Exploração do Controlador Eucalyptus: Através do Ataque DDoS

Ronierison de Souza Maciel
Orientador: Paulo Romero Martins Maciel

rsm4@cin.ufpe.br
http://www.cin.ufpe.br/~rsm4

Universidade Federal de Pernambuco - UFPE
Centro de Informática - CIn

Agenda

1. Introdução
    a. Contextualização
    b. Motivação
    c. Arquitetura geral
    d. Objetivos
2. Cenários
    a. Cenários de ataque DDoS
    b. Mapa de ataques
    c. Trabalhos relacionados
3. Modelos propostos
    a. Modelos
4. Próximas etapas
    a. Em desenvolviment

MoDCS Research Group

Cloud Security

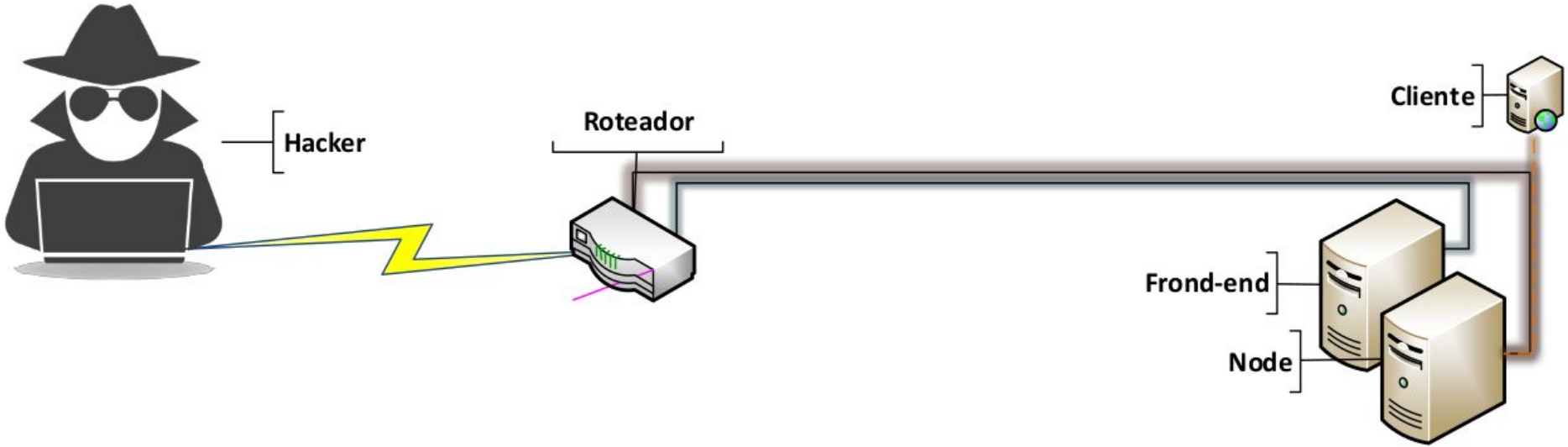
O que é?

É um conjunto de **procedimentos**, **processos** e **normas** **NBR ISO/IEC 27017** destinadas a fornecer uma **garantia de segurança da informação em um ambiente de computação em nuvem**. Esses serviços são prestados (modelo público, privado ou híbrido).

Motivação

Recorrentes e **massivos** ataques de negação de serviços (DDoS) a infraestruturas de nuvem. “O responsável pede 5 bitcoins (cerca de R$ 11 mil) para cessar os ataques se o dinheiro não for pago, o “resgate” aumenta em 5 bitcoins por dia de ataque. O **DDoS** contra os serviços é bastante poderoso, com taxas ultrapassando **1 terabit** por segundo” **tecnoblog**

Arquitetura geral de um sistema Cloud Computing



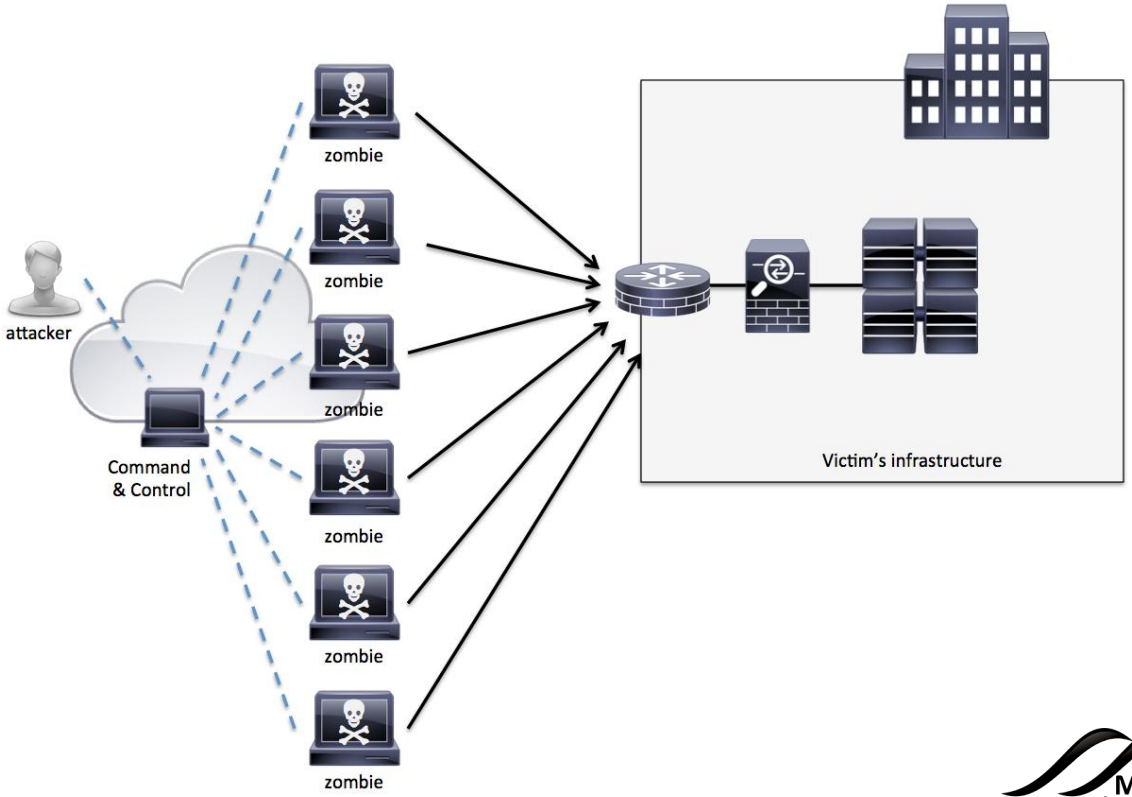
Objetivo geral

O propósito desta pesquisa é **apresentar uma solução composta de modelos analíticos para avaliação de disponibilidade e/ou desempenho** para avaliar a entrega de um serviço na **Cloud** mediante um ataque **DoS** ou **DDoS**. Este estudo deve aprovar a identificação de pontos de falha/melhoria em diferentes níveis do sistema em estudo.

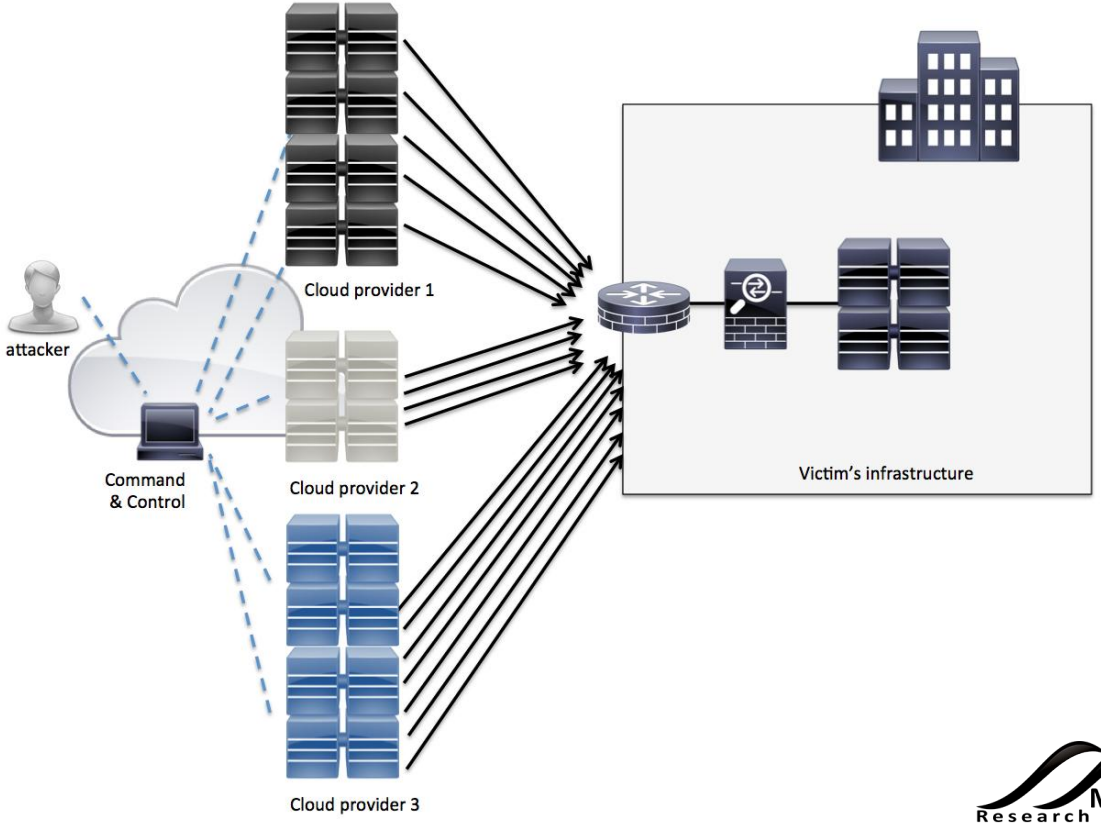
Objetivo específicos

- Propor uma **metodologia de avaliação de disponibilidade** no controlador da plataforma Eucalyptus;
- Sugerir e **analisar uma infraestrutura de Cloud privada** perante um **ataque DDoS** ou **DoS**;
- Apresentar modelos de dependabilidade para sistemas de Cloud privada, considerando falhas e reparos de **hardware** e **software** por intervenção de um **ataque de negação de serviço DoS**.

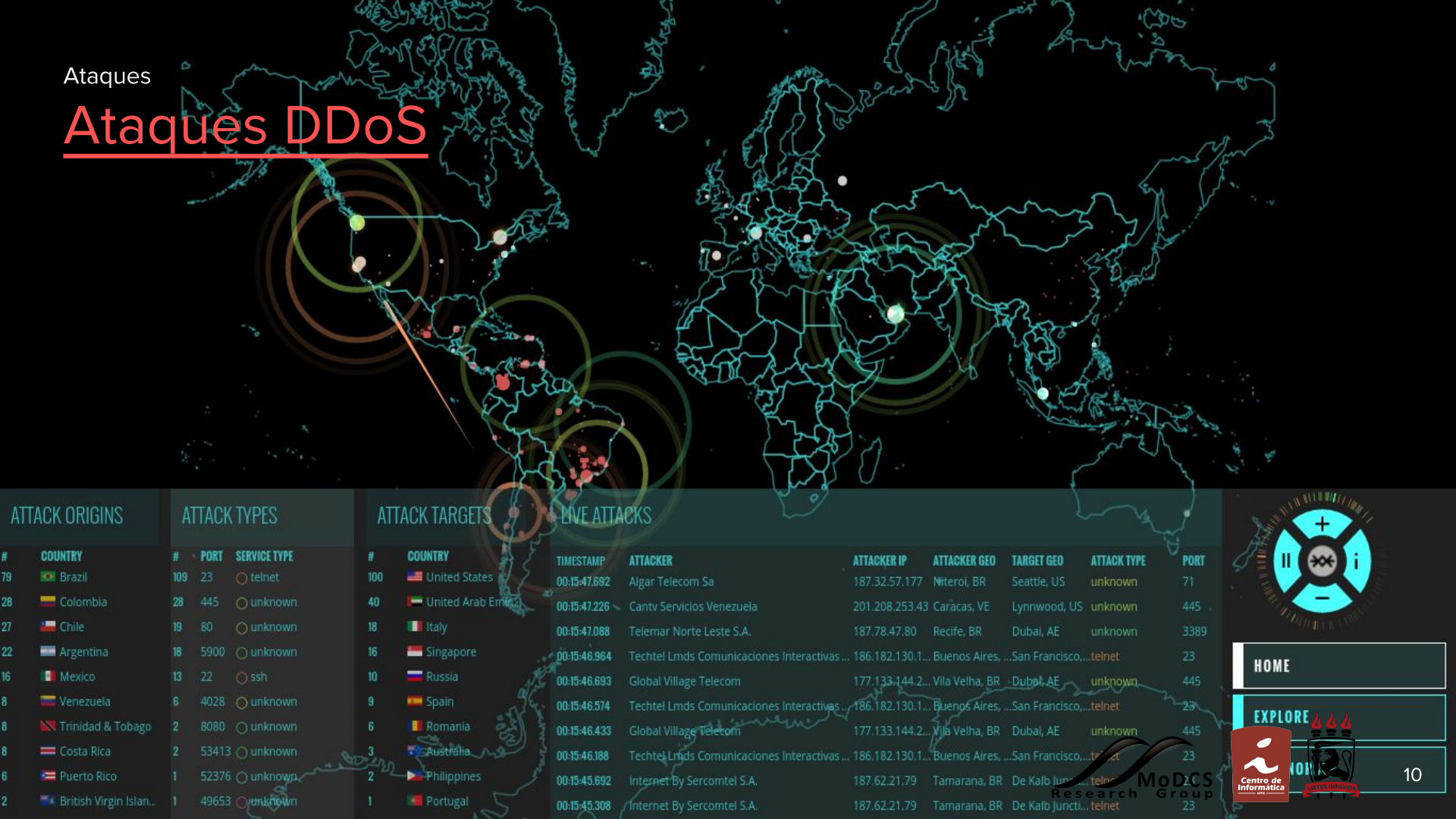
Cenário de ataque DDoS {botnets}



Cenário de ataque DDoS {botnets}



Ataques DDoS



ATTACK ORIGINS

#	COUNTRY
79	Brazil
28	Colombia
27	Chile
22	Argentina
16	Mexico
8	Venezuela
8	Trinidad & Tobago
8	Costa Rica
6	Puerto Rico
2	British Virgin Islan..

ATTACK TYPES

#	PORT	SERVICE TYPE
109	23	telnet
28	445	unknown
19	80	unknown
18	5900	unknown
13	22	ssh
6	4028	unknown
2	8080	unknown
2	53413	unknown
1	52376	unknown
1	49653	unknown

ATTACK TARGETS

#	COUNTRY
100	United States
40	United Arab Emir...
18	Italy
16	Singapore
10	Russia
9	Spain
6	Romania
3	Australia
2	Philippines
1	Portugal

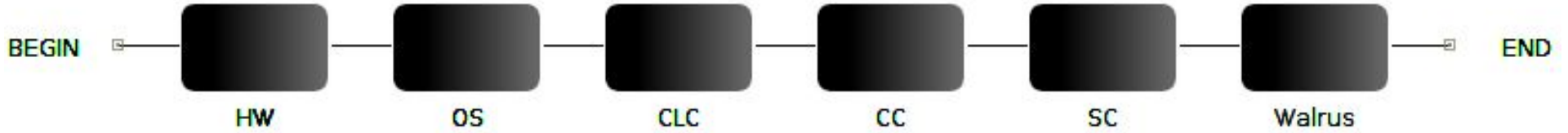
LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
00:15:47.692	Algar Telecom Sa	187.32.57.177	Niteroi, BR	Seattle, US	unknown	71
00:15:47.226	Cantv Servicios Venezuela	201.208.253.43	Caracas, VE	Lynnwood, US	unknown	445
00:15:47.088	Telemar Norte Leste S.A.	187.78.47.80	Recife, BR	Dubai, AE	unknown	3389
00:15:46.964	Techtel Lmds Comunicaciones Interactivas ...	186.182.130.1...	Buenos Aires, ...	San Francisco,...	telnet	23
00:15:46.693	Global Village Telecom	177.133.144.2...	Vila Velha, BR	Dubai, AE	unknown	445
00:15:46.574	Techtel Lmds Comunicaciones Interactivas ...	186.182.130.1...	Buenos Aires, ...	San Francisco,...	telnet	23
00:15:46.433	Global Village Telecom	177.133.144.2...	Vila Velha, BR	Dubai, AE	unknown	445
00:15:46.188	Techtel Lmds Comunicaciones Interactivas ...	186.182.130.1...	Buenos Aires, ...	San Francisco,...	telnet	23
00:15:45.692	Internet By Sercomtel S.A.	187.62.21.79	Tamarana, BR	De Kalb Juncti...	telnet	23
00:15:45.308	Internet By Sercomtel S.A.	187.62.21.79	Tamarana, BR	De Kalb Juncti...	telnet	23

HOME

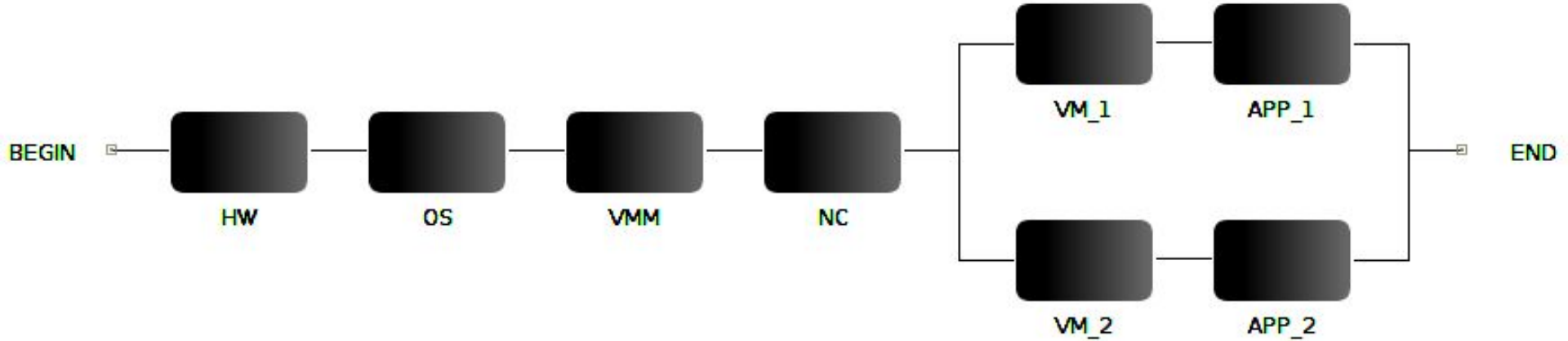
EXPLORE

Modelo RBD {Virtual Machine}

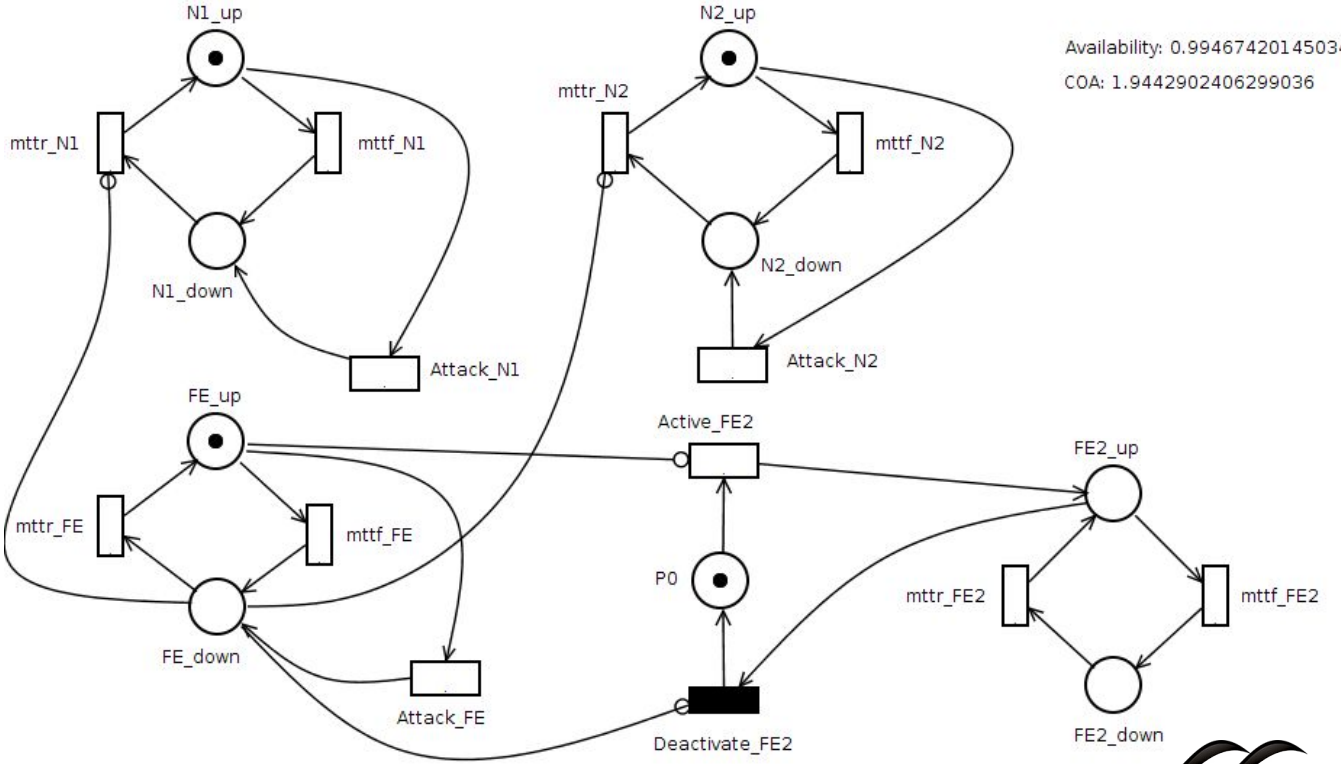


Componente	MTTF	MTTR
Hardware	8760h	100min
Sistema Operacional	2895h	15min
Controlador de Nuvem	788.4h	1h
Controlador de Cluster	788.4h...	1h...

Modelos RBD {Controller}



Modelo SPN

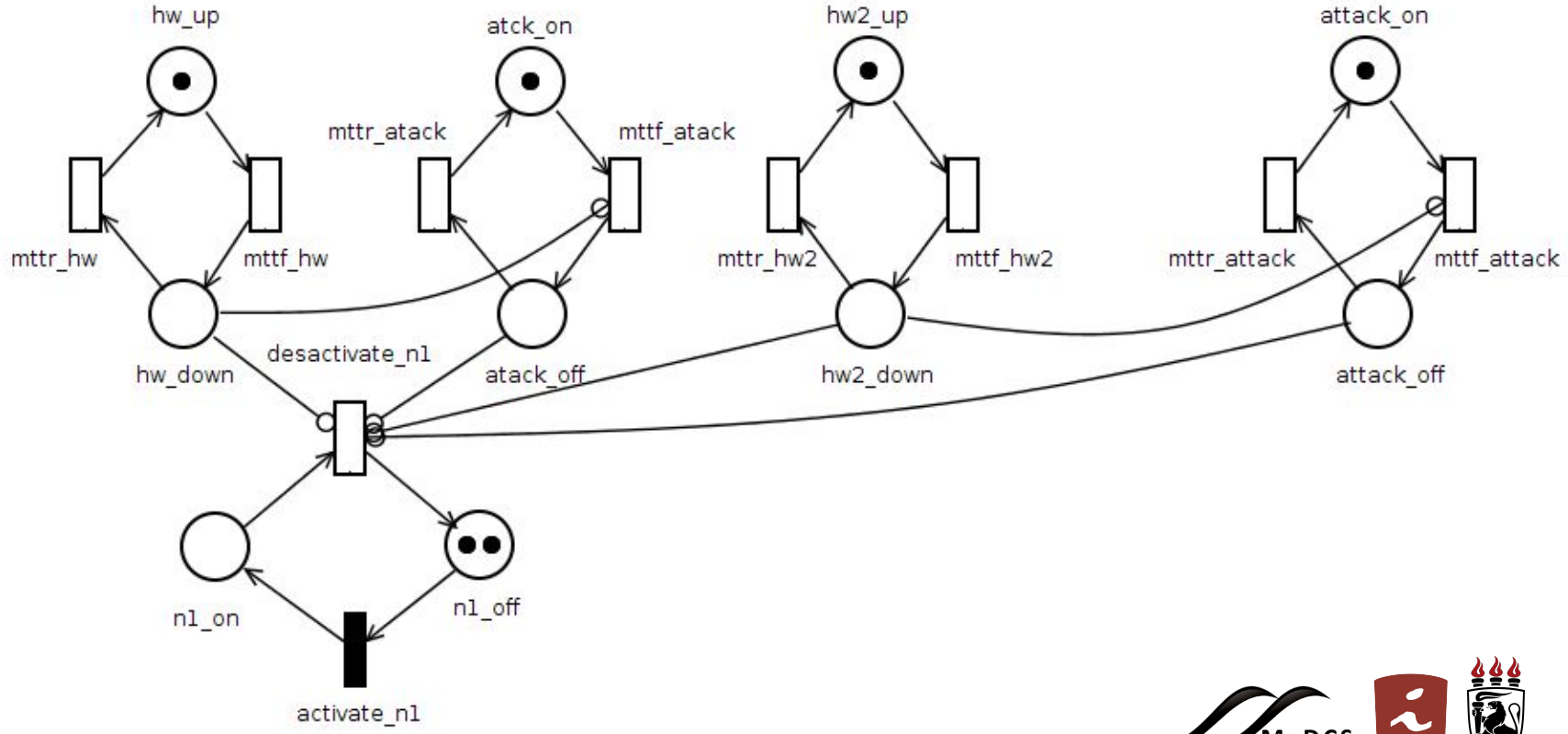

N1_up
mttr_N1
mttf_N1
N1_down
Attack_N1
N2_up
mttr_N2
mttf_N2
N2_down
Attack_N2
Availability: 0.9946742014503482
COA: 1.9442902406299036
FE_up
mttr_FE
mttf_FE
FE_down
Attack_FE
Active_FE2
P0
Deactivate_FE2
FE2_up
mttr_FE2
mttf_FE2
FE2_down

Trabalhos relacionados

	Cloud Security	Clou Computing	Modeling	Attack DDoS
Chang, et al., 2016	Yes	Yes	No	No
Hussain, et al., 2016	Yes	No	No	No
Somani, et al., 2015	Yes	Yes	No	Yes
Ahmad, et al., 2015	Yes	No	No	Yes
Matthew, 2015	Yes	No	No	Yes
Jing Li, 2015	Yes	Yes	No	No
Bakshi, et al., 2010	Yes	No	No	Yes
Krutz, et al., 2010	Yes	Yes	No	No
Mather, et al., 2009	Yes	Yes	No	Yes
This MSc. Project	Yes	Yes	Yes	Yes

Próximas etapas

Em desenvolvimento



Dúvidas?