Proposal of an Operational Network Architecture for Satellite Missions

L.S. Silva[1], A.E.M. Salgado[1,2]

[1] Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, São Paulo, Brazil.
[2] *Tribunal Superior Eleitoral (TSE), Brasília, Distrito Federal, Brazil.*

Abstract: In this paper an architecture to integrate the INPE ground segment operational network with Intranet and Internet is proposed in order to broad the data communication scope between INPE and external agencies in satellite missions. Through this architecture, data transmission operations can be fast executed improving the inter-institutional and internal communication efficiency.

New procedures and security technologies will installed to keep the protection level of the network according to the project requirement. Several safety layers foreseen on depth defense strategy will be applied, consisting of controlled access area for data sharing, traffic control devices (firewalls), safety administration tools, reinforcement of operational systems and intrusion detection system. Artificial intelligence techniques to detect network attacks are also considered.

Finally, this paper presents a summary of the project challenges, considering the reliability, security, accessibility and performance requirements for each mission.

Key-words: satellite operational network; secure data communication interchange; security in networks

1. Current Scenario and Proposal

Presently the operational network of SCD-1, SCD-2 and CBERS-1 satellites, operated by INPE, is totally disconnected from other internal and external networks of institutions cooperating on space missions. Thus, information are exchanged among users through disks and magnetic tapes. Although this network presents a high degree of protection against non authorized access, the data transfer system provided does not satisfy the current accessibility demands.

The proposal presented in this paper to improve the operational conditions above described consists in to integrate the INPE ground segment operational network with the internal and external networks through a secure network architecture.

2. Network Architecture

The proposed integration refers to a set of interlinked computer network to provide and to support the data communication among the ground segment components in Brazil and abroad, cooperating with each other in a specific satellite mission. This network is based on the protocol TCP/IP, Ethernet pattern and will use the patterns and technology already existent in the internal and external environments of the

involved institutions. The services available in this network are file transferring, Web page queries and electronic message exchanges.

The ground segment components in satellite missions include the Brazilian operational units of INPE, located in the cities: São José dos Campos (CCS unit – Satellite Monitoring and Control Center) and Natal (CRN unit – Natal Trace Control Center), and external operational units: foreign space agencies and other Brazilian institutions.

The basic network architecture, including the networks that will be integrated, active elements and security devices, is presented in figure 1 as follows.

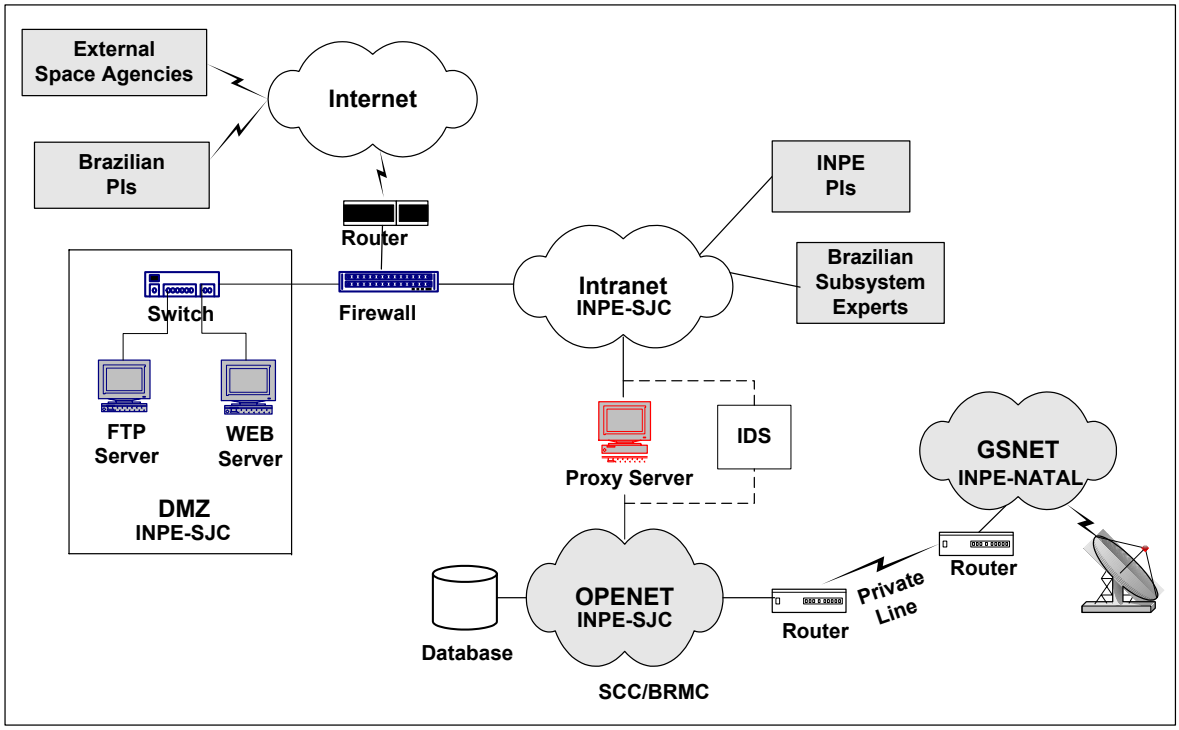

Figure1. Proposal Network Architecture.

This architecture presents the integration of the Ground Segment Operational Network (OPENET) with the other internal nets: Intranet, DMZ-INPE and Natal Ground Station Network (GSNET). Through Internet, OPENET will also be connected to the external space agencies and Brazilian institution networks participating in a satellite mission.

OPENET is the operational network that should assist all the foreseen needs of data communication related to the satellite controlling and monitoring, and command sending operations by CCS operational unit.

GSNET is the network environment net that should assist all the activities of data communication of CRC in Natal, allowing the ground station control, command sending and satellite monitoring operations.

Intranet is the internal computer network that makes use of the same data communication patterns of Internet and provide the internal communication and organizational administration of INPE. This network interconnect all organizational units of the Institute and involves the information and data administration, the processing of electronic document and system and database integration.

DMZ-INPE (INPE Demilitarized Zone) is the INPE protected public area that stores data and resources that are shared and accessed in a controlled way. Secure FTP (SFTP) and Web services will be supplied through DMZ-INPE.

Intranet and DMZ-INPE are networks in activity at INPE that will be updated to allow the data exchange operation in the satellite mission, while OPENET and GSNET are new networks to be implemented.

3. Data Communication

The data communication among the components of this proposed network is presented in figure 2. The arrows indicate the message and data transmission direction and it points to the information receiver.

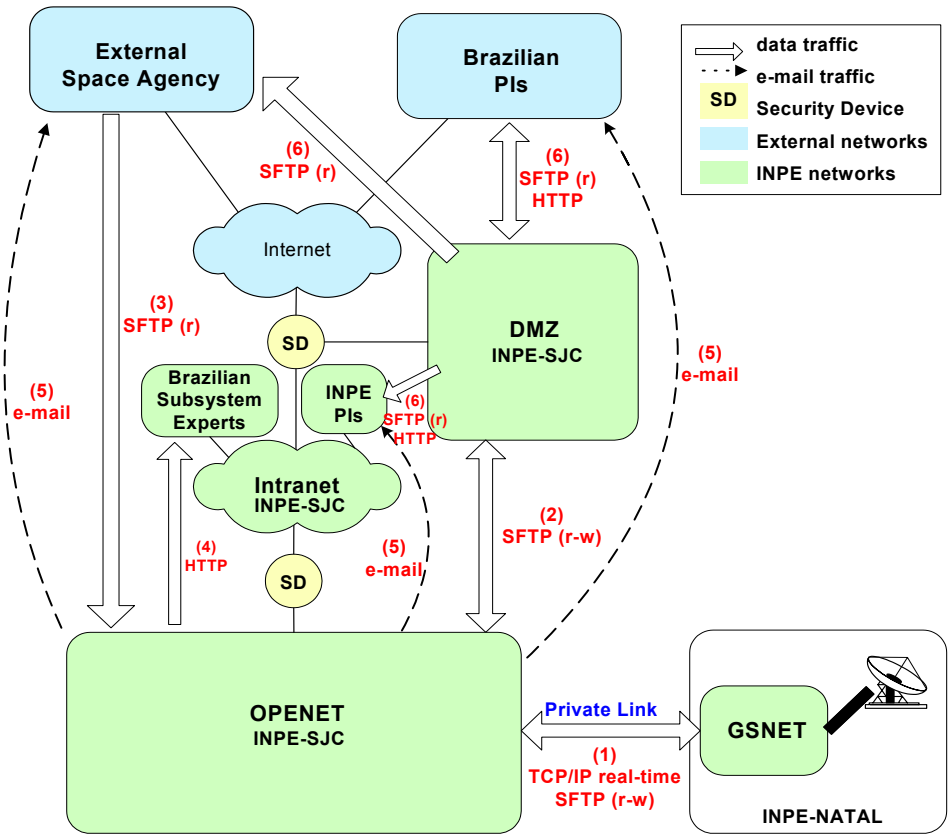

Figure 2. Data Communication for Network Components

The following operations, enumerated on figure 2, will be available in the network:

(1) During the satellite passage, the TCP/IP communication among the OPENET and GSNET users will be allowed in real time. Out of passage, data will be transferred among both nets through SFTP service (reading and writing).

(2) OPENET users will be able to input and to access data in DMZ-INPE through SFTP service for data transferring (reading and writing).

(3) OPENET users can access data from a external space agency through SFTP service (only reading).

(4) FBM Brazilian Subsystem Experts users can access information from OPENET through queries on a Web application.

(5) OPENET users can send e-mail to INPE PIs and external institutions.

(6) INPE PIs and external agency users can access information from DMZ-INPE (only reading) through Web page queries and data exchanges using SFTP service.

4. Security Strategy

To control the data flow between OPENET and internal and external networks, several security layers will be implemented, composing a Defense in Depth strategy. This strategy consists of implementing security mechanisms, as: controlled access public area for data sharing (DMZ-INPE), traffic control devices (firewalls), safety administration tools, operating systems reinforcement and intrusion detection system.

The configuration of security mechanisms should be accomplished according to the INPE security policies and according to the security requirements required for the project in each mission.

A brief explanation about some security resources to be used is described as follows.

4.1 Access Control

DMZ-INPE will be configured to allow the satellite mission data sharing with security, which can be accessed and updated for the ground segment components at INPE and other involved agencies in a controlled way.

To control the data traffic among the operational networks involved in a satellite mission and in order to keep the environment availability and protection, safety devices and network active elements will be installed.

The access to mission data located in DMZ-INPE for the OPENET, Intranet (INPE PIs) and external agency users will be controlled by the INPE's firewall server machine, through specific rules inserted in this server.

The data traffic between OPENET and Intranet will be controlled by a *proxy server* able to hide the internal customers' addresses, to block undesired URLs, to filter packages content, to verify the consistency of the protocol content, to block unauthorized routes and to provide occurrence registration and alert resources.

For the connection between OPENET and GSNET a SLDD dedicated line (Dedicated Line Service for Digital Signals) of 256 Kpbs will be installed, so that the data transmission among the networks be private and fast. There will be a router for OPENET as well as GSNET that will redirect the data to a valid destination.

4.2 Systems Reinforcement

Another safety layer is the server and client machines installation and security configuration, including the following operations: disk partitions planning; minimum installation of necessary packages; unnecessary services removal, installed by default; strong passwords definition for administrators; patches and hot fixes application to operating systems according to the manufacturer recommendation; system event logs creation and synchronization of network server machine clock.

4.3 Intrusion Detection Systems

At INPE there is a research and technological community and a specific network Group is implementing network intrusion detection systems, exploring modern techniques to represent the specialist knowledge in network attacks and using approaches of intelligent reasoning to improve the search process of illegitimate patterns in the network. These tools are a complementary part of the proposed safety infrastructure.

Two Intrusion Detection Systems (IDS) are in development. The first system is an intelligent agent that detects attack registrations in Web server access logs. This tool keeps a attack signatures list and a valid pattern list of HTTP requests and processes the rule actions when a observed event matches a search pattern, keeping in a file only the illegitimate log entries. This system reduces the entries in a web server logfile drastically, just maintaining the registration with unknown and illegal information. The second uses a approach of neural networks to detect attack information in TCP/IP packet crossing to the network. Nowadays, both systems are being improved, and with the last one there is a challenge to implement a detection mechanism in real time. In parallel with the implementation, a strategy to locate these IDS in the network, before or after the firewall, is being planned, so that the network can be more efficiently monitored.

4.4 Security Administration Tools

Besides security devices, tools to evaluate continuously the network infrastructure security will also be used. With these resources, it will be possible to verify the connectivity associated with the network services, to identify the problems with security appliances, the issues about the link layer related to ARP

protocol, and to generate vulnerability reports. Having this evaluation results in hand, the security practices of the network can be reinforced, the common vulnerabilities reduced, and the access rules to data and resources improved.

5. Benefits

The principal benefit provided by the creation of this presented network architecture will be the automation of the data transmission process in satellite controlling and monitoring operations, narrowing the gap and broadening the communication among INPE ground segment operational units and from these with external institutions located in different parts of the world. The wide and secure data accessibility proposal provides greater satisfaction to the network users. Besides, security tools created by our network group can be tested and improved in favor of INPE projects. Finally, with the security infrastructure specified in this project, the access protection of the operational network data and resources will be granted.

6. Challenges

Several challenges will be faced, beginning with the specification of the resources for secure integration of internal and external networks; which requests a cost-benefit analysis in the choice of network protection products.

Another issue to be carefully treated is the creation of access rules that meet all specifications, project requirements and applicable security policies, as well as security mechanisms installation and configuration to reduce risks of safety gaps in the network to the maximum.

To improve the intrusion detection systems in construction, through the advanced AI techniques on search of network traffic and events reports anomalies is another activity that is demanding effort.

Finally, there is the challenge of planning and accomplishing the integrated test and management of all components in the proposed operational network against the reliability, safety, accessibility and performance requirements specified for each mission.