Reunião GTS-11

Detecção de Anomalias Baseada em Análise de Entropia no Tráfego IP

Alex Soares de Moura
Orientador: Sidney C. de Lucena

Universidade Federal do Estado do Rio de Janeiro – UNIRIO
Programa de Pós-Graduação em Informática (PPGI)

Reunião GTS-11 - Salvador, BA - 01/06/2008

Introdução

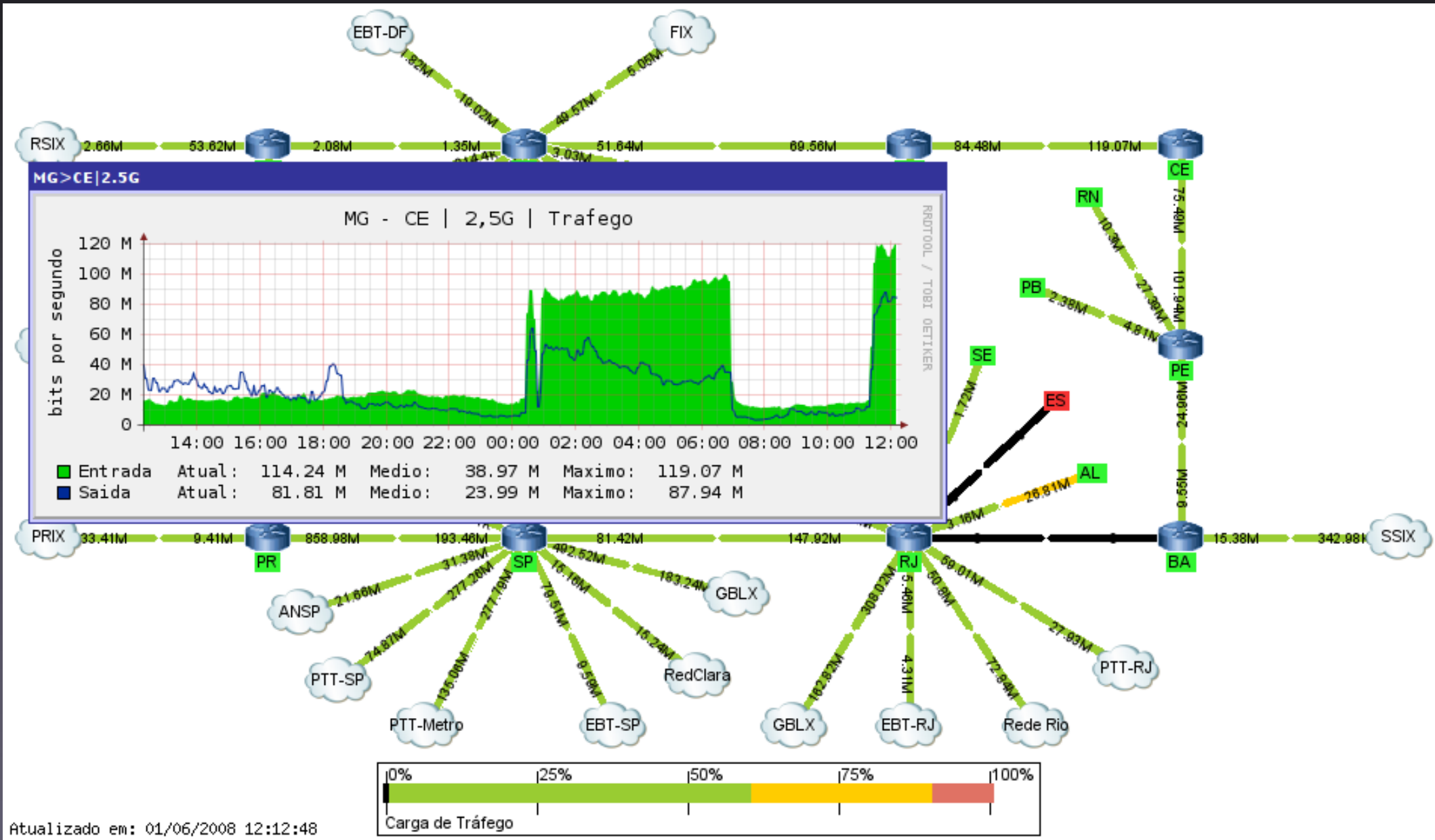
Introdução

- Metodologia proposta foi testada com amostras do tráfego da RNP
- Trabalho referente a dissertação de mestrado em andamento no PPGI/UNIRIO, com previsão de conclusão para 03/2009

Introdução

- Gerência das grandes redes incorporando análise do comportamento do tráfego em nível de aplicação
- NOCs: detecção de ataques e outros tráfegos maliciosos
- Tarefa que cresceu em complexidade

Introdução


EBT-DF
FIX
RSIX
PRIX
SSIX
CE
PE
PR
SP
RJ
BA
RN
PB
SE
ES
AL
ANSP
GBLX
PTT-SP
PTT-Metro
EBT-SP
RedClara
GBLX
EBT-RJ
Rede Rio
PTT-RJ
MG>CE|2.5G
MG - CE | 2,5G | Trafego
bits por segundo
120 M
100 M
80 M
60 M
40 M
20 M
0
14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00
Entrada Atual: 114.24 M Medio: 38.97 M Maximo: 119.07 M
Saida Atual: 81.81 M Medio: 23.99 M Maximo: 87.94 M
0%
25%
50%
75%
100%
Carga de Tráfego
Atualizado em: 01/06/2008 12:12:48

Introdução

Ferramentas comerciais

- Desenvolvidas para detectar anomalias e propor (ou executar) contra-medidas
- Base na coleta de fluxos dos roteadores e dados de protocolos de roteamento
- Outras funções, como matrizes de tráfego
- Custo: base na quant. de equips. monitorados
- Requerem período de ajustes (+/- 1 semana)
- Ex.: Peakflow, TrafIP, NetReflex, Anomaly Guard

Introdução

- Objetivo “macro”: Proposta de metodologia para refinar processos de gerência de redes, baseados em software livre, voltados para sinalizar ocorrências de potenciais ataques
- Caso típico de redes acadêmicas, tanto metropolitanas quanto nacionais

Introdução

- Objetivo “pontual”: combinar a técnica de análise de entropia com a estimativa de Holt-Winters para obter alertas de anomalias
- Uso de entropia proposto em [SIGCOMM2005]
  - NetReflex (Guavus): produto da tese
  - Solução para detecção de anomalias, gera matriz de tráfego e relatórios diversos

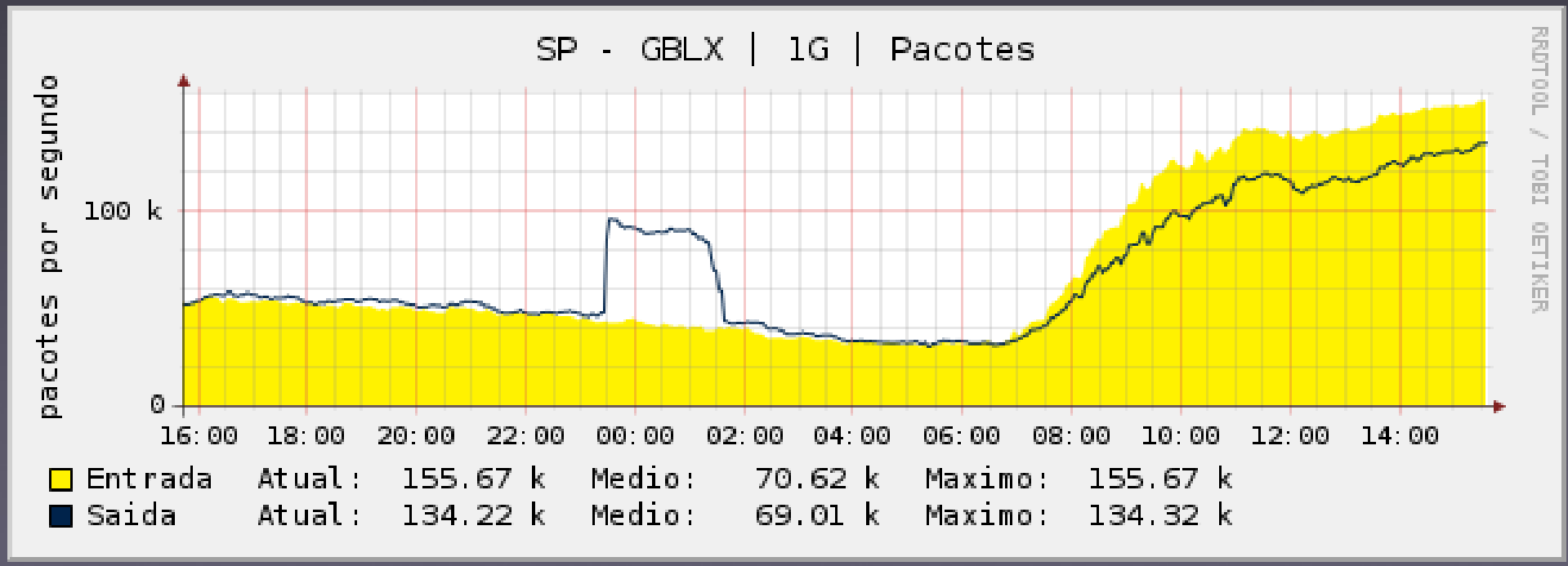
Formas de detecção de anomalias

Formas de detecção de anomalias

- Anomalia de tráfego: todo tráfego diferente do esperado
- Formas para detecção, conforme o tipo
  - Falhas em enlaces (*traps* SNMP, syslog)
  - Mudanças significativas nos anúncios de rotas (CLI de switches/roteadores/SNMP)
- Mais problemáticos de detectar:
  - “Flash crowds” (pode ser lícito)
  - Ataques (DDoS, Worm, Portscan)

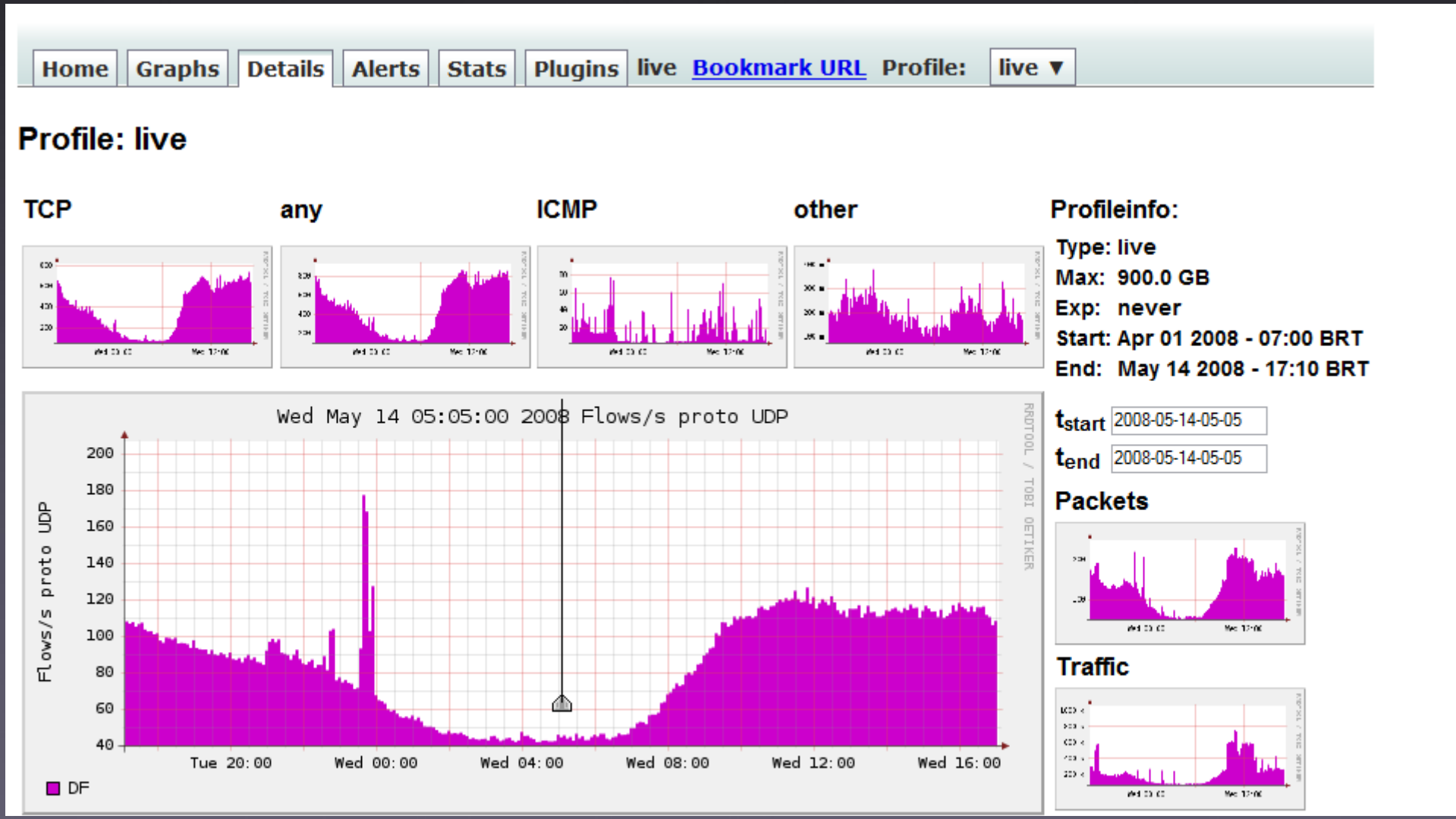
Formas de detecção de anomalias

- Tráfego IP “normal” pode ser estatisticamente caracterizado
- Anomalias: fugas deste comportamento estatístico. Ex.: volume de tráfego



Formas de detecção de anomalias

Muitas anomalias “escondidas” no volume de tráfego, impedindo sua visualização



Formas de detecção de anomalias

- Distribuições de IPs e portas, origem e destino, variam significativamente durante ataques
- DDoS: vários IPs de origem, um IP vitimado
- Portscan: muitas portas de destino
- Alternativa eficiente na investigação de ataques:
  - Analisar distribuição dos IPs e portas, periodicamente. Ex.: a cada 5min.

Análise baseada em entropia

Análise baseada em entropia

Métrica para investigar distribuições de IPs e portas:

Entropia de Shanon [SIGCOMM 2005]

$$E_S = -\sum_{i=0}^{N} p_i \log_2(p_i)$$

E_s assume valores de [0, $\log_2$N]

- Normalizando E_s:

0 = totalmente concentrado
(p_k= 1, p_i= 0, p/i <> k)

1 = totalmente disperso (p_i= 1/N p/ todo i)

Análise baseada em entropia

Valores normalizados obtidos a intervalos fixos de tempo resulta em série temporal para cada parâmetro do tráfego

- IP de origem, IP de destino,
- Porta de origem e porta de destino

Estratégia: buscar padrões anômalos nas 4 séries temporais de entropia

Problemas: sazonalidade das séries temporais, identificação da anomalia, falsos positivos

Análise baseada em entropia

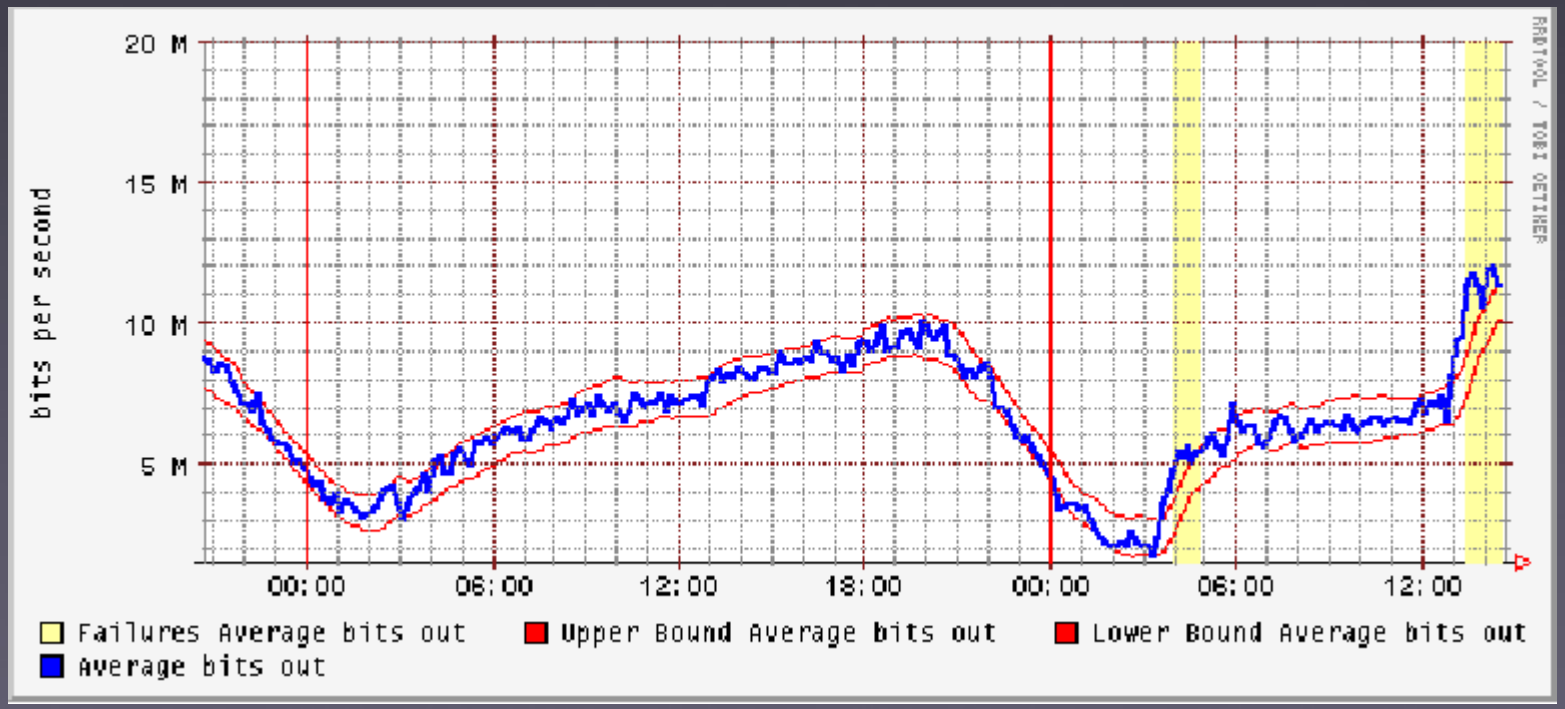
Método usado em [SIGCOMM 2005] é mais complexo:

- Baseia-se em coletas de fluxos IP (ex: netflow)
- Investigam fluxos separados por par origem-destino: mesmos pontos de entrada e de saída
- 4 matrizes (par OD x Ek), uma para cada parâmetro
- Método de subespaço p/ correlacionamento
- Necessita saber topologia e rotas (IGP e BGP)
- Nada pré-definido, mineração e classificação “on the fly” (identifica os tipos “day-0”)

Estimativa de Holt-Winters

Estimativa de Holt-Winters

- Necessário buscar padrão anômalo (ou “normal”) nas 4 séries temporais de entropia
- Várias alternativas para identificação de padrões.
- Estratégia adotada: estimativa de Holt-Winters



Estimativa de Holt-Winters

- Estima próximos valores numa série temporal, considerando variações sazonais e tendência de crescimento

- Série dividida em 3 termos independentes:

periodicidade, tendência de crescimento e parte residual

- Para cada termo, usa aproximação exponencial

$$x_{t+1} = \alpha X_t + (1-\alpha) x_t$$

X_t = amostra real no tempo t

Estimativa de Holt-Winters

Parâmetros da estimativa de Holt-Winters:

- α , β e γ : fatores de aproximação para cada termo (residual, tendência e periodicidade)
- *m*: tamanho do período

$$x_{t+1} = a_t + b_t + c_{t+1-m}$$

$$a_t = \alpha(X_t - c_{t-m}) + (1-\alpha)(a_{t-1} + b_{t-1})$$

$$b_t = \beta(a_t - a_{t-1}) + (1-\beta)b_{t-1}$$

$$c_t = \gamma(X_t - a_t) + (1-\gamma)c_{t-m}$$

Estimativa de Holt-Winters

De maneira análoga, faz-se uma aproximação exponencial do desvio gerado pelo H-W:

$$desvio_t = \gamma \left| X_t - x_t \right| + (1-\gamma)\, desvio_{t-m}$$

Limiares inferior e superior para x_{t+1} "normal" correspondem ao intervalo

$$(x_t - \delta . desvio_{t-m},\ x_t + \delta . desvio_{t-m})$$

onde δ = fator multiplicador

Estimativa de Holt-Winters

- Estimativa de Holt-Winters implementada no RRDtool:
  - Muitas ferramentas de código aberto para gerência SNMP usam bases RRD
  - Séries temporais facilmente transportadas para formato RRD
  - Uso do RRDtool para detecção de ataques facilita adoção desta metodologia por administradores de rede

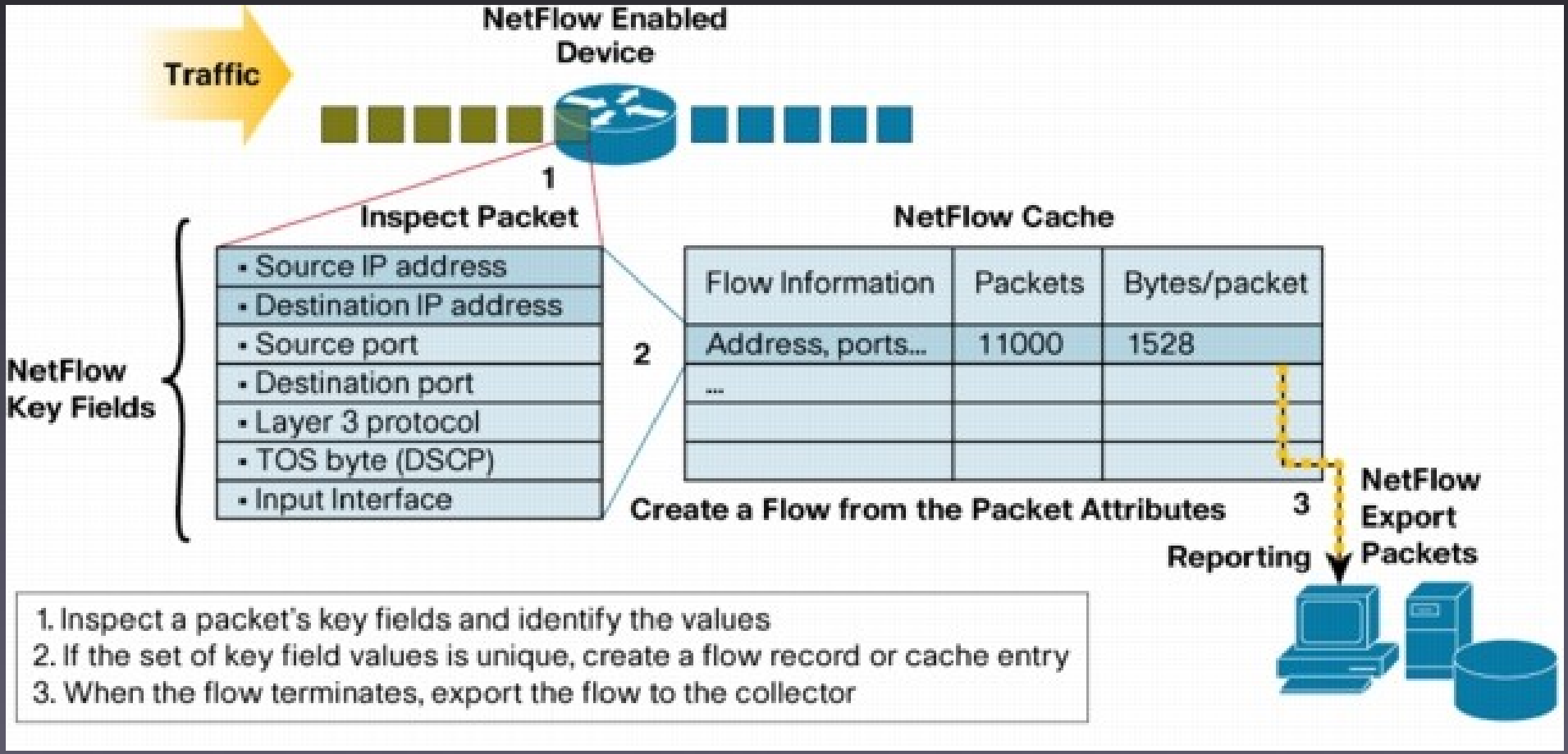
Medição em fluxos da RNP

Medição aplicada a fluxos da RNP

- Fluxo de pacotes: seqüência unidirecional de pacotes com mesmo IP de origem, IP de destino, porta de origem e porta de destino
- Expira caso intervalo de tempo entre pacotes supere um limite, tipicamente igual a 15seg.
- Tempo de vida máximo tipicamente expira após 30min.
- Bytes RST e FIN do TCP expiram fluxos

Medição aplicada a fluxos da RNP

Arquitetura da tecnologia netflow



Fonte: Cisco Systems

Medição aplicada a fluxos da RNP

Dados NetFlow versão 5:

DateFlowStart	Duration	Proto	SrcIPAddr:Port	DstIPAddr:Port	Packets	Bytes	Flows
2007-10-30 23:58:52.751	0.000	UDP	65.112.145.67:53	200.129.133.130:32768	1	139	1
2007-10-30 23:59:18.823	0.000	TCP	88.22.147.67:35611	200.17.33.48:1516	1	40	1
2007-10-30 23:59:24.705	0.000	UDP	61.171.148.67:47936	146.134.9.210:4659	1	55	1
2007-10-30 23:58:41.024	0.000	TCP	200.126.149.67:4513	200.137.130.150:54159	1	211	1
2007-10-30 23:59:18.956	0.000	TCP	82.55.150.67:9030	200.128.3.103:6577	1	1480	1
2007-10-30 23:58:52.389	0.000	TCP	84.54.152.67:17562	200.130.3.129:58766	1	52	1
2007-10-30 23:59:00.298	37.444	TCP	84.54.152.67:17562	200.130.3.129:58766	7	7648	1
2007-10-30 23:58:41.475	0.000	UDP	129.74.152.67:8099	150.165.15.18:8099	1	104	1
2007-10-30 23:59:27.840	0.000	TCP	90.27.155.67:4047	150.165.123.88:4661	1	48	1

Medição aplicada a fluxos da RNP

- Taxa de amostragem de 1 a cada 100 pacotes
- Interfaces selecionadas no roteador de núcleo do PoP-SP (Juniper M320):
  - PTT-Terremark, a 1 Gbps (Google, Oi)
  - PTT-Metro, a 1 Gbps (Terra, CTBC, BrT, UOL, Yahoo, Impsat, Telefônica)
  - Rede Clara, na época a 155 Mbps (Internet 2 e Géant)
  - Embratel, a 155 Mbps

Medição aplicada a fluxos da RNP

Período de coleta:

- 00:00 de 14/02/2008 a 00:00 de 28/02/2008
- 60 Gbytes de dados baixados do servidor de coleta de fluxos da RNP
- Arquivos no formato nfcapd, gerados a cada 5min. de coleta no roteador do PoP-SP, englobando a entrada de todas as interfaces
- Obtenção dos dados de interesse(parâmetros p/ cada interface) com uso do nfdump

Medição aplicada a fluxos da RNP

- Saída do nfdump gera aquivos contendo IPs e portas, origem e destino, para cada 5min. de coleta
- Cálculo de entropia para cada arquivo, resultando em séries temporais com granularidade de 5min.
- Entropias geradas são armazenadas em bases RRD criadas com estimativa de H-W

Medição aplicada a fluxos da RNP

Parâmetros usados no H-W (iguais para 4 entropias):

- α = 0,01
- β = 0,0035
- γ = 0,01
- m = 288 (288 amostras de 5min. = 1 dia)
- δ = 2
- Janela para análise dos dados estipulada em 5 dias
- Valores atribuídos de forma empírica, baseados em sugestões de [Brutlag, 2000]

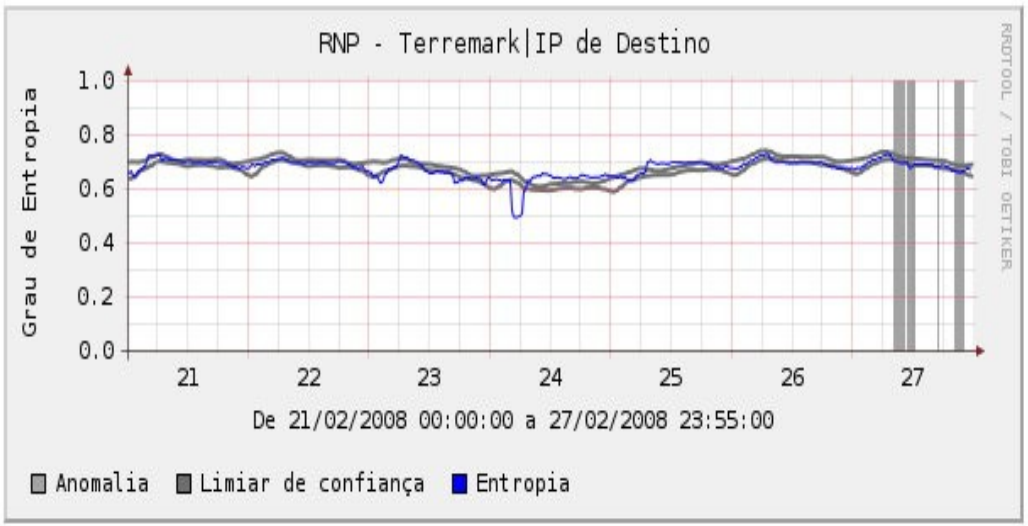
Resultados obtidos

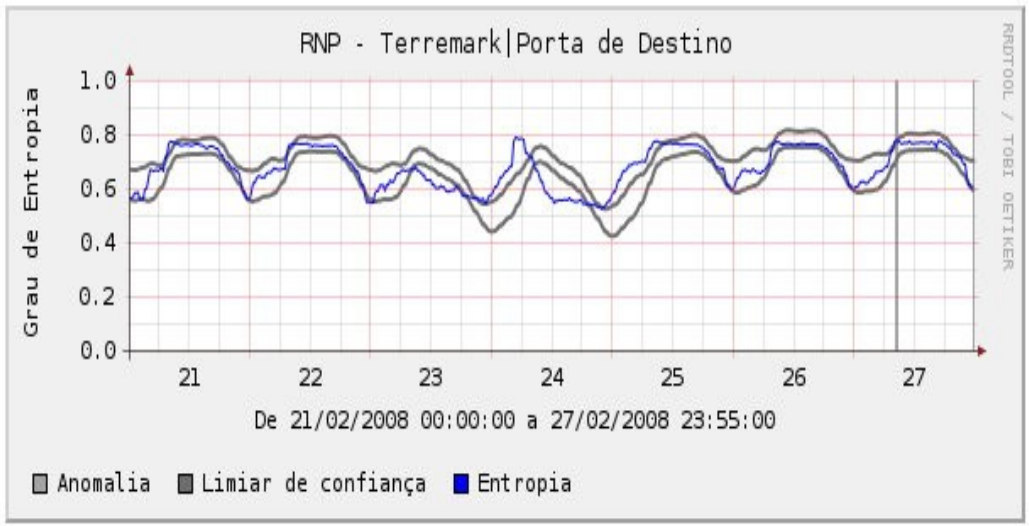
Resultados obtidos

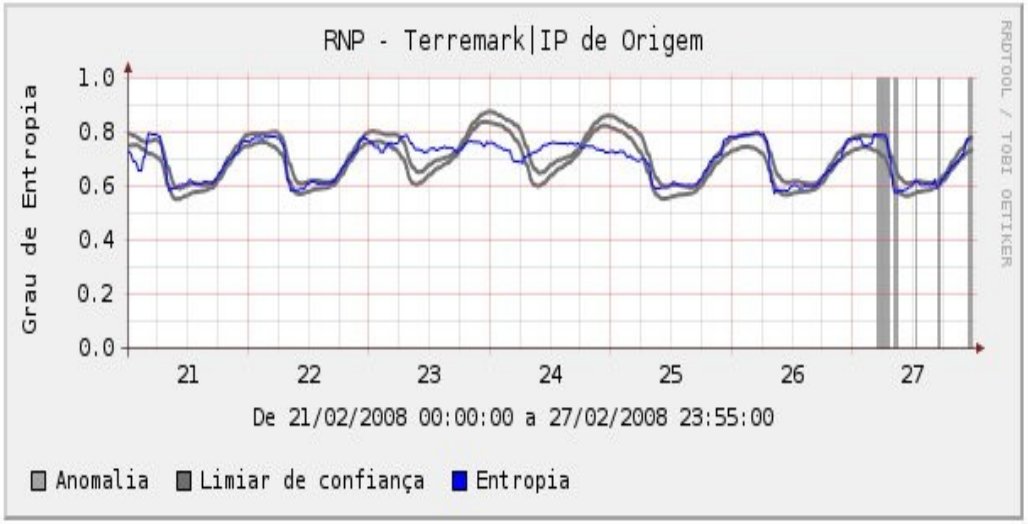
- Gráficos gerados a partir do RRDtool
- Fator limitante na análise do método: não houve registro de ataque durante o período de coleta!
- Na época, o storage só conseguia armazenar dois dias de arquivos nfcapd com coletas da RNP
- Resultados são parciais, pouco conclusivos quanto à eficiência do método

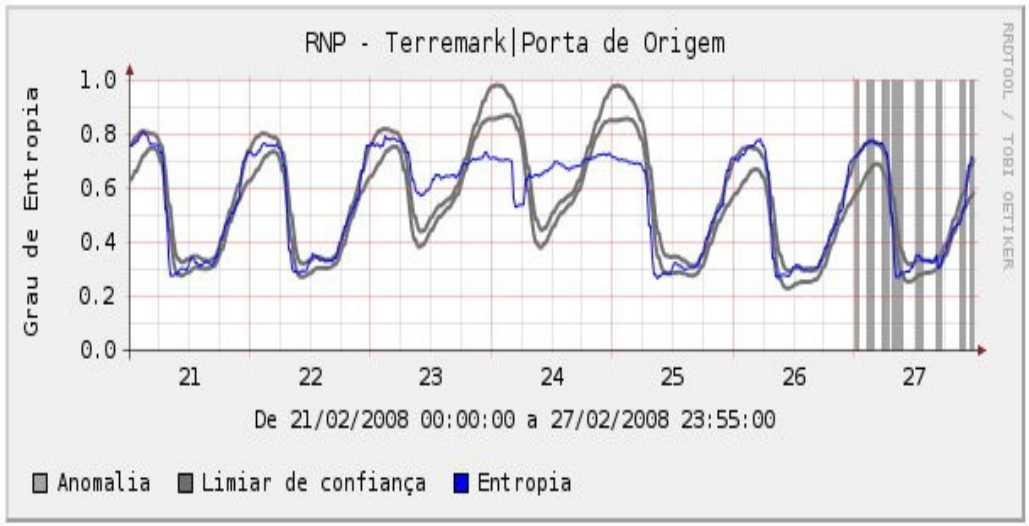
Resultados obtidos

Peering RNP / PTT-Terremark:



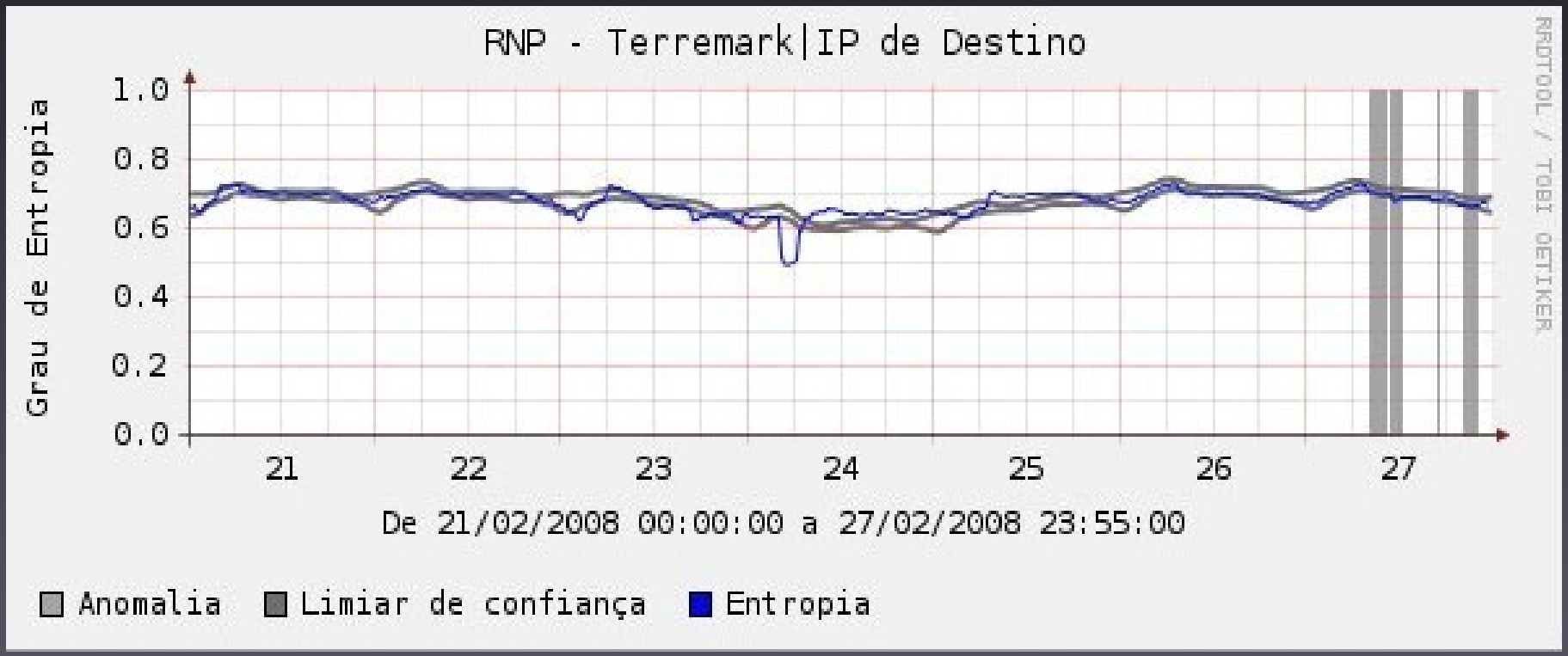






Resultados obtidos

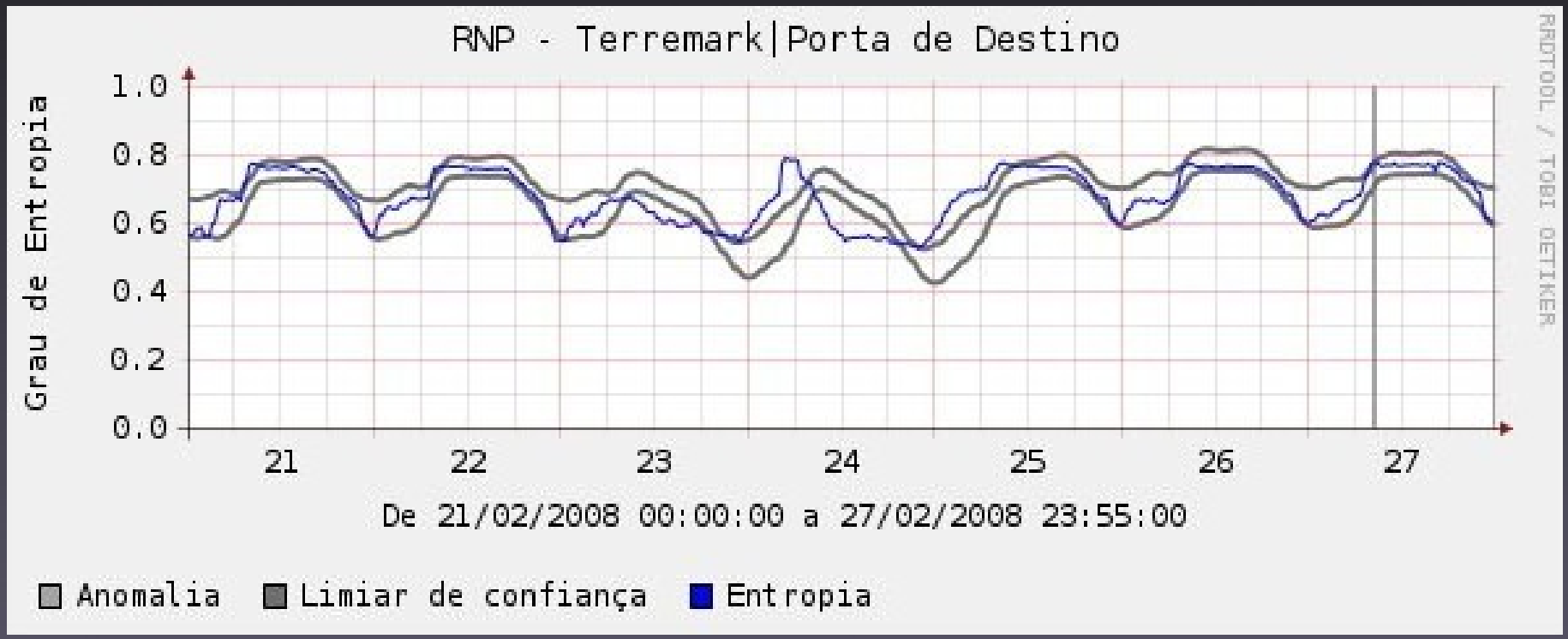
PTT-Terremark: possível *portscan* no dia 24



Dia 24, 06hs: concentração dos IPs de destino

Resultados obtidos

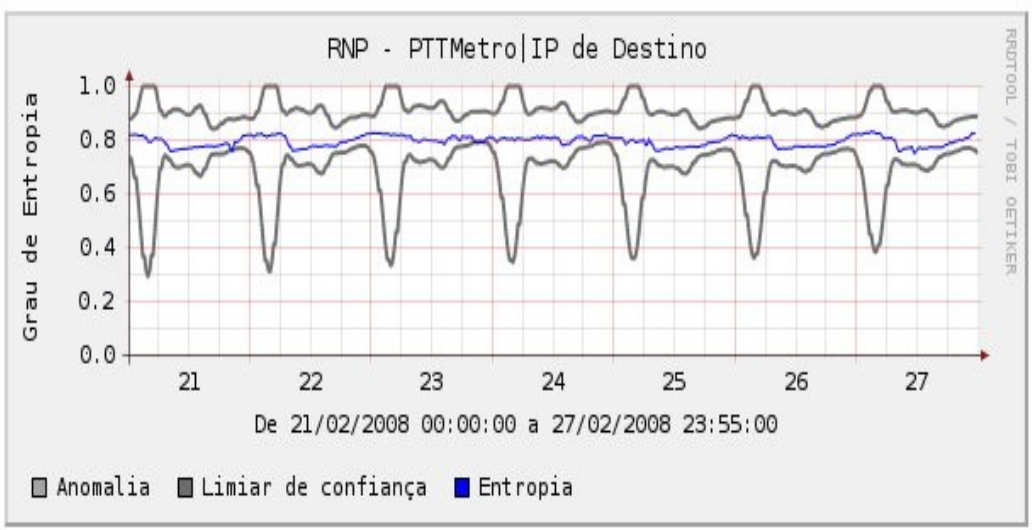
PTT-Terremark: possível *portscan* no dia 24

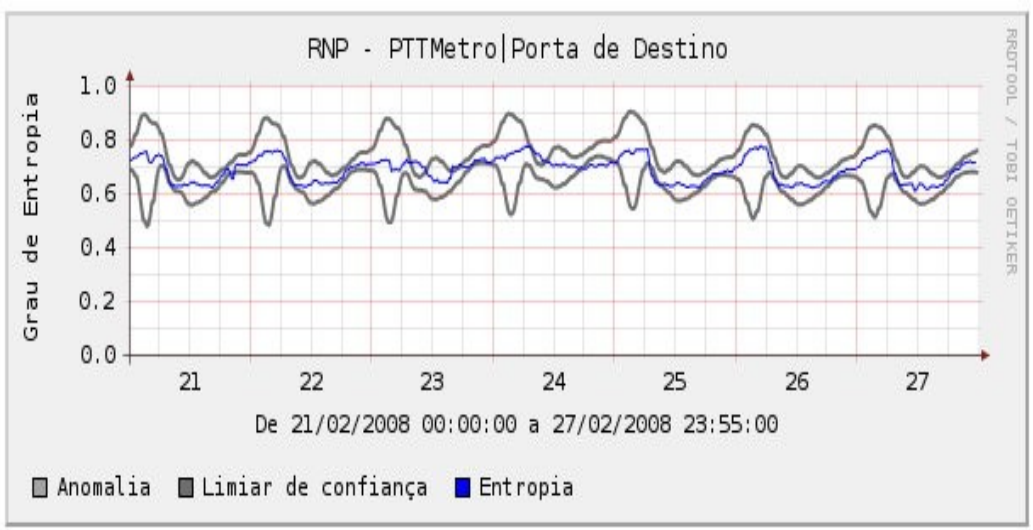


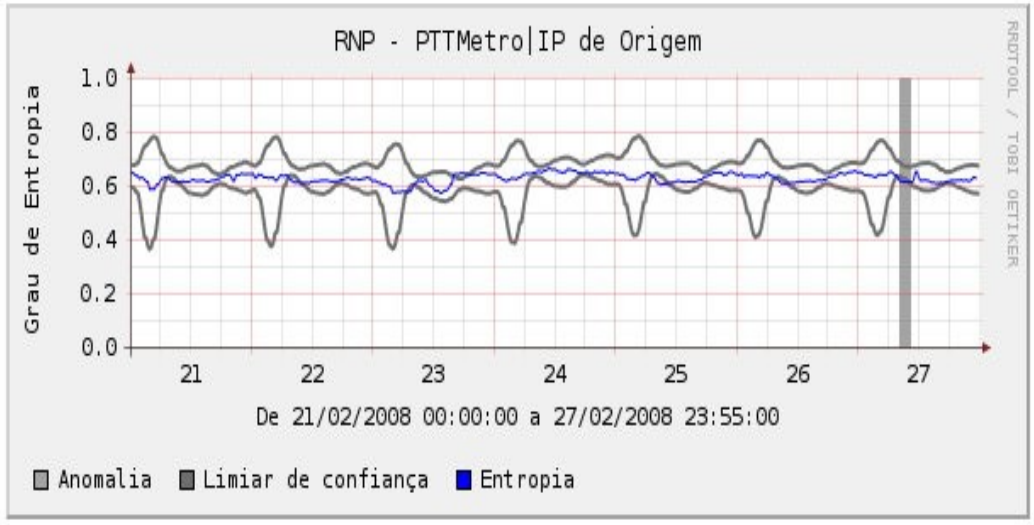
Dia 24, 06hs: dispersão das portas de destino

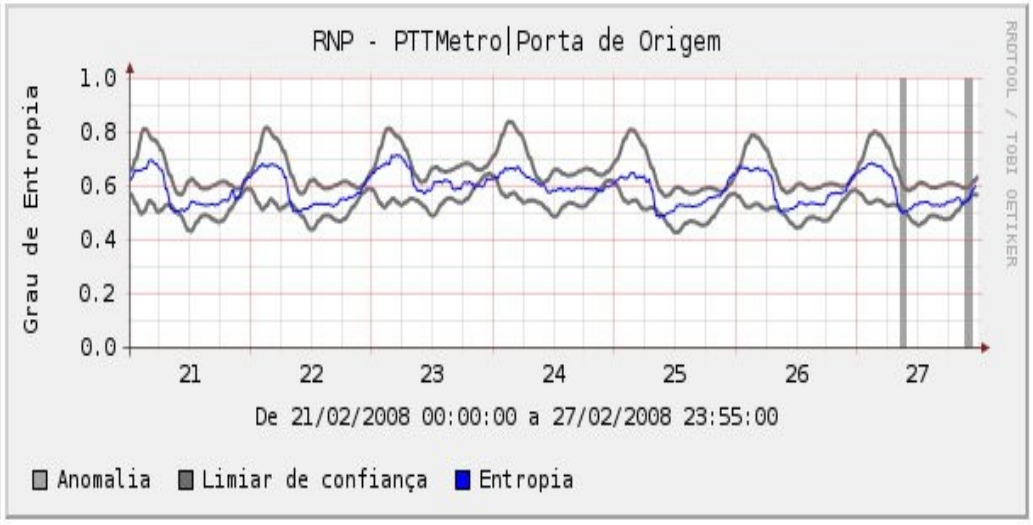
Resultados obtidos

Peering RNP / PTT-Metro: nada significativo



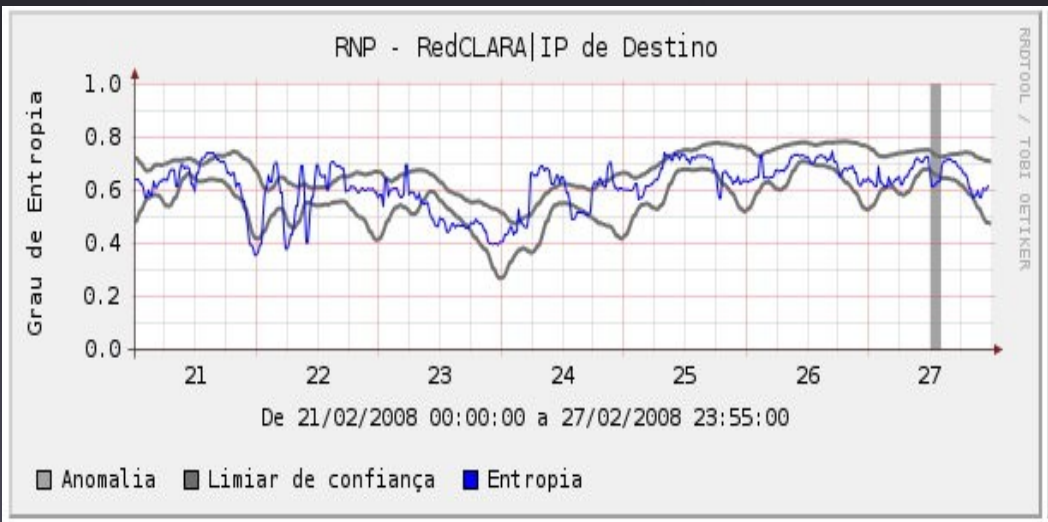


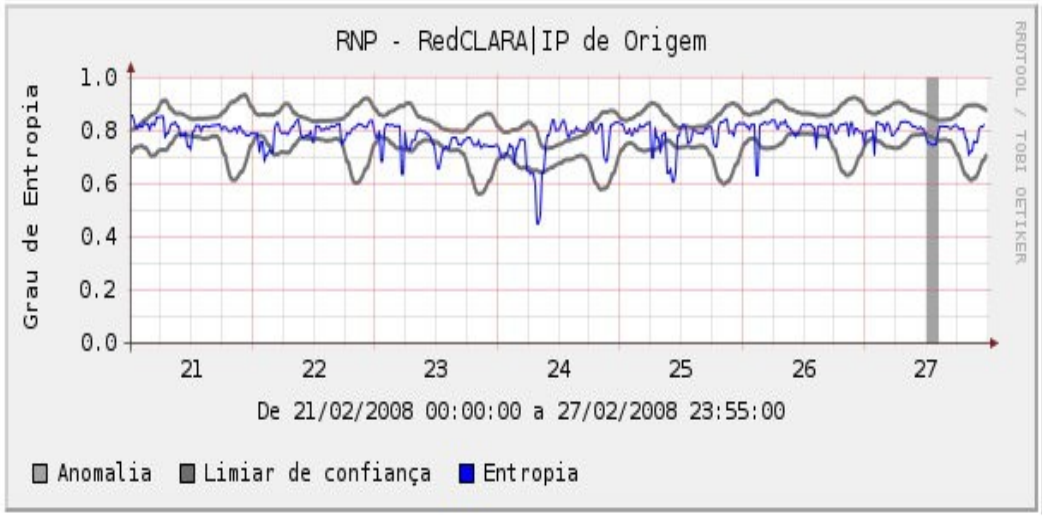


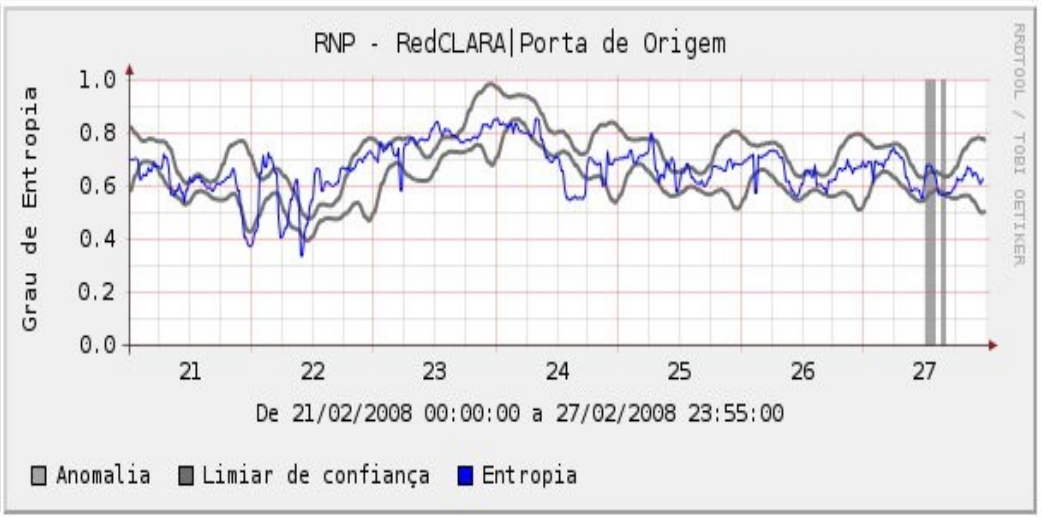


Resultados obtidos

Peering RNP / Rede Clara:







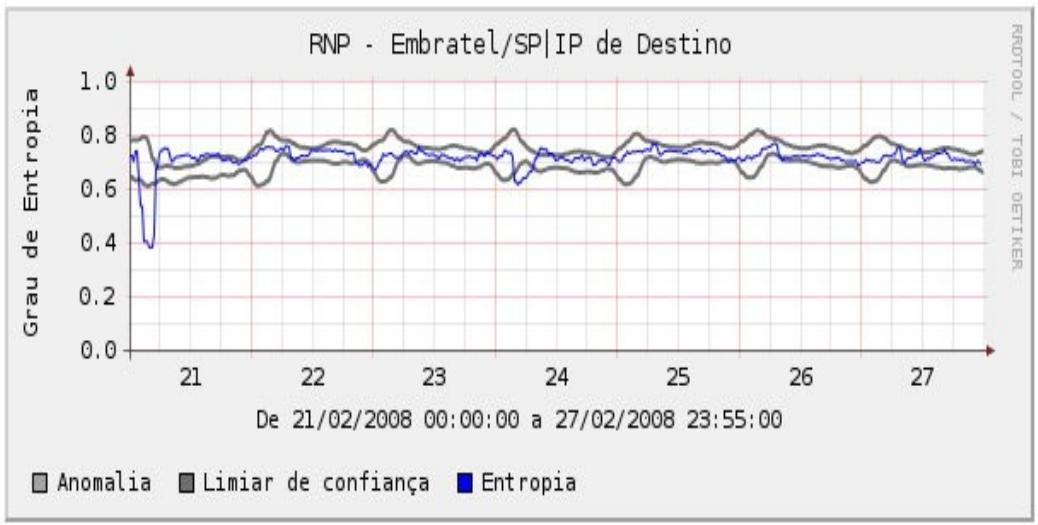
Resultados obtidos

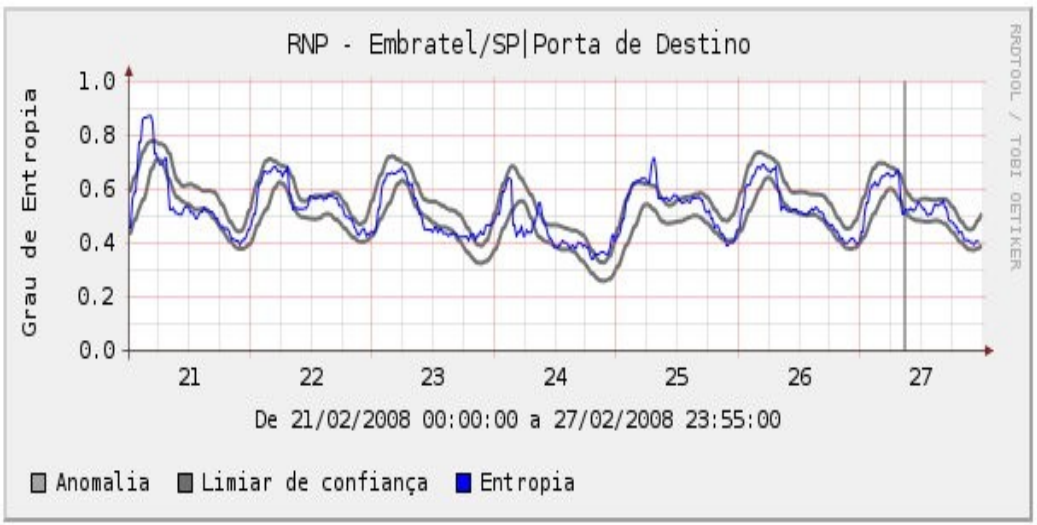
Peering Rede Clara: várias possibilidades

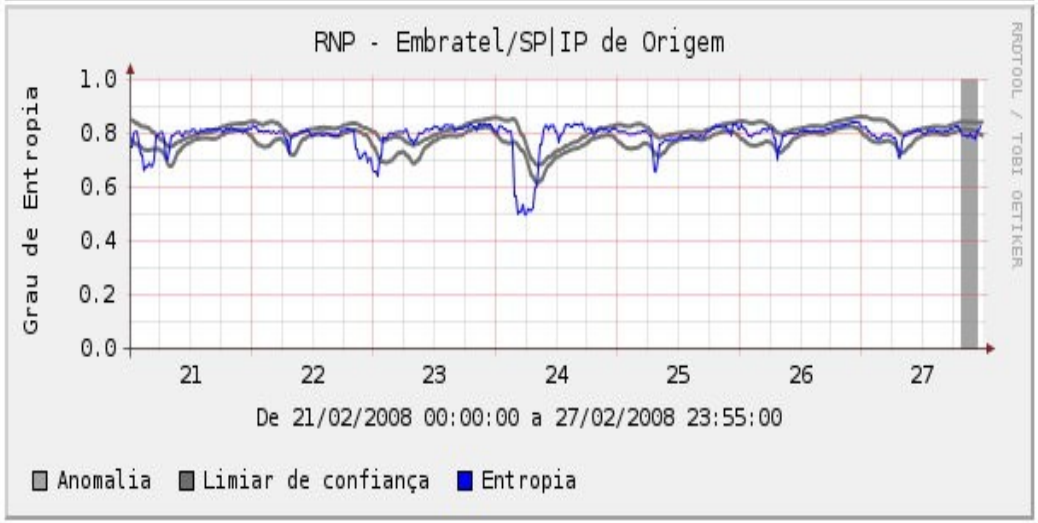
- Portscan dia 22 às 00hs, 06hs e 10hs
- Worm scan dia 23 às 06hs
- DoS dia 23 às 12hs
- DDoS dia 24 às 15hs

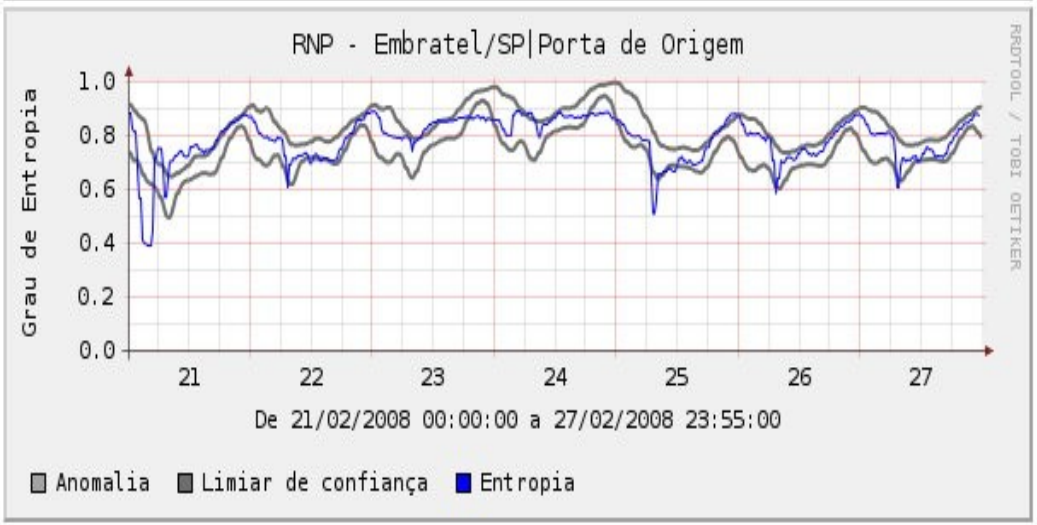
Resultados obtidos

Peering RNP / Embratel:









Resultados obtidos

Peering RNP / Embratel: Indícios de ataques

- Portscan dia 21 às 03hs
- Ataque de origem única p/ rede de destino explorando porta vulnerável, dia 24 às 06hs
- Portscan conjugado com varredura de rede, dia 25 às 07hs

Conclusões e trabalhos futuros

Conclusões e trabalhos futuros

- Trabalho propõe uso de análise de entropia combinado com estimativa de Holt-Winters para detecção de anomalias
  - Aspecto prático: método potencializa uso de ferramentas abertas de gerência a partir de bases RRD (RRDtool, Cacti, etc)
  - Foco principal: **sinalizar anomalias**, em especial ameaças contra a segurança

Conclusões e trabalhos futuros

- Resultados ainda parciais, trabalho em andamento
- Análise prejudicada: ausência de reportes de incidentes durante testes
- Planejamento
  - Inserções artificiais de anomalias em fluxos coletados (padrões reais), novas amostras
  - Estudar sensibilidade do método aos parâmetros da estimativa de Holt-Winters
  - Refinar método e testar em produção

Referências principais

- Lakhina, A., Crovella, M., and Diot, C. (2005) “Mining anomalies using traffic feature distributions”, *Proceedings of the ACM SIGCOMM'2005*, Philadelphia, PA, USA
- Brutlag, J. D. (2000) “Aberrant Behavior Detection in Time Series for Network Monitoring”, *Proceedings of the 14th Systems Administration Conference (LISA 2000)*.