

# Funcionalidade para *logoff* da autenticação do *Firewall* da Palo Alto na UFPI

Filipe S. Viana, Ênio R. Viana, Diego F. M. Oliveira

Superintendência de Tecnologia da Informação – STI  
Universidade Federal do Piauí (UFPI)

# *Firewall Next Generation*

- Detectar e bloquear ataques sofisticados:
  - Camada de aplicação (camada 7 modelo OSI);
  - Nível de protocolo, IP e porta ( camadas 3 e 4);
- 3 Recursos chaves:
  - Capacidade de *firewall* corporativo;
  - Sistema de prevenção de intrusão (IPS);
  - Controle de aplicação;

# *Firewall Next Generation*

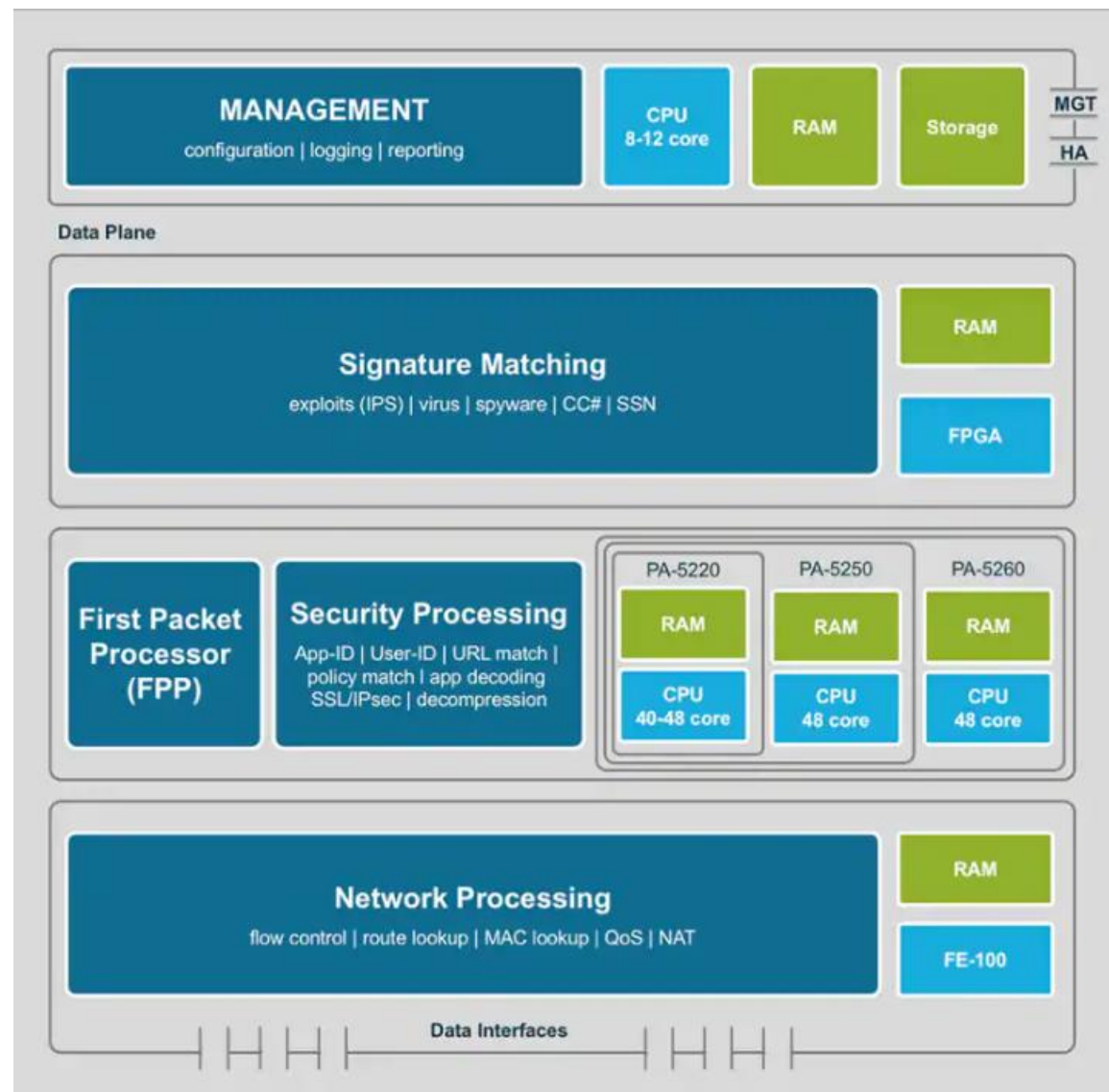
- Capacidade dos *firewalls* tradicionais;
- Funcionalidades adicionais:
  - Prevenção de intrusão (IPS);
  - Inspeção profunda (*deep inspection*);
  - Detecção de *malware* e URLs baseada em reputação;

# Palo Alto – PA-5220



## PA-5220

- **17/20 Gbps** Taxa de transferência do firewall
- **8/9 Gbps** Taxa de transferência de prevenção e ameaças
- **8 Gbps** Taxa de transferência IPsec VPN
- **4,000,000** max sessions
- **150,000** new sessions per second
- **20** roteadores virtuais
- **10/20** Sistemas virtuais (base/max)



# Motivação

- Marco Civil / [LEI Nº 12.965, DE 23 DE ABRIL DE 2014.](#)
- **Art. 13.** Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

# Autenticação na Rede

- Não possuímos *Active Directory*;
- Autenticação via *Captive Portal*;
- Sessão com IP e nome do usuário;



The image shows a captive portal login interface. At the top left is the UFPI (Universidade Federal do Piauí) crest. To its right, the text 'Acesse com seu login SIG-UFPI' is displayed. Below this, there are two input fields: the first is labeled 'Usuário:' and the second is labeled 'Senha:'. A blue 'Login' button is positioned below the password field. At the bottom right, there is a link that says 'Esqueceu a senha?' next to a small blue question mark icon.

# Problema

- *Captive Portal* não disponibiliza função para desconectar da sessão.
- Computador público continua com a sessão (8h)
- *Log* não confiável, acesso não confiável

# Solução

UNIVERSIDADE  
FEDERAL DO PIAUÍ

API

[Commit](#)  
[Configuration Commands](#)  
[Export](#)  
[Import](#)  
[Logs](#)  
[Operational Commands](#)  
[Reports](#)  
[User ID](#)



# Solução - API Palo Alto

[API](#) > [Operational Commands](#) > [clear](#) > [user-cache](#) > [ip](#)

## XML

```
<clear><user-cache><ip></ip></user-cache></clear>
```

Submit

## Rest API Url

</api/?type=op&cmd=<clear><user-cache><ip></ip></user-cache></clear>>

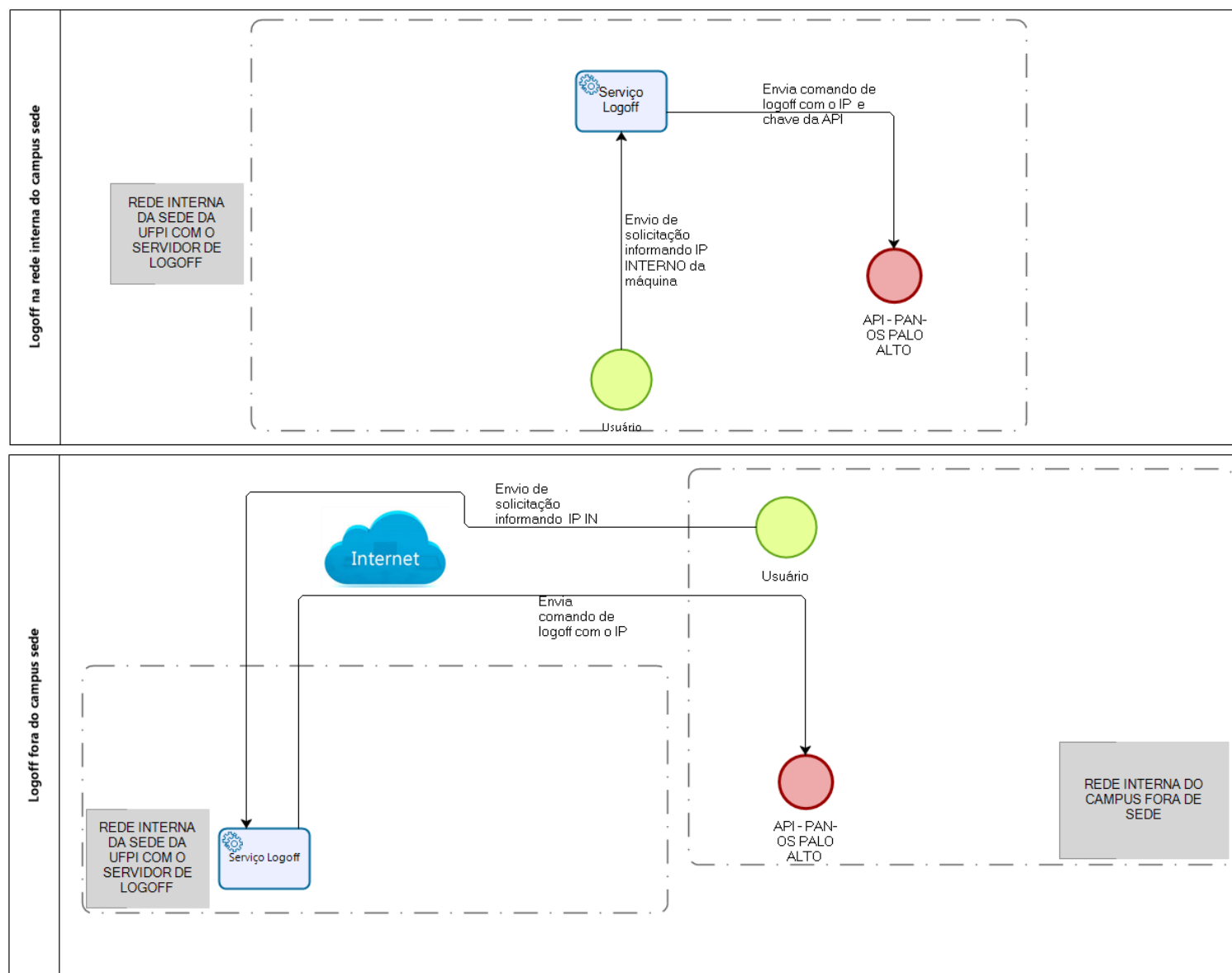
# Solução - API Palo Alto

- API PaloAlto
  - Management Plane(MP)
    - `https://hostname/api/?type=op&key=key&vsys=vsys1&cmd=<clear><user-cache-mp><ip>ipnumber</ip></user-cache-mp></clear>`
  - Data Plane(DP)
    - `https://hostname/api/?type=op&key=key&vsys=vsys1&cmd=<clear><user-cache-mp><ip>ipnumber</ip></user-cache-mp></clear>`

# Solução - API Palo Alto

- API PaloAlto
  - Necessário API key
  - Utilização de usuário com acesso limitado
  - Utilizar IP interno para desconexão

# Solução



# Resultado

- Possibilidade de desconexão;
- Maior confiabilidade
- Proteção ao usuário
- Sem mudança no desempenho do *firewall*
- Possibilidade de aplicar outro projeto que limitou a quantidade de sessões por usuário

# Conclusão

- Necessidade de conhecimentos de programação mesmo na área de infraestrutura;
- Conhecer as ferramentas com as quais trabalhamos.

OBRIGADO!

Contato:

[filipe@ufpi.edu.br](mailto:filipe@ufpi.edu.br)

STI

SUPERINTENDÊNCIA DE TECNOLOGIA  
DA INFORMAÇÃO

