Identificação de Endereços IP Dinâmicos com Dados Públicos

Gabriel Pains de Oliveira Cardoso Leonardo B. Oliveira Ítalo Cunha

UFMG
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO
Softex
SENAI
HACKERS DO BEM
RNP

O que são IPs dinâmicos?

> IPs que são associados à dispositivos diferentes esporadicamente

O que são IPs dinâmicos?

> IPs que são associados à dispositivos diferentes esporadicamente

vmware ESXi

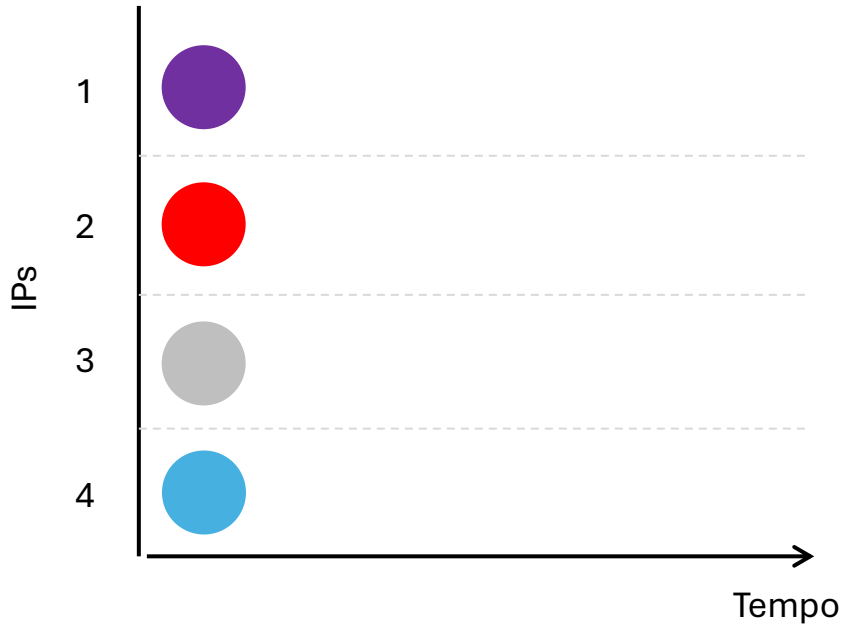
Microsoft Hyper-V

AHV

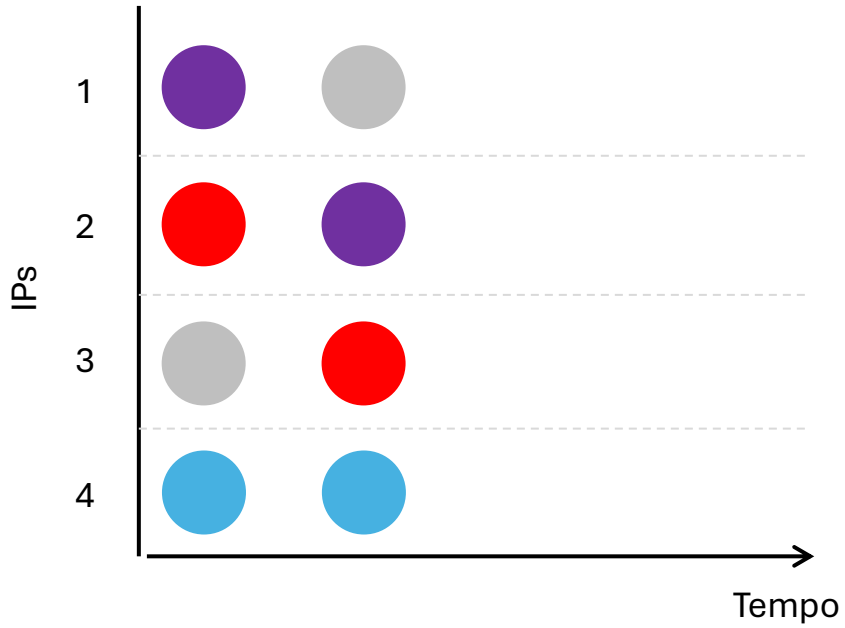
aws

Azure

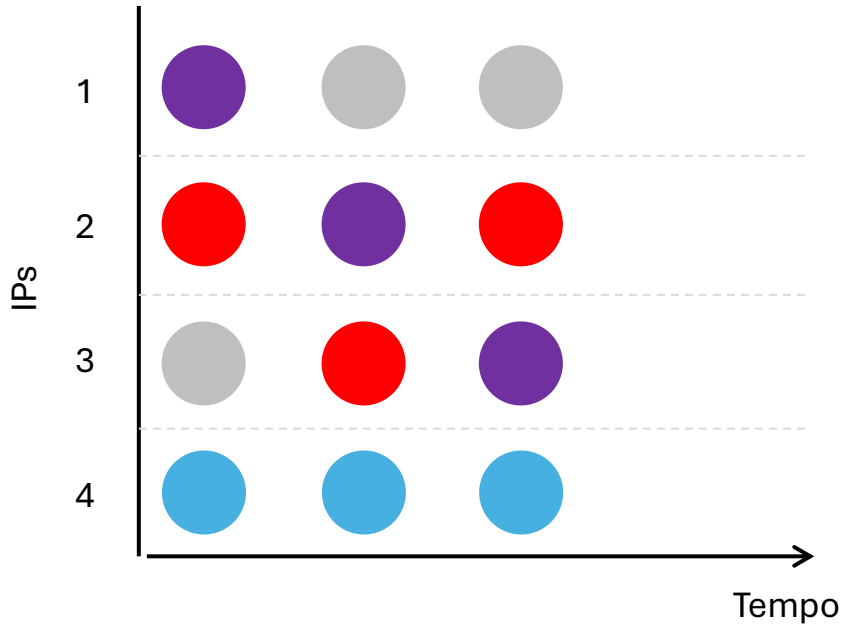
Comportamento de IPs dinâmicos



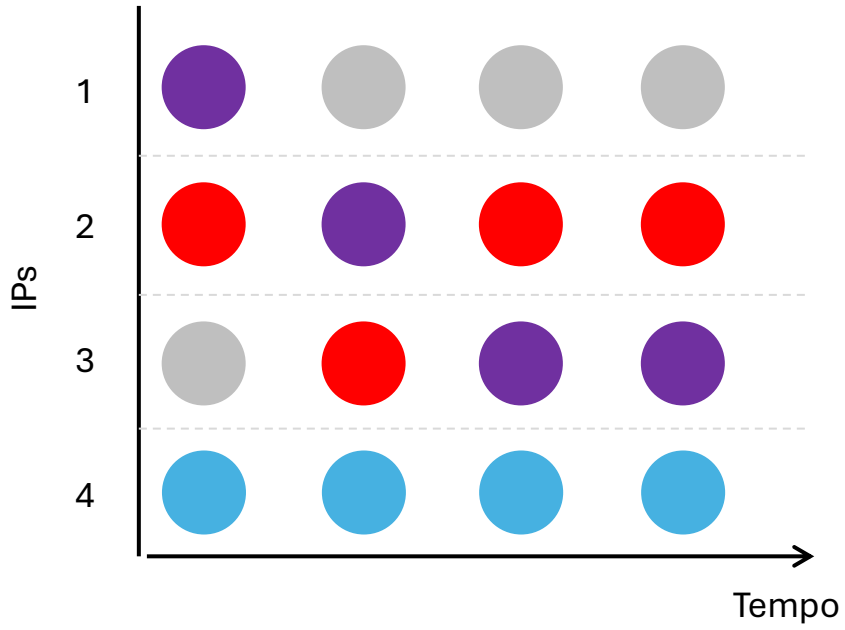
Comportamento de IPs dinâmicos



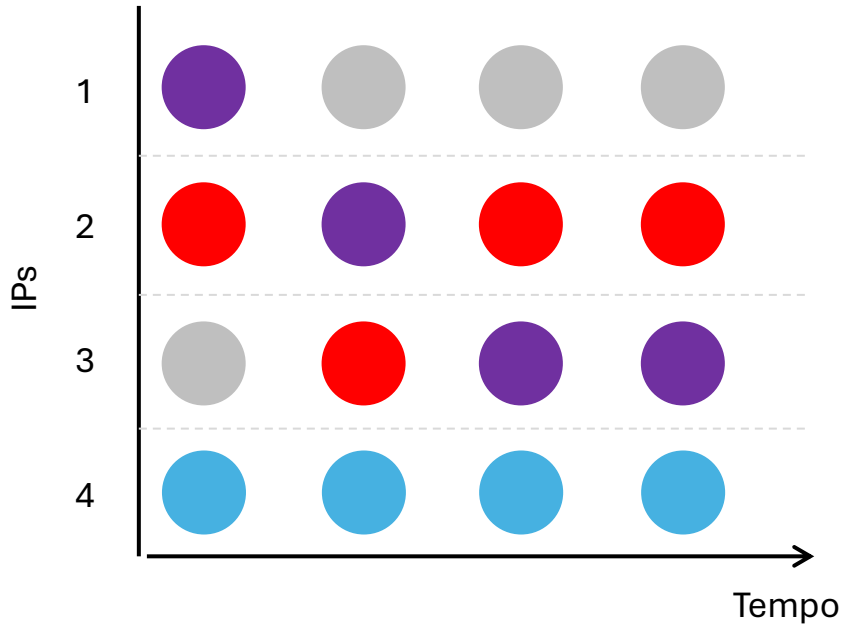
Comportamento de IPs dinâmicos



Comportamento de IPs dinâmicos



Comportamento de IPs dinâmicos

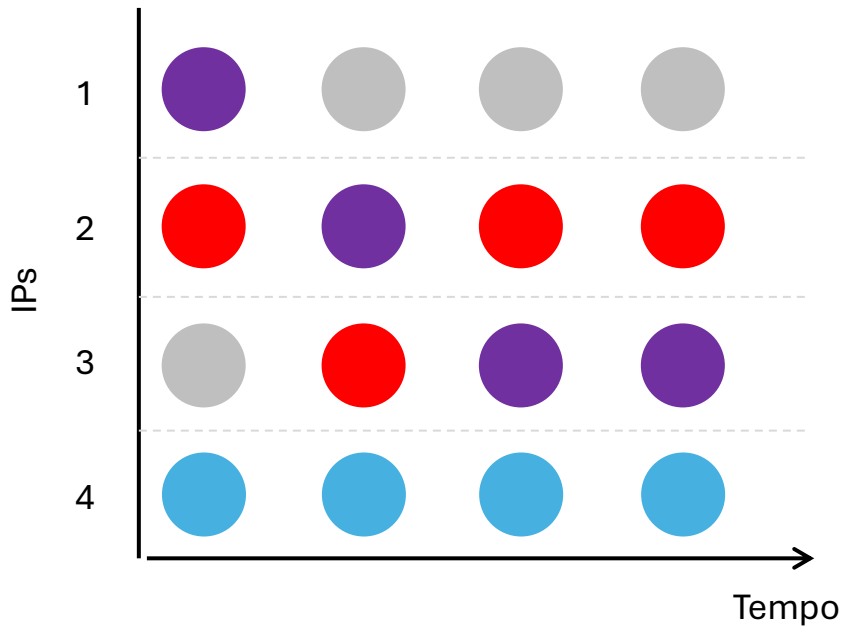


1 – 2 – 3 – 3

2 – 3 – 2 – 2

3 – 1 – 1 – 1

Comportamento de IPs dinâmicos



1 – 2 – 3 – 3

2 – 3 – 2 – 2

3 – 1 – 1 – 1

4 – 4 – 4 – 4

Propriedades de IPs dinâmicos

> Dispositivos distintos utilizam o mesmo IP ao longo do tempo

> Ambiguidades no mapeamento de vulnerabilidades para dispositivos

Propriedades de IPs dinâmicos

> Dispositivos distintos utilizam o mesmo IP ao longo do tempo

> Ambiguidades no mapeamento de vulnerabilidades para dispositivos

Problema

> Não temos como saber quais IPs são dinâmicos

Métodos de identificação

Dados públicos não confiáveis:

> DNS reverso (RDNS)

> Busca de indicadores de dinamicidade

(ec2-15-229-172-154.sa-east-1.compute.amazonaws.com, dynamic.200-49-28-32.amxinternet.com.br)

Métodos de identificação

Dados públicos não confiáveis:

> DNS reverso (RDNS)

> Busca de indicadores de dinamicidade

(ec2-15-229-172-154.sa-east-1.compute.amazonaws.com, dynamic.200-49-28-32.amxinternet.com.br)

Dados privados não disponíveis:

> Metadados sobre o IP para classificar um bloco

> Análise de tráfego de rede

Métodos de identificação

Dados públicos não confiáveis:

> DNS reverso (RDNS)

> Busca de indicadores de dinamicidade

`(ec2-15-229-172-154.sa-east-1.compute.amazonaws.com, dynamic.200-49-28-32.amxinternet.com.br)`

Pergunta: é possível alcançar um meio termo?

Dados privados não disponíveis:

> Metadados sobre o IP para classificar um bloco

> Análise de tráfego de rede

DynMap

> Propõe um método que seja **aplicável de forma geral** e que forneça bons resultados

> Utilização de **dados públicos** de fácil acesso

Rastreio de Dispositivos

É necessário um **identificador único** para relacionar um **IP a um Dispositivo**

UDmap:

> ID do usuário no Hotmail

> Privado

Rastreio de Dispositivos

É necessário um **identificador único** para relacionar um **IP a um Dispositivo**

UDmap:

> ID do usuário no Hotmail

> Privado

DynMap:

> SHA256 do certificado SSL

> Público

DynMap: Seleção de Blocos Candidatos

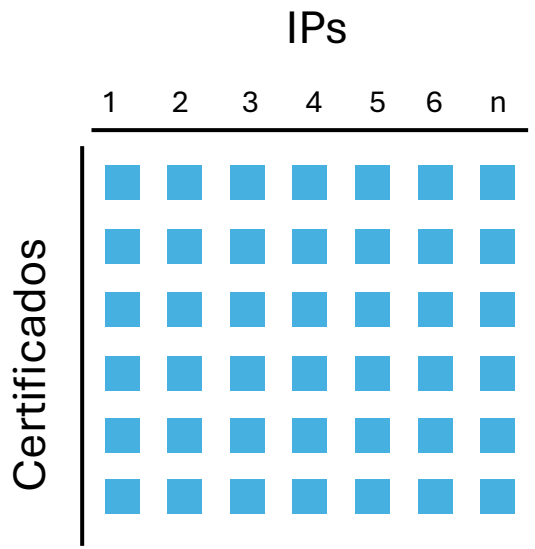
Seleção de blocos de IPs ***contíguos*** que satisfazem:

1. Mesmo prefixo IP
2. Número mínimo de IPs
3. Sem lacunas grandes

DynMap: Cálculo da Entropia de Uso por IP

Pergunta: Os certificados de um IP são observadas de forma uniforme nos outros IPs do bloco?

> Matriz Certificados x IPs

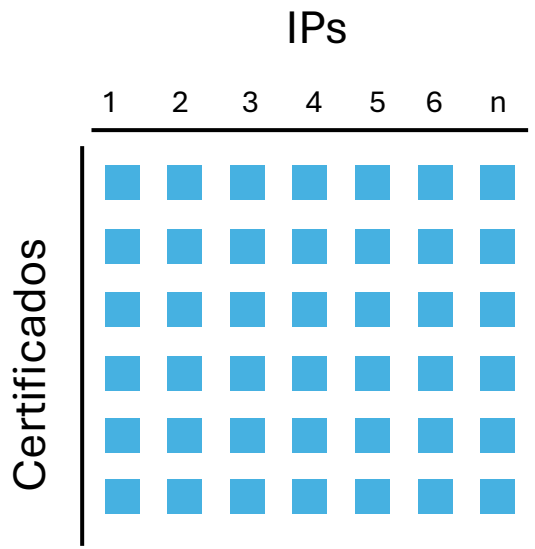


Alta dinamicidade
Entropia ≈ 1

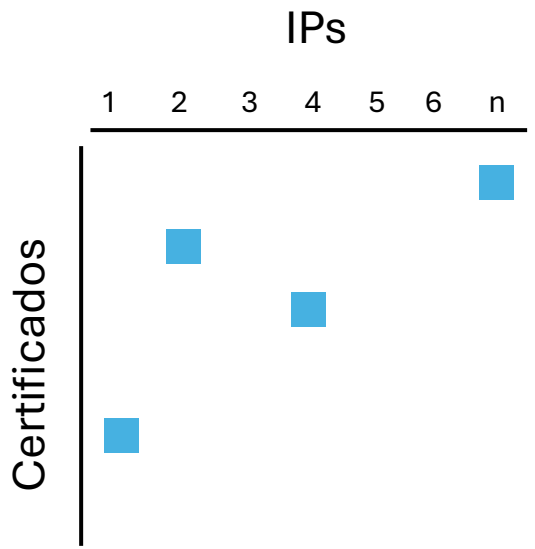
DynMap: Cálculo da Entropia de Uso por IP

Pergunta: Os certificados de um IP são observadas de forma uniforme nos outros IPs do bloco?

> Matriz Certificados x IPs



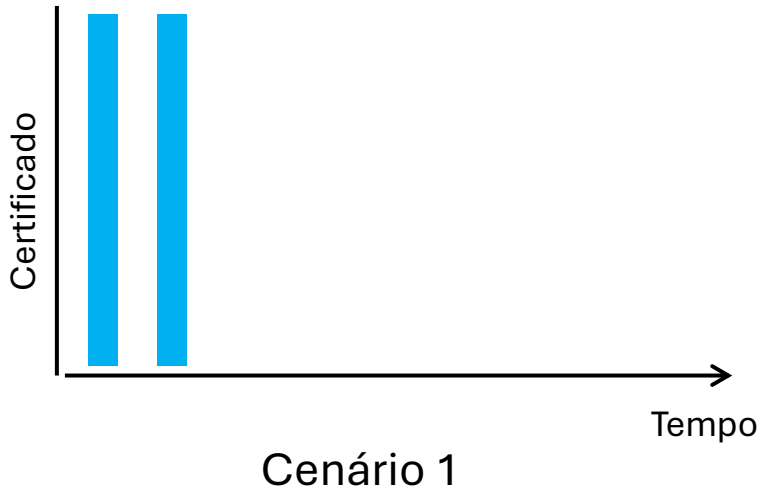
Alta dinamicidade
Entropia ≈ 1



Baixa dinamicidade
Entropia ≈ 0

DynMap: Cálculo da Dinamicidade de Domínio por IP

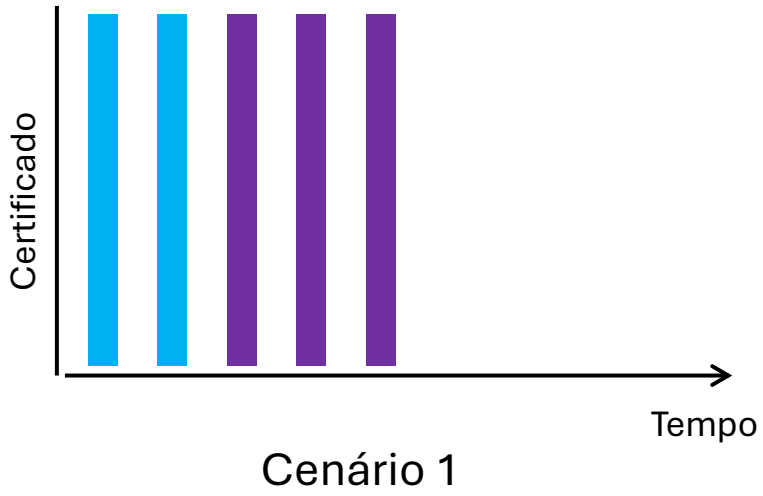
Problema: compartilhamento e renovação de certificados geram ambiguidades



Cenário 1

DynMap: Cálculo da Dinamicidade de Domínio por IP

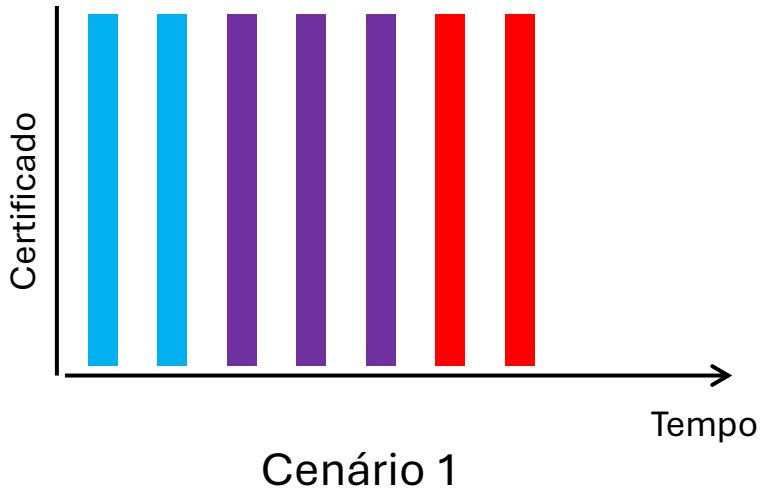
Problema: compartilhamento e renovação de certificados geram ambiguidades



Cenário 1

DynMap: Cálculo da Dinamicidade de Domínio por IP

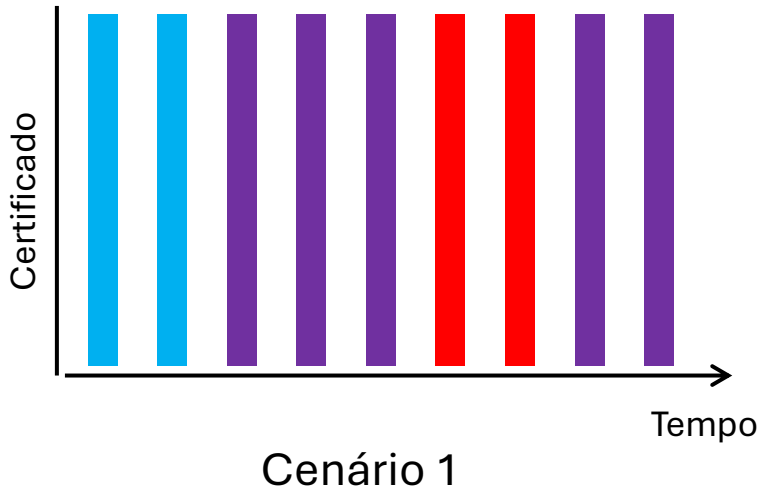
Problema: compartilhamento e renovação de certificados geram ambiguidades



Cenário 1

DynMap: Cálculo da Dinamicidade de Domínio por IP

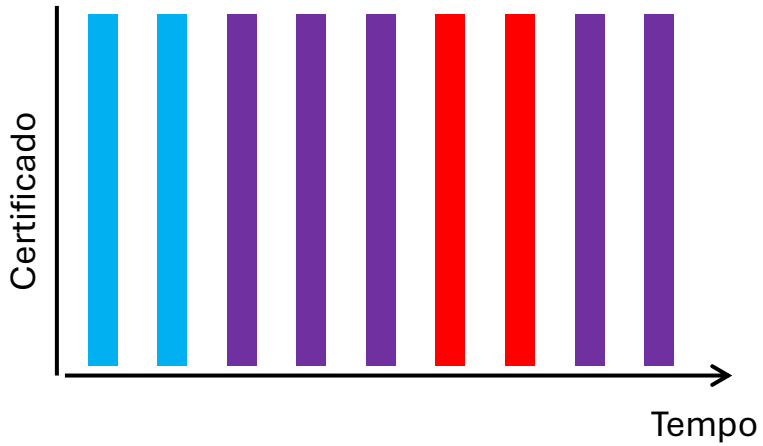
Problema: compartilhamento e renovação de certificados geram ambiguidades



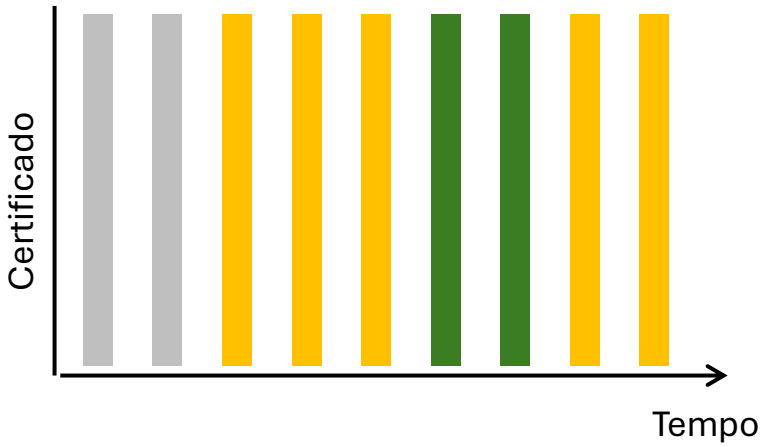
Cenário 1

DynMap: Cálculo da Dinamicidade de Domínio por IP

Problema: compartilhamento e renovação de certificados geram ambiguidades



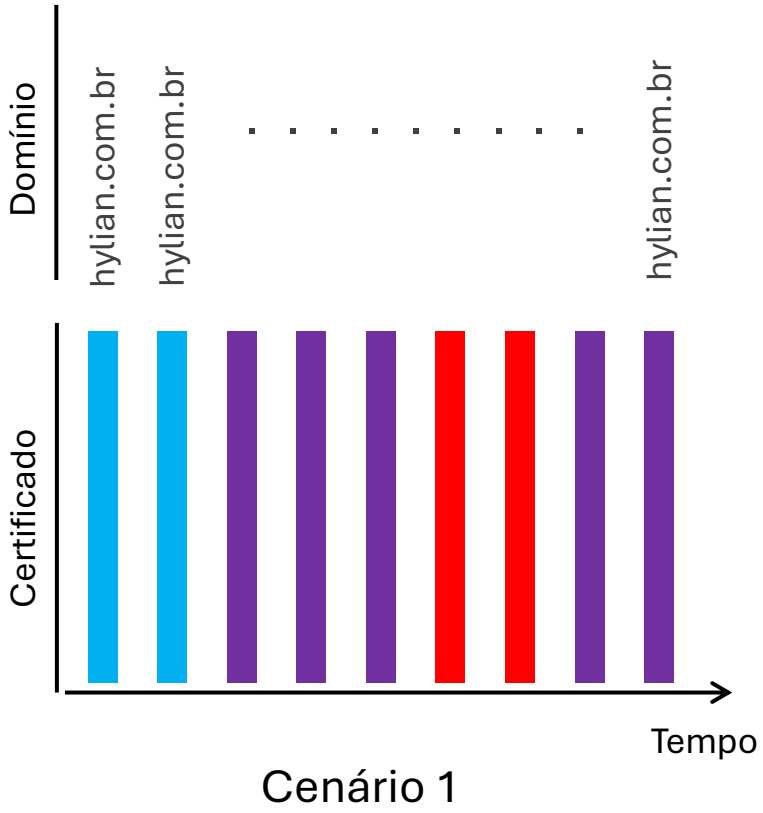
Cenário 1



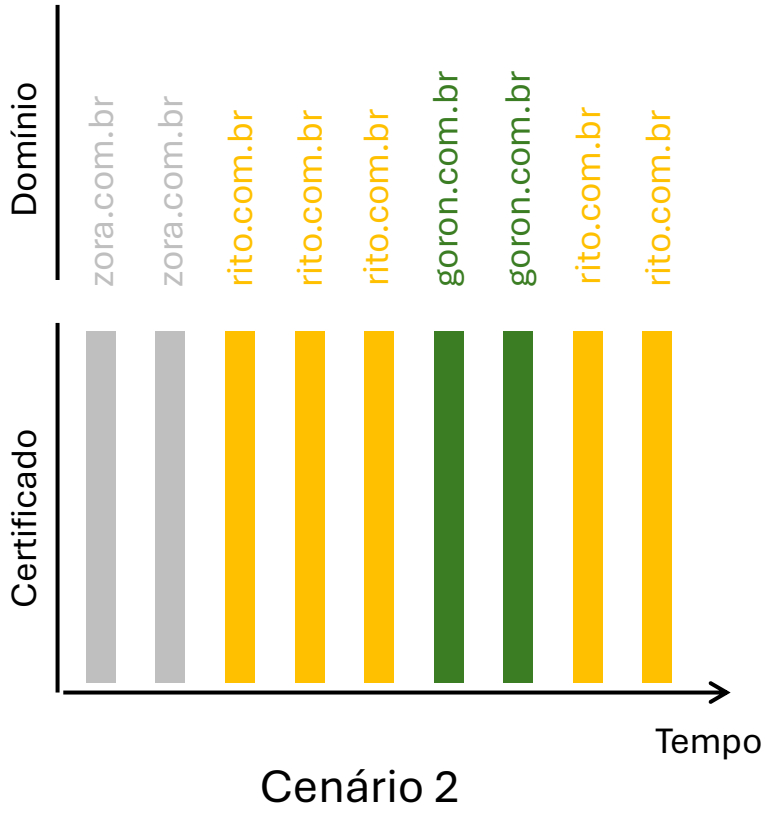
Cenário 2

DynMap: Cálculo da Dinamicidade de Domínio por IP

Problema: compartilhamento e renovação de certificados geram ambiguidades



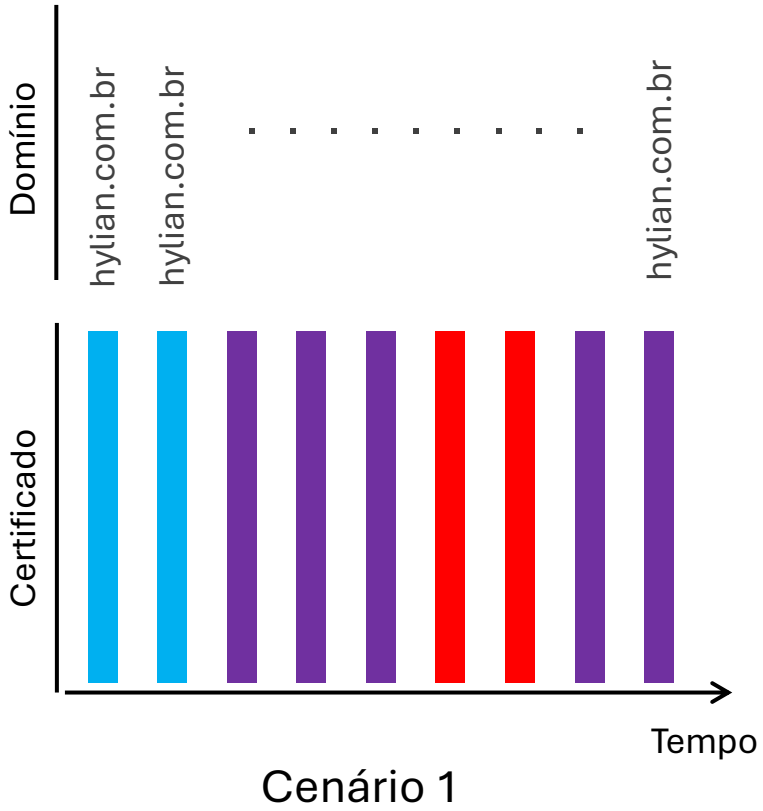
Cenário 1



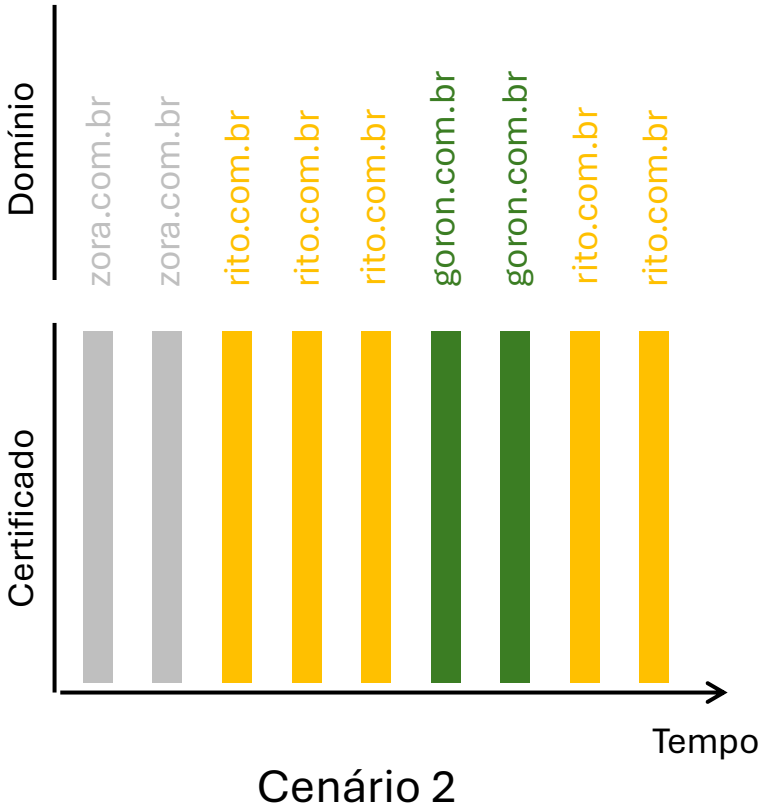
Cenário 2

DynMap: Cálculo da Dinamicidade de Domínio por IP

Problema: compartilhamento e renovação de certificados geram ambiguidades



Cenário 1



Cenário 2

Cenário 1 se trata de **renovação de certificados** ao passo que o Cenário 2 se trata da **mudança de dispositivos**

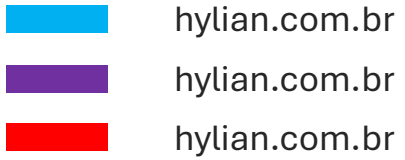
DynMap: Cálculo da Dinamicidade de Domínio por IP

Ideia: verificar se domínios variam de acordo com os certificados

> Cálculo é feito para cada IP em um bloco

Alta dinamicidade

$$\frac{Dominios}{Certificados} \approx 1$$



Baixa dinamicidade

$$\frac{Dominios}{Certificados} \approx 0$$

DynMap: Análise de Comportamento

Entropia de Uso	Dinamicidade de Domínio	Resultado

DynMap: Análise de Comportamento

Entropia de Uso	Dinamicidade de Domínio	Resultado
0	0	Estático

DynMap: Análise de Comportamento

Entropia de Uso	Dinamicidade de Domínio	Resultado
0	0	Estático
1	1	Dinâmico

DynMap: Análise de Comportamento

Entropia de Uso	Dinamicidade de Domínio	Resultado
0	0	Estático
0	1	Dinâmico
1	1	Dinâmico

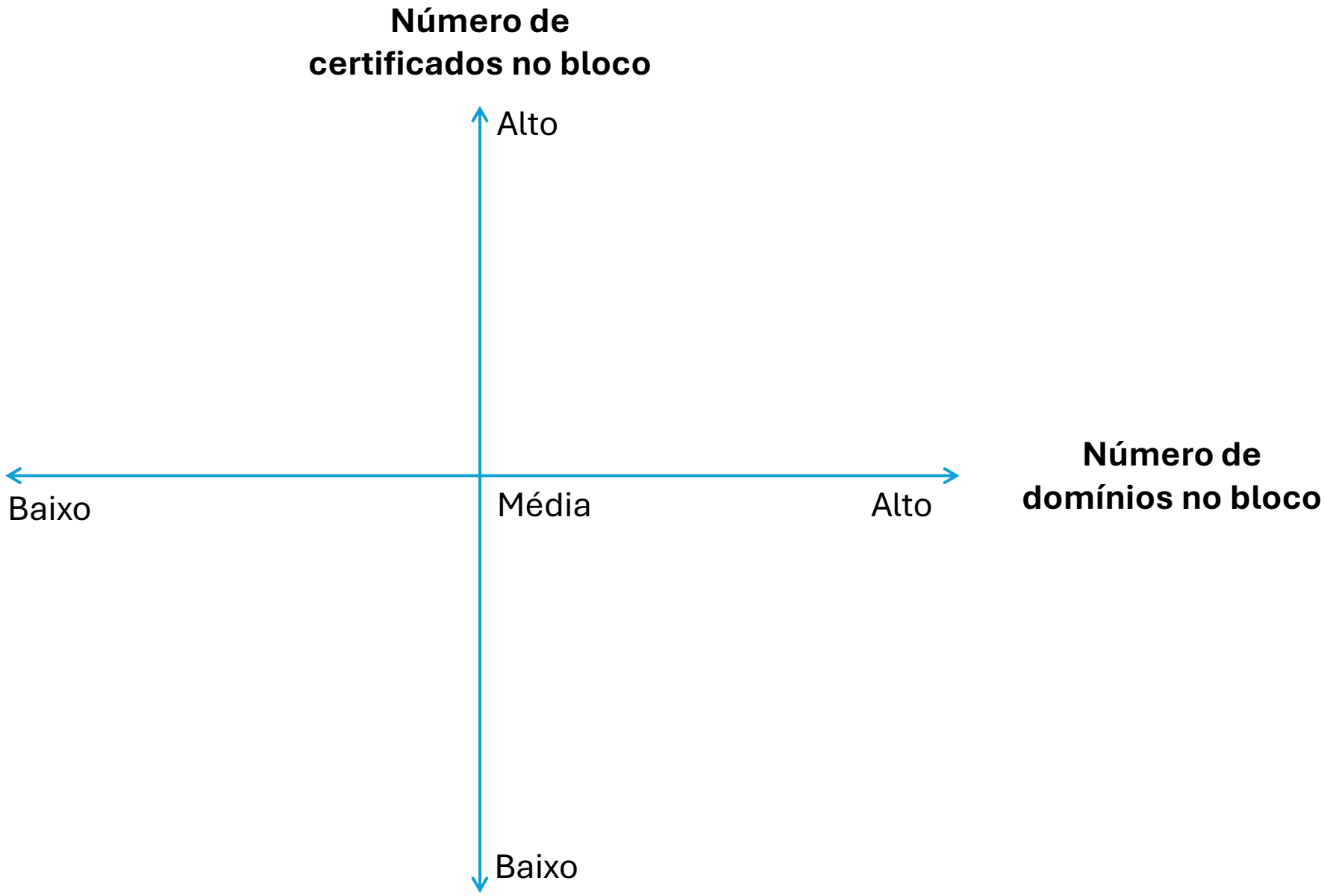
DynMap: Análise de Comportamento

Entropia de Uso	Dinamicidade de Domínio	Resultado
0	0	Estático
0	1	Dinâmico
1	1	Dinâmico
*	*	*Outlier*

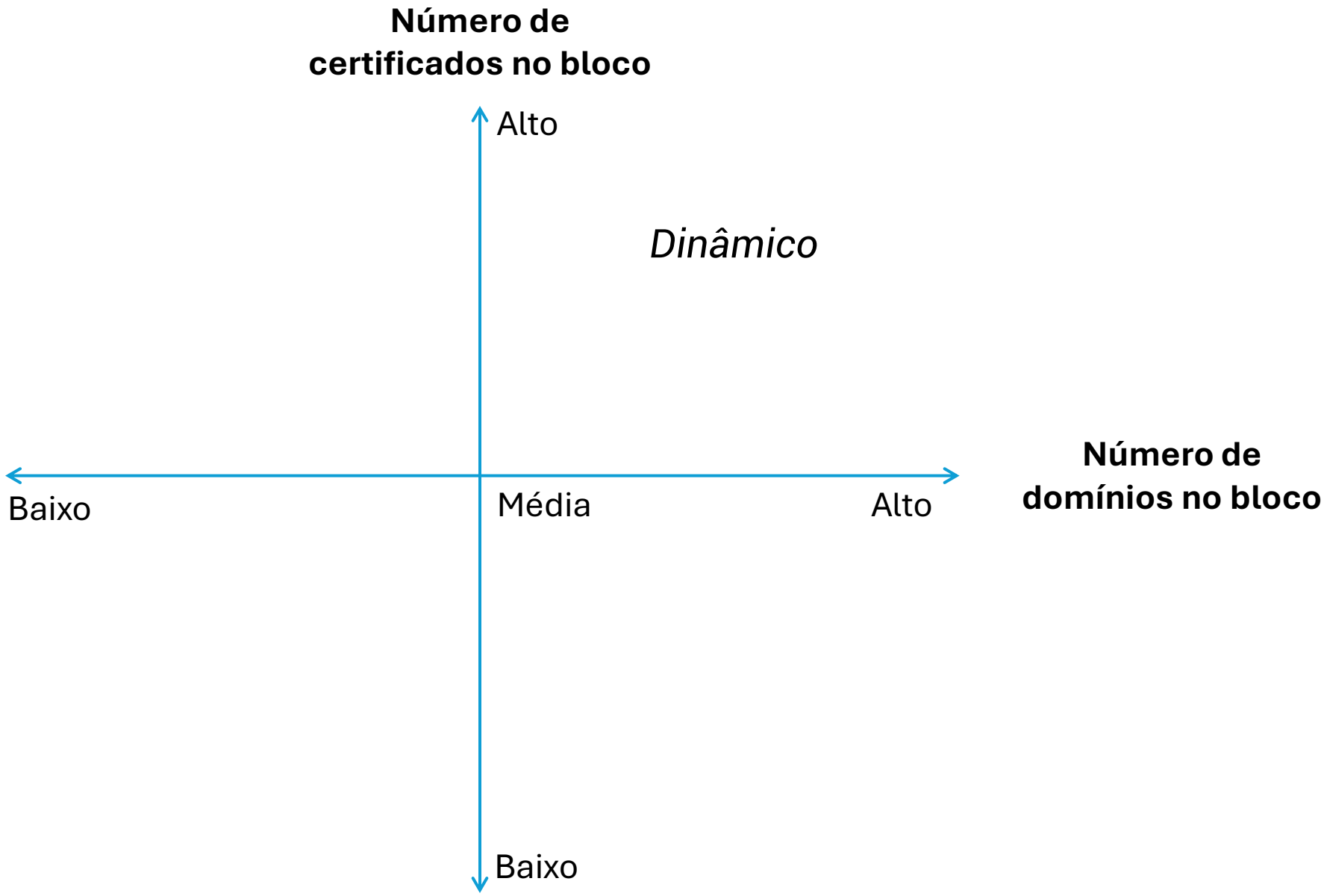
DynMap: Análise de Comportamento

Entropia de Uso	Dinamicidade de Domínio	Resultado
0	0	Estático
0	1	Dinâmico
1	0	Dinâmico
1	1	Dinâmico
*	*	*Outlier*

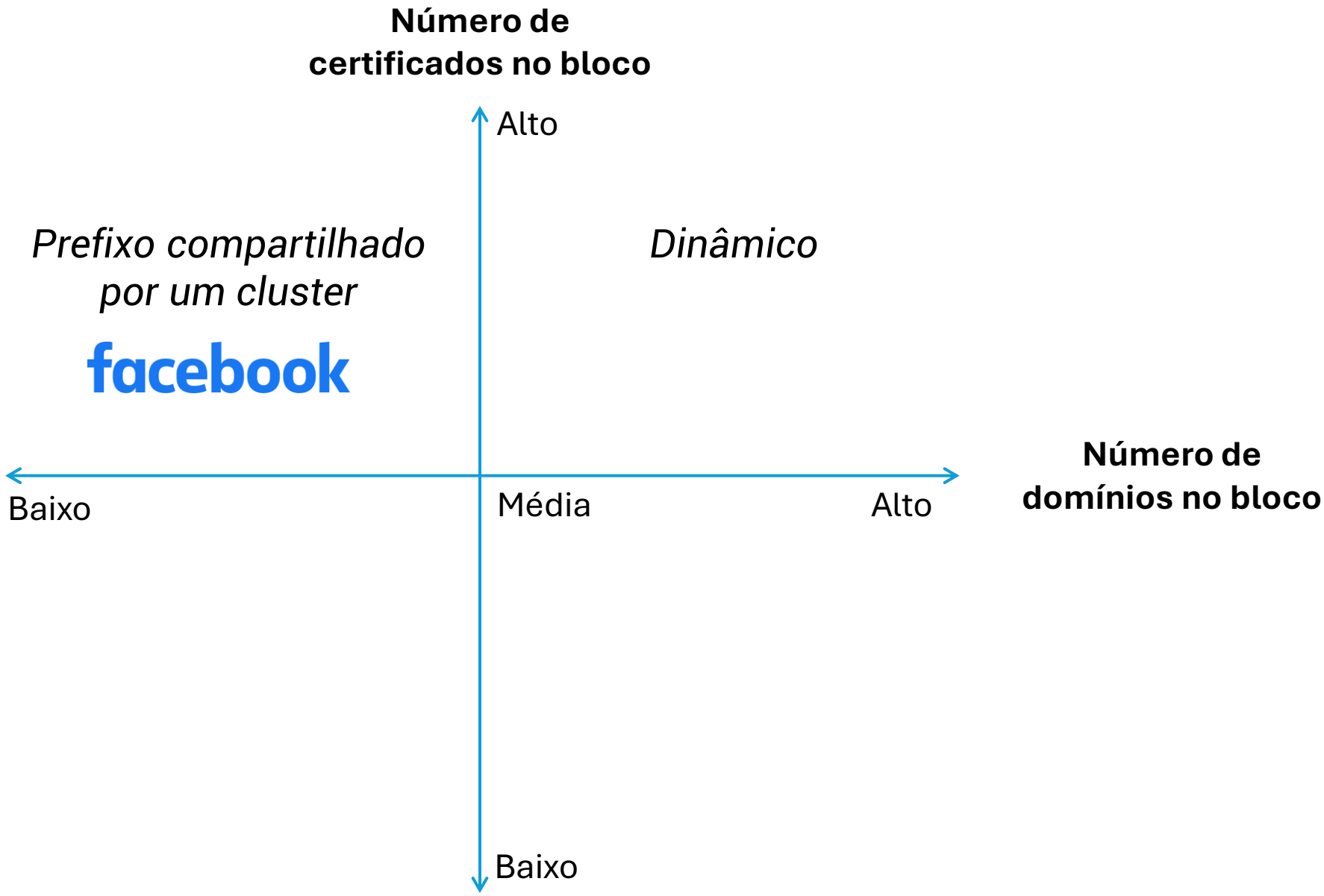
DynMap: Análise de Comportamento



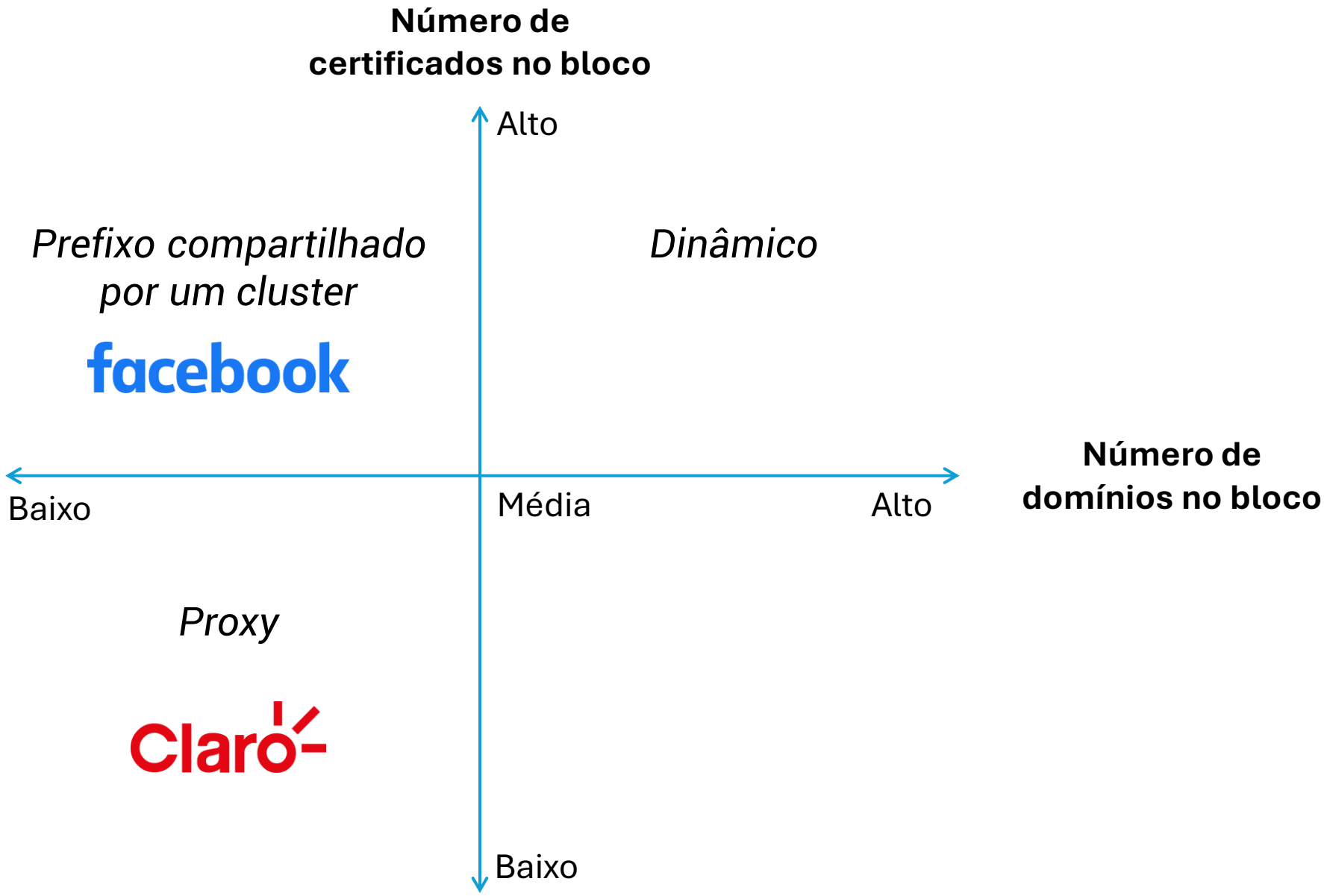
DynMap: Análise de Comportamento



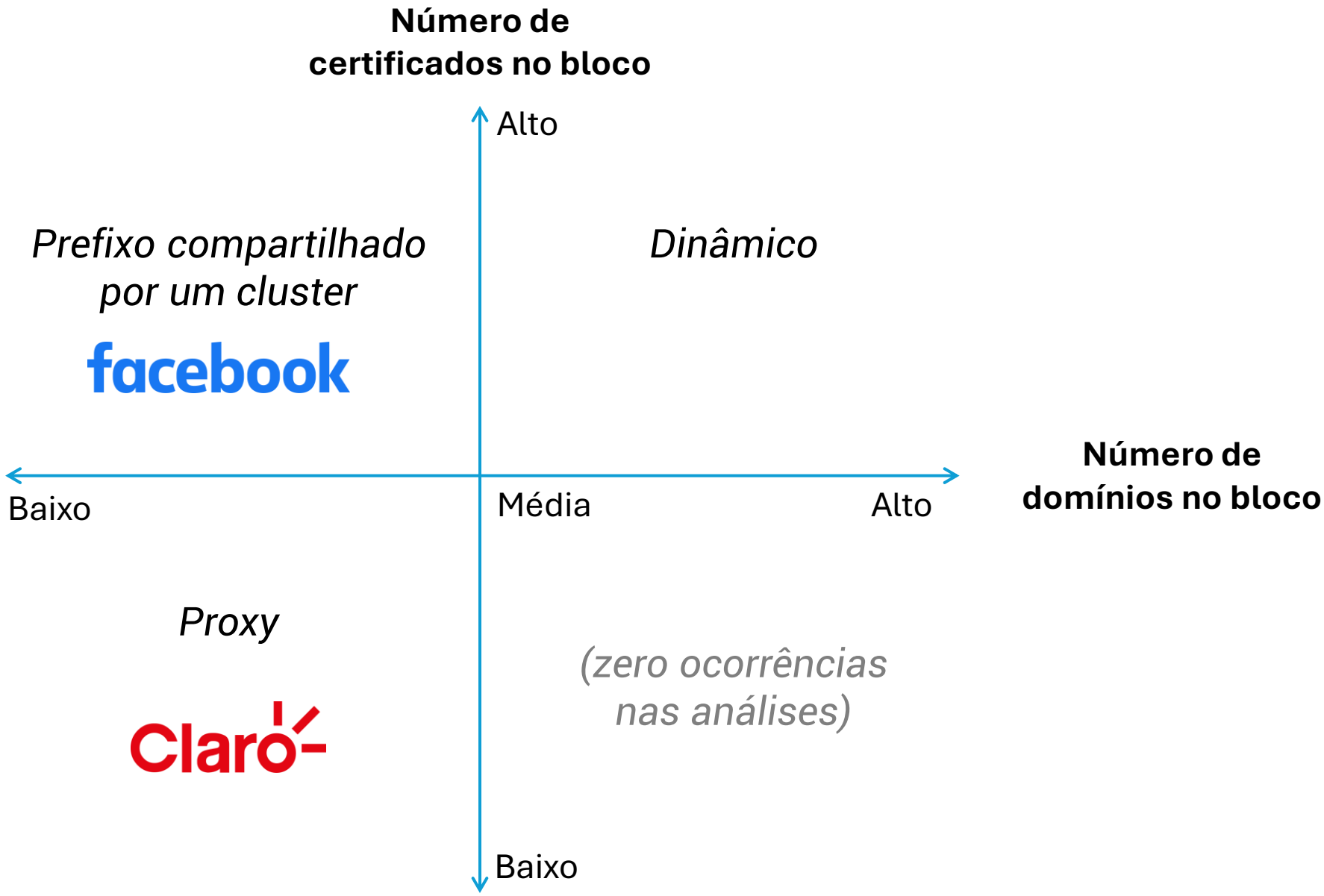
DynMap: Análise de Comportamento



DynMap: Análise de Comportamento



DynMap: Análise de Comportamento



DynMap: Análise de Comportamento

Entropia de Uso	Dinamicidade de Domínio	Resultado
0	0	Estático
0	1	Dinâmico
1	0	Dinâmico Dinâmico (Cluster) Dinâmico (Proxy)
1	1	Dinâmico
*	*	*Outlier*

Preparação dos Experimentos

Aplicação do DynMap em um conjunto de dados de varreduras de rede realizadas pelo Shodan na Internet brasileira

> Certificado: ***fingerprint* SHA256** do certificado SSL

> Nome de domínio: ***common name*** do certificado SSL

Preparação dos Experimentos

Aplicação do DynMap em um conjunto de dados de varreduras de rede realizadas pelo Shodan na Internet brasileira

> Certificado: ***fingerprint* SHA256** do certificado SSL

> Nome de domínio: ***common name*** do certificado SSL

> **Outubro 2023 – Dezembro 2023**

> **1.422.737** endereços IP distintos

> Validação por **correlação**

10 Redes com maior número de IPs

Nome da Rede	Número de IPs
Amazon	**75000**
Locaweb	**12000**
Microsoft	**6000**
Totvs	2600
BRC Telecom	1600
Deznet Telecom	1200
Akamai	1000
Secrelnet Informatica	1000
AMX Internet	1000
Vitoria Networks	1000

10 Redes com maior número de IPs

Nome da Rede	Número de IPs
Amazon	75000
Locaweb	12000
Microsoft	6000
Totvs	2600
BRC Telecom	**1600**
Deznet Telecom	**1200**
Akamai	**1000**
Secrelnet Informatica	**1000**
AMX Internet	**1000**
Vitoria Networks	**1000**

10 Redes com maior número de IPs

Tamanho mínimo de bloco = 8	
Nome da Rede	**Número de IPs**
Amazon	**75000**
Locaweb	**12000**
Microsoft	**6000**
Totvs	2600
BRC Telecom	1600
Deznet Telecom	1200
Akamai	1000
Secrelnet Informatica	1000
AMX Internet	1000
Vitoria Networks	1000

Tamanho mínimo de bloco = 128	
Nome da Rede	**Número de IPs**
Amazon	**8500**
Locaweb	**8500**
Microsoft	**4000**
Deznet Telecom	1200
AMX Internet	1000
Vitoria Networks	1000
Digo Internet	900
Pcsupri Informatica	700
Secrelnet Informatica	700
Megalynk Sistemas	600

10 Redes com maior número de IPs

1156 Redes

Tamanho mínimo de bloco = 8	
Nome da Rede	**Número de IPs**
Amazon	**75000**
Locaweb	**12000**
Microsoft	**6000**
Totvs	2600
BRC Telecom	1600
Deznet Telecom	1200
Akamai	1000
Secrelnet Informatica	1000
AMX Internet	1000
Vitoria Networks	1000

Tamanho mínimo de bloco = 128	
Nome da Rede	**Número de IPs**
Amazon	**8500**
Locaweb	**8500**
Microsoft	**4000**
Deznet Telecom	1200
AMX Internet	1000
Vitoria Networks	1000
Digo Internet	900
Pcsupri Informatica	700
Secrelnet Informatica	700
Megalynk Sistemas	600

51 Redes

Maiores tipos de rede por categoria de IP

Tipo	Dinâmico	Proxy	Cluster
Empresarial	**86,7%**	**12,3%**	**1,0%**
Conteúdo (CDN)	**44,2%**	**50,3%**	**5,5%**
Fibra/DSL/ISP	**59,2%**	**19,3%**	**21,5%**
NSP	26,0%	35,6%	38,4%
Educação/Pesquisa	65,4%	18,3%	16,2%
Governamental	38,6%	39,7%	21,7%
Serviços de rede	34,5%	52,4%	13,1%
Sem fins lucrativos	2,5%	77,7%	19,8%

Conclusão

> DynMap é capaz de identificar IPs claramente dinâmicos

> Introdução de duas subcategorias de blocos de IPs: **proxy** e **cluster**

> Foco em **tratar de anomalias que provém da utilização de dados públicos**

Conclusão

> DynMap é capaz de identificar IPs claramente dinâmicos

> Introdução de duas subcategorias de blocos de IPs: **proxy** e **cluster**

> Foco em **tratar de anomalias que provém da utilização de dados públicos**

Conclusão

> DynMap é capaz de identificar IPs claramente dinâmicos

> Introdução de duas subcategorias de blocos de IPs: **proxy** e **cluster**

> Foco em **tratar de anomalias que provém da utilização de dados públicos**

Obrigado!

> Email para contato: gabrielpains@dcc.ufmg.br

Análise e Categorização de IPs

Tabela 3: Relação de endereços IP dinâmicos e DNS Reverso

Expressão Regular	$B = 8$		$B = 128$	
.*dyn.*	272	0,19%	868	2,39%
.*cloud.*	949	0,65%	5614	15,46%
.*server.*	319	0,22%	43	0,12%
.*compute.*	22982	15,85%	3003	8,27%
.*hospeda.*	316	0,22%	1228	3,38%
.*host.*	2324	1,60%	776	2,14%
Restante	6938	4,79%	3768	10,38%
RDNS indisponível	110891	76,48%	21012	57,87%
Total	144991	100,00%	36312	100,00%

Análise e Categorização de IPs

Tabela 3: Relação de endereços IP dinâmicos e DNS Reverso

Expressão Regular	$B = 8$		$B = 128$	
`.*cloud.*`	949	0,65%	5614	15,46%
`.*server.*`	319	0,22%	43	0,12%
`.*compute.*`	22982	15,85%	3003	8,27%
Restante	6938	4,79%	3768	10,38%
RDNS indisponível	110891	76,48%	21012	57,87%

DynMap: Identificação de Sub-blocos de IP Dinâmicos

Suavização de variâncias bruscas transientes de entropia

> Aplicação do filtro da mediana como janela deslizante

DynMap: Identificação de Sub-blocos de IP Dinâmicos

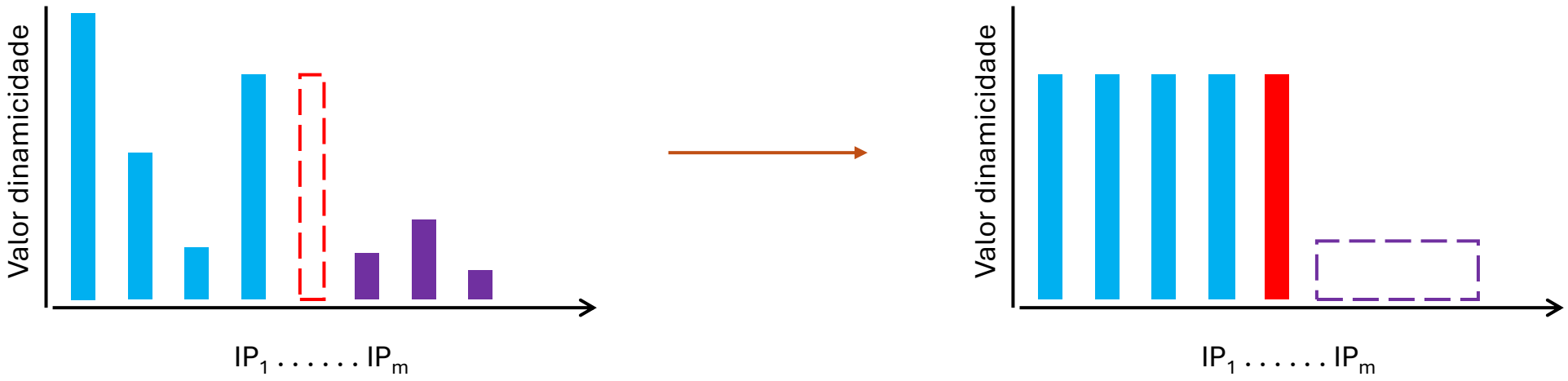
Suavização de variâncias bruscas transientes de entropia

> Aplicação do filtro da mediana como janela deslizante

DynMap: Identificação de Sub-blocos de IP Dinâmicos

Suavização de variâncias bruscas transientes de entropia

> Aplicação do filtro da mediana como janela deslizante



DynMap: Identificação de Sub-blocos de IP Dinâmicos

Após aplicação do filtro, são selecionados:

> Sub-blocos de IPs ***contíguos*** sem lacunas cuja métrica de dinamicidade é alta

DynMap: Identificação de Sub-blocos de IP Dinâmicos

Após aplicação do filtro, são selecionados:

> Sub-blocos de IPs ***contíguos*** sem lacunas cuja métrica de dinamicidade é alta