“A Cabo Verde Telecom e a segurança dos Sistemas de Informação”

Almiro L. Almeida Rocha
Departamento de Sistemas de Informação
Gestão e Manutenção de Infraetruturas

Praia,
27 a 29 de Novembro de 2007

Sumário

1. Enquadramento inicial
2. A fraude na Rede de Telecomunicações
3. Protecção dos Sistemas de Informação (SI)
4. Pontos críticos e desafios

Sumário

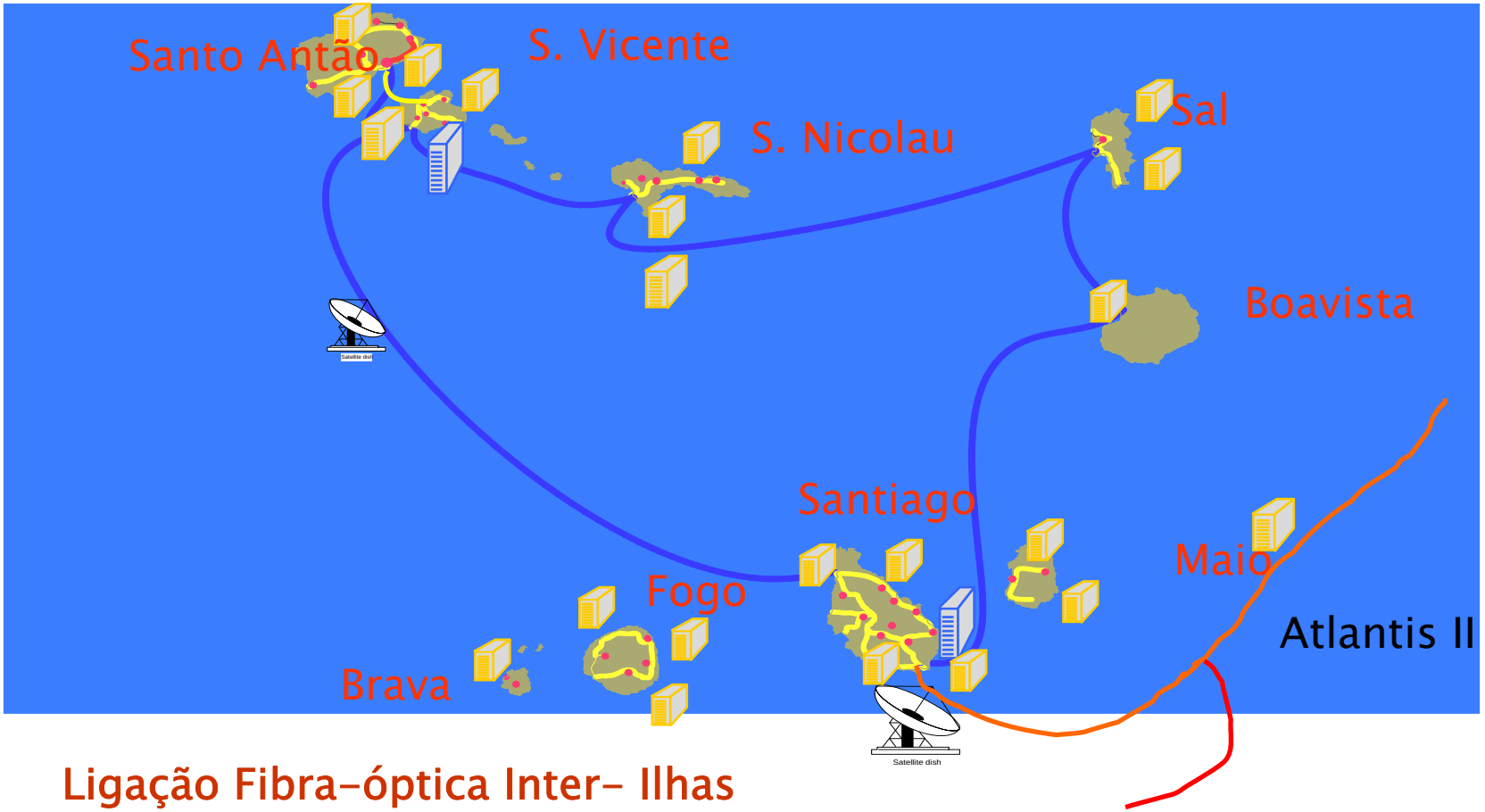
Serviços:

- TELEFONE FIXO
- TELEFONE MÓVEL
- INTERNET
- COMUNICAÇÃO DE DADOS
- CIRCUITOS ALUGADOS
- VIDEOCONFERÊNCIA
- TV-CABO (DSL)
- MÓVEL MARÍTIMO

"A Cabo Verde Telecom e a segurança dos Sistemas de Informação"

Alguns marcos Importantes:

- 1991-Era da digitalização (Instalação das primeiras centrais telefónicas digitais)
- 1995 – Privatização com alienação de 40% do seu capital Social à Portugal Telecom
- 1997 – Instalação e entrada em operação do cabo submarino inter-ilhas em fibra óptica.
- 1997 – Rede Móvel GSM – Internet e Rede de Dados
- 2000 – Entrada em operação do Cabo Submarino Internacional- Atlantis II
- 2002 – Fecho do anel de fibra Óptica inter-ilhas
- 2004 – Introdução do Serviço Internet Banda Larga (ADSL)
- 2005 – Criação das Empresas CVMóvel e CVMultimedia
- 2006 – Introdução serviço TV por Assinatura
- 2007 – Liberalização do mercado de Telecomunicações



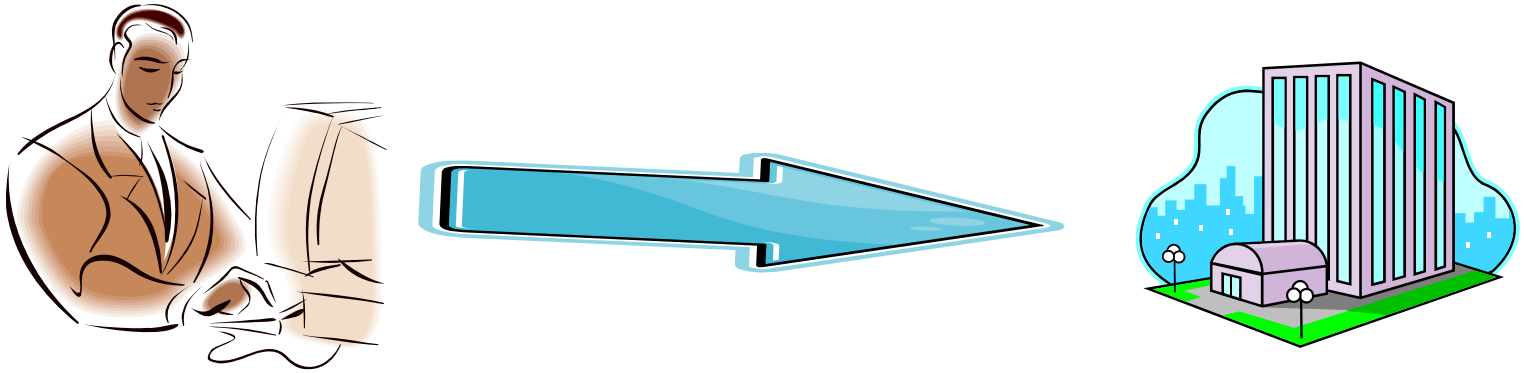
Ligação Fibra-óptica Inter- Ilhas

Sumário

1. Enquadramento inicial
2. A fraude na Rede de Telecomunicações
3. Protecção dos Sistemas de Informação (SI)
4. Pontos críticos e desafios

- **Alguns casos de falhas e fraudes:**

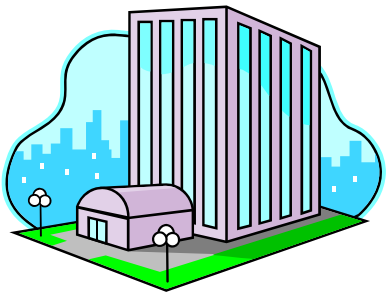
  Vírus gerador de tráfego em clientes Dial-up



- **Alguns casos de falhas e fraudes:**

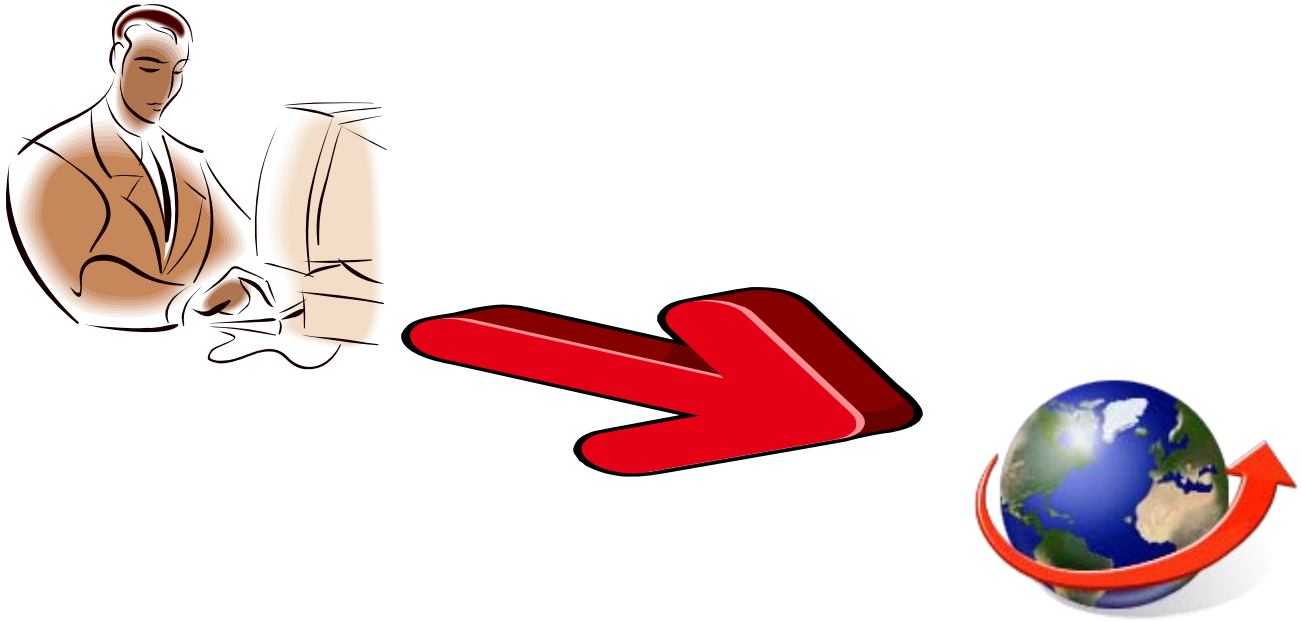
  Vírus gerador de tráfego em clientes Dial-up





- **Alguns casos de falhas e fraudes:**

Vírus gerador de tráfego em clientes Dial-up



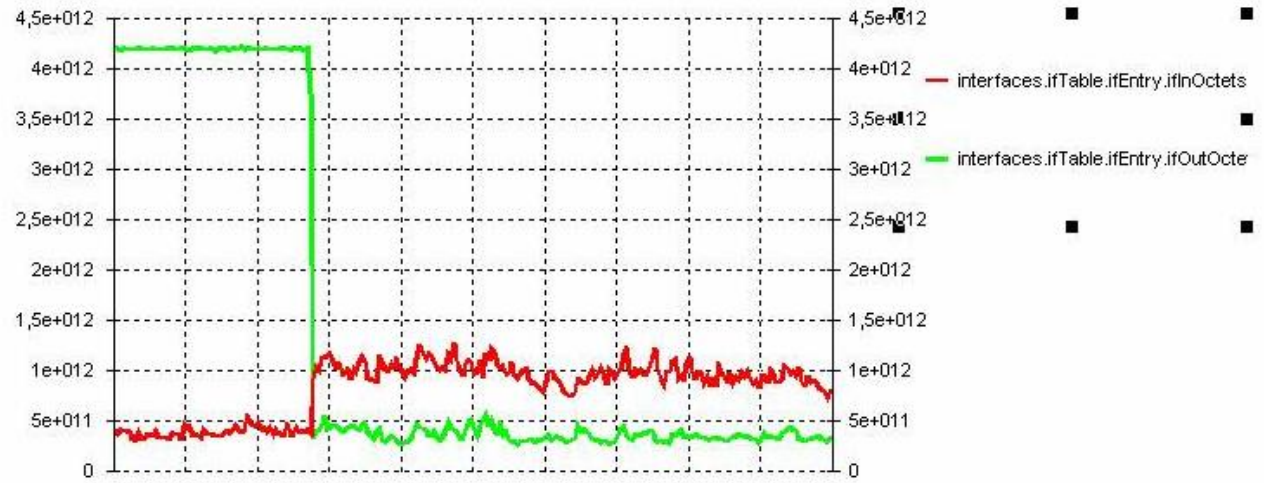
- **Alguns casos de falhas e fraudes:**

  Aplicações com segurança deficitária (Pré-pago)

- códigos de cartões pré-pagos com algorítmos frágeis
- Vários dias de paragem na venda destes cartões

Alguns casos de falhas e fraudes:

- Ataque de vírus de utilização massiva da Internet
  - degradação de serviço



A verde trafego Out -> para a Marconi
A vermelho Tráfego In <- da Marconi

"A Cabo Verde Telecom e a segurança dos Sistemas de Informação"

- **Alguns casos de falhas e fraudes:**

  Fraude na Rede de Assinantes

  Ataques a PABX

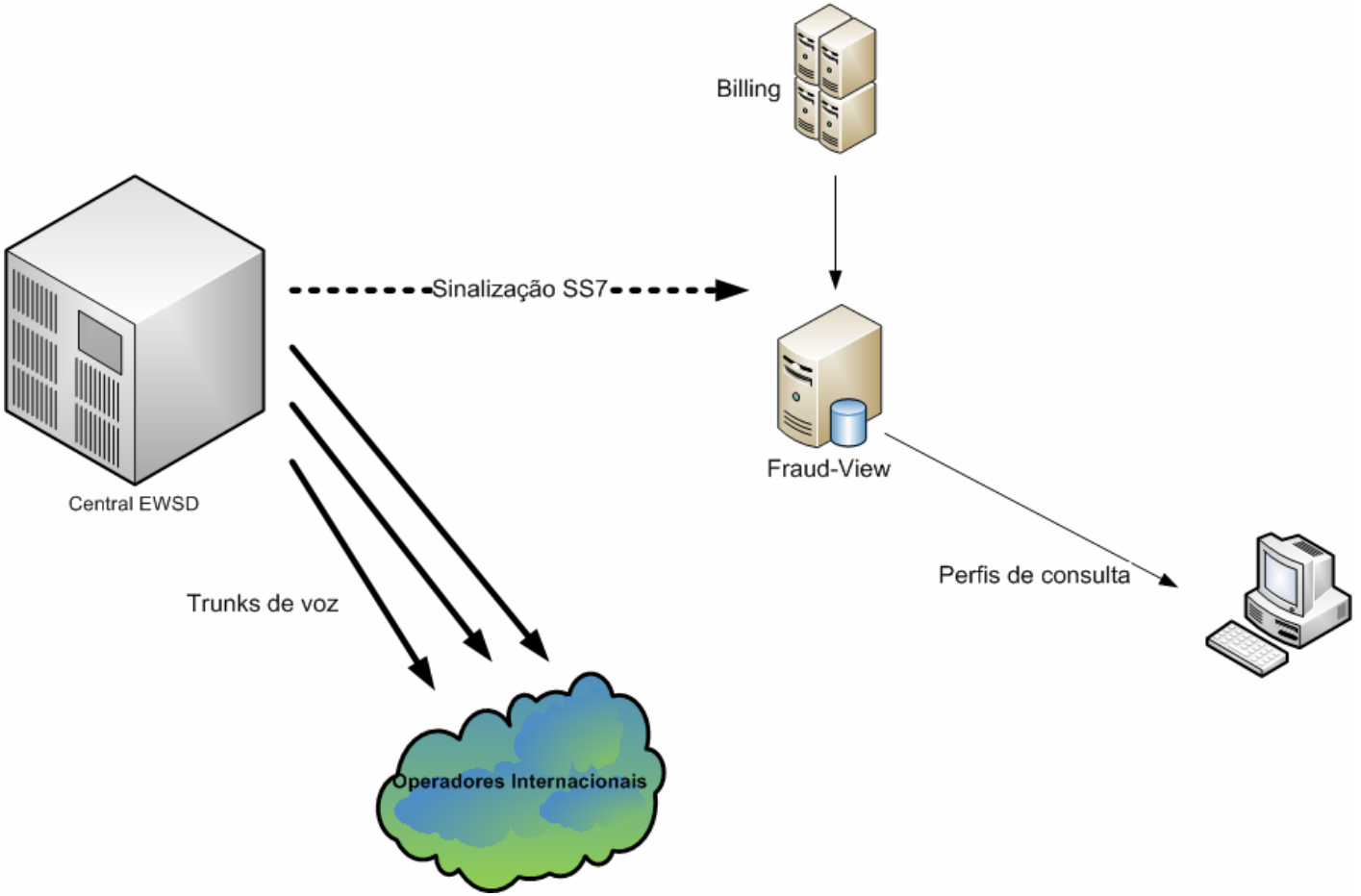
  Fraude nas cabines telefónicas

  Falha na assinatura do serviço (Móvel)

Combate à Fraude

- Actuação defensiva
- Parcerias: FINNA, QSDG e CFCA
- Menos de 50% dos casos são levados a tribunal
- Sistema de detecção de fraude (ECTEL's FraudView)

"A Cabo Verde Telecom e a segurança dos Sistemas de Informação"



- Sistema Anti-Fraude: Esquema simplificado

Sumário

1. Enquadramento inicial
2. A fraude na Rede de Telecomunicações
3. Protecção dos Sistemas de Informação (SI)
4. Pontos críticos e desafios

- **Protecção de Infraestruturas Críticas**
- Plano de Normas e Políticas de segurança
  - Política de Gestão de Acessos
  - Documentação de Procedimentos
  - Plano de Backup e Recovery
  - Instalação de Alarmística
  - Health Checking e aplicação de correctivos de segurança
  - Gestão de incidentes

Protecção de Infraestruturas Críticas

Protecção física

- Circuito de vigilância interna e externa
- Registro electrónico de acesso
- Securização geral de Energia
- Securização da Climatização do centro de dados

Protecção de Infraestruturas Críticas

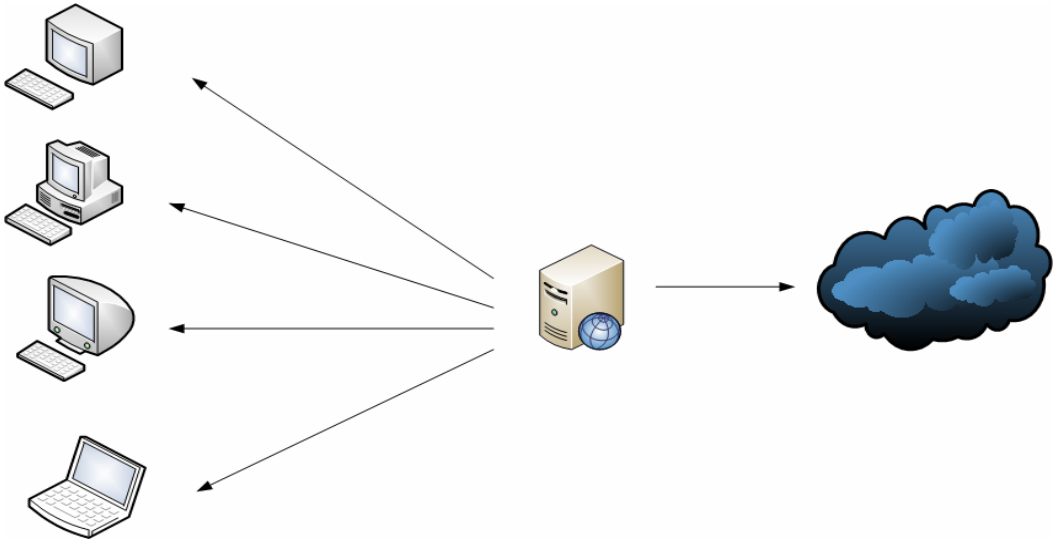
- A política de segurança

  - Monitoria de tráfego dos Equipamentos activos da rede (Switches, Firewalls, VPN, Routers, etc)

Protecção de Infraestruturas Críticas

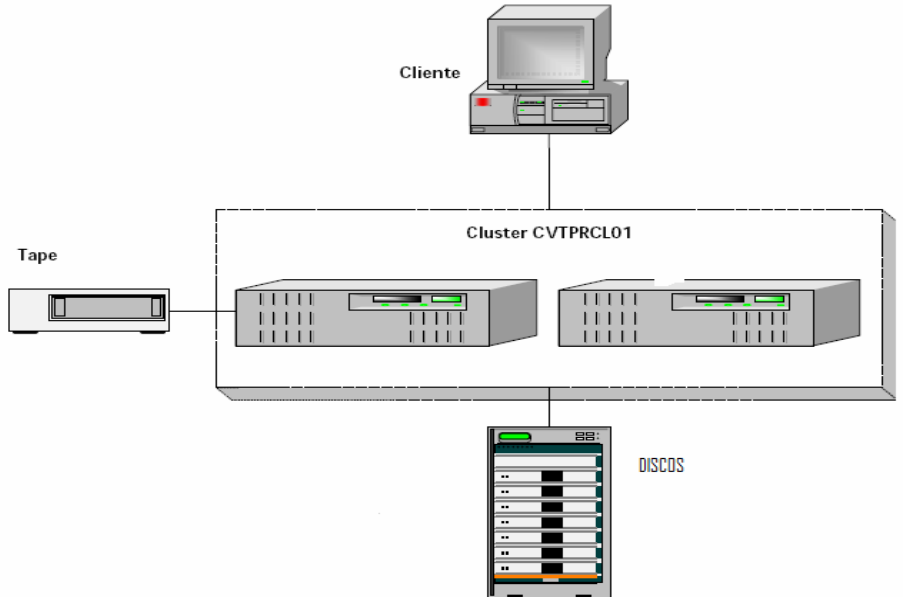
- A política de segurança

  - Antivírus Central e Antispamming



Protecção de Infraestruturas Críticas

- A política de segurança
- Backup Centralizado



Protecção de Infraestruturas Críticas

- A política de segurança

  - Uma estação de trabalho padrão

Protecção de Infraestruturas Críticas

- A política de segurança

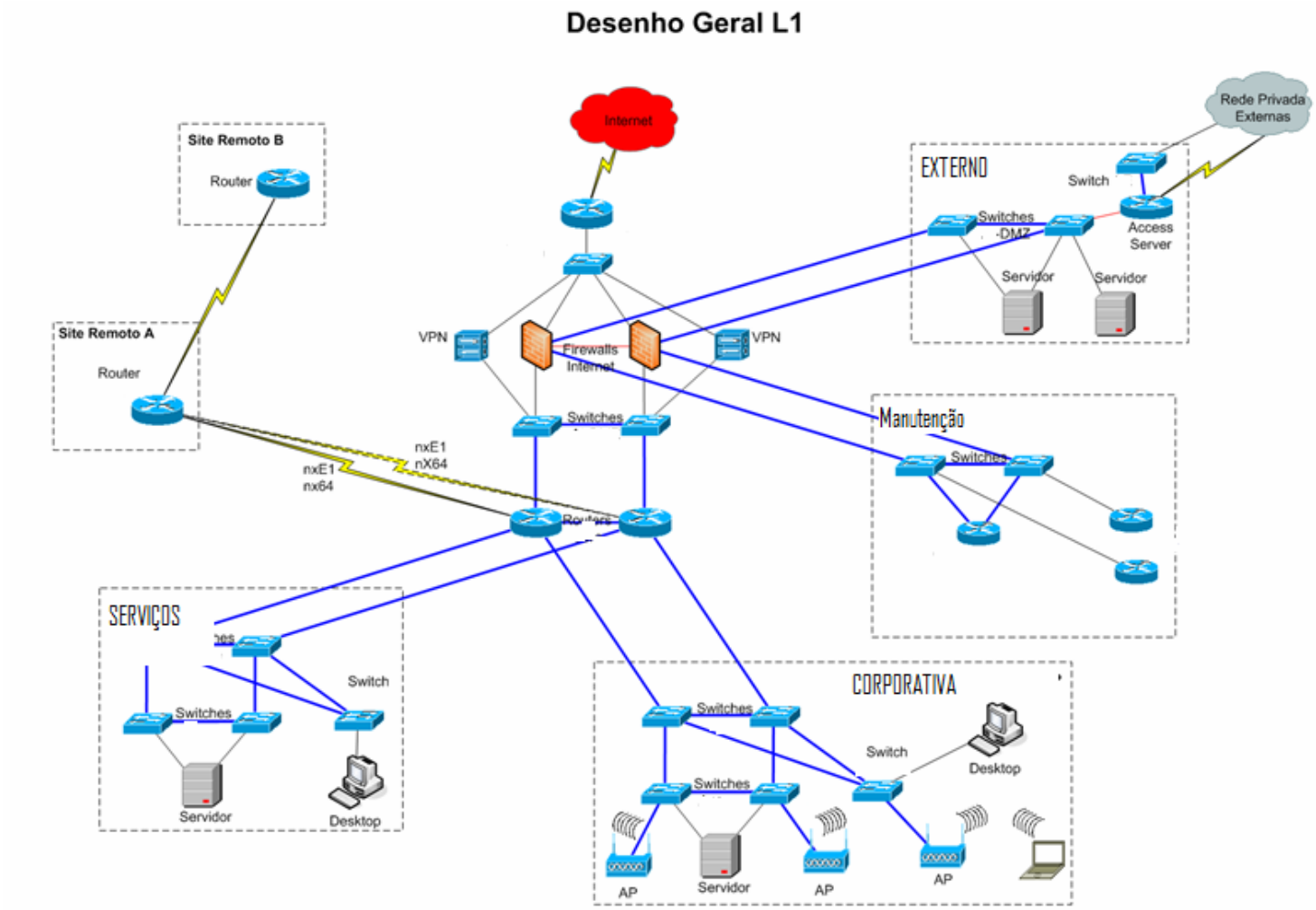
  - Detecção periódica de vulnerabilidades

Protecção de Infraestruturas Críticas

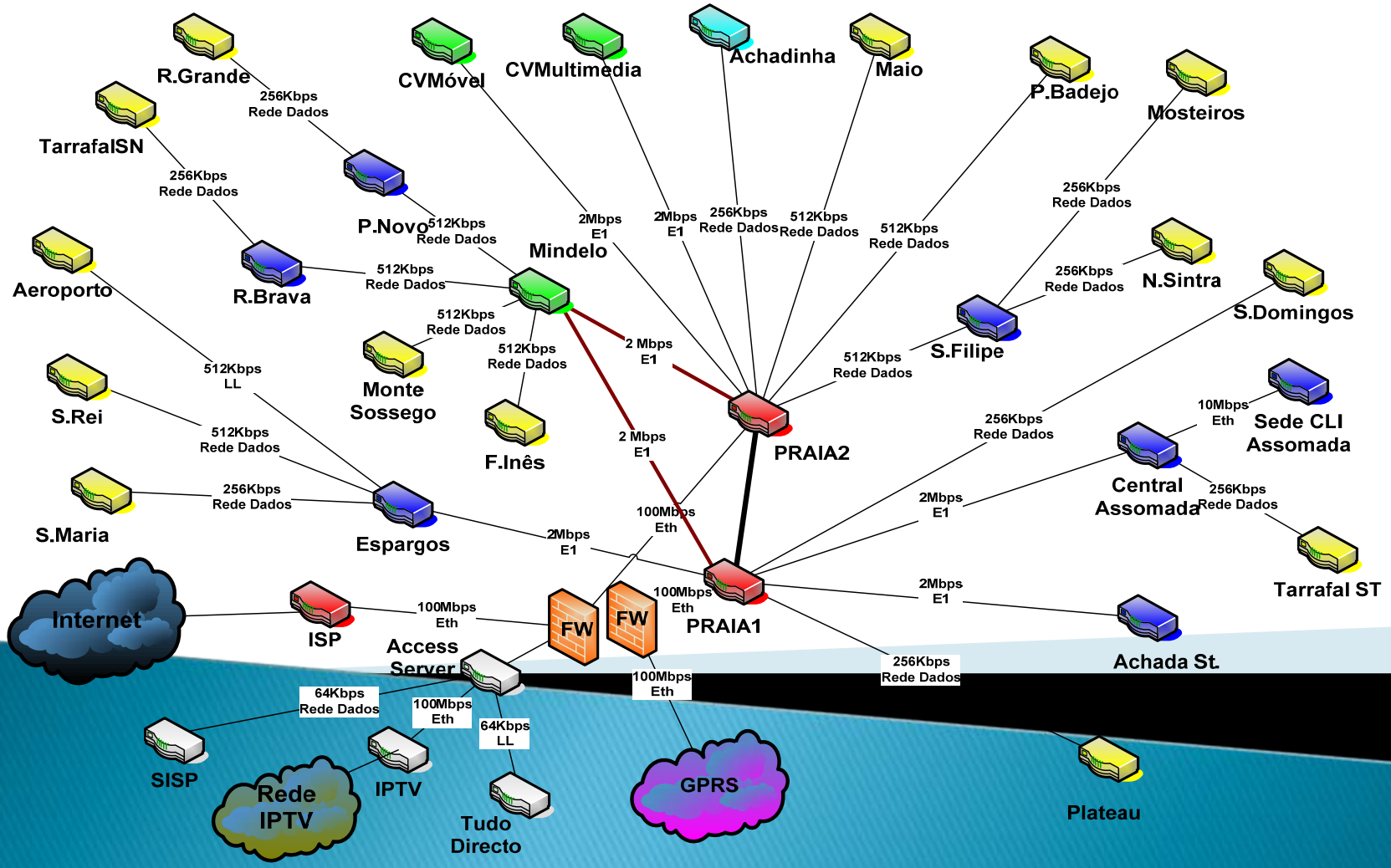
- A Política de segurança

  - As redes físicas LAN e WAN

Rede Informática LAN



Rede Informática WAN



- **Protecção de Infraestruturas Críticas**
  - A política de segurança
    - Detecção de intrusões (IDS)

Protecção de Infraestruturas Críticas

- A política de segurança

  - Acções de sensibilização dos colaboradores e parceiros

Plano de Disaster Recovery

Sumário

4. Pontos críticos e desafios

- **Organização interna orientada para a segurança.**
- **Actualização de "Know-How"** dos técnicos.
- Ferramentas apropriadas para **automação de tarefas de controlo.**

4. Pontos críticos e desafios

- **Actuação proactiva.**
- Existência de **Planos de contingência.**
- A nossa tradicional **cultura de confiança.**
- Existência de **parcerias** com Organizações e de contratos de Assistência.

Obrigado!
Merci!
Thank You!

almiro.rocha@cvt.cv