GTER 38 | GTS 24

SEGURANÇA de REDES com SOFTWARE LIVRE

GTER 38 | GTS 24

Segurança de Redes com Software Livre

Osmany Dantas R. de Arruda

GSI – MBA²

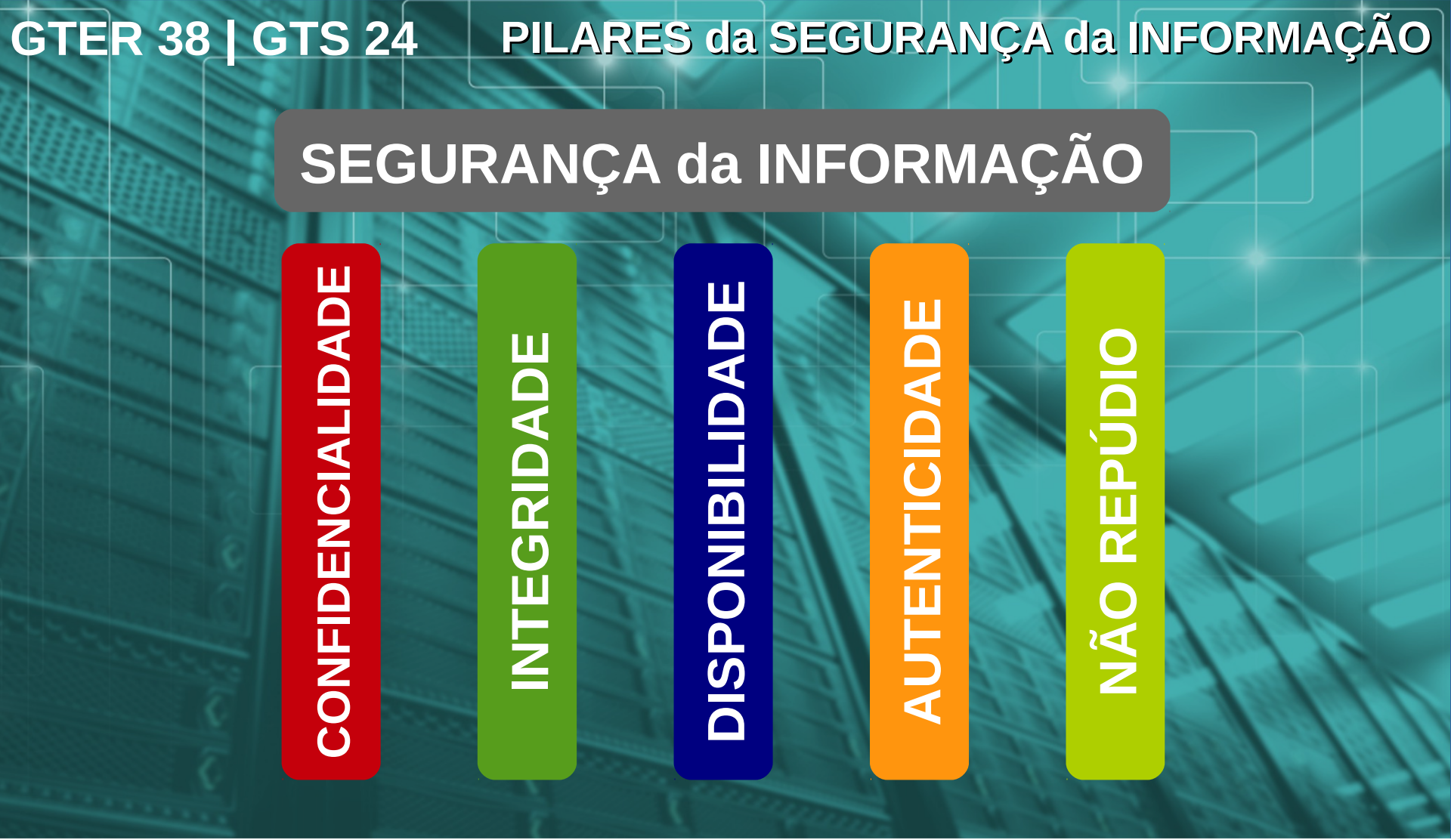
Objetivo

- Apresentar algumas das soluções em **FOSS** (FREE and OPEN SOURCE SOFTWARE) implementadas com sucesso em case **REAL**

Agenda

- ✓ Os **Pilares** da Segurança da informação e de Redes
- ✓ Principais **ameaças**
- ✓ Os **Princípios** básicos da segurança
- ✓ Case real baseado em soluções **FOSS**

PILARES da SEGURANÇA da INFORMAÇÃO



DEFINIÇÃO de SEGURANÇA em REDES

Resumidamente, a **CISCO** coloca que:

“ ... **segurança** de **redes** refere-se a qualquer atividade destinada a proteção da rede, mais especificamente, a **usabilidade**, **confiabilidade**, **integridade** da rede e dados. “

Ainda segundo a **CISCO**, as ameaças mais comuns à **segurança** de **redes** são:

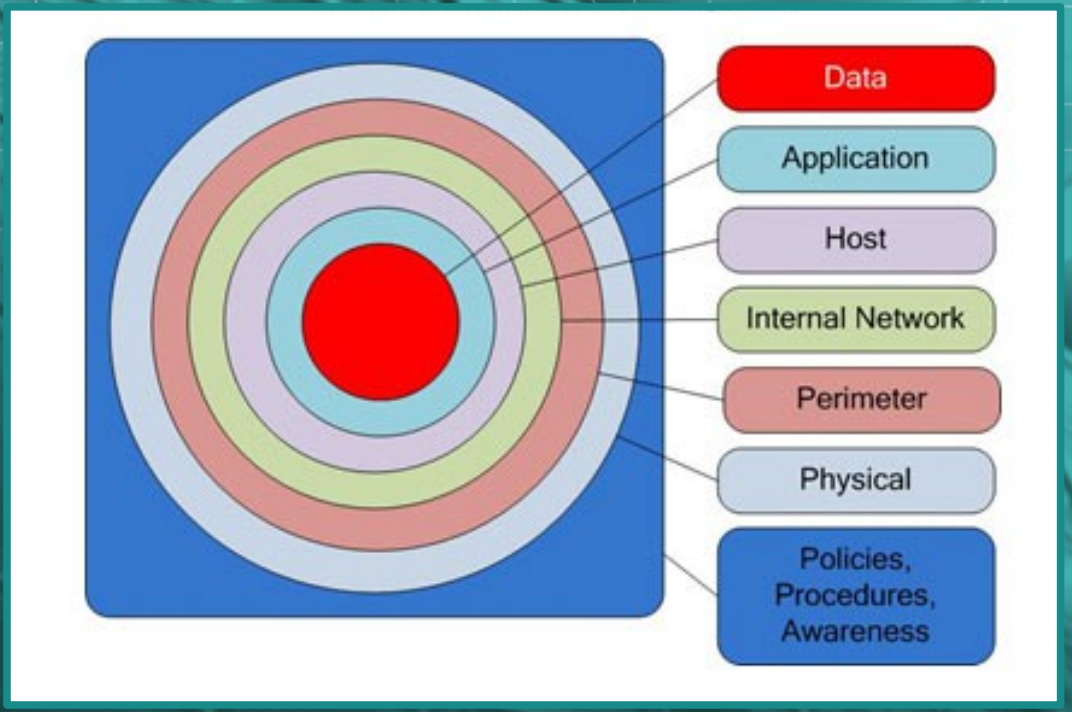
- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day (zero-hour) attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

MECANISMOS para PROTEÇÃO

Alguns dos mecanismos mais comumente empregados à **segurança** de **redes** são:

- Anti-virus and anti-spyware
- Firewall (UTM)
- IPS/IDS
- VPNs

DEFESA em PROFUNDIDADE



DEFESA em DIVERSIDADE

CUIDADO

Vulnerabilidades inerente
Configurações padrão
Skin-deep differences
Herança comum

A SIMPLICIDADE

& SMART !!

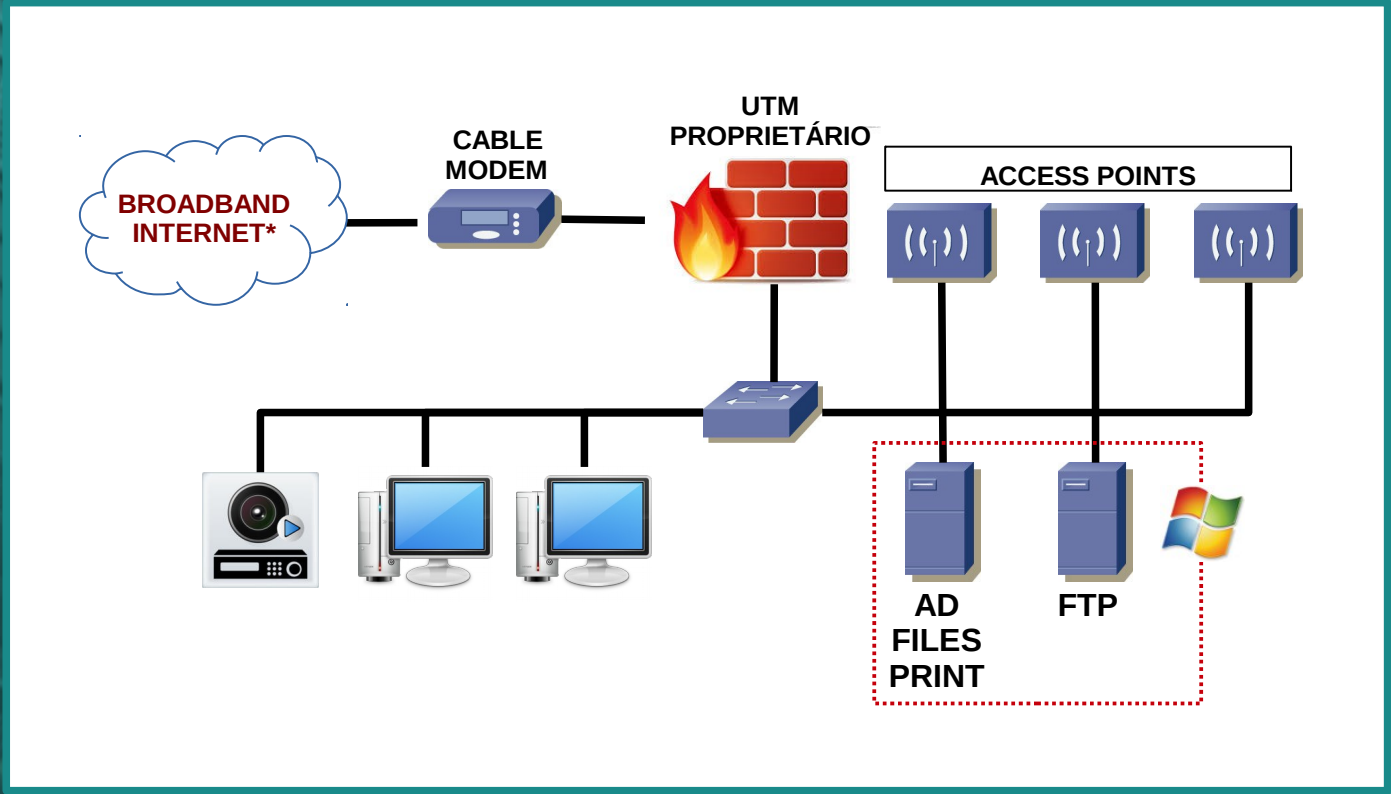
O PONTO de EQUILÍBRIO

Trade OFF

GTER 38 | GTS 24

SEGURANÇA de REDES com SOFTWARE LIVRE

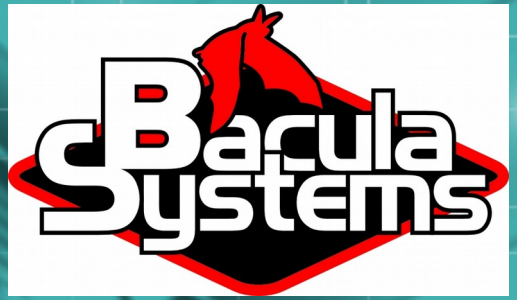
ESTUDO de CASO – INICIAL



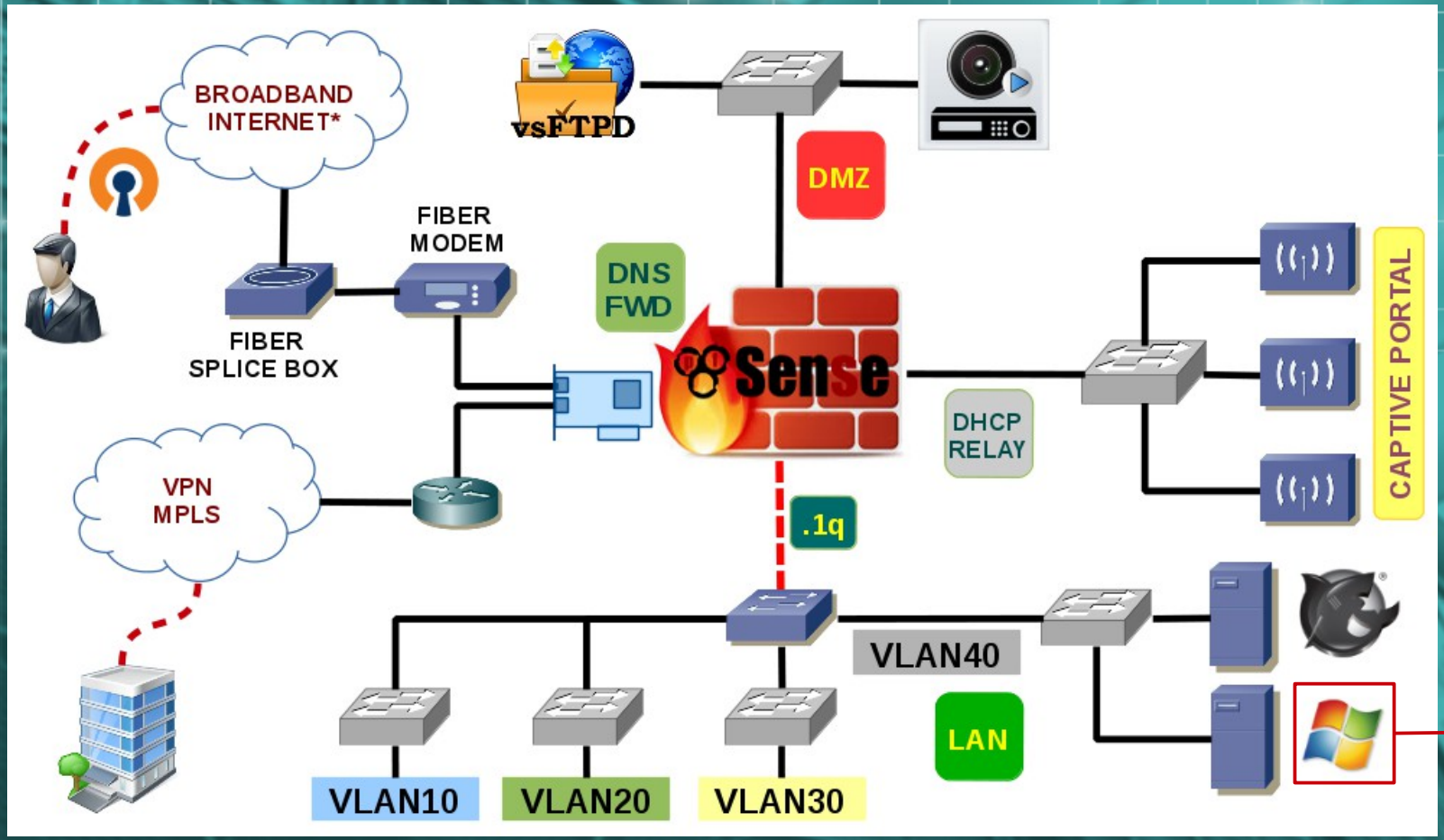
PREMISSAS BÁSICAS do CENÁRIO

- Substituição do atual UTM
- Segregação do serviço de compartilhamento de arquivos (NAS)
- Redução do domínio de broadcast
- Ajustes no serviço FTP e de BACKUP
- Acesso remoto ao sistema câmeras de monitoramento
- Acesso remoto seguro às aplicações
- Autenticação e controle de acesso à rede wireless

PRINCIPAIS SOLUÇÕES ADOTADAS



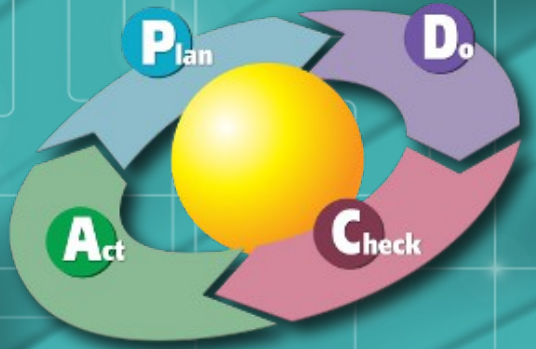
ESTUDO de CASO - FINAL



Concluindo:

- Soluções em **FOSS** podem ser tão confiáveis e robustas quanto soluções proprietárias
- Muitas soluções **proprietárias** baseiam-se em **FOSS**

Concluindo:



- Acima de tudo, a **segurança** de **redes** / da **informação**, requer **planejamento** adequado, sendo um processo de melhoria **contínua**

Obrigado

Fatec
São Caetano do Sul

opensecurity

osmany.arruda@opensecurity.com.br