# IMPLEMENTAÇÃO DE FIREWALL NEXT GENERATION PARA OS CAMPI DOS INTERIORES DA UFPA

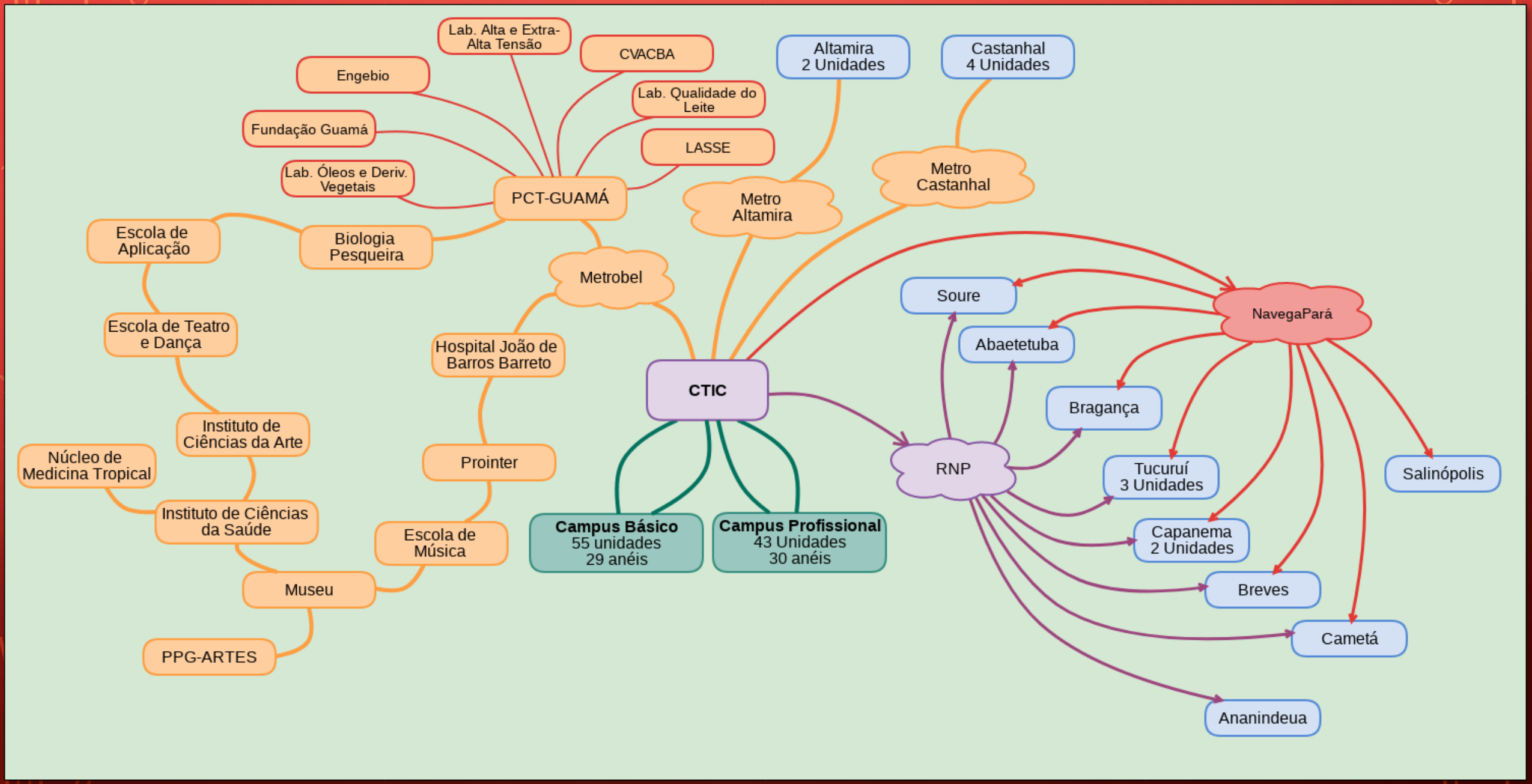
ANALISTA: JOÃO SALVATTI

UNIVERSIDADE FEDERAL DO PARÁ - UFPA

CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – CTIC

COORDENADORIA DE REDES

# TOPOLOGIA DOS CAMPI DOS INTERIORES



# PRINCIPAIS PROBLEMAS

- Os principais problemas detectados nas redes dos campi dos interiores são:
  - MAU USO DA REDE DE DADOS:
    - Torrents;
    - YouTube;
    - Jogos On-Line;
    - Redes Sociais;
    - Sites indevidos (pornografia | pedofilia | compartilhamentos de mídia com direitos autorais);
  - REGISTRO DE ACESSOS:
    - Não havia nenhum log de acesso dos usuários;
    - Implicações legais;

# IMPLEMENTAÇÃO DE FIREWALL

- FIREWALL OPENSOURCE:
  - Firewalls Tradicionais:
    - Camada 3 – REDE (IP);
    - Camada 4 – TRANSPORTE (TCP);
    - Implementações de Terceiros (patches) para camada 7 (Aplicação) – **USO NÃO RECOMENDADO**
  - OPÇÕES:
    - Linux/NetFilter (IPTables);
    - OpenBSD/Packet Filter (PF);
  - CONCLUSÕES:
    - Nenhuma dessas soluções nos atenderiam perfeitamente.

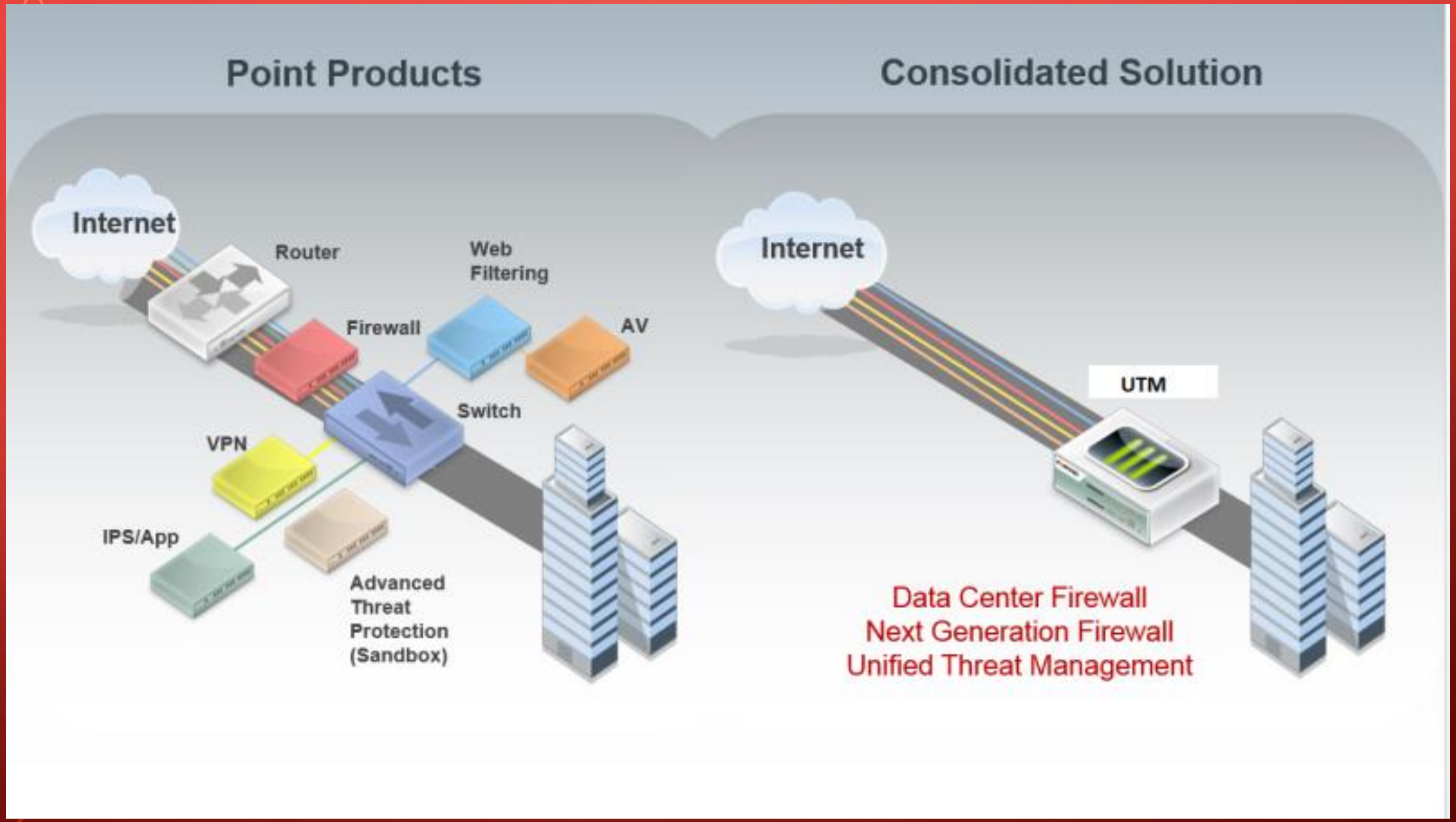
# IMPLEMENTAÇÃO DE FIREWALL

- FIREWALL CORPORATIVO (ENTERPRISE):
  - Diversos Fabricantes:
    - FortiNet;
    - CheckPoint;
    - Palo-Alto;
    - Cisco;
    - SonicWall;
  - Solução Escolhida:
    - **FortiGate-300D**
  - Motivos:
    - Líder no Quadrante Mágico Gartner em UTM (Centro Unificado de Ameaças);
    - Menor Custo Benefício;
    - Treinamento;

# IMPLEMENTAÇÃO DE FIREWALL

# FORTIGATE-300D

# O QUE É UTM?

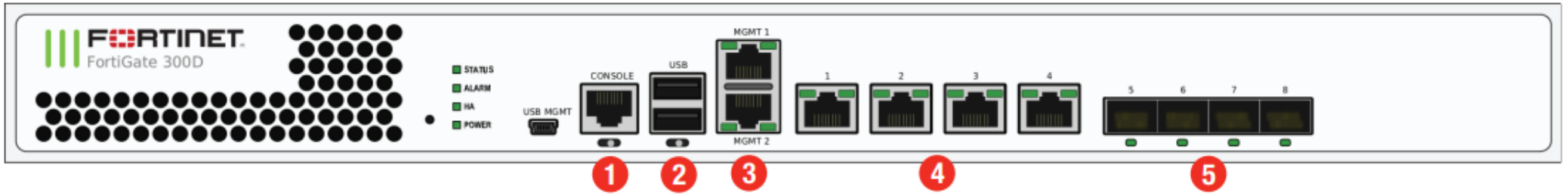

Point Products
Internet
Router
Web Filtering
Firewall
AV
Switch
VPN
IPS/App
Advanced Threat Protection (Sandbox)
Consolidated Solution
Internet
UTM
Data Center Firewall
Next Generation Firewall
Unified Threat Management

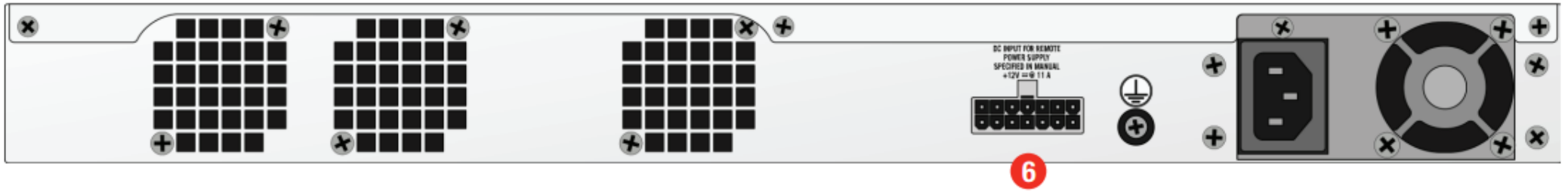
# FUNCIONALIDADES DO FG-300D

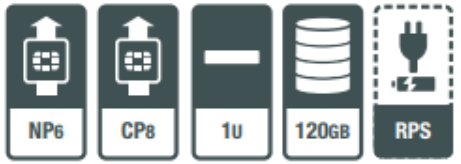
- Firewall Next Generation (Firewall Próxima Geração):
  - Firewall:
    - Camada de Rede (IP);
    - Camada de Transporte (TCP);
    - **Camada de Aplicação (HTTP / HTTPS / TORRENT / STREAMING ...);**
    - IDS/IPS;
    - Antivírus;
    - Mail Gateway;
    - **LOGS DE ACESSO;**

# CARACTERÍSTICAS DO EQUIPAMENTO

## FortiGate 300D



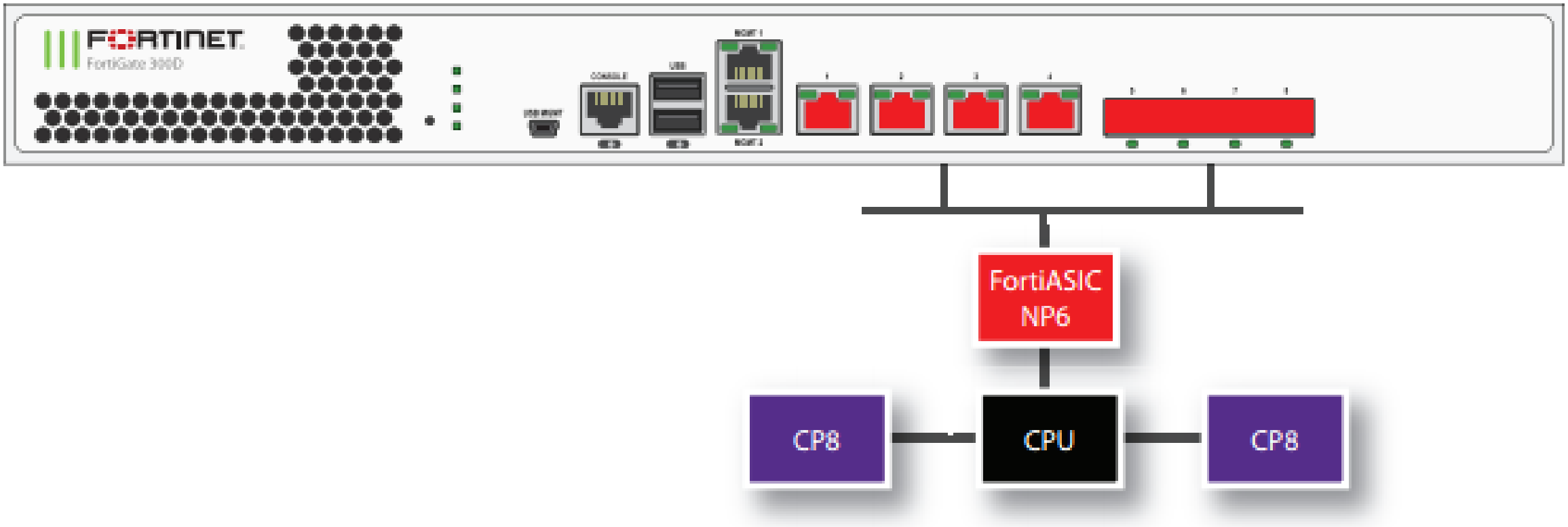




## Interfaces

1. Console Port (RJ45)
2. 2x USB Ports
3. 2x GE RJ45 Management Ports
4. 4x GE RJ45 Ports
5. 4x GE SFP Slots
6. FRPS Connector

# CARACTERÍSTICAS DO EQUIPAMENTO

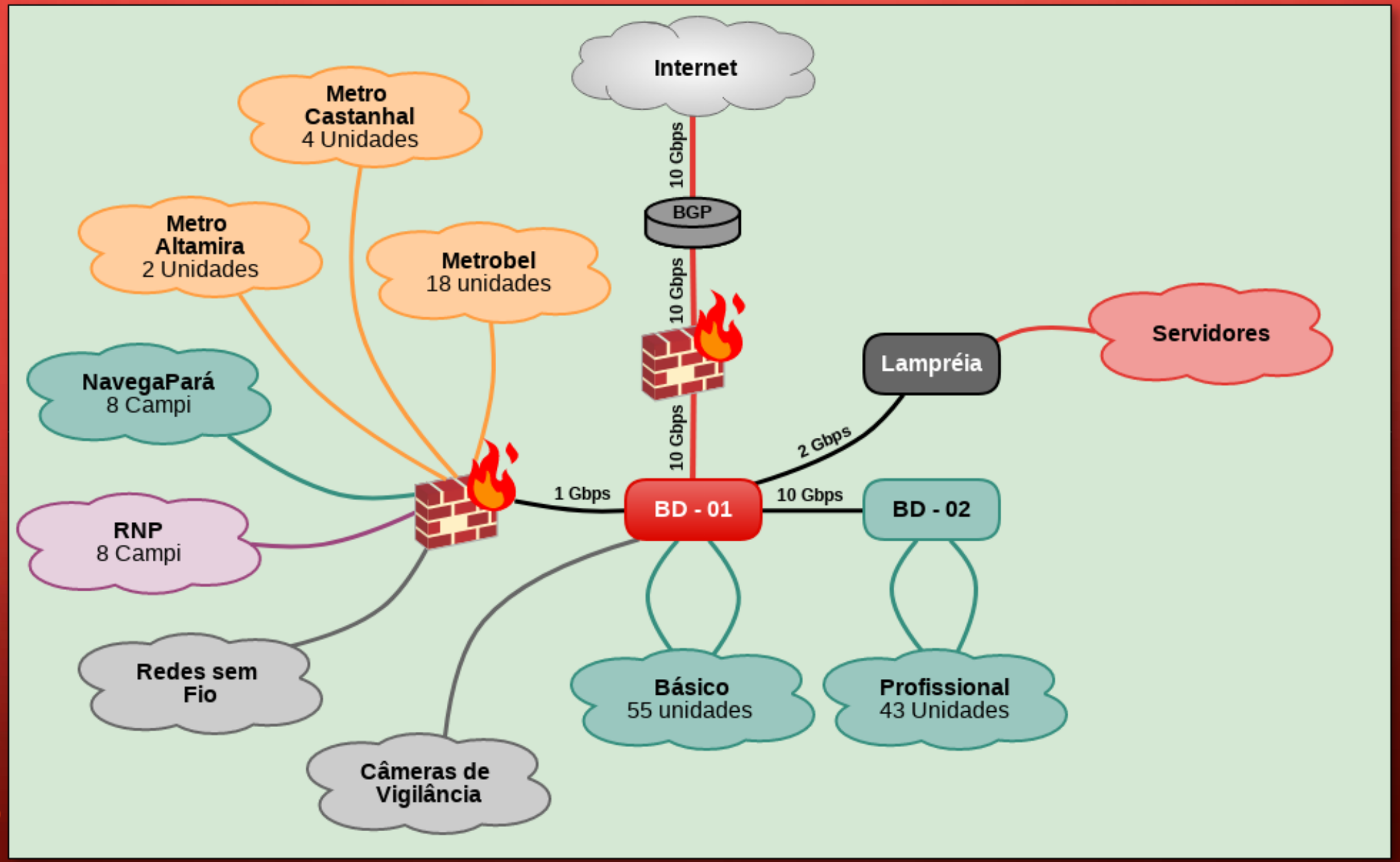


# CARACTERÍSTICAS DO EQUIPAMENTO

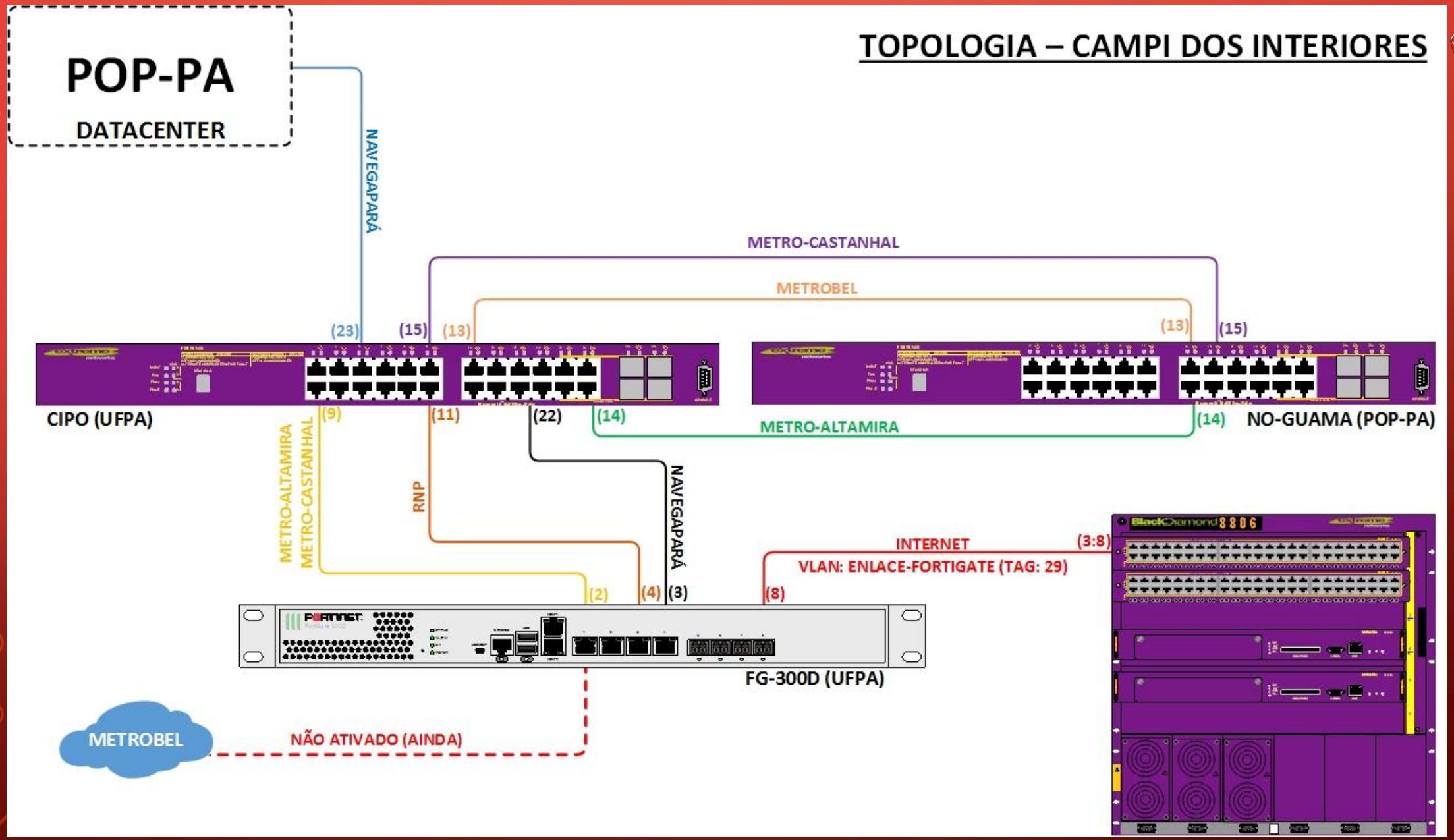
```
FW-CAMPI-UFPA # diagnose npu np6 port-list
Chip   XAUI Ports             Max   Cross-chip
                              Speed offloading
------ ---- -------           ----- ----------
np6_0  0
       1    port1             1G    Yes
       1    port2             1G    Yes
       1    port3             1G    Yes
       1    port4             1G    Yes
       1    port5             1G    Yes
       1    port6             1G    Yes
       1    port7             1G    Yes
       1    port8             1G    Yes
       2
       3
------ ---- -------           ----- ----------

FW-CAMPI-UFPA #
```

# NOVA TOPOLOGIA DOS CAMPI DOS INTERIORES



# NOVA TOPOLOGIA DOS CAMPI DOS INTERIORES



# ENLACES E PORTAS


METROBEL

REDE METRO-ALT1 (VLAN: 3051)
REDE METRO-LAT2 (VLAN: 3052)
---
REDE METRO-CAS1 (VLAN: 3053)
REDE METRO-CAS2 (VLAN: 3054)
REDE METRO-CAS3 (VLAN: 3055)
REDE METRO-CAS4 (VLAN: 3056)

CP-NVP-ABAETETUBA (VLAN: 200)
CP-NVP-BRAGANÇA (VLAN: 2020)
CP-NVP-BREVES (VLAN: 2039)
CP-NVP-CAMETÁ (VLAN: 2040)
CP-NVP-CAPANEMA1 (VLAN: 2032)
CP-NVP-CAPANEMA2 (VLAN: 2033)
CP-NVP-SALINÓPOLIS (VLAN: 2028)
CP-NVP-SOURE (VLAN: 2036)
CP-NVP-TUCURUÍ (VLAN: 2004)

UP-LINK INTERNET — BD-01

REDE SEM FIO VISITANTES (VLAN: 11)

REDE SEM FIO INSTITUCIONAL VLAN:13)

CP-RNP-CAMPI (VLAN: 3001)

# REGISTRO DOS LOGS DE ACESSO

- **GRAYLOG (https://www.graylog.org/)**
  - Solução de log remoto;
  - Arquiva;
  - Pesquisa;
  - Possui um linguagem de pesquisa de alto nível;
  - Trabalha com índices;
  - Fácil configuração;
  - Market Place:
    - **Extratores para diversos fabricantes (FortiNet / Palo Alto / Cisco, etc);**

# PROBLEMAS DE PERFORMANCE DO SERVIDOR

- Graylog é em Java (consome muita memória e processamento);
- Rodando em VM (VMWare ESXi);
- Sistema Operacional CentOS 64 bits;
- Setup Inicial 8G de RAM (Falhou);
- Segundo Setup 12G de RAM (falhou);
- Setup Atual 16G de RAM (Funcionando);

# PROBLEMA NA IDENTIFICAÇÃO DOS USUÁRIOS

- A UFPA não possui controlador de domínio para todos os usuários;
- Os LOGs gerados não identificam os usuários, apenas o IP das estações;
- Alguma localidades usam DHCP sem controle por MAC;
- **Extremante difícil atribuir responsabilidades sem um registro por login;**
- Recebemos frequentemente solicitações judicias para localização de acessos indevidos (diversos motivos);
- SOLUÇÃO:
  - Implementar a atutenticação de todos os usuários da rede da UFPA;
  - Rede WIFI VISITANTE (crítico – administração superior já solicitou uma solução para o problema);
  - Parque tecnológico muito heterogêneo;
  - Resistência por parte dos usuários;

# PROBLEMA DE ARQUIVAMENTO DOS LOGS

- Atualmente são feitas 900-1200 entradas de logs/s;
- São armazenados 23G de logs/dia;
- Sem período de retenção (diretoria solicitou);
- Em média de 460G de log/mês;
- Como Armazenar?
  - Backup?
  - Compactação?
  - Tape?

# APRESENTAÇÃO DAS SOLUÇÕES

# OBRIGADO