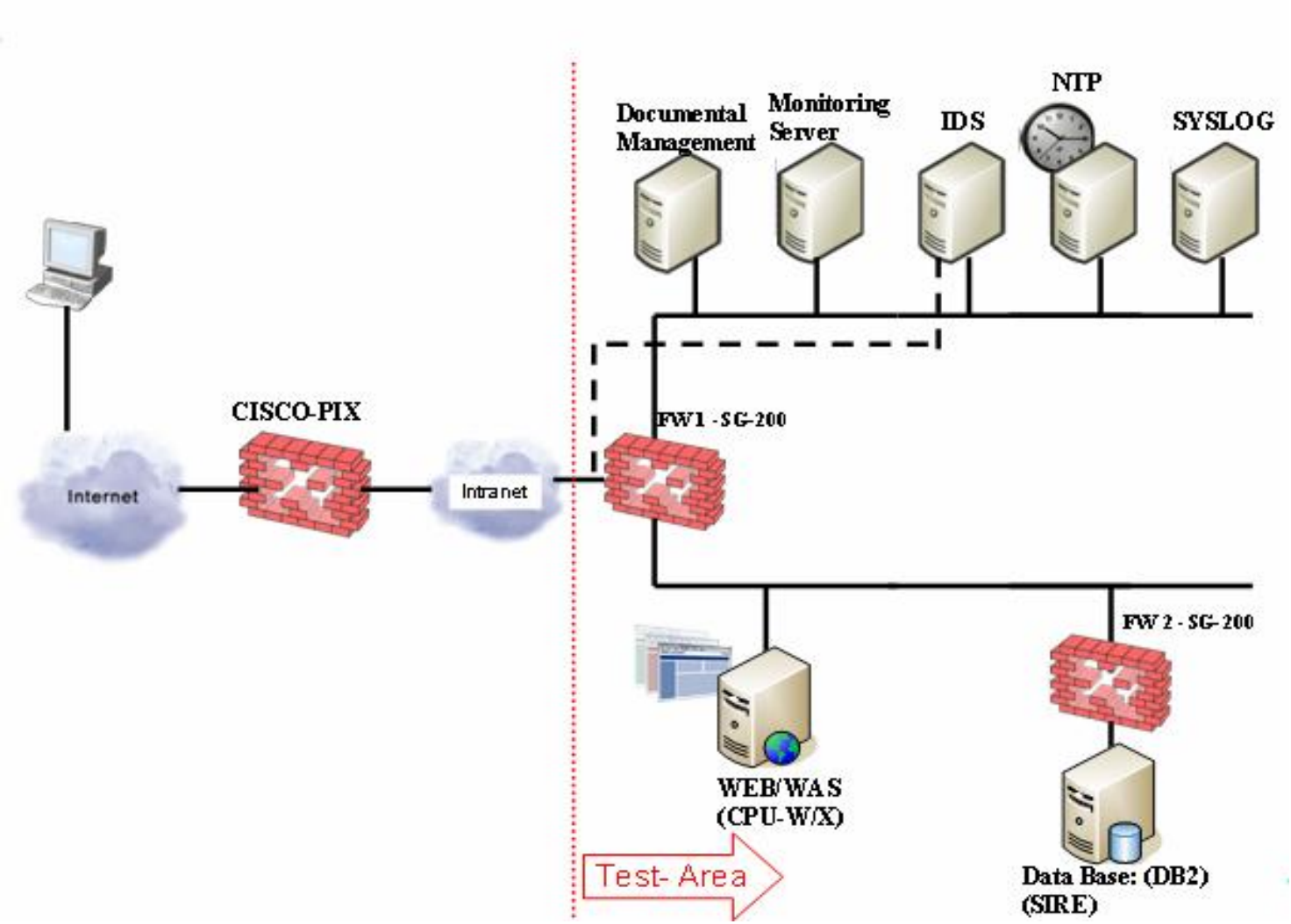
TIKNET Service Logical Model



TIKNET Service Description



Test-Bed architecture



Dependability properties

DEPENDABILITY PROPERTIES PER SERVICE	Security					
	Availability	**Integrity**	**Confidentiality**	**Reliability**	**Safety**	**Maintainability**
Web information	High	High	Low	Medium	Low	Low
Ticket Selling	High	High	High	High	High	Medium
Timetable Information	Medium	High	Low	High	Low	Low

DEPENDABILITY PROPERTIES PER COMPONENT	Security					
	Availability	**Integrity**	**Confidentiality**	**Reliability**	**Safety**	**Maintainability**
Web Server	High	High	Low	Medium	Low	Medium
Data Base Server	High	High	Medium	High	High	Medium
Application server	High	High	Medium	High	High	Medium
Firewall	High	High	High	High	High	Medium
IDS	High	High	Medium	High	Low	Low
NTP	Low	High	Low	Medium	Low	Low
Syslog	Medium	High	High	High	Low	Low
Documental Server	Medium	High	High	Medium	Medium	Low
Monitoring Server	High	High	High	High	Medium	Low

Threats

THREATS	ACTIONS	Security Requirements
DoS Attack	*Monitor:* Sitescope, already described Manual operation 24x7x365. They act following a protocol, performance depends of web status, at last action; they reboot server or service. IP´s blockage is used by communication department. Anyway RENFE´s web is “akamaized”, since Akamai service is given for RENFE, no DoS attack has been done against RENFE´s Web.	Availability
Physic or Logic failure, hardware or software.	*Monitor:* Sitescope, already described at D 1.1 Manual operation 24x7x365 Maintenance HW and SW contracted Periodical backups and backup servers are used against failure.	Availability
Information sent it, Electronically Intercepted	*Monitor:* N/A *Preventing Actions:* Ciphered SSL	Integrity Confidentiality
Physical Intrusion to the Data Center	Surveillance 24x 7, alarms and TV control	Integrity Confidentiality Availability
Hacking over TCP/IP network	*Monitor:* Sitescope, already described, furthermore, logs & study. *Preventing Actions:* Firewall, filtered rules into routers, filter ports into switches (devices), updates of systems, maintenance of applications, hash generations functions, malware detection (IDS) *Reactive Actions:* Ports´ blockage, IP´s blockage, stopping of services, restore configurations	Integrity Confidentiality

Monitoring Summary

	Can be monitored?	Log type	Log retrieval
FW 1 - SG-200	Log server inside Fw console	Proprietary format, convertible to Syslog	Real time
FW 2 - SG-200	Log server inside Fw console	Proprietary format, convertible to Syslog	Real time
DB2	No		
IDS Snort	Yes, in Syslog Server	Syslog	Real time
Web Sphere	It's possible if the application use log4j	log4j	Real time
Web server	Yes, in Syslog Server	Syslog	Real time
Documental server	Yes, in Syslog Server	Syslog	Real time
Monitoring server	Yes, in Syslog Server	Syslog	Real time

Reactions

	Reaction used?	Technology	Remote Interaction
IP source blockage to destination IP	yes	StoneGate	manual intervention through GUI
IP source blockage to destination Port	yes	StoneGate	manual intervention through GUI
Service Killing	yes	/etc/init.d/service stop	script though SSH
Service Restarting	yes	/etc/init.d/service restart	script though SSH
Suspicious connections killing	yes	kill	manual intervention through CLI
Suspicious processes killing	yes	kill	manual intervention through CLI
Change of database user in aplication server configuration file	no		
Disable database connection in aplication server configuration file	no		
Apply ACLs in a Web Server	no		
Deny Directory Listing in Web Server	yes	Apache	manual intervention through CLI
Deny recursion in DNS Server	yes	BIND	script though SSH
Deny zone tranfers in DNS Server	yes	BIND	manual intervention through CLI
Switch to Passive mode in FTP Server	no		
Deny mail relay in SMTP Server	yes	postfix	manual intervention through CLI
Add an IP in a blacklist of an SMTP Server	yes	postfix	
Disable aggressive mode in IPSEC VPN Gateway	no		

OTE SCENARIO

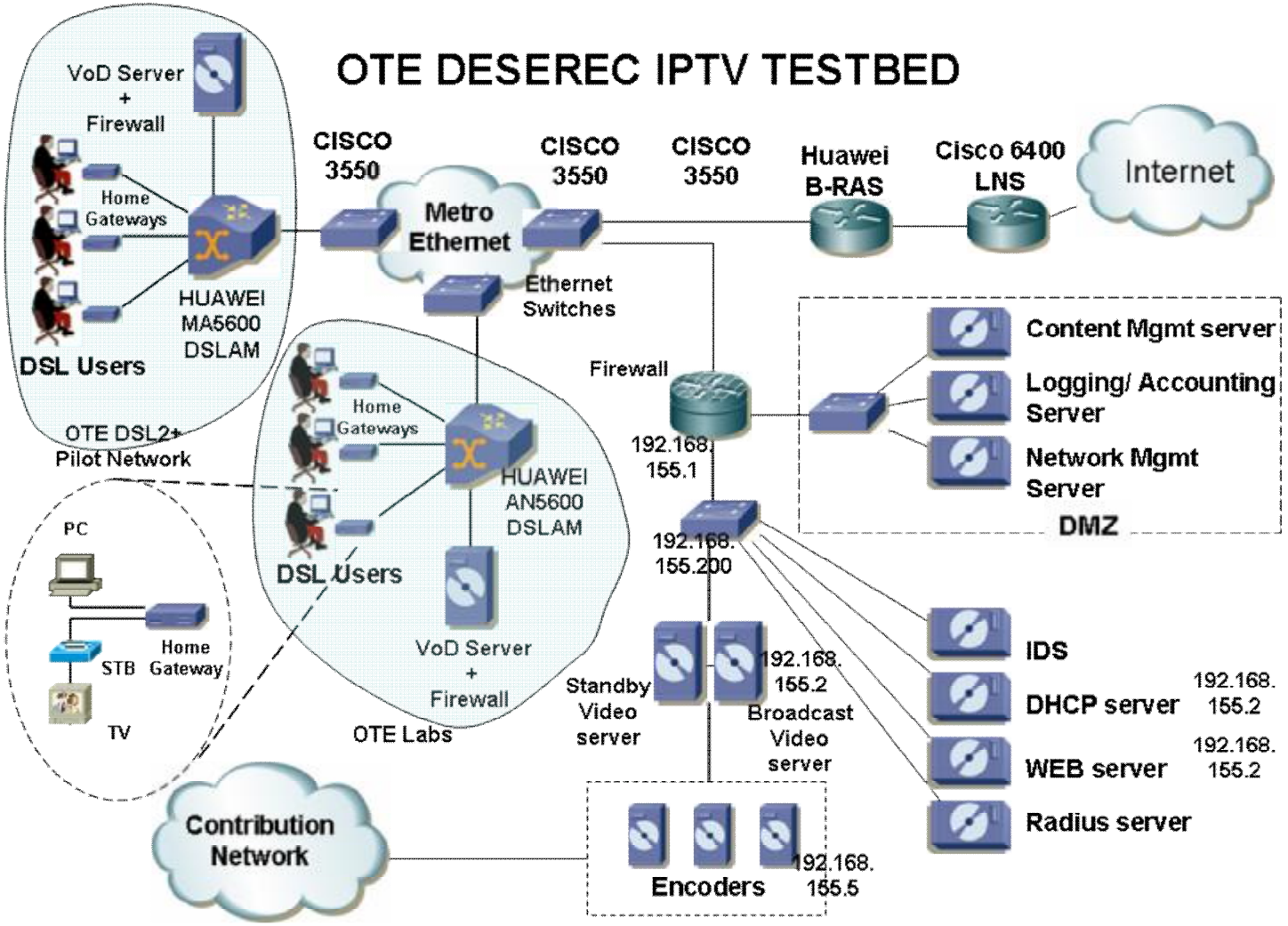
Business Services

- Fast Internet Access: The Home User is provided with broadband access through a typical xDSL broadband network.
- IPTv Services: The Home User receives video content (VoD or Live Video) through a typical xDSL broadband network

Fast Internet Access Service Description

Service	Component	Description
Fast Internet	Cisco 6400 LNS HUAWEI 5200 G BRAS	Terminate the PPP user session and provide internet connectivity.
Fast Internet	Metro Ethernet Devices	Transport internet traffic between BRAS and Access Network
Fast Internet	DSLAM	Transport internet traffic between metro network and user CPE
Fast Internet	RADIUS Server	Implements AAA functionality.
IP address assignment for Fast Internet	B-RAS	The assignment of the IP Address upon PPPoE request is assigned by the B-RAS
User Authentication	RADIUS Server	The Authentication is performed by the RADIUS server located “behind” the firewall.
Configuration of DSLAMs, Cisco routers, B-RAS	Network Management Server	The Management of all the network elements is performed from the respective Network Management Servers located “behind” the firewall.
Firewalling	Bridge Firewall	A bridge firewall protects the main service components, while allowing DHCP requests
Logging/Accounting	Logging Server	A syslog based logging server that aggregates all events for loggin and accounting purposes
Broadband Access	DSLAM	A DSLAM is provide broadband access to the users
LAN Networking	Ethernet Switches	The Metro Ethernet architecture is implemented using various ethernet switches

Test-Bed architecture



Dependability properties

Fast Internet Access

Component	Dependability	Resilience	Security	Notes
DSLAMs	●	◑	◑	The operation of the DSLAMs is critical for the service only with local impact
Metro Ethernet	●	◕	◑	The operation of the metro is critical for the service depending on how close to the root is the failure
BRAS	◑	◑	◕	Exposed to internet Threats, but has no access to IPTV service. Necessary only for the Internet service
Firewall	◔	◔	◑	Blocks all fast Internet users
Network Management Server	◔	◑	◔	Inside the DMZ, performs management of the DSLAM and the Metro Ethernet
Customers' CPE	○	○	◑	Vulnerable to attacks

CONCLUSIONS

Conclusions

- DESEREC must handle different formats of events coming from different sources:
  - syslog, SNMP, proprietary format
- DESEREC must know all the systems / elements under monitoring
- DESEREC must correlate events & incidents
  - A single event may be a simple incident
  - A combination of events may be a simple incident
  - A simple incident can be a part of a complex one
  - The time needed to detect incidents is variable
- DESEREC must provide different detection techniques
- DESEREC should reduce the “noise” (false positives and others)

Conclusions

- Fast Reactions Vs Short Term Reactions
  - Some reactions can be applied automatically (scripts) while others manually
  - Certain reactions are purely focused on symptoms while others take into account the context (element triggering the event and it's dependability properties and requirements)
  - Some local reactions may affect other elements / subsytems
  - Some actions must be authorized by the operator (system expert)
- DESEREC must provide detailed information on detected incidents and possible reactions.
- DESEREC must provide an interface that allow the operator to configure the application

THANK YOU
FOR
PAID ATTENTION