Firewalls de próxima geração (NGFW) Funcionalidades, aplicações e vulnerabilidades

Tiago W.Morais, Nicolas N.Faria, Silvio E. Quincozes, Diego Kreutz, Juliano F. Kazienko, Vagner E.Quincozes
E Mário C. Peixoto

LEA
Laboratório de Estudos Avançados em Computação

DEFESA CIBERNÉTICA Since 2022 DC

Como proteger redes e sistemas contra ameaças avançadas e emergentes?

Motivação

- **Aumentar a segurança cibernética com o uso de ferramentas robustas e modernas**

Principais problema(s)

- **31,5 Bilhões de tentativas de ataques no primeiro semestre de 2022 (Brasil)**
- **20% do capital global movimentado na internet é perdido (fraudes, roubos e cancelamentos)**

Desafio(s)

- Manter as redes e sistemas protegidos
- Escolher e implementar o NGFW adequado
- Avaliar a eficiência desses dispositivos

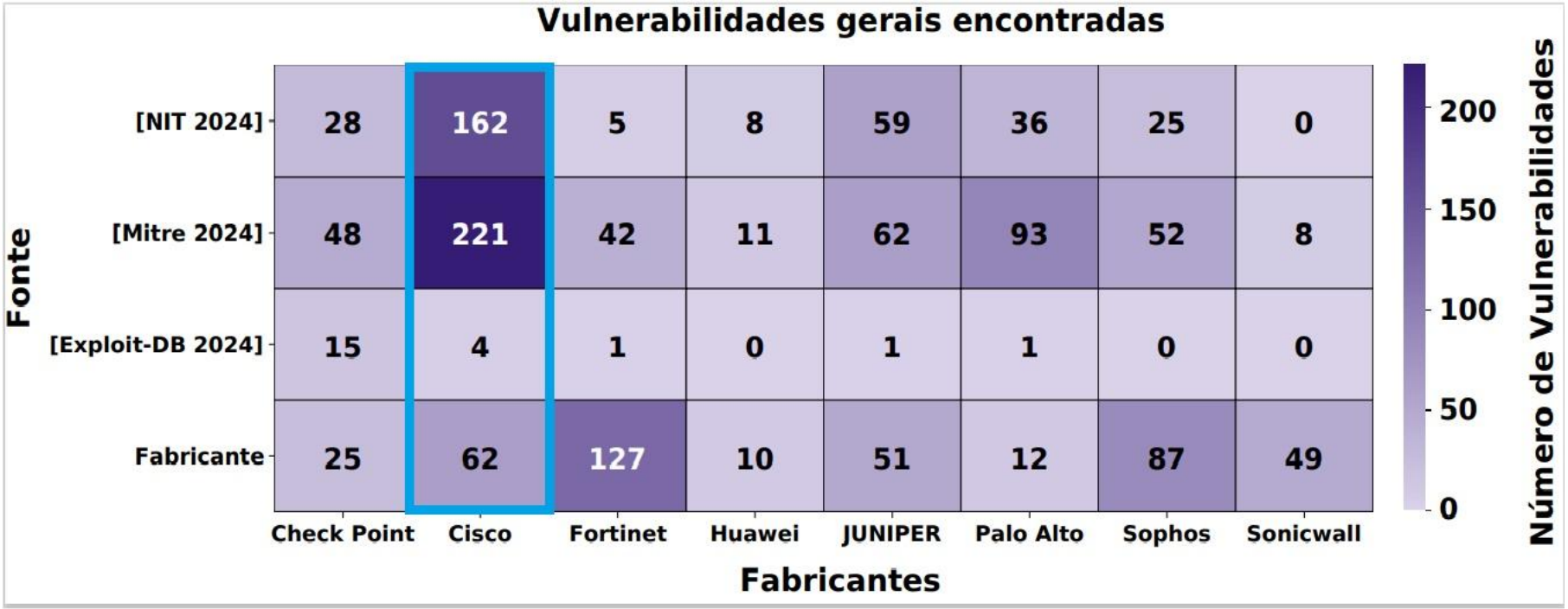
NGFW

- Proteção da camada 2 até 7 OSI
- Inspeção profunda de pacotes
- Proteção contra Malwares e Zero Days
- IPS e IDS
- Proteção Web e IoT

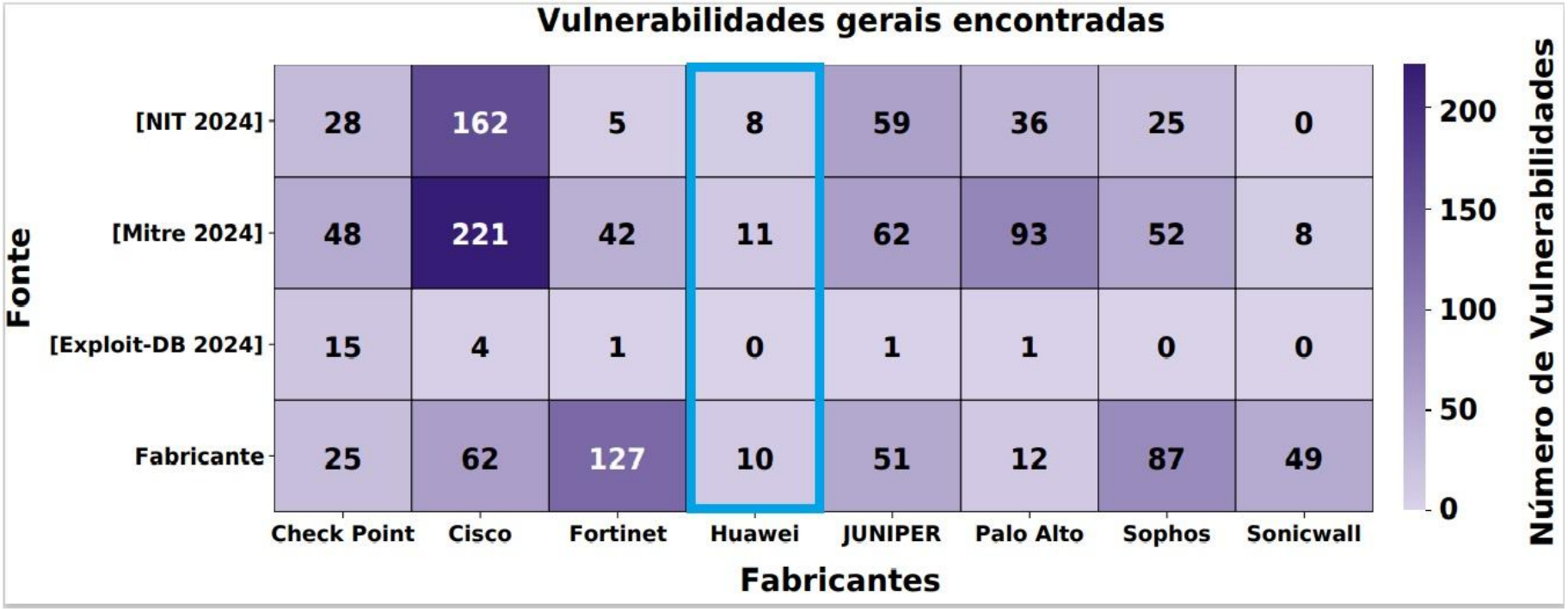
NGFWs e Market Share (6Sense)

CISCO	Firepower 9300 SM-56 X3	20,3%
Fortinet	FortiGate FG 7121F	15,9%
Palo Alto	Palo Alto PA-7500	11,0%
Sonicwall	Supermassive 9800	0,3%
Sophos	Sophos XGS 8500	0,2%
Check-Point	Quantum Force 29200	0,1%
Juniper	Juniper SRX 5800	0,1%
Huawei	Huawei USG 12008	0,03%

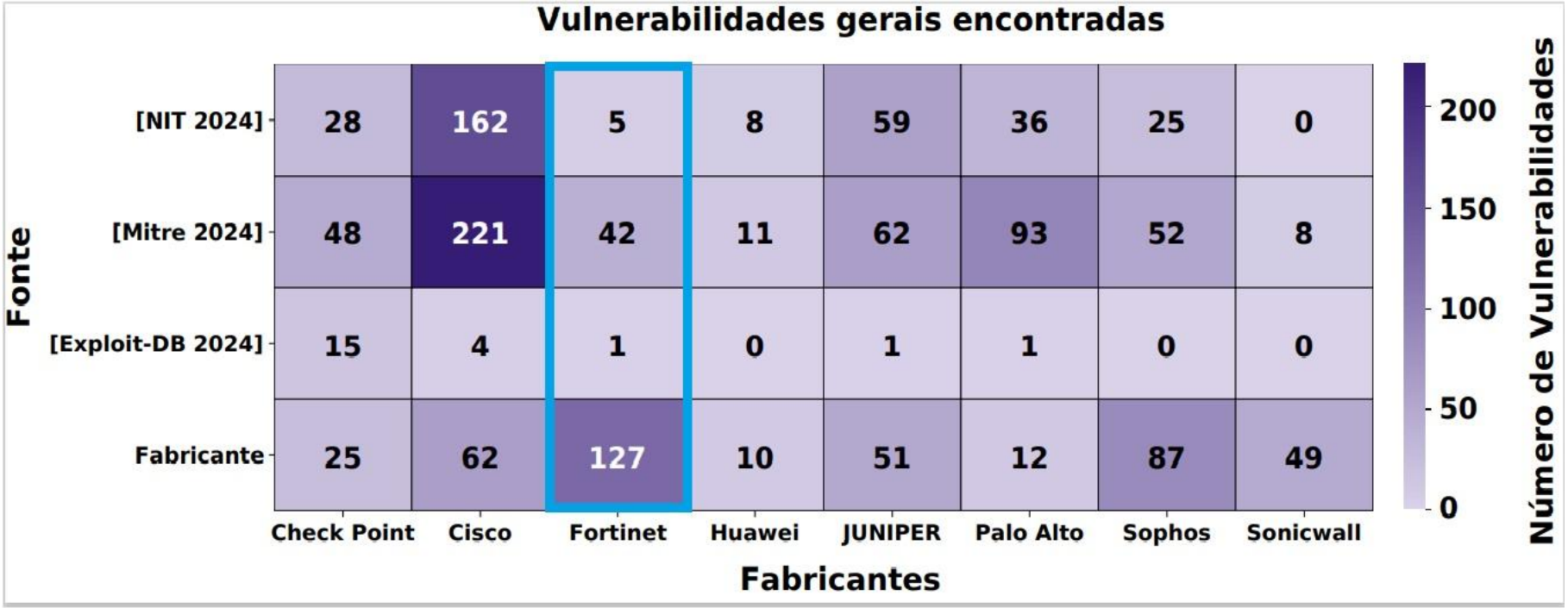
Mais vulnerabilidades conhecidas



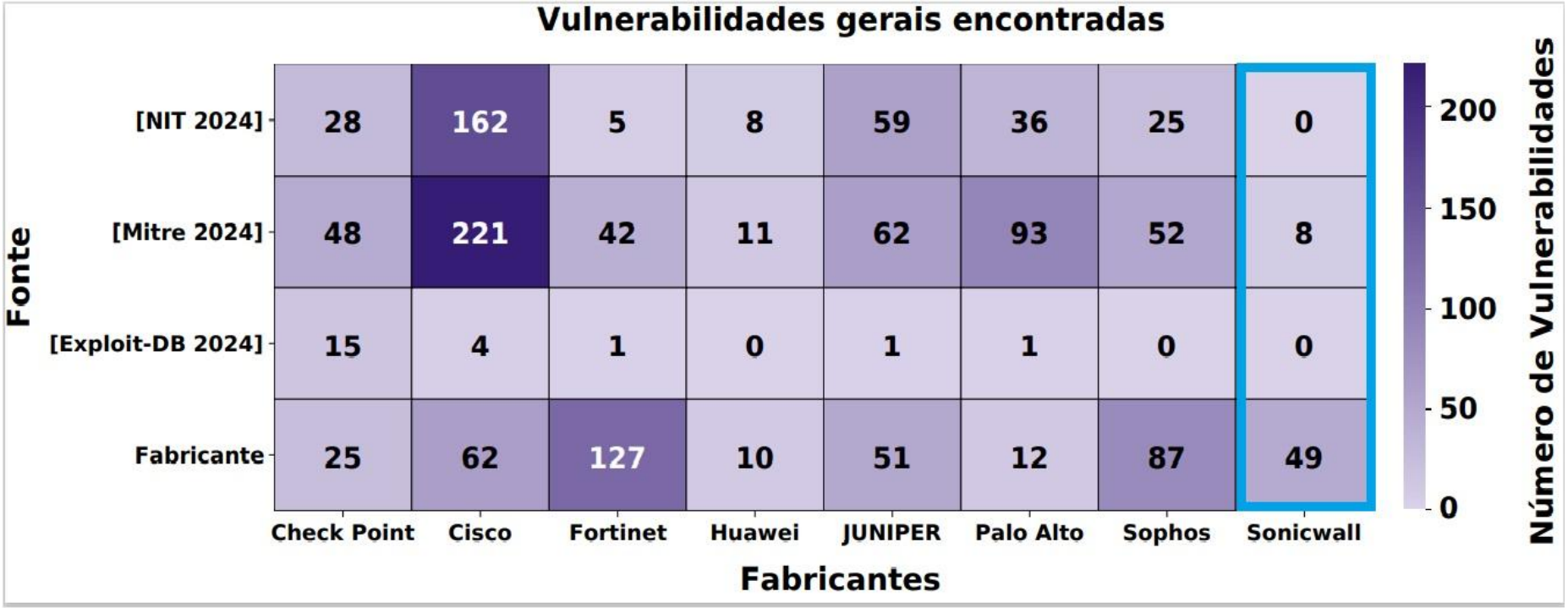
Menos vulnerabilidades conhecidas



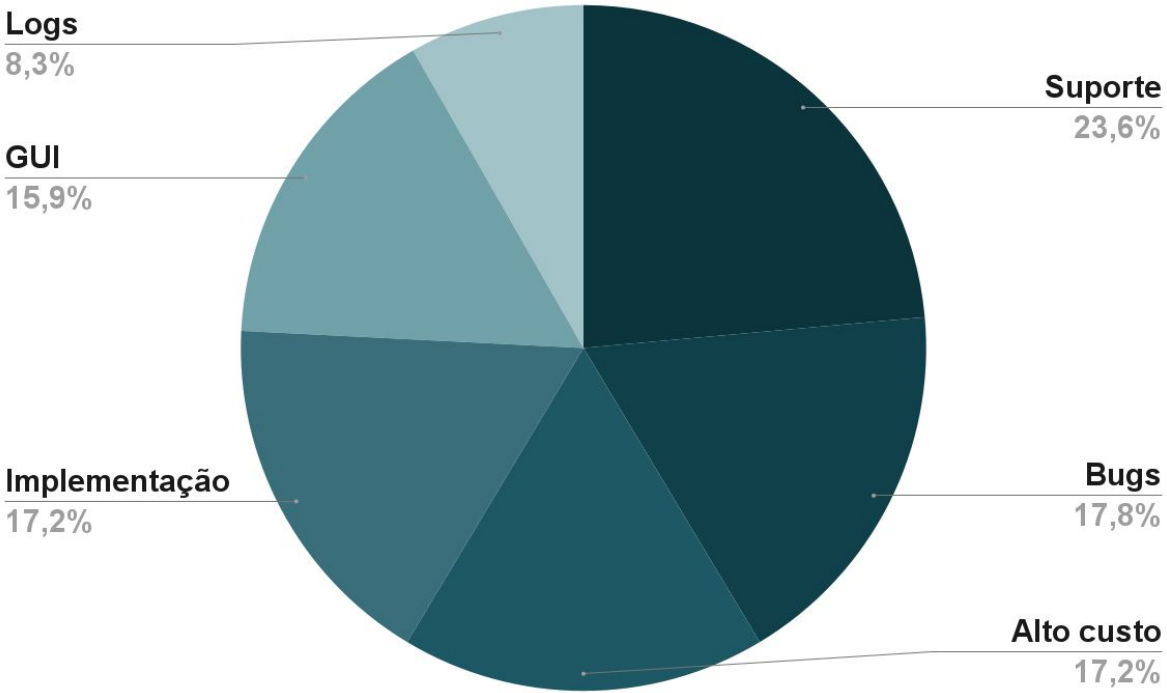
Mais vulnerabilidades (fabricante)



Menos vulnerabilidades (outros)



Dificuldades encontradas (NGFW)



Features em comum nos NGFWs

- ML ou AI
- DPI
- IPS/IDS
- Anti Malwares e Zero Day
- Proteção a serviços Web
- Configuração centralizada

Maior *throughput* em DPI

	IOT	4G/5G	SANDBOX	LEAKEAGE	DPI GB	FIREWALL
CHECK-PONT	●		●	●	63,5	500
CISCO			●		28	235
FORTINET	●	●	●	●	540	550
HUAWEI		●			307	2,4T
JUNIPER		●	●		504	3,3T
PALO ALTO		●	●		1,5T	1,4T
SOPHOS	●			●	34	190
SONICWALL	●	●	●	●	23	31,8

Maiores *throughputs* em Firewall

	IOT	4G/5G	SANDBOX	LEAKEAGE	DPI GB	FIREWALL
CHECK-PONT	●		●	●	63,5	500
CISCO			●		28	235
FORTINET	●	●	●	●	540	550
HUAWEI		●			307	2,4T
JUNIPER		●	●		504	3,3T
PALO ALTO		●	●		1,5T	1,4T
SOPHOS	●			●	34	190
SONICWALL	●	●	●	●	23	31,8

NGFWs mais completos(features)

	IOT	4G/5G	SANDBOX	LEAKEAGE	DPI GB	FIREWALL
CHECK-PONT	•		•	•	63,5	500
CISCO			•		28	235
FORTINET	•	•	•	•	540	550
HUAWEI		•			307	2,4T
JUNIPER		•	•		504	3,3T
PALO ALTO		•	•		1,5T	1,4T
SOPHOS	•			•	34	190
SONICWALL	•	•	•	•	23	31,8

Conclusão

- NGFWs podem garantir uma maior proteção
- Market share pode indicar melhores produtos
- Vulnerabilidades podem diminuir a proteção
- Opiniões de clientes podem trazer insights
- ML e AI podem trazer mais eficiência
- Contribuições desta pesquisa

Trabalhos futuros

- Comparativo entre Mercado e literatura
- Mapear as features mais importantes
- Apresentar o Top 10 features
- Concluir e publicar o Survey

Obrigado!

Tiago W.Morais