UFRGS

Grupo de Trabalho em Segurança – GTS2007

Um IDS utilizando SNMP e Lógica Difusa

Apresentador: Émerson Virti

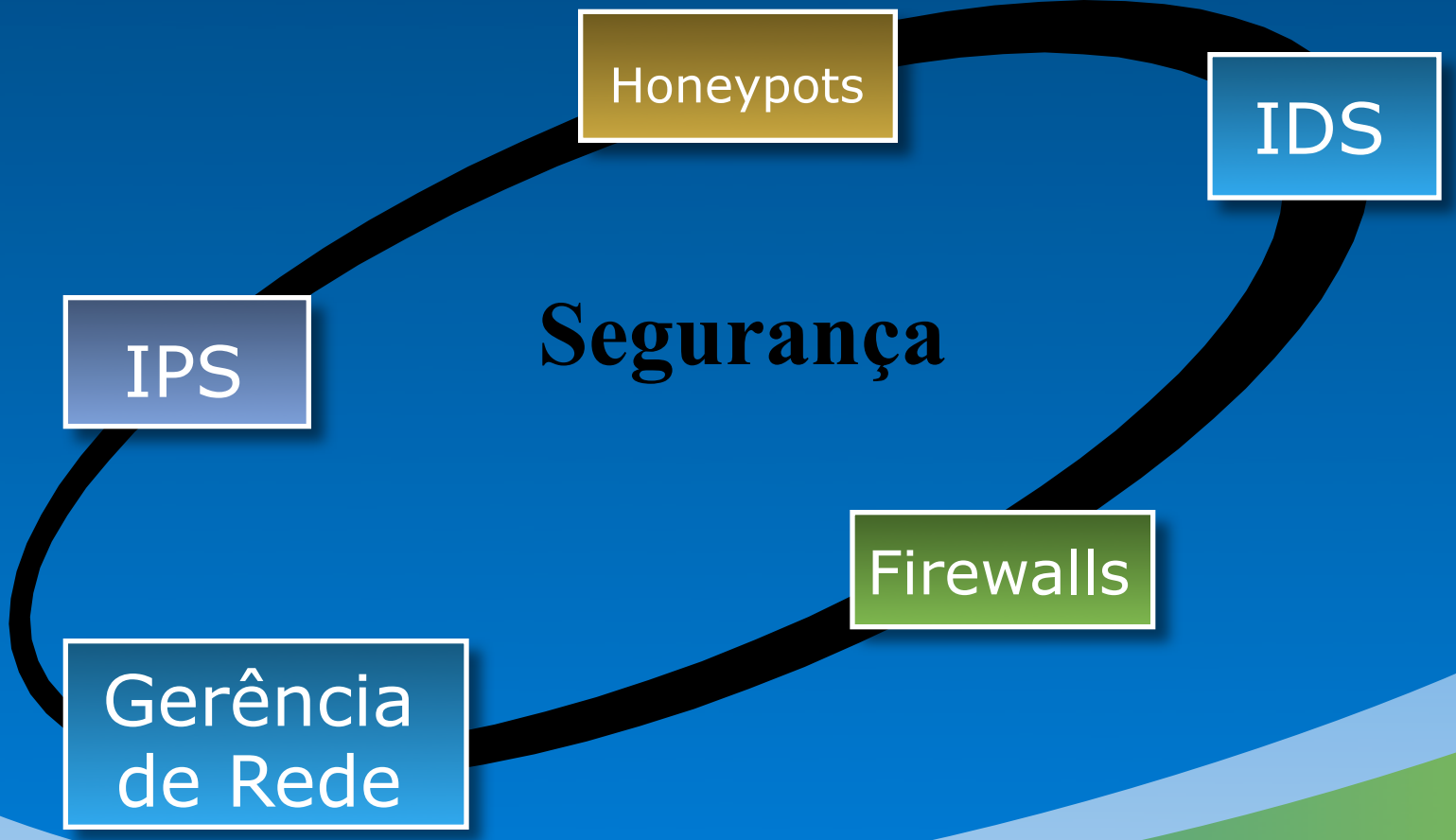
Autores: Émerson Virti, Liane Tarouco

Índice

1. Motivação

- Situação da segurança:
  - Gastos mundiais com segurança foram de US$ 38 bilhões em 2006 (Convergência Digital)
- Necessidade de integração entre tecnologias de segurança e de rede.
  - Diminuição de custos;
  - Aproveitamento de recursos;

1. Cooperação



2. IDS - Classificação

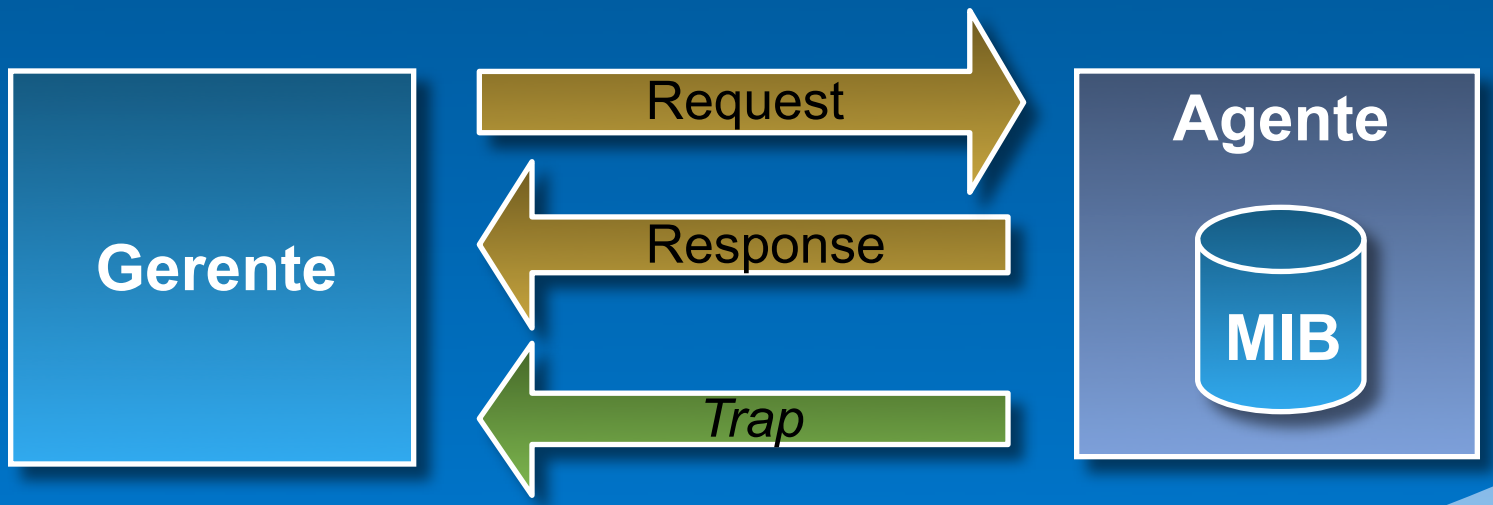
- Local de captura
  - IDS de rede x IDS de host
  - IDS proporto: rede
- Forma de detecção
  - Por anomalia x por assinatura
  - IDS proposto: híbrido

2. IDS - Problemas

- Problemas peculiares aos IDSs:
  - Número elevado de falsos-positivos e falsos-negativos;
  - Complexidade das extruturas dos IDSs;
  - Exigência de alta capacidade de processamento;
  - Consumo excedente de banda direcionada a atividade de monitoramento.

2. SNMP

- **SNMP:** ***Simple Network Management Protocol***
  - **Problemas de segurança (V1 e V2)**



2. MIBs RMON

- **MIBs para moritoramento remoto:**
  - **RMON1 RFC1757**
  - **RMON2 RFC2021**

2. RMON - Peculiaridades

- Implementam também os grupos *system* e *interfaces* da MIB-II.
- Se implementa um grupo, tem de fazê-lo de forma completa.
- Application Layer: camadas superiores ao nível de rede.

2. RMON2 – Alguns Grupos

- ***protocolDir***: informações sobre os protocolos suportados;
  - ***protocolDist***: tráfego em octetos e pacotes por protocolo suportado;
    - ***addressMap***: faz a relação entre MAC e IP;
- ***nlHostTable***: tráfego em octetos e pacotes (entrada e saída) por endereço de rede.
  - ***nlMatrix***: tráfego em octetos e pacotes (entrada e saída) por par IP fonte e destino;
  - ***alHost***: estatísticas de tráfego em pacotes e octetos de entrada e saida por um dado protocolo (configurável) por host;
- ***alMatrix***: tráfego em octetos e pacotes por endereço IP;

2. Ferramentas RMON

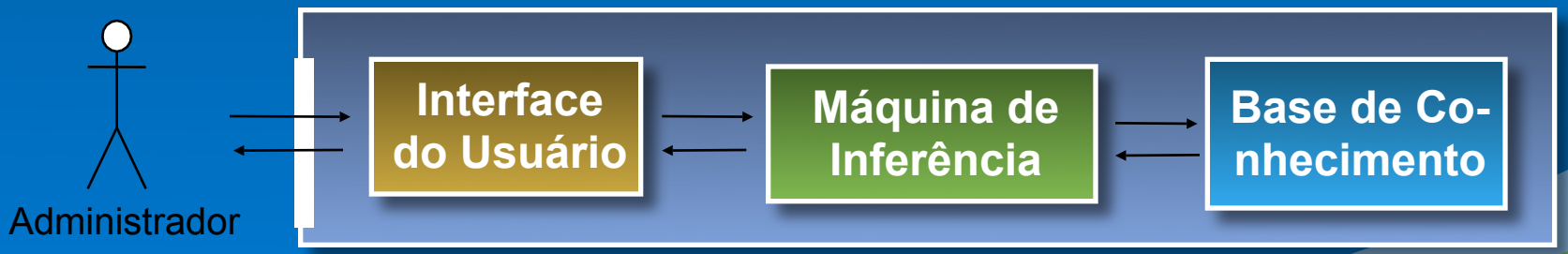
- Agentes:
  - Em dispositivos (RMON1 e RMON2)
    - Cisco, 3COM…
  - Linux (RMON 2)
    - http://rnsanchez.wait4.org/Trace/rmon2.php (Unisinos)
  - Windows (RMON1 e RMON2)
    - Rmonster
  - A questão da performance.

2. Inteligência Artificial e IDS

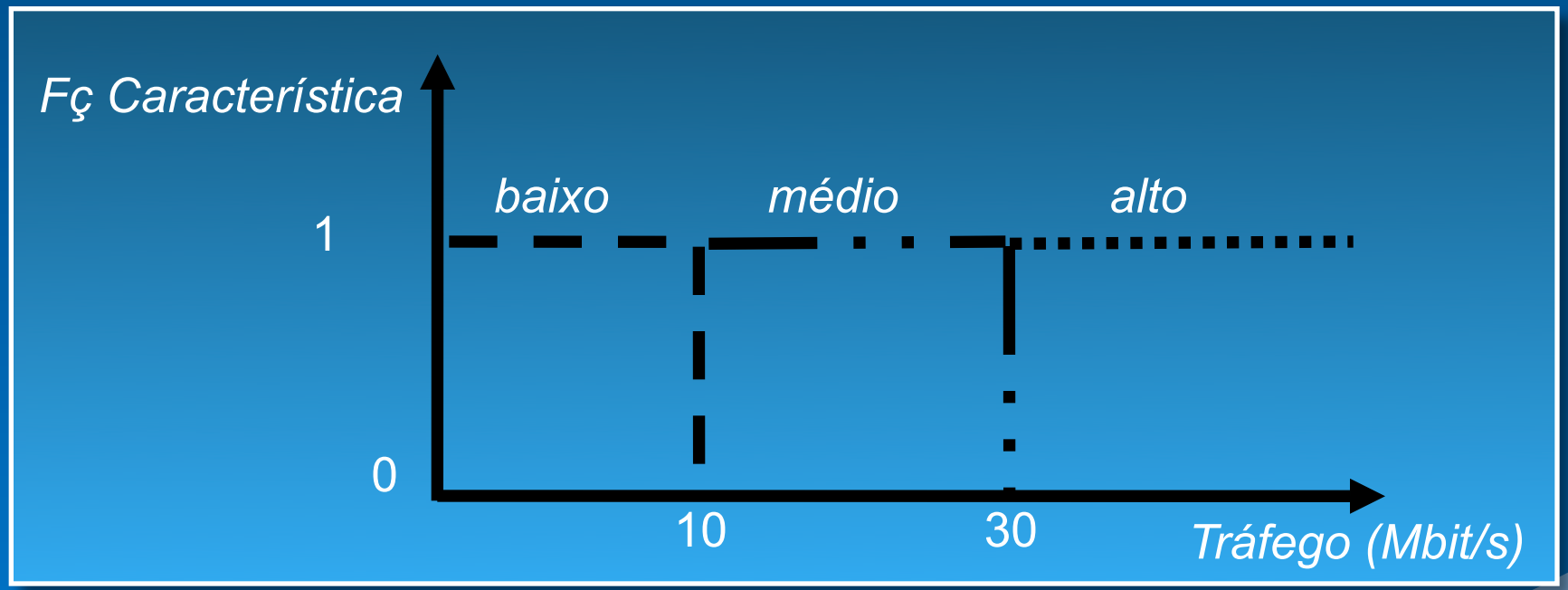
- Sistemas que utilizam Redes Neurais
- Sistemas com algoritmos genéticos
- Sistemas com lógica difusa (*Fuzzy*)
  - Adequação à natureza relativa e imprecisa dos dados provenientes de monitoramentos em redes em operação.
    - Sistemas de classificação *Fuzzy [3][4]*
    - Sistemas de inferência Fuzzy [1][2]

2. Sistemas Fuzzy

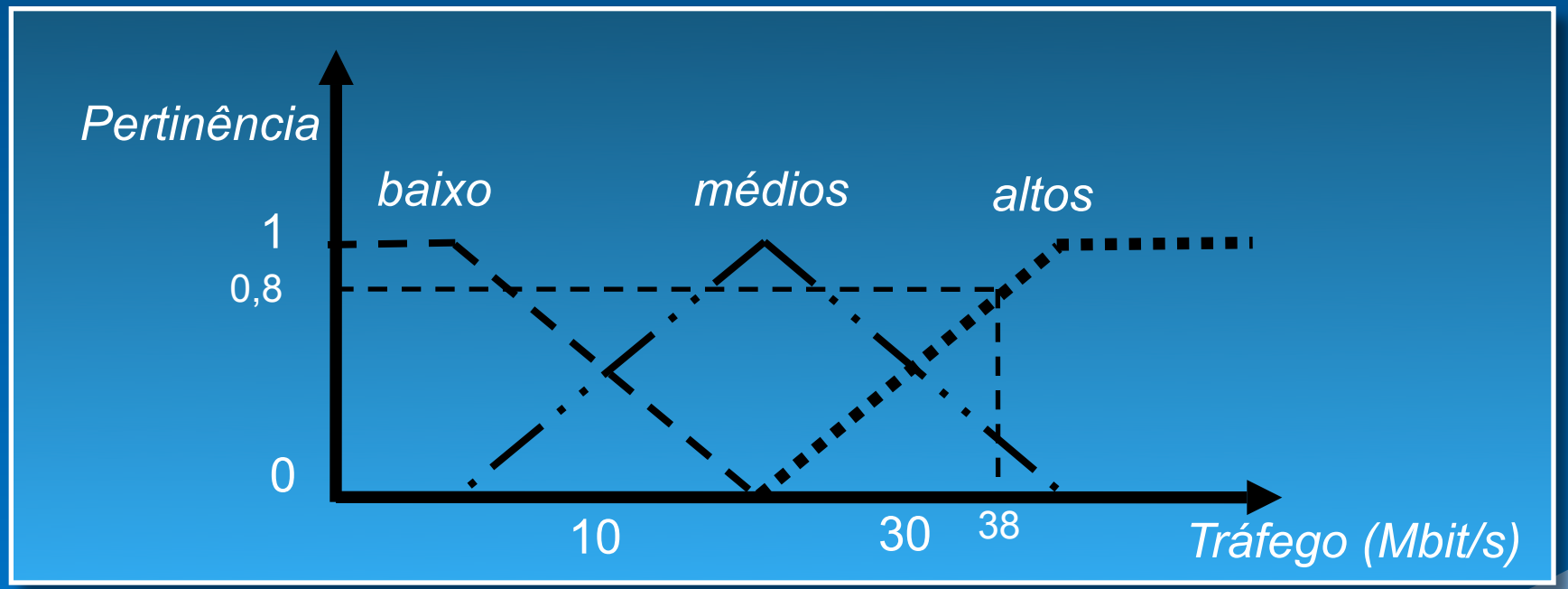
- Sistemas de lógica difusa (nebulosa)
  - Sistemas baseados em regras
  - Máquina de inferência *Fuzzy*



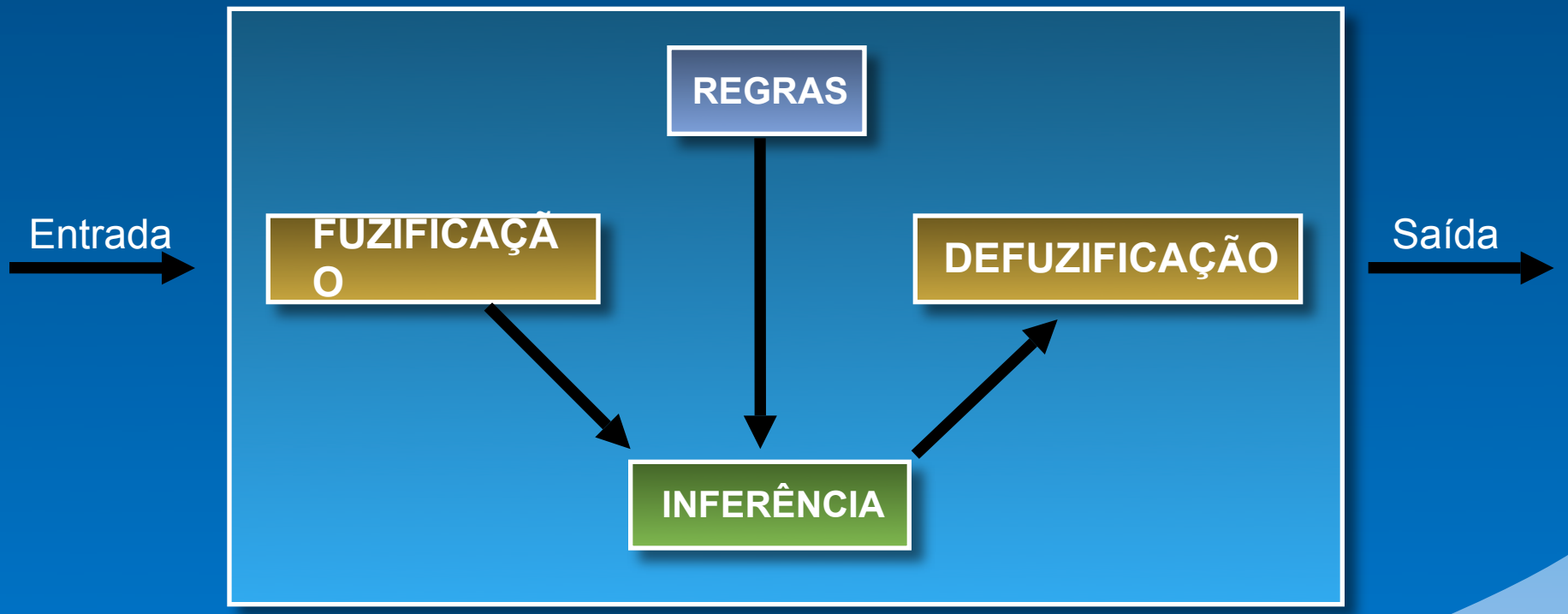
2.Pertinência – Conjuntos Crisp



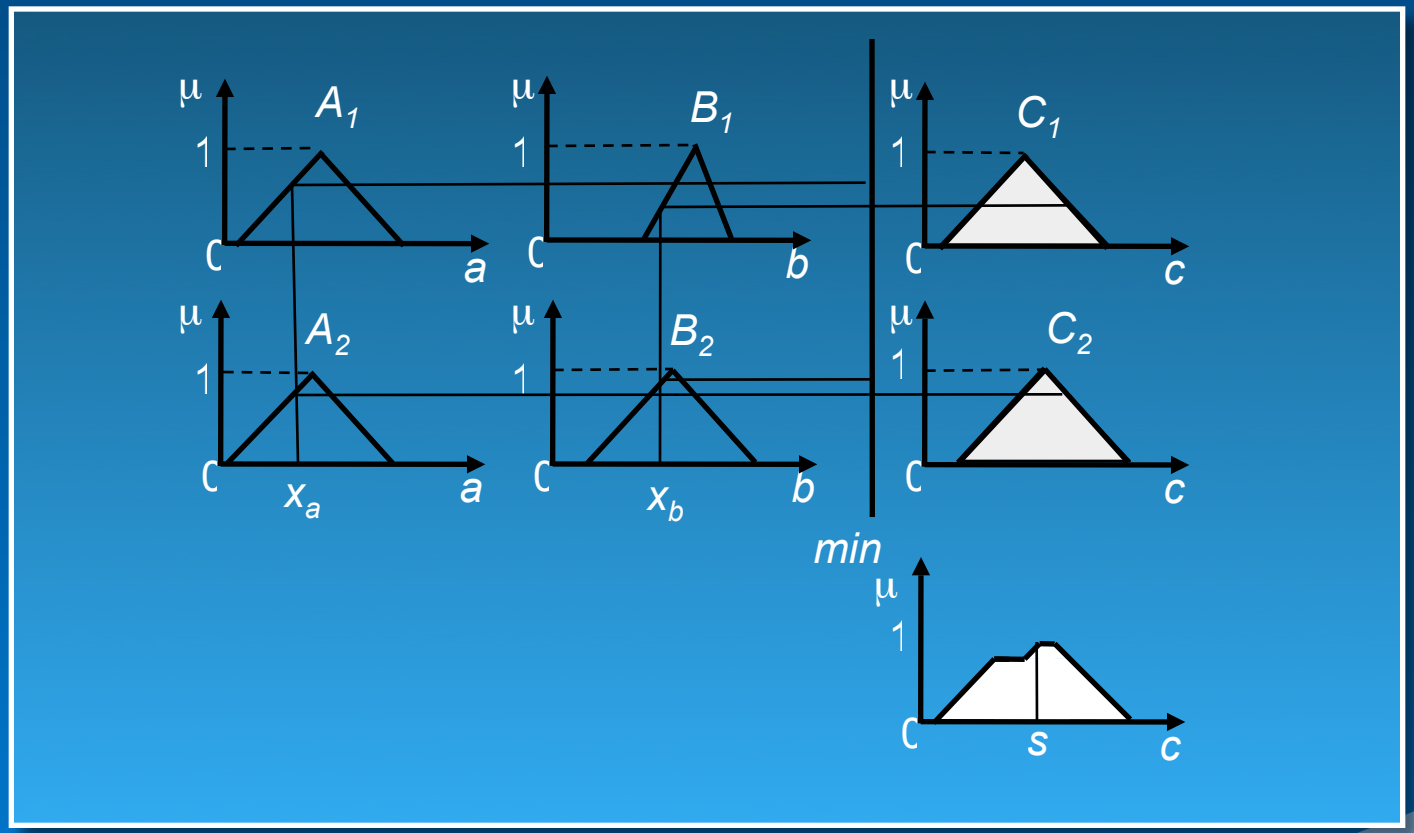
2. Pertinência – Conjuntos Fuzzy



2. Sistemas Fuzzy

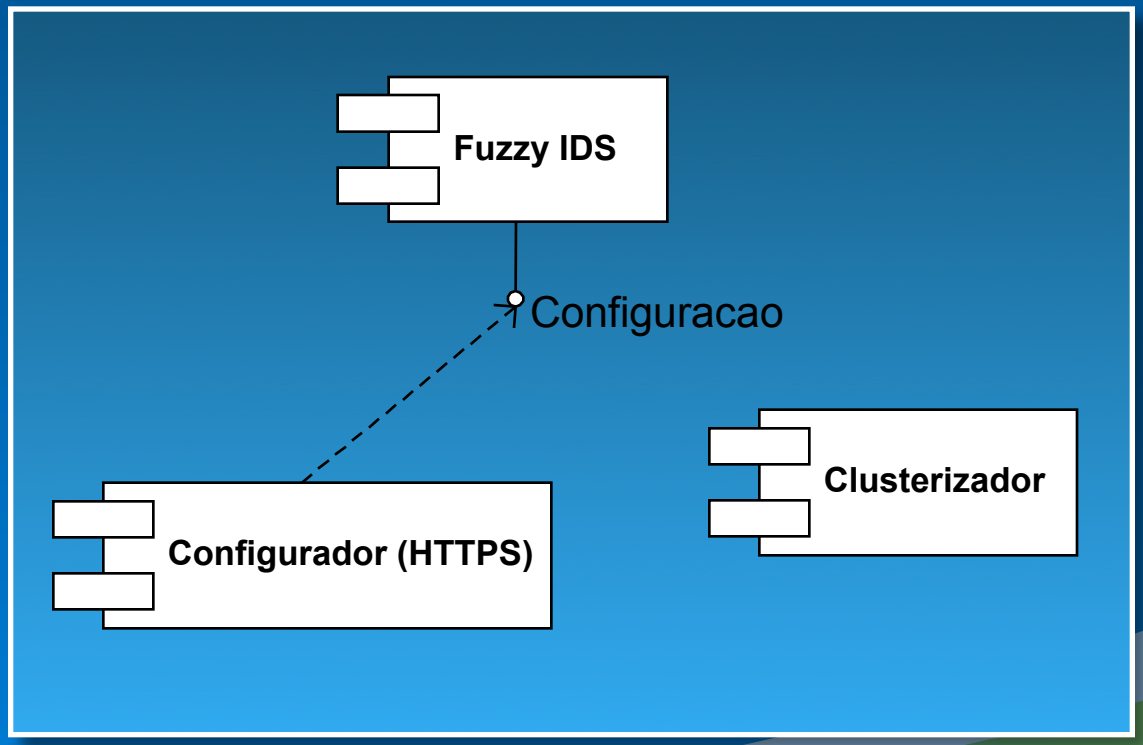


2. Método de Mamdani



3. IDS Proposto

Elementos do IDS proposto:



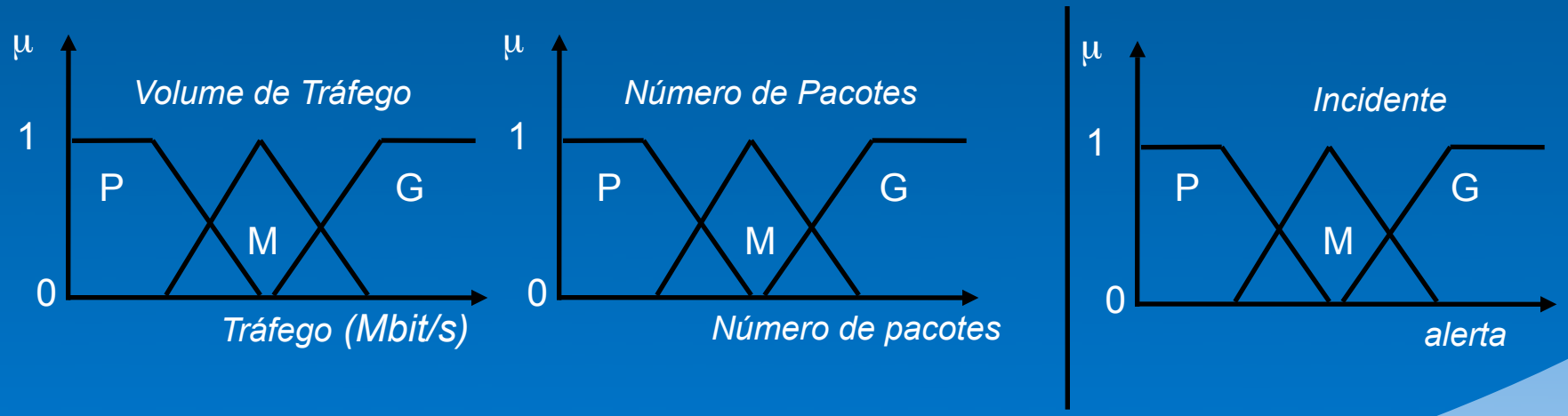
3. IDS Proposto - Funcionamento

1. Definir os objetos a serem monitorados;
2. Definir a forma das variáveis linguísticas;
3. Definir as regras de inferência.

3. Regras

Exemplo: Para uma dada rede,

Se tráfego é pequeno e núm pacotes é alto então alerta é grande



3. Dificuldades

Definição dos OIDs Monitorados	Variáveis Linguísticas	Regras
Dificuldade em definir quais os objetos a serem monitorados.	**Arbitrar o comportamento das variáveis é uma provável chance de erro.**	A criação das regras exige conhecimento profundo da rede monitorada

3. Possíveis Soluções

- Definição de um agregado inicial de OIDs monitorados?
  - Retira do administrador de segurança a necessidade de conhecer plenamente o funcionamento das suas redes;
  - Transfere ao desenvolvedor a tarefa de adequar as regras ao ambiente monitorado.
- Definicão de um escopo inicial de regras?
  - Retira do administrador de segurança a necessidade de conhecer plenamente o funcionamento das suas redes;
  - Transfere ao desenvolvedor a tarefa de adequar as regras ao ambiente monitorado.

3. Possíveis Soluções

- Geração de regras Fuzzy de forma automática por redes neurais.
  - Necessidade de separar comportamento normal x comportamento anormal [5].
- Auxiliar a criação dos gráficos das variáveis linguísticas
  - Através da captura do histórico da rede monitorada, é possível criar gráficos das variáveis linguiísticas através de métodos de *CLUSTERIZAÇÃO.*

3.Clusterização: Fuzzy Cmeans

- Uma forma de melhorar a precisão dos resultados do IDS através da utilização do histórico dos objetos monitorados

1. Armazenar o histórico dos objetos monitorados

1. Processar os dados obtidos e, utilizando o método de clusterização fuzzy cmeans, criar gráficos de variáveis linguísticas que melhor se adaptem ao comportamento real da rede monitorada.

3. Fuzzy Cmeans - Algoritmo

- Dados os $v_1, v_2 \ldots v_i$ centros do cluster, o índice de fuzificação m e a condição de parada ϵ.

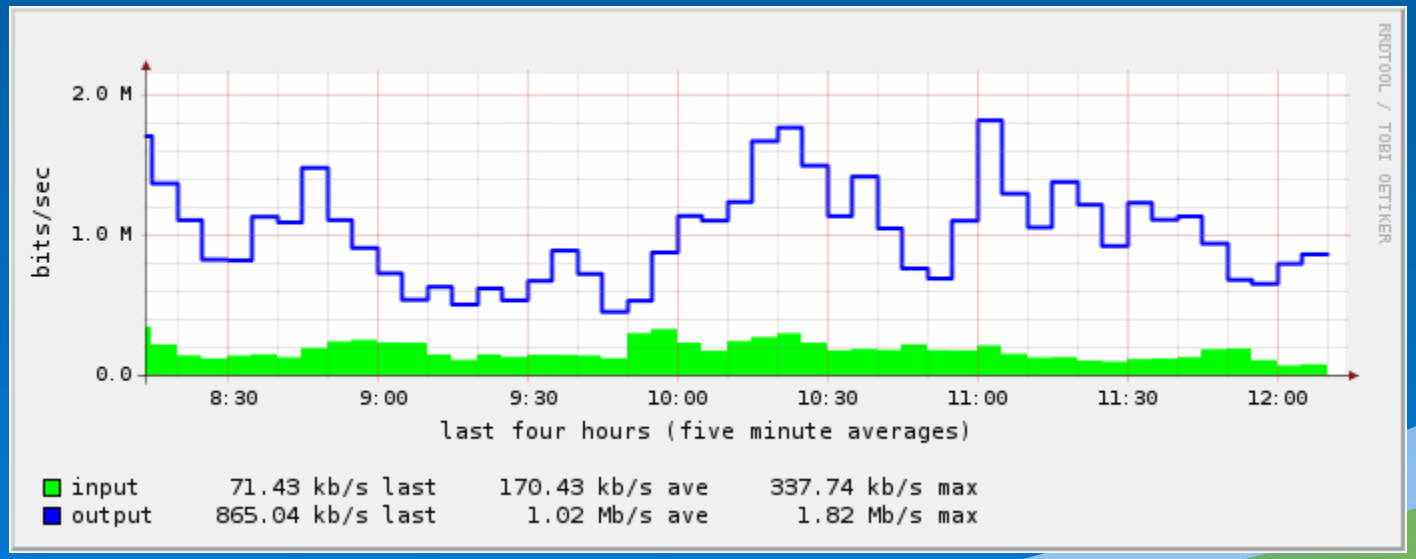
$$\varepsilon < \max \left| A_i^{(t+1)}(x_k) - A_i^{(t)}(x_k) \right|$$

$$v_i = \frac{\sum_{k=1}^{n} [A_i(x_k)]^m x_k}{\sum_{k=1}^{n} [A_i(x_k)]^m}$$

$$A_i^{(t+1)}(x_k) = \left[\sum_{j=1}^{c} \left(\frac{\left| x_k - v_i^{(t)} \right|^2}{\left| x_k - v_j^{(t)} \right|^2} \right)^{\frac{1}{m-1}} \right]^{-1}$$

4. Testes

- Realizados através do espelhamento do tráfego de uma pequena rede ligada ao Ponto de Presença da Rede Nacional de Ensino e Pesquisa – POP-RS/RNP
- Utilizado o agente RMON2 produzido pela equipe na Unisinos.



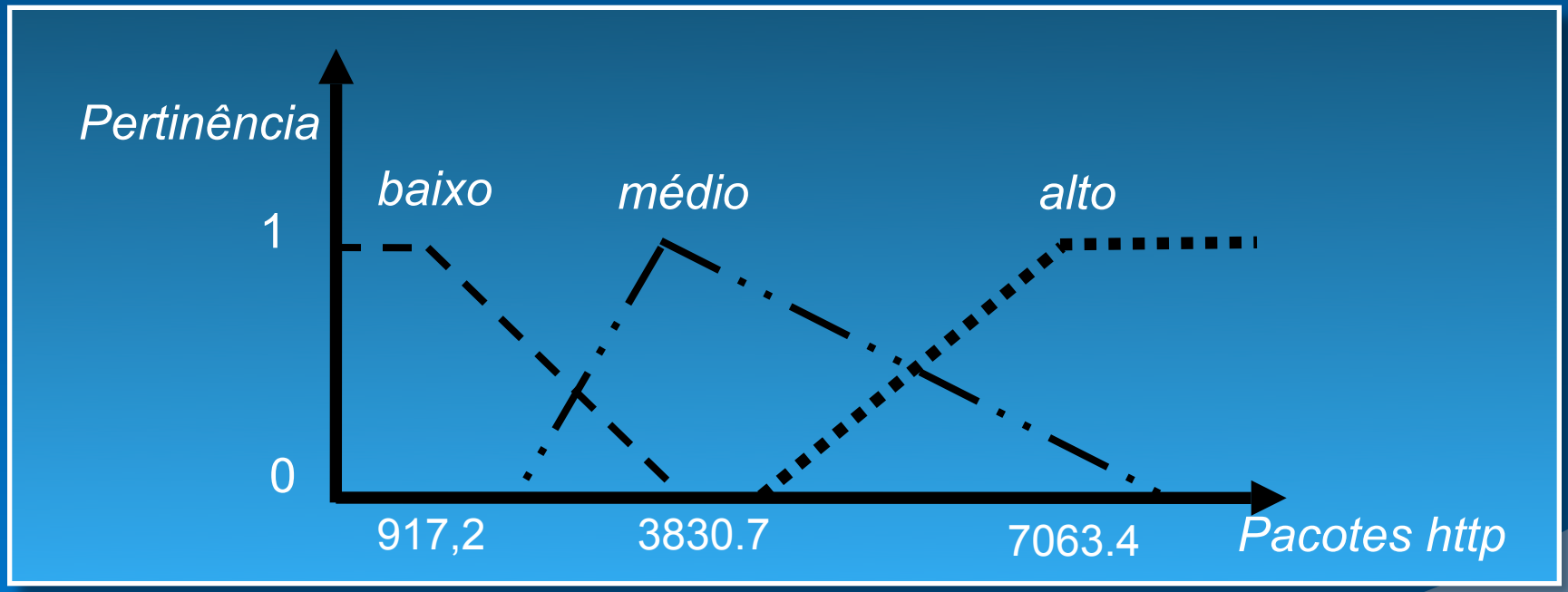
4. Aplicação do Cmeans

- **Estatísticas referentes a aplicação do Cmeans ao tráfego http.**

Tempo de Captura	1 semana
Número de pontos	20160
Intervalo de Polling	30 s

4. Aplicação do Cmeans

- **Gráfico resultante:**



4. Criação das Regras

- Criação das regras por funcionalidade exercida por cada sistema monitorado:

- **Sistema de e-mail:**
  - **se *octetos-in* é alto e *octeto-out* é baixo então *alerta* é alto**
  - **se *pacotes-ftp* é alto e *pacotes-http* é alto então *alerta* é baixo**
- **Servidor web:**
  - **se *pacotes-in-p80* é alto e *pacotes-out-80* é baixo então *alerta* é alto**
  - **se *pacotes-out-outras-portas* é alto então *alerta* é alto**
- **Firewall:**
  - **se *pacotes-in* é alto então *alerta* é alto**

5. Conclusões

- Eficiente forma de integrar e melhor aproveitar recursos de gerência e segurança;
- Eficaz método para verificar comportamentos anômalos;
- Possibilidade de colocar probes RMON2 em redes vitais à segurança da rede privada;
- Possibilidade de adaptar o IDS ao monitoramento detalhado da rede;
- Necessidade de uma administrador com bom nível de conhecimento sobre a operação da rede para a criação das regras iniciais.

5. Trabalhos Futuros

- Estudo e implementação de formas de criação automatizada de regras para a diferenciação entre o comportamento normal e anormal.

References

• [1] DICKERSON, J. E.; DICKERSON, J. A. Fuzzy Network Profiling for Intrusion Detection. FUZZY INFORMATION PROCESSING SOCIETY, 19, 2000, Atlanta. **Proceedings...** [S.l]: IEEE, 2000, p. 301-306.

• [2] SILVEIRA, E. R.; DANTAS, M. A. R. **Uma Abordagem de Monitoração de Tráfego de Rede Utilizando Lógica Difusa**. Infocomp: The Journal of Computer Science, 2004, [S.l]. p. 32-41.

• [3] MILL, J., INOUE, A. Support Vector Classifiers and Network Intrusion Detection. In: IEEE INTERNATIONAL CONFERENCE ON FUZZY SYSTEMS, Budapest. 2004. **Proceedings…** Budapest: IEEE, 2004. p. 25-29.

• [4] GOMEZ, J., DASGUPTA, D. Evolving Fuzzy Classifiers for Intrusion Detection. In: WORKSHOP ON INFORMATION ASSURANCE, 2001, New York. **Proceedings…** [S.l]: IEEE, 2002, p. 68-75.

• [5] GOMEZ, J et al. Complete Expression Trees for Evolving Fuzzy Classifier Systems with Genetic Algorithms to Network Intrusion Detection. In: FUZZY INFORMATION PROCESSING SOCIETY, NAFIPS, 2002, [S.l]. **Proceedings…** [S.l]: IEEE, 2002, p. 469-474.

Agradecimentos

- Equipe do POP-RS – Leandro Bertholdo e João Ceron
- Desenvolvedores do agente RMON2 Linux
- Equipe do Serpro – Regional Porto Alegre.

Questões?

Émerson Virti
emerson@tche.br

Universidade Federal do Rio Grande do Sul - UFRGS