UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

IMPLEMENTAÇÃO DO MÓDULO DE RETENÇÃO DA *EXPERTISE* GERENCIAL (MREG) ATRAVÉS DE *TROUBLE TICKET* NO SISTEMA INTEGRADO DE MONITORAMENTO DE REDES (S.I.M.)

TRABALHO DE GRADUAÇÃO

Henrique Sobroza Pedroso

Santa Maria, RS, Brasil

2012

IMPLEMENTAÇÃO DO MÓDULO DE RETENÇÃO DA EXPERTISE GERENCIAL (MREG) ATRAVÉS DE TROUBLE TICKET NO SISTEMA INTEGRADO DE MONITORAMENTO DE REDES (S.I.M.)

por

Henrique Sobroza Pedroso

Trabalho de Graduação apresentado ao Curso de Ciência da Computação da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de
Bacharel em Ciência da Computação

Orientador: Profª. Drª. Roseclea Duarte Medina

Santa Maria, RS, Brasil

2012

Universidade Federal de Santa Maria
Centro de Tecnologia
Curso de Ciência da Computação

A Comissão Examinadora, abaixo assinada,
aprova o Trabalho de Graduação

IMPLEMENTAÇÃO DO MÓDULO DE RETENÇÃO DA EXPERTISE GERENCIAL (MREG) ATRAVÉS TROUBLE TICKET NO SISTEMA INTEGRADO DE MONITORAMENTO DE REDES (S.I.M.)

elaborado por
Henrique Sobroza Pedroso

como requisito parcial para obtenção do grau de
Bacharel em Ciência da Computação

COMISSÃO EXAMINADORA:

Roseclea Duarte Mediana, Dra.
(Presidente/Orientador)

Benhur de Oliveira Stein, Dr. (UFSM)

Juliana Kaizer Vizzotto, Dra. (UFSM)

Santa Maria, 04 de junho de 2012.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais, Inocencio Rodrigues Pedroso e Teresinha Elsa Sobroza Pedroso, pelo apoio, incentivo e carinho prestados e por sempre acreditar em meu sucesso e nas minhas decisões.

A minha família, pela amizade e carinho, em especial ao meu irmão Inocencio Sobroza Pedroso (*in memoriam*), que sempre serviu de inspiração de irmão, profissional e pessoa.

A UFSM, pelo ensino gratuito e de qualidade.

A professora Roseclea Duarte Medina, pela paciência, ensinamentos e orientação realizada no TG.

Aos membros da banca, Benhur de Oliveira Stein, Juliana Kaizer Vizzotto, e suplente ,Oni Reasilvia de Almeida Oliveira Sichonany, pela leitura e contribuições ao trabalho desenvolvido.

Ao corpo docente do Curso de Ciência da Computação, pela dedicação ao ensino.

À minha namorada Andreise Moreira, pelo carinho, paciência e apoio prestados nos momentos de decisivos.

Aos colegas do GRECA pela amizade e companheirismo.

EPÍGRAFE

“Os computadores são incrivelmente rápidos, precisos e burros;
os homens são incrivelmente lentos, imprecisos e brilhantes;
juntos, seus poderes ultrapassam os limites da imaginação.”
Albert Einstein

RESUMO

Trabalho de Graduação
Curso de Ciência da Computação
Universidade Federal de Santa Maria

IMPLEMENTAÇÃO DO MÓDULO DE RETENÇÃO DA EXPERTISE GERENCIAL (MREG) ATRAVÉS TROUBLE TICKET NO SISTEMA INTEGRADO DE MONITORAMENTO DE REDES (S.I.M.)

AUTOR: HENRIQUE SOBROZA PEDROSO
ORIENTADOR: ROSECLEA DUARTE MEDINA
Data e Local da Defesa: Santa Maria, 04 de junho de 2012.

Com a finalidade de manter o ambiente computacional estável e sobre controle do gestor é necessário utilizar ferramentas para auxiliar a coleta de dados e aplicar um plano de tomada de decisão para obter uma rápida resposta a incidentes sob suspeita ou confirmadas, como ataques, instabilidades e indisponibilidades. Com as ferramentas de monitoramento é possível obter um maior entendimento sobre a rede, tanto de seu funcionamento, como a desvios comportamentais ocorridos. Com a finalidade de auxiliar o gestor na tarefa de solucionar tais problemas, o Grupo de Redes e Computação Aplicada da Universidade Federal de Santa Maria (GRECA/UFSM) estudam ferramentas existentes e desenvolvem o Sistema Integrado de Monitoramento (S.I.M.). Este é um aplicativo que integra e correlaciona à saída de alertas dos monitores de redes, deste modo gera bilhetes automáticos que são mostrados em uma única interface, facilitando a interpretação de possíveis incidentes ocorridos. Para que esta ferramenta possa auxiliar o gerente a obter a solução em tempo reduzido, tem-se como finalidade desenvolver e integrar o Módulo de Retenção de Expertise Gerencial (MREG). Este módulo destina-se a reter uma parte da *expertise* gerencial, criando uma base de informação (agregando às causas do incidente a descrição textual de como o gestor o solucionou). Neste contexto o S.I.M. buscará na base, as soluções relacionadas ao incidente detectado e tornará possível a visualização das tomadas de decisões. Assim o gestor pode fundamentar-se em ocorrências passadas, tornando mais eficiente e pontual a ação do gerente, objetivando eliminar os falsos positivos e buscando reduzir a demora no atendimento.

Palavras-chave: Gerencia de redes, MREG, Sistema de monitoramento, base de informação, S.I.M.

ABSTRACT

Trabalho de Graduação
Undergraduate Program in Computer Science
Universidade Federal de Santa Maria

IMPLEMENTATION MODULE FOR RETENTION OF EXPERTISE MANAGEMENT (MREG) THROUGH TROUBLE TICKET IN INTEGRATED NETWORK MONITORING (S.I.M.)

AUTHOR: HENRIQUE SOBROZA PEDROSO
ADVISOR: ROSECLEA DUARTE MEDINA

In order to keep the computing environment stable and under control manager tools are required to assist in data collection and implement a plan for decision making for rapid response to suspected or confirmed incidents, such as attacks, instability and outages . With monitoring tools you can get a better understanding of the network, both for its operation, as the deviant occurred. In order to assist the manager in the task of solving such problems, the Group and Network Applied Computing, Federal University of Santa Maria (GRECA / UFSM) study existing tools and develop the Integrated Monitoring (SIM). This is an application that integrates and correlates the alerts output monitors network thus generates automatic tickets that are displayed in a single interface, facilitating the interpretation of possible incidents. For this tool can assist the manager to get the solution in a short time, has as purpose to develop and integrate the module retention Expertise Management (MREG). This module is intended to retain part of the expertise management, creating an information base (aggregating the causes of the incident textual description of how the manager solved). In this context the S.I.M. search the base, the solutions related to the incident detected and make possible the visualization of decision making. So the manager can be based on past occurrences, making it more efficient and timely action manager, aiming to eliminate false positives and reduce the delay in seeking care.

Keywords: Manages network, system monitoring, information base.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

CC	*Cluster Controller*
CLC	*Cloud Controller*
GRECA	Grupo de Redes e Computação Aplicada
ICMP	Internet Control Message Protocol
ISO	International Organization for Standardization
MREG	Módulo de Retenção de Expertise Gerencial
NAT	Network Address Translation
NC	*Node Controller*
OSI	Open Systems Interconnection
PoP	Ponto Operacional de Presença
SC	*Storage Controller*
SGDB	Sistema Gerenciador de Banco de Dados
S.I.M.	Sistema Integrado de Monitoramento
QoS	Quality of Service
RNP	Rede Nacional de Pesquisa
TI	Tecnologia da Informação
UFSM	Universidade Federal de Santa Maria
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WS3	*Walrus Storage Controller*

SUMÁRIO

INTRODUÇÃO

Com o advento da interconexão entre computadores, um novo ambiente de troca de informações se formou criando a necessidade de comunicação, a automatização e disponibilização de aplicações para a difusão em larga escala de serviços. Juntamente as demandas criadas através das novas necessidades de comunicação pelos usuários, cresceram as exigências de ter-se o controle sobre o ambiente interligado, com seus meios e processos. Esta gerência visa à disponibilidade em tempo integral dos serviços, evitando indisponibilidades temporárias ou totais, bem como rápida detecção e solução de algum problema que venha ocorrer. Portanto, coletar dados com a finalidade de prever anomalias, como falhas e ataques são de fundamental importância para gerir tais ambientes computacionais. Para tanto, são utilizados sistemas de monitoramento para detectar e definir um plano de ação/reação.

Em redes computacionais de pequeno e médio porte, com poucos ativos e geograficamente centralizados ou pouco esparsos, normalmente são pesquisadas soluções que se utilizem de código aberto com a finalidade de redução de custos e possibilidade de personalização para as devidas necessidades. Tendo esta ideia central, sistemas como SNORT (SNORT, 2012), NTOP (NTOP, 2012), NAGIOS (NAGIOS, 2012), CACTI (CACTI, 2012) são largamente utilizados atingindo assim, os objetivos a que se dispõe.

No gerenciamento de redes de grande porte, normalmente distribuídas geograficamente e heterogêneas, um software de monitoramento é adequado e extremamente necessário. Os grandes produtos comerciais, como o IBM Tivoli (IBM, 2012) ou o HP System Mananger (HP, 2012) aperfeiçoam este trabalho, mas eles não são abertos ou de baixo custo, além de possuírem uma complexidade de uso, o que pode gerar algum trabalho extra caso seja necessário ajustá-los às suas necessidades (SEIFRIED, 2011).

Para estes ajustes, utilizando ferramentas livres ou não, é necessário que o gerente de rede com sua experiência e técnicas capacitadas torne os sistemas de monitoramento eficientes para desenvolver suas tarefas. Após isto, as ferramentas geram alertas com a finalidade de informar o administrador sobre possíveis

problemas ocorridos na rede e armazenam em uma base de dados para uma possível pesquisa ou auditoria.

Um dos grandes problemas das equipes de TI refere-se à formação e experiência dos técnicos envolvidos no processo. Na área computacional, é muito frequente a migração destes profissionais para outras empresas, afetando diretamente a "*expertise*" da equipe quando ocorre à saída de profissionais aptos/especialistas.

Com a finalidade de integrar diferentes interfaces de aplicativos de monitoramento de rede de código aberto, o Grupo de Redes e Computação Aplicada (GRECA) da Universidade Federal de Santa Maria (UFSM) desenvolveu o Sistema Integrado de Monitoramento (S.I.M.). Este programa tem como objetivo facilitar a análise por parte do administrador de redes, reduzindo os falsos positivos através da comparação dos alertas dos sistemas de monitoramentos e mostrando todos os dados em uma interface unificada.

Com a utilização do sistema denominado S.I.M., identificou-se a necessidade de documentar as soluções tomadas para prover um repositório de resoluções aos possíveis incidentes detectados. Deste modo tem-se como justificativas deste trabalho tentar reduzir a perda de conhecimento devido à troca de gerência ou equipe de TI. Outro ponto a ser abordado refere-se na aquisição de conhecimento quando existe uma equipe TI com diferentes níveis tecnicidade, tornando o S.I.M. um meio de transferência de conhecimento entre um gestor Sênior e um administrador Júnior.

Para possibilitar o objetivo central de transferir parte do conhecimento gerencial para o Sistema Integrado de Monitoramento, este trabalho de graduação tem como objetivo desenvolver um módulo para a integração ao S.I.M. com a finalidade de reter parte da *expertise* gerencial e propor estas soluções na interface. Para isto, tem-se como objetivos específicos:

- Criar uma base de informação;
- Tornar o aplicativo capaz de relacionar eventos;
- Reduzir o tempo de respostas aos incidentes.

1 REVISÃO BIBLIOGRÁFICA

1.1 Gerência de Redes de Computadores

O papel de gerenciar redes compõe uma área fundamental para o bom funcionamento e disponibilidade do meio e serviços, sendo assim, devem-se tomar atitudes para manter este ambiente favorável, evitando possíveis problemas gerados por agentes anômalos ou falhas. Deste modo, Saydam e Magedanz (1996) definem que o administrador de rede é o agente capaz de gerir o fornecimento, a integração e a coordenação de elementos de hardware, software e humanos, tendo como foco satisfazer as exigências operacionais de desempenho e de qualidade de serviço em tempo real e a um custo razoável.

Para facilitar, segmentar e organizar esta tarefa, a Organização Internacional para Padronização definiu no Modelo Básico de Referência (ISO, 1989) a divisão da gerência em cinco áreas funcionais: Gerência de Falhas, Gerência de Contabilidade, Gerência de Configuração, Gerência de Desempenho e Gerência de Segurança. A seguir tem-se a caracterização de cada uma destas, de acordo com ISO (1989):

1.1.1 Gerência de Falhas

Existe uma distinção entre a ocorrência de erros e falhas, mas a primeira pode suceder à segunda. Um erro é um processo pontual ou ocasional que pode ocorrer em um sistema, por exemplo, o envio de um pacote incorretamente. Mas, caso sucessivos erros ocorram, estes se tornam falhas, podendo ser de sistema, o qual pode comprometer parcial ou totalmente a comunicação. Outro exemplo refere-se à retransmissão de sinal, neste pode ocorrer distorções ocasionando erros temporários causando atrasos de retransmissão, por algumas vezes nem notados pelo usuário final. Por outro lado, caso o sistema de retransmissão seja incapaz de

realizar o mesmo, como uma queda de link, este se torna uma falha comprometendo o processo.

Para tanto, a partir da Gerência de Falhas tem-se definido proporcionar a detecção, isolamento e correção de eventos anômalos, transitórios ou permanentes, que podem intervir nos objetivos operacionais dos sistemas. A mesma pode ser dividida em cinco funções:

- Manter e examinar logs de erros;
- Aplicar e agir frente notificações de detecção de erros;
- Traçar e identificar falhas;
- Criar sequências de diagnósticos e testes;
- Solucionar falhas.

1.1.2 Gerência de Contabilidade

Possui como objetivo manter um monitoramento e informativos constantes sobre os custos e uso dos recursos da rede e de usuários com a finalidade de controlar a utilização do meio. Esta área possui as funções de:

- Informar os usuários sobre os custos, recursos consumidos e utilização consciente do ambiente disponibilizado;
- Definir e aplicar limites de utilização e custos de tarefas associadas aos recursos do usuário, evitando utilização excessiva de recursos tanto coletivamente como para a utilização pessoal;
- Habilitar custos combinados quando múltiplos recursos são invocados para atingir uma dada comunicação.

1.1.3 Gerência de Configuração

Possui o objetivo de gerir operações de inicialização da rede, habilitação ou desabilitação parcial ou total. Também, permite que o administrador de rede saiba

quais dispositivos fazem parte da rede administrada e quais suas configurações de hardware e software.

Com isto, pode-se definir como utilizar os recursos existentes, tanto de hardware e software que melhor se enquadra para a realização de uma tarefa, como a definição de poder de processamento de um servidor para realização de uma mesma tarefa ou configuração de equipamento de rede para transmissão de uma comunicação.

Esta capacidade de controlar e reconfigurar a rede possuem como objetivo de reação a falhas, desenvolver planos que possam melhorar o desempenho, corrigir problemas de segurança e atualização de tecnologias com a finalidade de atender a demanda requerida.

As tarefas desempenhadas podem ser divididas em:

- Definir parâmetros que controlem as rotinas de operação de sistemas abertos, como aplicar controle de fluxo entre comunicações;

- Definir objetos gerenciados e determinar nomes a estes, assim tomando conhecimento dos recursos disponíveis;

- Inicializar e finalizar objetos gerenciados, como rotas alternativas caso ocorra falhas de equipamentos;

- Coletar informações sob a demanda dos sistemas e suas condições;

- Estar ciente sobre mudanças significativas ocorridas nos sistemas;

- Possuir a capacidade de mudar configurações dos sistemas quando for requerido ou necessário.

1.1.4 Gerência de Desempenho

Quando se busca atender uma Qualidade de Serviço (QoS – *Quality of Service*) de recursos aos usuários, esta área de gerência demonstra-se fundamental. Nela são utilizadas ferramentas para a medição, definição de métricas e estudos que possam determinar níveis de desempenho.

Para esta tarefa são necessários coletas de dados para a identificação de problemas de gargalos de redes, como altas taxas de processamento em servidores e links congestionados. Assim são definidas coletas aleatórias seguindo regras

estatísticas possibilitando identificar a situação atual da rede.

Nesse contexto, as tarefas desta área de gerência são:

- Reunir informações estatísticas;

- Criar e examinar logs de histórico de desempenho de sistemas;

- Determinar desempenho de sistemas em condições naturais e artificiais;

- Definir modos de desempenho de sistemas.

1.1.5 Gerência de Segurança

A gerência de segurança prevê determinar mecanismos de segurança tanto no nível de rede, sistemas, aplicativos e dados. Para isto é necessário estabelecer uma política de segurança onde estejam definidos acessos às informações e a rede somente à usuários pertinentes evitando, assim, acessos indevidos.

Para isto são previstos as tarefas de:

- Gerenciar sistemas de permissão: criar, deletar e controlar acessos de usuários;

- Buscar e distribuir informativos de segurança, para evitar incidentes;

- Reportar eventos de segurança relevantes para os responsáveis, como medida de reduzir o escopo do impacto.

1.1.6 Estrutura da Gerência no modelo OSI

Para possibilitar estas metas gerenciais são necessárias ferramentas capazes de manter o administrador informado de tais ocorrências. Como explanado por Kurose e Roos (2006) são utilizados sistemas com a seguinte arquitetura (Figura 1):

- Entidade Gerenciadora: Controla a coleta, o processamento, a análise e/ou apresentação das informações do gerenciamento;

- Dispositivo Gerenciado: Composto pelo equipamento de rede que reside em uma rede gerenciada;

- Objeto Gerenciado: Contido no objeto gerenciado, são peças de hardware e software;

- Base de Informação de Gerenciamento: Informações associadas aos objetos gerenciados, disponibilizados à entidade gerenciadora;

- Agente de gerenciamento: Processo nativo ao dispositivo gerenciado, responsável por se comunicar com a entidade gerenciadora e que executa ações no dispositivo;

- Protocolo de Gerenciamento: É a padronização de comunicação entre a entidade e o agente.

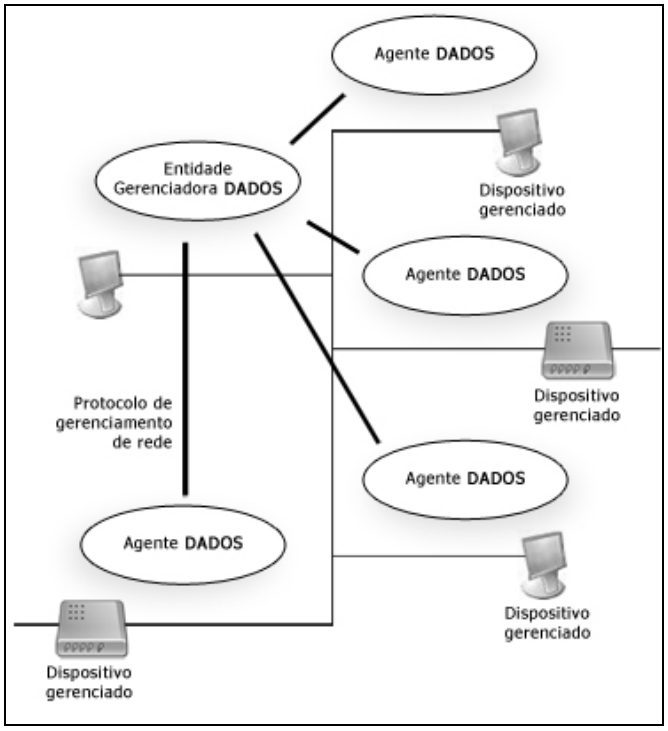

Figura 1 - Estrutura de Gerenciamento no Modelo OSI.
Fonte: Kurose e Roos (2006, p. 576).

1.2 Sistema de Registro de Problemas (*Trouble Ticket System*)

O sistema de *Trouble Ticket* é uma ferramenta que auxilia a equipe de TI para registrar o problema em uma base de dados e garantir que os responsáveis serão notificados sobre o mesmo, evitando perda de mensagem e garantindo sua resposta (EST, 2011).

A potencialidade de uma ferramenta de *Trouble Ticket* depende muito de como são organizados internamente os chamados. É desejável a possibilidade de criar "filas", nas quais estarão associados tickets relacionados a um assunto em particular. Para exemplificar, pode-se verificar todas as reclamações oriundas do maior cliente da empresa, ou ainda, pedidos encaminhados pelo setor de marketing. Cada fila possuirá sua política de acesso e de tratamento de chamados. A maneira como um ticket é atribuído a uma fila, em geral, pode ser feita tanto manualmente (pelo administrador da ferramenta) quanto em função do e-mail para o qual foi enviado o chamado. Cada fila, por sua vez, também poderá conter outras divisões lógicas que ajudem na hora de listar ou organizar os tickets da fila (LUCENA, 2001).

O processo que desencadeia a ocorrência de atendimento no sistema de chamados é o “problema”, a peça de hardware ou software que produz uma parada por determinado período de tempo e que pode ser materializado no sistema de atendimento de *ticket* pelo bilhete, pois através deste são notificados e reportados os problemas às pessoas responsáveis da equipe de TI. Assim, no sistema de atendimento o bilhete possui um ciclo de vida como o demonstrado na figura 2.

Inicialmente o bilhete é aberto, este pode ser realizado automaticamente ou através de um usuário de sistema, e é adicionada a ele a descrição dos problemas encontrados. Após os responsáveis tomarem ciência, é realizado um estudo de caso para definir uma tomada de decisão e testes são realizados. Caso a solução obtenha um resultado satisfatório, o cliente que gerou o bilhete é avisado do fechamento e o mesmo é armazenado em um banco com a solução adotada. Em caso negativo na tentativa de obter uma solução, nova definição de possível solução é criada até que se obtenha sucesso.

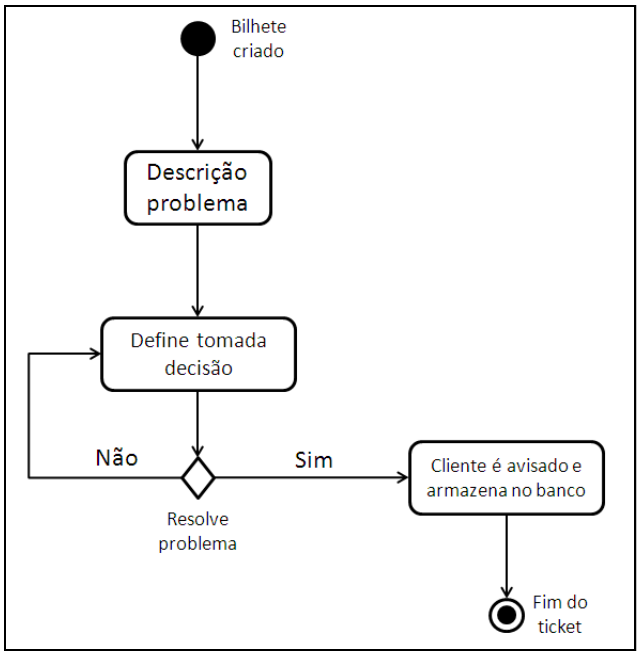

Figura 2 - Ciclo de vida do bilhete no contexto do MREG.

Segundo Johnson (JOHNSON, 1992), que descreveu a RFC 1297, um bom sistema de *Trouble Ticket* deve servir para muitos propósitos, como:

- Conter detalhamento e histórico do problema, para que qualquer operador possa entender e trabalhar buscando a solução rápida, utilizando uma linguagem formal para fazê-lo. Assim, mesmo que o atendente seja trocado, caso esteja no momento de folga, em férias ou não presente, outro pode assumir mesmo não consultando o atendente anterior.

- Possuir um sistema com diferentes prioridades. O sistema deve ser capaz de ordenar os registros abertos em de acordo com prioridades, com isto o operador pode definir o próximo *ticket* a ser atendido.

- Integrar um sistema de correios, para que seja possível a atribuição de tarefas ou consultas sejam feitas através de e-mail.

- Definição de tempo de atendimento aberto. Decorrido o tempo, utilizar-se de alertas para informar que determinado chamado não foi solucionado. Tendo como objetivo relembrar que atitudes devem ser tomadas para finalizar o atendimento.

- Criar e enviar relatórios eletrônicos para os representantes de sub-redes, com um resumo dos problemas correntes na rede. Isto possui a finalidade de informar os gestores sobre o estado de cada bilhete em aberto.

- Análise estatística. Gerar formulários sobre os equipamentos e a produtividade possibilitando analisar e definir um controle da qualidade para realizar a detecção de equipamentos defeituosos e que possibilite que atitudes sejam tomadas anteriormente a uma falha efetiva.

- Filtro de alertas correntes, tornando visível aos operadores relacionamentos de registros anteriores.

- Visualização das atividades pelos usuários e gestores. Através deste demonstrar que a equipe de TI está empenhada na função de resolver as falhas existentes na rede.

1.3 Base de Conhecimento

A Base de conhecimento é uma especialização de uma base de dados, pois nela as informações são coletadas, categorizadas, organizadas, compartilhadas e utilizadas.

Deste modo a base de conhecimento tem como objetivo tornar o conhecimento acessível a todos que o necessitem para realização de uma tarefa semelhante. Os aplicativos de gerenciamento que utilizam na arquitetura uma base de conhecimento tornam o ambiente de atendimento capaz de absorver os processos envolvidos para solução do problema apresentado, tornando mais eficiente e minimizando o tempo de análise. [Dingding et al, 2011].

Assim desenvolver programas de atendimento a bilhetes faz-se necessário para categorizar os atendimentos do cliente requisitante. Agregando-se a este aplicativo uma base de conhecimento com os atendimentos e soluções realizadas, torna mais eficaz o processo de solução, pois após um chamado ser atendido, ele pode ajudar a solucionar outro que possua semelhança. [Dingding et al, 2011].

Segundo Fong (Fong e HUI, 2001) criar e utilizar uma base de informação juntamente a um aplicativo de atendimento de incidentes tradicional traz benefício importantes para uma empresa. Um ponto positivo encontrado pode ser notado quando se necessita manter uma equipe em constante treinamento para realizar atendimentos de suporte. Desta maneira utilizam-se regras para filtrar casos

semelhantes de atendimentos armazenados na base para complementar este treinamento mediante a um atendimento.

Outro trabalho semelhante foi realizado na Universidade de Federal no Rio Grande do Sul (UFRGS) por Melchiors (MELCHIORS C., 2000) implementou o DUMBO (Descobrindo Soluções Manipulando uma Base de Ocorrências). Esta é uma ferramenta de atendimento de bilhetes com a capacidade de armazenar as ocorrências passadas, com a finalidade de criar uma base de informação. Para extensão deste sistema utilizou-se o paradigma de Raciocínio Baseado em Caso (RBC) para propor soluções utilizando descrições de ocorrências passadas.

As implementações realizadas por Fong (Fong e HUI, 2001) e Melchiors (MELCHIORS C., 2000) detectaram que estes tipos de técnicas podem ser afetadas dependendo das consulta a serem realizadas. Deste modo ele demostrou que dependendo da precisão de pré-processamento (chaves utilizadas para busca) o resultado pode ser afetado diretamente, pois na escolha de elementos a serem buscados tem-se uma consulta com maior exatidão para obter-se uma solução correlata entre os eventos passados e correntes.

O pronto de limitação identificado por Fong (Fong e HUI, 2001) e Melchiors (MELCHIORS C., 2000) foram relacionadas à descrição da solução, pois a qualidade da descrição da resolução tomada depende diretamente do conhecimento do administrador. Sendo assim quanto maior a o entendimento a capacidade de transmitir as informações do gestor maior será a exatidão da descrição e consequentemente a transmissão do conhecimento para outros futuros atendentes de casos semelhantes.

.

1.4 Sistema Integrado de Monitoramento (S.I.M.)

O S.I.M. é um aplicativo que integra ferramentas de monitoramento de redes de código aberto, com a finalidade de facilitar a gerência e automatizar a geração de *tickets* automáticos de incidentes (PEDROSO et. al., 2011). Através dele é possível visualizar os dados dos diferentes monitores em um ambiente integrado, evitando erros de interpretação devido à análise de múltiplas interfaces (Figura 3). Além disto,

o S.I.M. foi projetado para obter a redução dos falsos positivo, pois realiza a comparação dos alertas disparados por diferentes sensores.

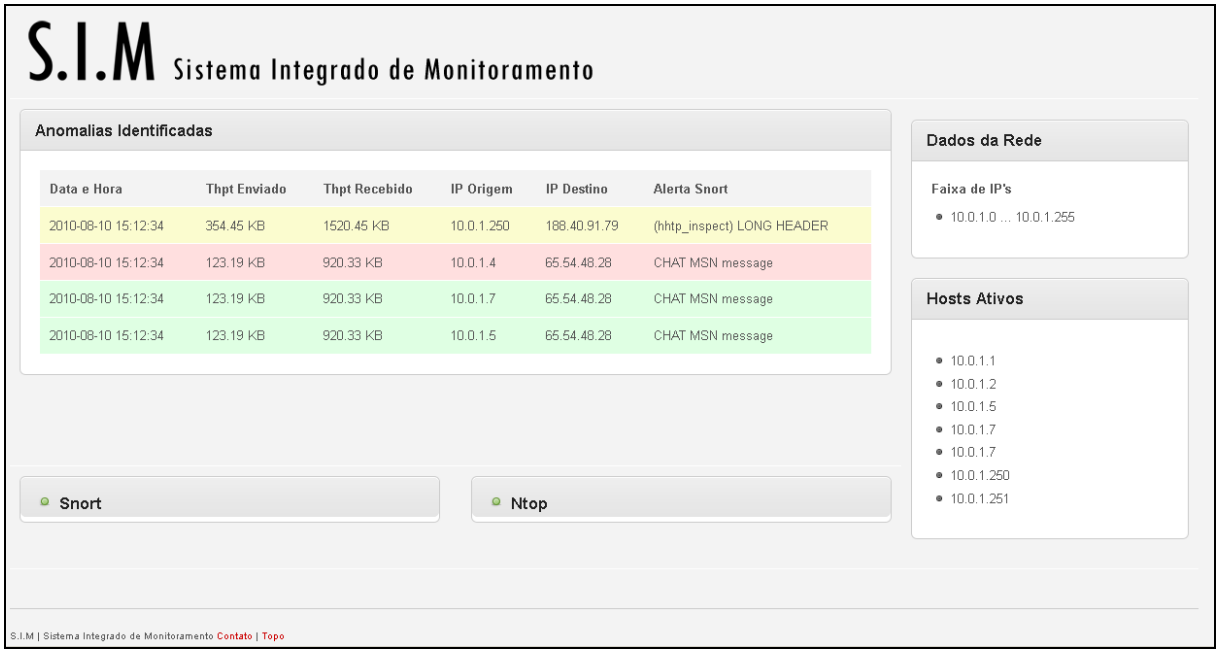

Figura 3 - Interface do Sistema Integrado de Monitoramento (S.I.M.).

1.4.1 Funcionamento lógico

O funcionamento lógico do S.I.M. baseia-se na sistemática do semáforo, onde são utilizadas três cores primárias para identificar os estados do ativo de rede, sendo elas vermelho, amarelo e verde.

Inicialmente o *host* é adicionado à rede sendo, neste momento detectado pelos sistemas de monitoramento. Após a detecção é definido o seu estado “verde”, quando este não possui funcionamento anômalo e sendo constantemente monitorado. Caso alguns dos aplicativos detectem um incidente, ele é marcado com o estado “vermelho”, neste momento são coletados os dados do incidente e mostrados na interface.

Após o gestor tomar ciência do incidente ocorrido, ele pode optar por dois estados, “verde” ou “amarelo”. Quando o administrador possui conhecimento para solucionar o problema ele o resolve e define o estado “verde” (ativo sem incidente).

Caso necessite estudar e/ou realizar verificações sobre a anomalia define o estado “amarelo” (anomalia em análise).

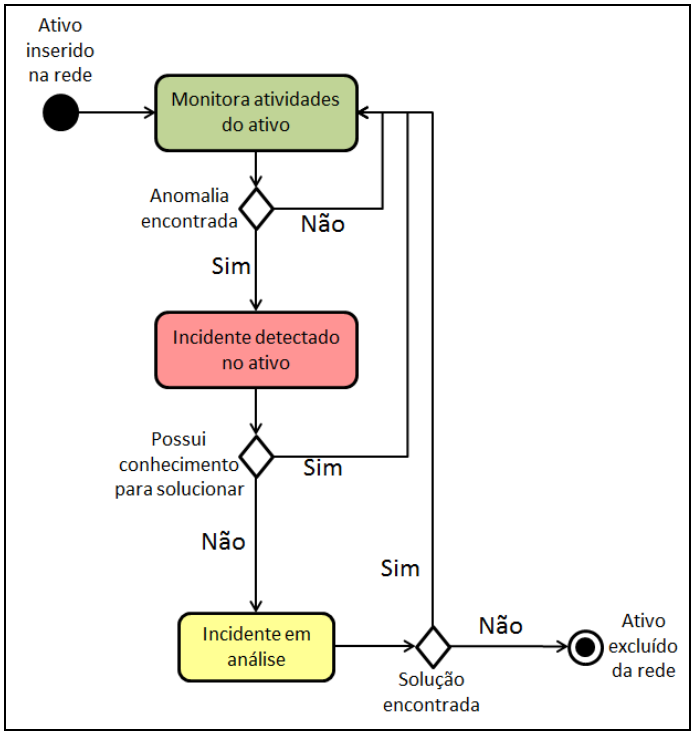

Figura 4 - Funcionamento lógico do S.I.M..

1.4.2 Ferramentas Integrantes

O monitoramento do tráfego de rede é realizado pelo NTOP e a captura de pacotes pelo SNORT. A *baseline* (média de tráfego) do host é definida pelo *Data Dump* do NTOP, sempre que for percebida alguma anomalia no tráfego de banda o S.I.M. buscará informações mais detalhadas sobre o que está acontecendo através do relacionamento das informações de consumo geradas pelo NTOP com a captura de pacotes do SNORT. A aplicação também funciona a partir dos alertas gerados pelo Snort realizando a busca pelo tráfego de rede do ativo envolvido na anomalia no momento em que ela foi detectada pelo mesmo (Figura 5).

Figura 5 - Interface de atendimento do S.I.M..

Com a finalidade de agregar mais informações sobre o estado do host envolvido, foi desenvolvido um script em Perl chamado de Coletor de Informação de Objetos (CIO). Este tem como foco obter os dados dos objetos gerenciados, programas rodando, programas instalados, mac's e ips das interfaces. Sendo assim com os dados gerados a partir do monitoramento realizado pelo NTOP e SNORT, o CIO recebe como parâmetro o ip do host envolvido na anomalia, requisita as informações via SNMP e alimenta o banco de dados com informações referentes ao host.

Por fim, todas as informações sobre a anomalia identificada são unificadas e armazenadas na base de dados da ferramenta, além disso, e-mails de alerta são disparados para avisar ao gestor sobre a ocorrência do comportamento anômalo. Tal funcionamento pode ser visto através do esquema apresentado na figura 6.

Por ser uma ferramenta de monitoramento, o S.I.M. tem a capacidade de funcionar com autonomia e em tempo integral, desde que atenda a algumas premissas: NTOP, SNORT, Perl e servidor web devem estar em execução e funcionando corretamente. Para atender a esta necessidade, quando instalada, a ferramenta utiliza um programa do Unix chamado "crontab", que edita o arquivo onde são especificados os comandos a serem executados, a hora e dia de

execução, funcionando como uma agenda de tarefas a serem realizadas a cada período de tempo pré-estabelecido.

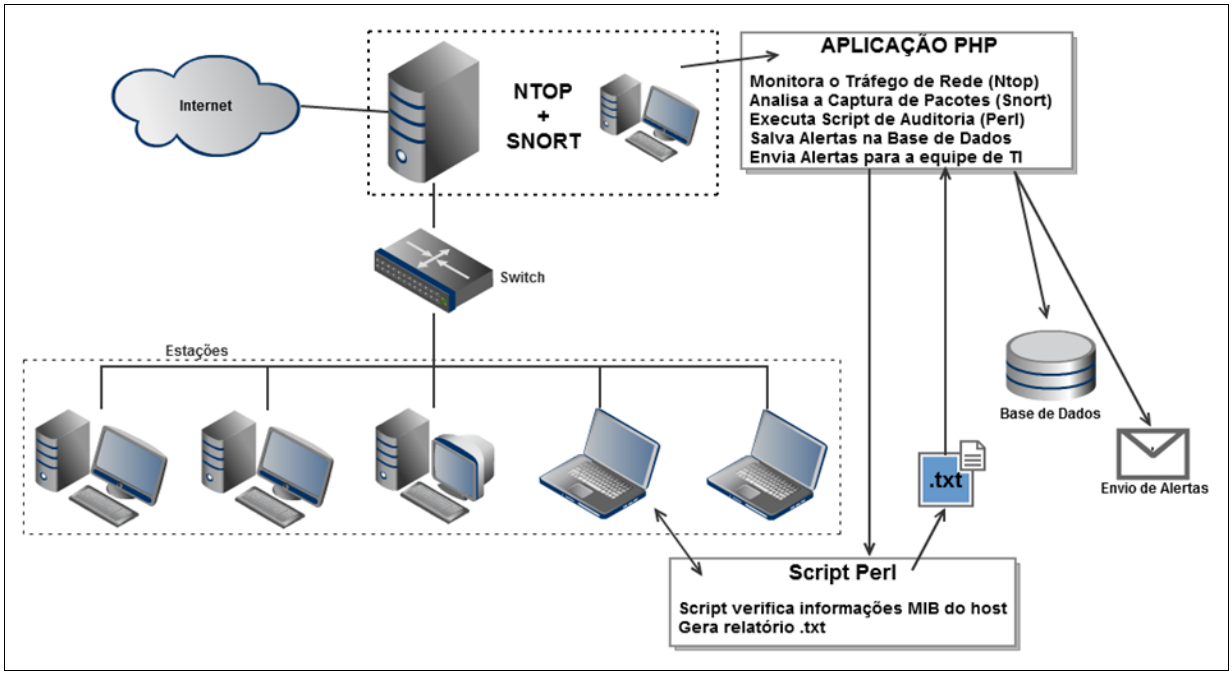

Figura 6 - Funcionamento do S.I.M..
Fonte: Pedroso et. al. (2011).

2 METODOLOGIA

2.1 Ambiente Monitorado

A Rede Nacional de Ensino e Pesquisa (RNP) oferece conexão gratuita utilizando a infra-estrutura da Rede Ipê à Internet para instituições de ensino e de pesquisa, públicas e privadas, através dos pontos de presença (PoP), espalhados por todos os Estados Brasileiros e no Distrito Federal.

O PoP - RS é a representação da RNP no Rio Grande do Sul, dentro desta está inserida a Universidade Federal de Santa Maria (UFSM) e nesta última aloca-se a rede do Grupo de Redes e Computação Aplicada (GRECA).

O GRECA é um grupo de pesquisas que desenvolve trabalhos em diversas áreas utilizando como fundamento as tecnologias de transmissão de dados. Para isto são estudados ambientes virtuais de aprendizagem, problemas de transmissão com e sem fio, novas tecnologias físicas e de virtualização, todos estes com a finalidade de resolver problemas já existentes ou que possivelmente possam ocorrer.

Para proporcionar o desenvolvimento das pesquisas, possui uma arquitetura de redes composta por um switch, com VLANs definidas para segmentação das redes utilizadas. Outro equipamento utilizado é um servidor denominado Servidor Central, o qual provém serviços internos e externos. Sobre o servidor está hospedado o gateway virtual, que possui sistemas de *firewall*, nat, proxy e VPN, apresentado na (Figura 7). Através deste é fornecido o acesso à Internet para todos os alunos e colaboradores integrantes do laboratório.

Com a finalidade de realizar a análise do tráfego e desvincular a carga e processamento gerado pelo monitoramento, foi atribuída a tarefa de diagnóstico de pacotes ao servidor chamado de S.I.M.. Como este serviço não está sendo realizado pelo gateway foi necessária a criação de uma porta de *mirroring* no *switch*, sendo assim configurou-se o espelhamento de todos os pacotes que trafegam na rede para a porta que o S.I.M. está conectado. Através da porta de *mirroring* e do

espelhamento do tráfego, foi possível realizar a análise de todos os pacotes gerados e recebidos pelos ativos de redes.

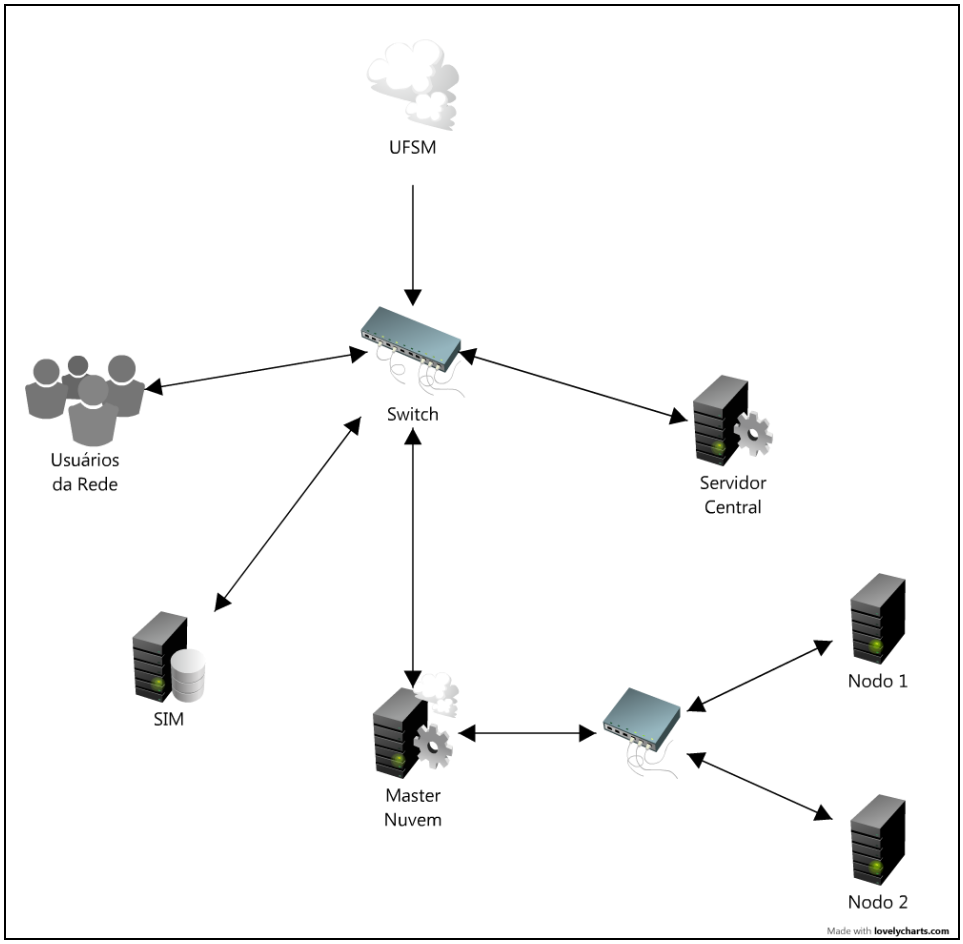

Figura 7 - Rede do GRECA.

Como está inserido em uma rede acadêmica, o servidor do GRECA está suscetível a ataques de inúmeras fontes, tanto em âmbito nacional como internacional. Em função da ocorrência de ataques faz-se necessário estudar e desenvolver técnicas de monitoramento na tentativa de evitar acesso indevido de pessoas não autorizadas. A tecnologia adotada pelo GRECA para auxiliar nesta tarefa é a utilização de virtualização, com foco em nuvem, com a finalidade de obter um ambiente de testes e homologação de sistemas.

Esta nuvem é composta fisicamente por três computadores, sendo um deles o master, contendo o *Cluster Controller* (CC), *Cloud Controller* (CLC), *Storage*

Controller (SC) e *Walrus Storage Controller* (WS3). Os outros dois componentes foram definidos como nodos, possuindo instalado e configurado o *Node Controller* (NC).

2.2 Banco de Dados

Para a implementação do trabalho, é utilizado o servidor de banco de dados MySQL (MYSQL, 2012) na versão 5.5.25a. Este foi escolhido devido aos requisitos necessários para o desenvolvimento:

- Compatibilidade com linguagens de programação web;
- Otimização para consultas em tempo real;
- Baixo consumo de processamento, reservando memória para os sistemas de monitoramento;
- Utiliza instruções SQL para manipulação de dados;
- Suportável em diferentes sistemas operacionais.

Tendo estes pontos para a escolha do SGBD foi definido o MySQL como banco de dados a ser utilizado no projeto.

2.3 Linguagem de Programação

Para o desenvolvimento do projeto buscou-se uma linguagem de programação que possibilitasse as características do requeridas para o desenvolvimento, como facilidade de tratamento de cadeias de caracteres e programação para web. Além dos requisitos iniciais, a linguagem de programação PHP foi escolhida por também possuir as características descritas abaixo:

- Linguagem Server-Side, que execute multi-funções;
- Compatível com MySQL;
- Multi-plataforma;
- Funções disponíveis para integração;
- Possui módulos de integração com outras linguagens;
- Documentação.

Assim o PHP atendeu as necessidades de projeto para o desenvolvimento do S.I.M. e do MREG, sendo adotado para a implementação dos mesmos.

3 MÓDULO DE RETENÇÃO DA EXPERTISE GERENCIAL (MREG)

Com a implementação e utilização do S.I.M. para visualizar e solucionar problemas de rede surgiram novos objetivos a serem atingidos. Uma destas metas possi como foco documentar as soluções tomadas para resolver as ocorrências criando uma base de informação (problema e soluções), sendo retido parte da *expertise* dos administradores no S.I.M.

Outra meta refere-se a propor na interface possíveis ações que possam solucionar o alerta, utilizando à base de informação a favor do gerente. Desta maneira correlacionando as assinaturas de eventos para propor as soluções documentadas.

Com os objetivos acima se tem como justificativa de transferir parte do conhecimento gerencial para o aplicativo, minimizando os problemas ocasionados com trocas de recursos humanos na equipe de TI. Outra justificativa refere-se à possibilidade de um administrador de menor conhecimento adquirir conhecimento através das soluções propostas pelo aplicativo e resolver o incidente em questão, liberando o administrador Sênior para a realização de outras tarefas.

Com a finalidade reter parte da *expertise* gerencial, foi implementado o MREG, sendo realizadas modificações em banco de dados, como descrito na seção 3.1, e criação de regras de correlação de eventos atuais e armazenados na base de informação, como explanado na seção 3.2.

3.1 Banco de Dados

O S.I.M. possui um banco de dados que integra as saídas dos monitores de redes o qual registra os possíveis ataques realizados na rede, integrando as saídas dos monitores integrantes NTOP e SNORT (Figura 8). Com isto o gerente toma ciência sobre o possível incidente ocorrido, atende, define um plano de decisão e finaliza o atendimento. Através destas informações armazenadas no banco é

possível realizar auditorias sobre os ativos e definir perfis comportamentais, utilizando os dados do banco constituído pelos componentes abaixo:

- *id*: Identificador do incidente em questão;
- *averagercvdthpt*: Média de tráfego recebido;
- *averagesentthpt*: Média de tráfego enviado;
- *averagethpt*: Média do tráfego total (recebido e envidado);
- *actualrcvdthpt*: Tráfego recebido atualmente;
- *actualsentthpt*: Tráfego enviado atualmente;
- *hostresolvedname*: Nome do ativo de rede;
- *hostnumipaddress*: IP do ativo de rede;
- *ethaddressstring*: Endereço físico do *host*;
- *date*: Data de registro do incidente;
- *alertsnort*: Alerta gerado pelo SNORT;
- *alertperl*: aplicativos que estão rodando no *host*;
- *situacao*: Situação do atendimento (Não verificado, Em andamento e Verificado).

Para adicionar informação na base descrita acima é necessário desencadeamento do processo de atendimento. Processo ocorre com a ativação do alerta por um dos monitores de rede, criação do *ticket* com a unificação das informações dos sistemas de monitoramento integrantes e definição do status de atendimento, podendo o status ser definido de três maneiras. O primeiro status definido como “Não verificado” ocorre quando um chamado é aberto pelos sistemas de monitoramento e o gestor não tomou ciência do ocorrido. Outra alternativa refere-se ao administrador de redes definir o status como “Em andamento”, quando o incidente necessita uma análise mais detalhada de suas causas e por último “Verificado”, quando o incidente foi solucionado.

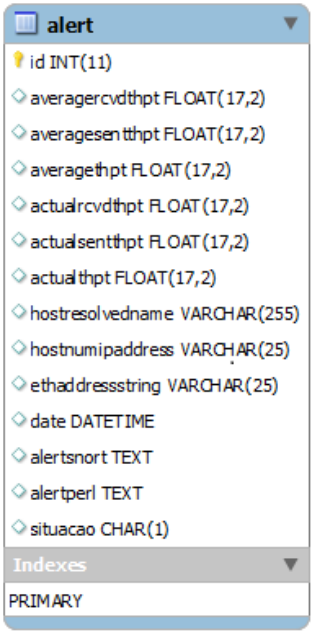

Figura 8 - Tabela de alertas do banco de dados do S.I.M..

Com a finalidade de transformar esta base de problemas em uma base de conhecimento (problema/solução), foram adicionados na base do S.I.M. dois campos de textos, destacados em verde na figura 9. Um destes campos é chamado de “descr”, este é reservado para que o gestor possa descrever a solução para o dado problema encontrado na rede e armazenar este na base de informação.

Outro campo chamado de “processos” é destinado à marcação de programas que desencadeiam o alerta em questão, o qual a sua utilização é melhor especificada na sessão 3.2. Na figura 9 pode ser observada a base do S.I.M. e MREG com os campos adicionados necessários para a retenção de parte da *expertise* e constituição da base de informação.

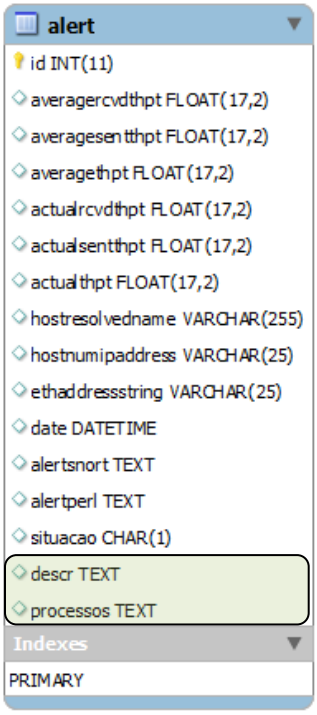

Figura 9 - Modificações na tabela de alertas da base S.I.M.
com a integração do MREG.

Para a criação da base de informação é necessário que o gestor detenha conhecimento, pois para definir uma solução são realizados testes de verificação. Com isto para resolver um problema o principal atuante é a experiência adquirida pelo administrador em conhecer o relacionamento entre os integrantes de rede. Desta maneira as modificações realizadas na base do S.I.M., permitem registar os testes e as soluções tomadas para resolver os problemas detectados, retendo parte da *expertise* gerencial no aplicativo.

Com o relacionamento de problema e solução, criaram-se consultas ao banco de conhecimento para correlacionar eventos correntes com anteriormente tratados. Deste modo é possível mostrar possíveis soluções na interface, auxiliando o gestor e logicamente possibilitando a redução do tempo de resposta ao incidente, como descrito na seção 3.2.

3.2 Consultas de soluções

Como mostrado na seção 3.1, as soluções armazenadas em banco são apresentadas em duas caixas distintas na interface, uma com alertas de mesmo IP e de outros IPs. Os alertas podem ter sido gerados pelo SNORT ou NTOP, sendo assim, possuem diferentes consultas realizadas em banco para obterem-se os resultados que serão propostos ao gestor.

Quando um alerta é gerado as saídas dos sistemas de monitoramento são analisadas e caso a detecção do incidente for disparado pelo SNORT, o processo de busca segue como descrito abaixo e ilustrado na figura 10:

1) Alerta é disparado pelo SNORT.

2) As informações são buscadas no NTOP e o coletor de dispositivos é disparado.

3) O bilhete é gerado e gravado as informações na base do S.I.M..

4) Busca-se no banco o alerta em questão e extrai-se a entrada que gerou o alerta, classificação do SNORT.

5) Realiza um filtro no banco buscando dentre todos os alertas que possuem a mesma assinatura.

6) O resultado é divido em duas categorias, aplicadas no ativo em questão ou aplicadas em outro ativo, mas que possuem similaridade de ocorrência.

7) As informações são mostradas na interface de atendimento de incidentes, para análise por parte do gerente.

8) O gestor escolhe entre as opções disponibilizadas ou cria uma nova documentação sobre o alerta.

Caso o NTOP gere o alerta e não seja detectada nenhuma ocorrência na base de dados do SNORT, os passos para a geração e visualização do NTOP são apresentados na figura 11 e descritos a seguir:

1) Alerta é disparado pelo NTOP.

2) As informações são buscadas no SNORT, tomando a data e horário que o alerta foi disparado para procurar o alerta na base, e o coletor de dispositivos é disparado.

3) O bilhete é gerado e gravado as informações na base do S.I.M..

4) Busca-se no banco o alerta em questão e extrai-se a entrada que gerou o alerta, classificação do SNORT.

5) Sendo negativo a busca pela assinatura do SNORT são verificados os programas envolvidos e aplicado um filtro no banco buscando dentre todos os alertas que possuem um dos programas como problemático.

6) O resultado é divido em duas categorias, aplicadas no ativo em questão ou aplicadas em outro ativo, mas que possuem similaridade de ocorrência.

7) As informações são mostradas na interface de atendimento de incidentes, para análise por parte do gerente.

8) O gestor escolhe entre as opções disponibilizadas ou cria uma nova documentação sobre o alerta.

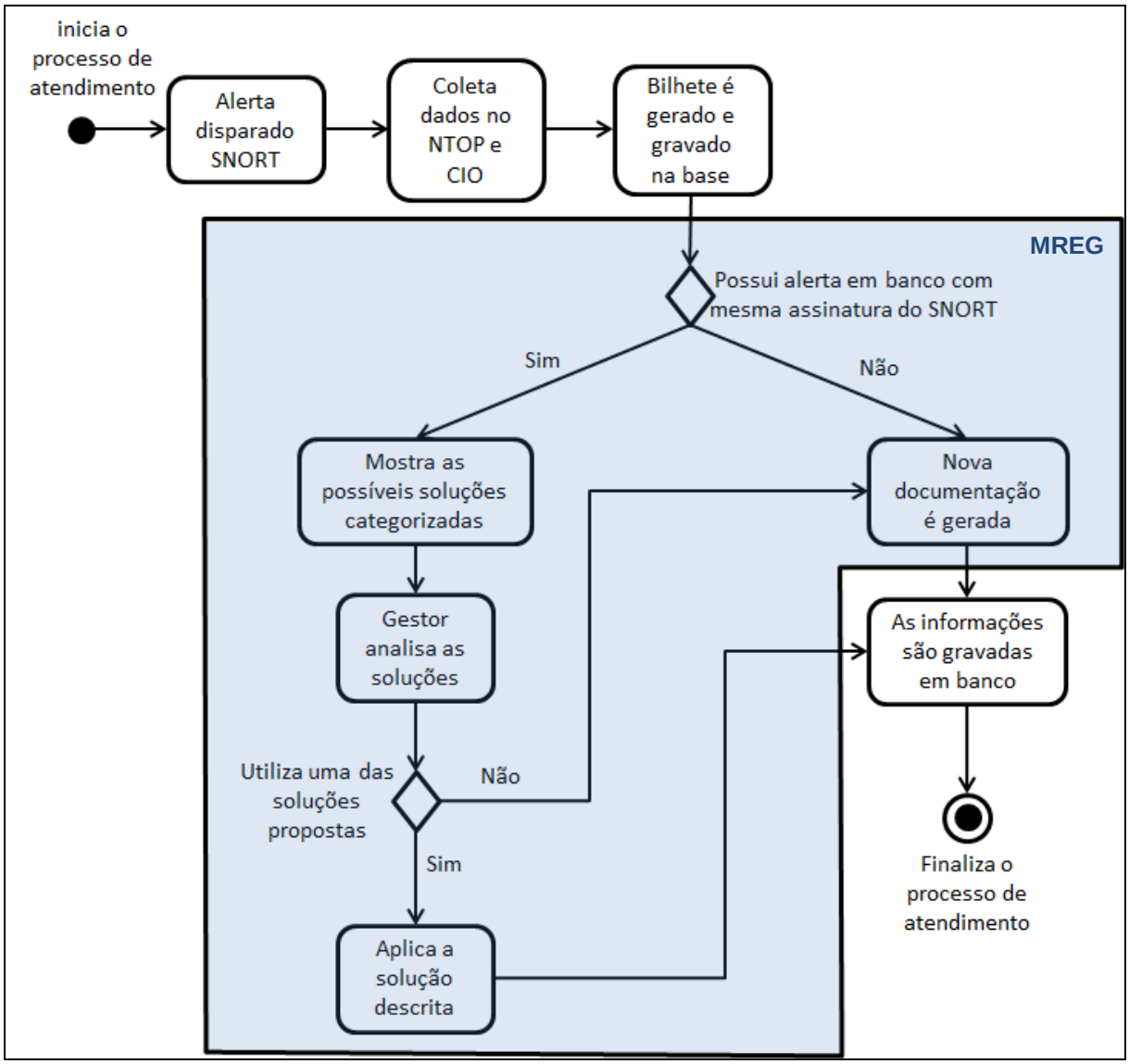

Figura 10 - Alerta gerado pelo SNORT, em azul o módulo MREG.

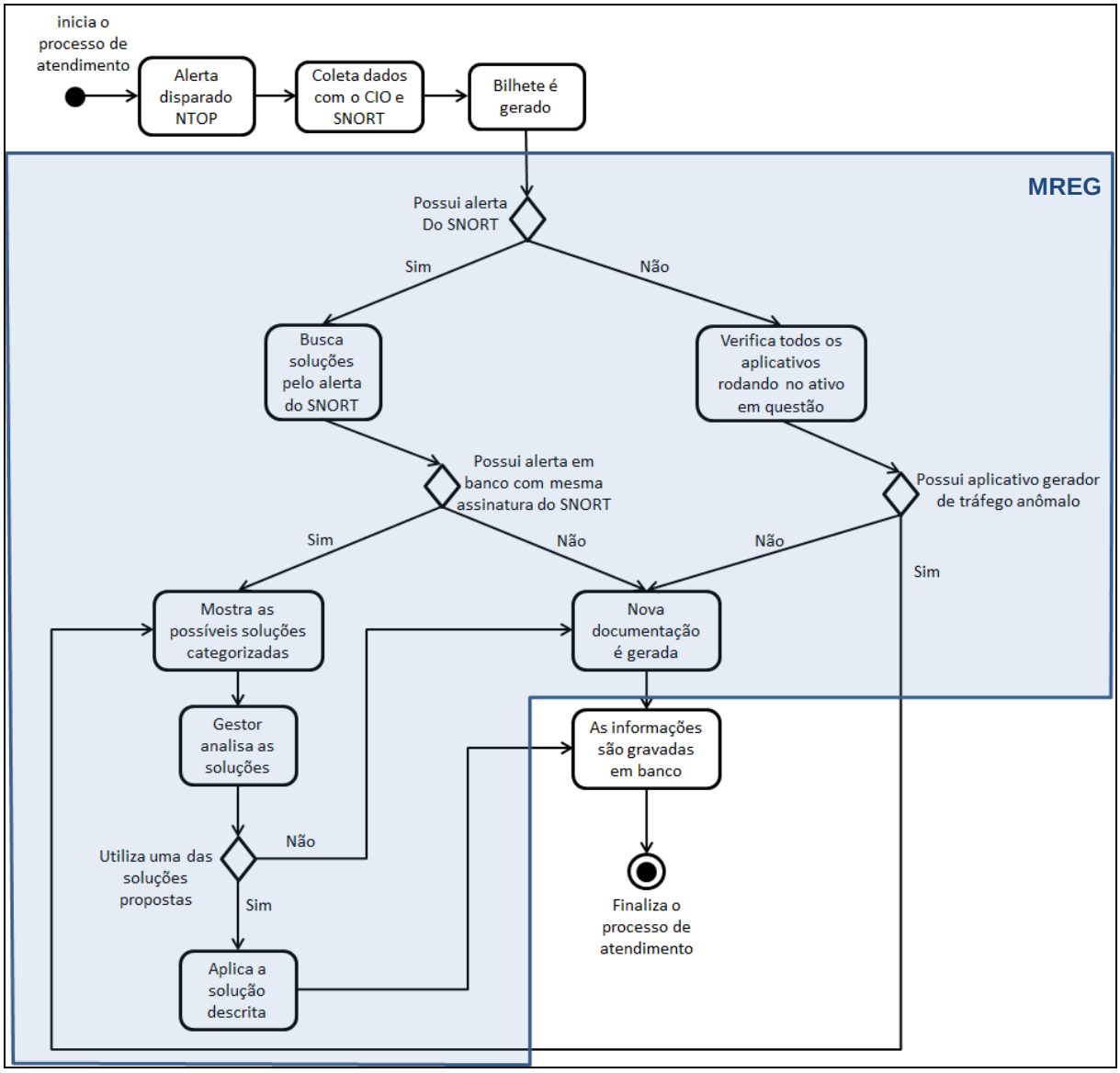

Figura 11 - Alerta gerado pelo NTOP, em azul o módulo MREG.

3.3 Modificações da Interface do SIM com integração do MREG

Com a finalidade de capturar as soluções criadas para resolver os incidentes, foi-se necessário realizar modificações na interface do S.I.M.. Quando o alerta é disparado pelo SNORT é mostrado na interface um campo de texto chamado “Descrição/Documentação”. Este pode ser visualizado no exemplo da figura 12, que é atendido e descrito os passos para solucionar o incidente sobre o worm Conficker.

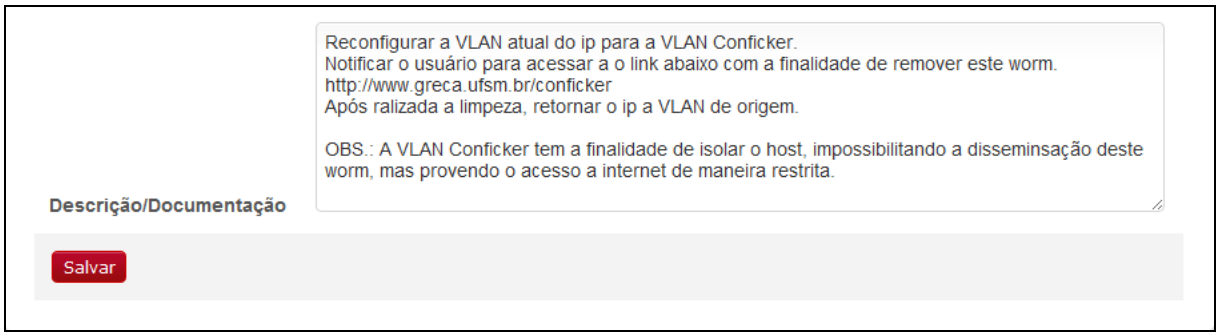

Figura 12 - Campo para documentação do incidente no MREG.

Sendo o NTOP o disparador do alerta são necessários mais dados para realizar a correlação dos incidentes. Portanto para definir os programas, adicionou-se na interface além do campo de descrição, outra caixa de texto chamado “Processos Responsáveis”. Como ilustrado na figura 13, quando detectado uma alta taxa de tráfego em um host, sendo descrito que esta foi devido ao aplicativo wget e que é utilizado para transferência de dados entre sistemas.

Figura 13 - Campos para documentação e definição de programas relacionados do possível incidente do MREG.

Para mostrar as soluções propostas pelo sistema baseado nos atendimentos anteriormente realizados foram categorizados dois tipos de soluções, aplicadas no ativo em questão e aplicados em outros hosts. Em ambos os caso possuem correlação de assinatura de ocorrência, sendo estas assinaturas identificadas através da categoria de incidente detectado pelo SNORT ou aumento de tráfego identificado pelo NTOP, este último juntamente com um processo já definido como gerador desta largura de banda anômala. A codificação da busca por soluções passadas para incidentes detectados pelo SNORT é visualizada na figura 14 e na

figura 15 o gerente pode verificar o retorno das buscas em banco na interface com as soluções anteriormente criadas, posicionando o mouse sobre os IP's das caixas "Sugestões de mesmo IP's" e "Sugestões de outros IP's". Deste modo o administrador de redes pode optar por uma gama de resoluções, aplicando a que melhor se adequa aquele momento ou, caso queira, criar uma nova solução utilizando o campo de documentação da figura 12.

```
// Recupera os dados referentes ao inciente em questão
$sql = "select * from alert where id = {$id}";
$rs1 = $this->db2->Execute($sql);

// O inicidente possui alerta do SNORT
if($rs1->fields['alertsnort'] != NULL){
    // Recupera a assinatura do SNORT
    $alertsnort = explode('[&]',$rs1->fields['alertsnort']);
    $alert = explode('[x]',$alertsnort[0]);

    //Busca no banco de informações os dados de identificação de alerta e
    //documentação existente de host de mesmo IP e que possuiem mesma assinatura do SNORT.
    $sq = "select id,descr from alert where hostnumipaddress like
          \"{$rs1->fields['hostnumipaddress']}\" and alertsnort like \"%$alert[3]%\"";

    $rs = $this->db2->Execute($sq);

    if($rs && $rs->RecordCount() != 0)
    {
        while(!$rs->EOF)
        {
            // Adiciona na interface "Sugestões Mesmo IP" a solução encontrada
            $html .= "<li><a href=\"#descr\" onclick=\"$('#descr').val('{$rs->fields['descr']}');\"
                title='{$rs->fields['descr']}'>{$rs->fields['hostnumipaddress']}</a></li>";
            $rs->MoveNext();
        }
    }
}
```

Figura 14 - Busca de soluções existentes no banco de dados.

As soluções disponibilizadas na interface são links que, quando clicados, os campos de documentação e programas relacionados são automaticamente preenchidos com as informações do incidente anterior. Outra opção para visualização é posicionando o mouse sobre o IP, assim as informações serão visualizadas em um balão de informação e com isto pode-se decidir qual tomada de ação gostaria de executar.

Com a integração do módulo MREG foram adicionadas à interface de atendimento do S.I.M. mais informações sobre os possíveis incidentes ocorridos. Além dos dados providos através dos sistemas de monitoramento, possibilitou

documentar os atendimentos de rede realizados, como visualizado no quadro em vermelho número 1 da figura 16. Desta maneira o administrador relaciona o problema detectado a uma tomada de decisão planejada e aplicada, assim possibilitado construir a base de informação sobre atendimentos prestados anteriormente.

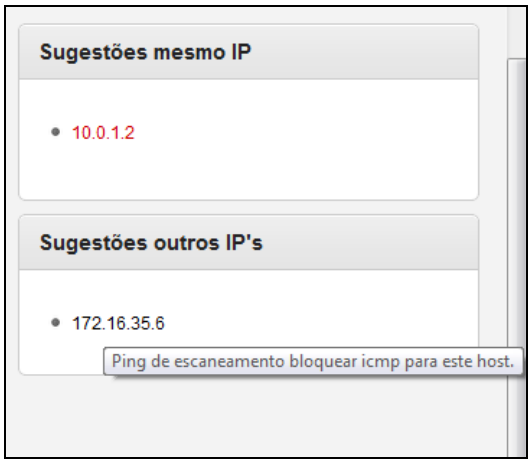

Figura 15 - Campo de soluções propostas do módulo MREG.

Outro ponto desenvolvido refere-se a possibilitar ao administrador não somente ter a possibilidade de criar a base de informação, mas trazer como benefício esta parte da *expertise* retida no aplicativo à interface, disponibilizando as possíveis soluções ao gestor no momento do atendimento. Com a finalidade de prover este acesso são implementadas consultas para retornar as soluções relacionadas na base com o incidente corrente, como demonstrado na seção 3.2.

Para melhor visualização na interface das possíveis soluções retornados das consultas, elas são dividias em duas categorias “Sugestões de mesmo IP” e “Sugestões de outros IP’s”, destacado no quadro vermelho número 2 da figura 16.

Em “Sugestões de mesmo IP” são disponibilizadas as possíveis soluções aos incidentes que foram aplicados no IP em questão. Desta maneira além de relembrar e facilitar a reação do administrador ao incidente é possível detectar problemas persistentes e cíclicos no *host*, quando o IP aparece inúmeras vezes neste campo.

As documentações categorizadas como “Sugestões de outros IP’s” são soluções criadas para resolver problemas encontrados em outros IP’s da rede,

diferentes do IP em questão. Deste modo são mostradas tomadas de decisões que foram aplicadas em outros ativos na rede, mas que possuem semelhanças de assinaturas do SNORT ou aplicativos que gerem taxas de tráfegos anômalas detectados pelo NTOP e o CIO. Outro objetivo desta categorização é a possibilidade de verificar problemas de configuração de rede ou disseminação de pragas cibernéticas, quando ocorre um grande número de ativos nela.

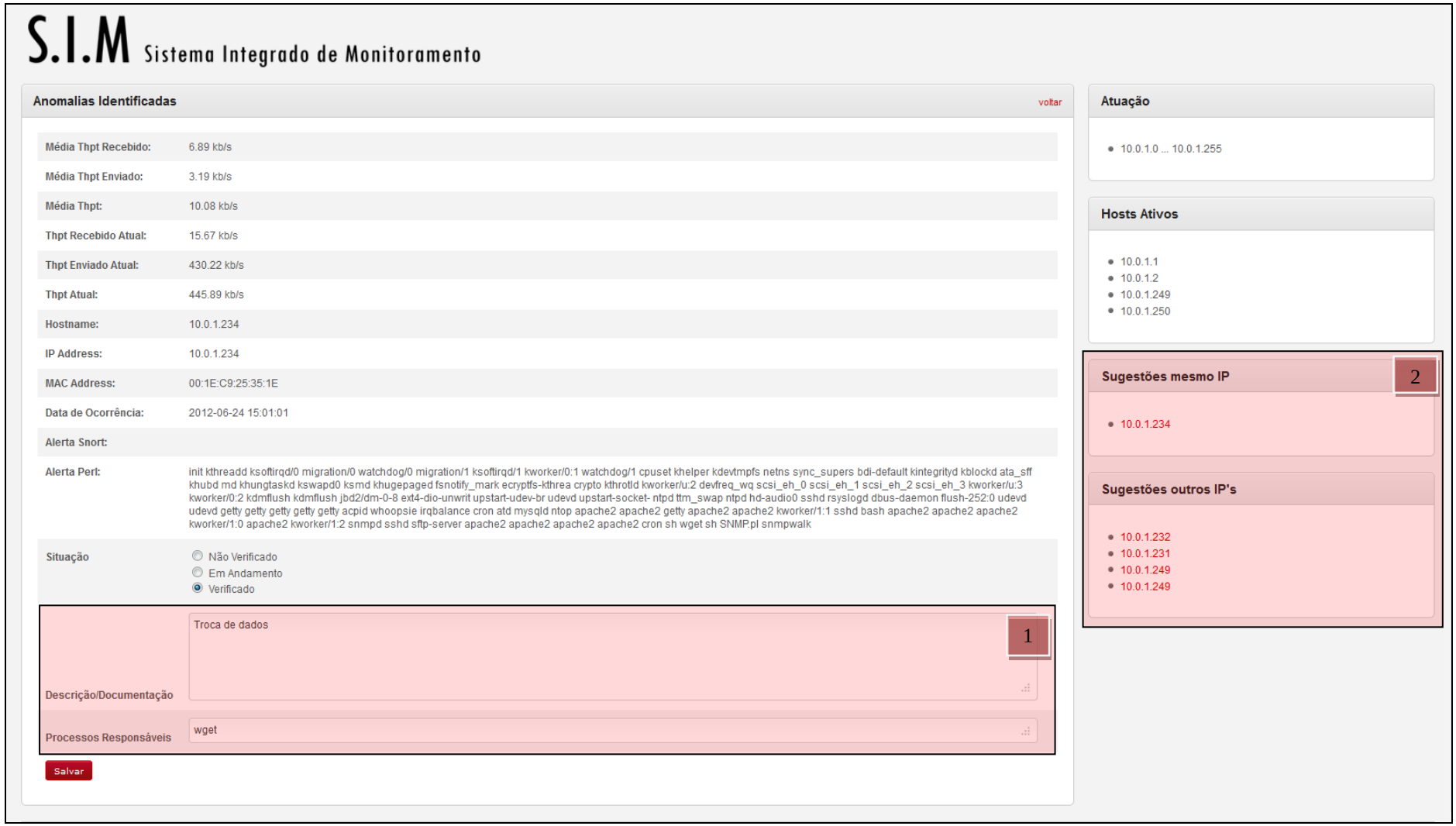

Figura 16 - Interface atendimento de incidente S.I.M. com MREG em vermelho.

4 RESULTADOS

Com a finalidade de testar a criação e busca de soluções foram realizados testes de ataques. Estes foram projetados para abranger dois tipos de diretivas:

- Gerar alertas através do SNORT possibilitando buscar assinaturas de incidentes;

- Gerar alertas através do NTOP criando tráfego de rede anômalo.

Para atingir a primeira diretiva foi selecionado um aplicativo que simula tentativas de intrusão, através de escaneamento de rede. O programa utilizado foi um scanner conhecido como Zenmap (ZENMAP, 2012), o qual utiliza o NMAP (NMAP, 2012) para realizar varredura da rede ou conjunto de *hosts*. Para este teste foi definida a descoberta total da rede do GRECA. Portanto realizou-se o escaneamento padrão, sendo primeiro utilizado o protocolo ICMP (DEERING, 1991) para cada uma das máquinas da subrede e logo após efetuou-se o escaneamento das portas abertas nos sistemas, como pode ser observado na figura 17.

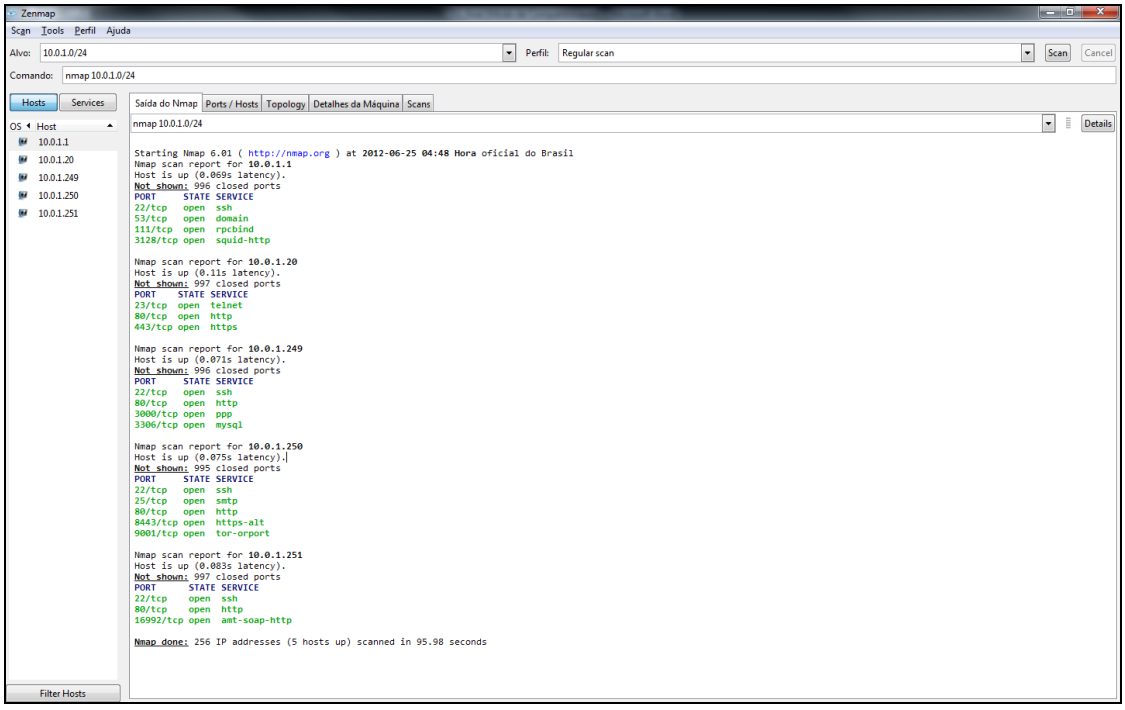

Figura 17 – Varredura e escaneamento de rede do GRECA com Zenmap.

Com a atividade de escaneamento realizado pelo programa Zenmap, gerou-se o alerta no S.I.M., e um bilhete de atendimento é apresentado na interface com os dados coletados pelas ferramentas de monitoramento. Após a análise do incidente ocorrido, o administrador realiza a documentação da solução e o processo de atendimento é finalizado através do salvamento das informações na base de informação.

Por seguinte realizou-se novamente o escaneamento para gerar um novo bilhete, tendo como finalidade de testar a capacidade do MREG de relacionar os eventos gerado pelo NTOP através dos aplicativos responsáveis pelo tráfego. Assim as soluções criadas anteriormente foram propostas na interface. No campo de “Sugestões mesmo IP” foi apresentada a solução criada para o incidente detectado no IP 10.0.1.2, no endereço de rede de atendimento corrente. No campo “Sugestões de outros IP’s“ é mostrado o atendimento e solução realizados em outro IP da rede, mas com mesma assinatura do SNORT. Sendo possível visualizar a solução posicionando o mouse sobre o IP, como mostrado na figura 18.

Com esta divisão de IP’s em categorias, torna possível visualizar hosts que possuem problemas persistentes. Pois caso isto ocorra, serão mostrados sucessivamente a listagem todas as ocorrências no campo de “Sugestões mesmo IP” como mostrado na figura 18, como o *host* 10.0.1.2. Tendo verificado isto, o gestor pode tomar medidas corretivas para evitar possíveis pontos de vulnerabilidades do sistema.

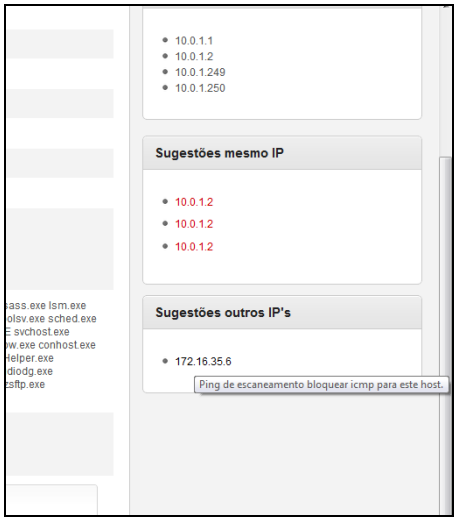

Figura 18 - Soluções propostas pelo MREG.

Para atingir a segunda diretiva proposta para teste, executou-se o aumento do tráfego de rede por parte de um *host* com o objetivo de criação de *ticket* pelo NTOP. Para isto foi utilizado o aplicativo wget (WGET, 2010) que realiza download através do protocolo http, https e ftp de arquivos disponíveis na rede, local ou Internet. Assim, um ticket foi gerado através do NTOP sem ocorrer alerta no SNORT, pois este não se encaixou em nenhuma assinatura existente no banco de dados do aplicativo (Figura 19).

Para o relacionamento dos dados deste tipo de incidente é utilizado uma caixa auxiliar, chamada “Processos Responsáveis” com a finalidade de coletar o(s) nome(s) dos programas envolvidos no incidente. Desta maneira, quando é gerado nova taxa de tráfego, a busca no banco é realizada através deste(s) aplicativo(s). Visualiza-se nos quadros em destaque da figura 19, o aplicativo wget presente no campo “Alerta Perl”, desta maneira o programa está sendo utilizado no *host* em questão. Também pode ser observado o mesmo aplicativo presente no campo “Processo Responsáveis”, sendo este programa o responsável por gerar o tráfego anômalo identificado pelo administrador em atendimentos anteriores e utilizado como parâmetro para a recuperação da documentação “Troca de dados”.

Por meio da realização destes testes pode-se avaliar as funcionalidades agregadas ao S.I.M. através da implementação e integração do módulo MREG. A partir da análise e descrição dos resultados observou-se satisfatória indicação de soluções a serem utilizadas no atendimento à incidentes de rede, tornando o trabalho do administrador de redes mais eficiente.

Com a integração do Módulo de Retenção Gerencial ao Sistema Integrado de Monitoramento possibilitou-se documentar no campo “Descrição/Documentação” as soluções para resolver os desvios de padrões dos ativos detectados pelos sistemas de monitoramento. Permitiu-se ainda identificar quando um *host* aparece inúmeras vezes no campo de sugestões de soluções, sendo possível constatar “ativos problemas” integrantes da rede que possuem anomalias persistentes ou atacantes. Como o observado no ativo de IP 10.0.1.249 da figura 19 que aparece duplicado no campo de “Sugestões de outros IP’s”, demostrando que o *host* utiliza o aplicativo wget para realizar troca de dados, demonstrando ser necessária uma análise mais aprofundada sobre este tráfego. Desta maneira, tornando mais clara à identificação de sistemas desprovidos de segurança ou que proporcionem aos usuários um ambiente suscetível à invasão e inseguro para a transmissão de dados.

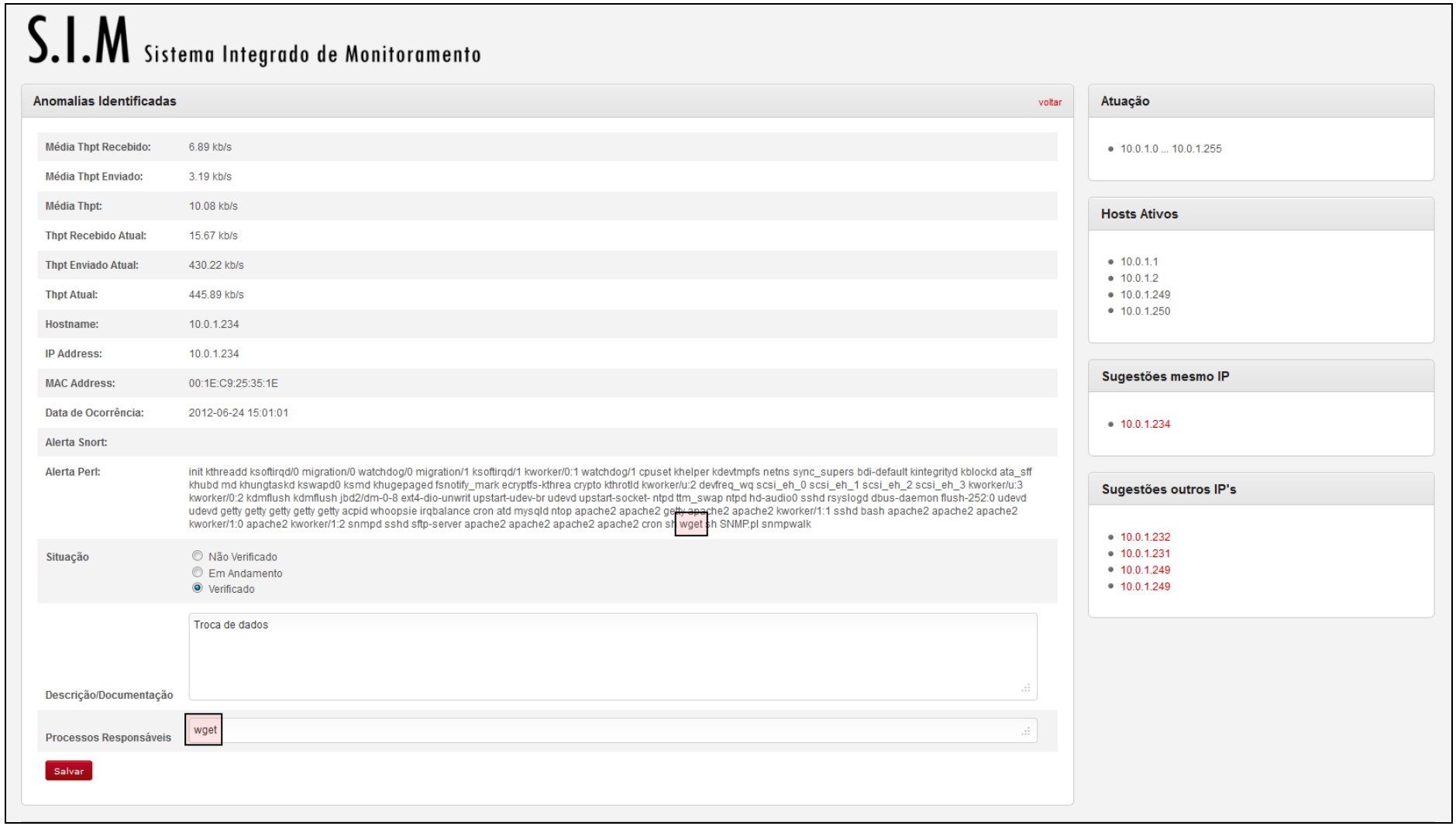

Figura 19 - Busca de incidente pelo processo gerador do tráfego.

Através desta documentação possibilitou-se ampliar as informações disponíveis ao gerente na interface tornando mais conciso e embasado o planejamento da tomada de decisão, pois, quando um alerta é gerado as soluções relacionadas com o possível incidente, que estão na base de informação são disponibilizadas no ambiente de monitoramento. Neste sentido, o administrador pode utilizar-se destas para se embasar em estudos realizados anteriormente sobre o alerta, com a finalidade de aplicar a regra ao incidente.

Outro ponto que este módulo busca, refere-se à tentativa de possibilitar a redução do tempo de análise e planejamento de reações contra ataques, visto que, através dos atendimentos anteriores é possível gerar uma nova solução utilizando uma combinação destes ou melhoramentos de ações que solucionaram em parte o problema ocorrido. Assim, o administrador pode empregar maior tempo na realização de suas tarefas de estudos, implementação e melhoramentos da rede.

Como exemplo de aplicação do trabalho pode-se observar na figura 20 a detecção de uma tentativa de ataque à rede do GRECA indicado pelo S.I.M.. Os ataques à rede são oriundos de computadores da Coreia do Sul (IP 221.143.46.144) e Lituânia (IP 24.32.143.147). Identificados os ataques o MREG propôs a solução “Tentativa de escaneamento de escaneamento externo, bloquear IP”. A solução foi registrada na base de informação e poderá ser novamente utilizada quando incidente semelhante ocorrer.

Além de tentar reduzir o tempo de respostas o módulo pode auxiliar em momentos críticos do gerenciamento de uma rede, como troca de gestor ou equipe de TI. Dessa maneira, o impacto ocasionado pode ser minimizado, pois quando este tipo de situação ocorrer, além dos treinamentos investidos e estudos iniciais realizados pelo novo administrador a base com as soluções propostas, através da interface ajudarão na construção do conhecimento da lógica e da dinâmica do ambiente (Figura 21).

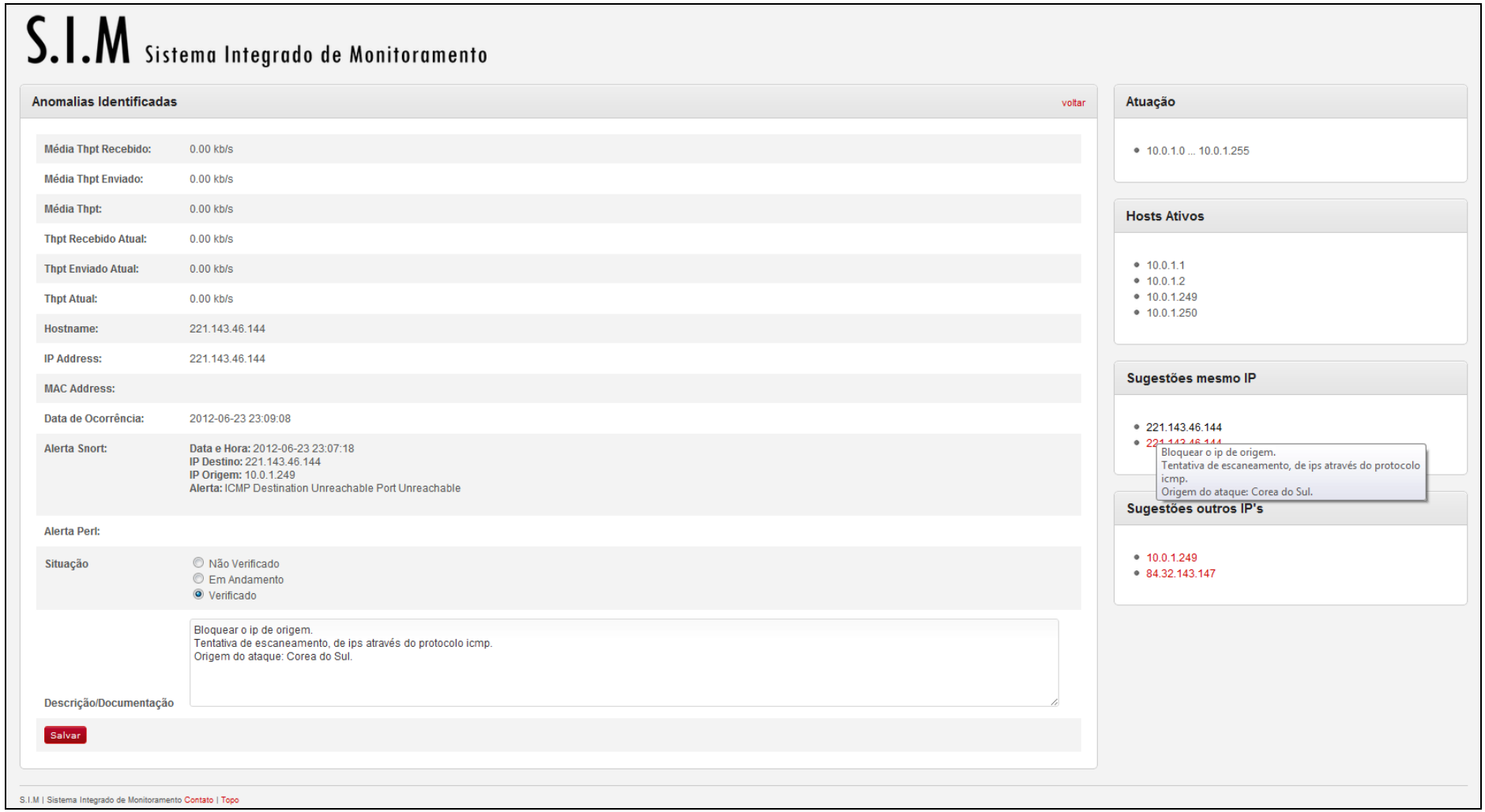

Figura 20 - Ataques *hosts* externos à rede do GRECA.

Outro aspecto relevante refere-se à equipes de TI que possuem diferentes níveis de administradores de rede. O MREG possibilita a um Gestor Técnico Jr. utilizar soluções analisadas e documentadas por um Técnico Sênior. Deste modo, evitando que camadas superiores nos níveis de gestores detenham-se com programas de atendimentos já analisados e, consequentemente contribuido para a capacitação dos níveis mais inexperientes/técnicos Jrs (Figuras 21 e 22).

Na figura 21 é possível verificar a transferência da expertise para o S.I.M. através do MREG para as camadas mais inexperientes da equipe de gerenciamento ou quando ocorra troca de equipe de TI. Estra retenção é observada através do atendimento do incidente “Conficker detectado”, pois o Técnico Sênior ou atual gestor primeiramente realiza estudos sobre as atividades e comportamentos deste worm. Após estes estudos preliminares, realiza modificações na rede configurando uma VLAN com a finalidade de isolar o *host* com o incidente e logo após documentou esta resposta ao problema encontrado. Quando novamente este alerta for gerado pelos sistemas de monitoramentos, o técnico menos experiente ou em treinamento, poderá aplicar esta regra sem a necessidade de consultar os níveis superiores ou o novo gestor pode adquirir conhecimento para reagir ao incidente.

Outro exemplo visualizado na figura 22 refere-se à transferência de conhecimento com relação à configuração de serviços em um servidor. O alerta de “Acesso ao SNMP com comunidade pública” exige que o atendente possua conhecimento técnico para configurar a comunidade no serviço SNMP, demandando tempo para pesquisar em fontes (livros ou sites especializados) para reconfigurar tal serviço. Após o atendimento e documentação desta atividade, a troca de gestor ou atendimento por camadas de gerência com menos experiência pode ser realizado sem perda de tempo para buscar em fontes auxiliares com a finalidade de solucionar o alerta em casos futuros.

Pode-se destacar, que a implementação do MREG integrado ao S.I.M. constitui-se como mais uma ferramenta de auxílio na efetivação dos trabalhos do administrador de rede, uma vez que, busca diminuir o tempo de planejamento e resposta aos incidentes por manter em seu banco de dados soluções prévias e inserção de novas alternativas.

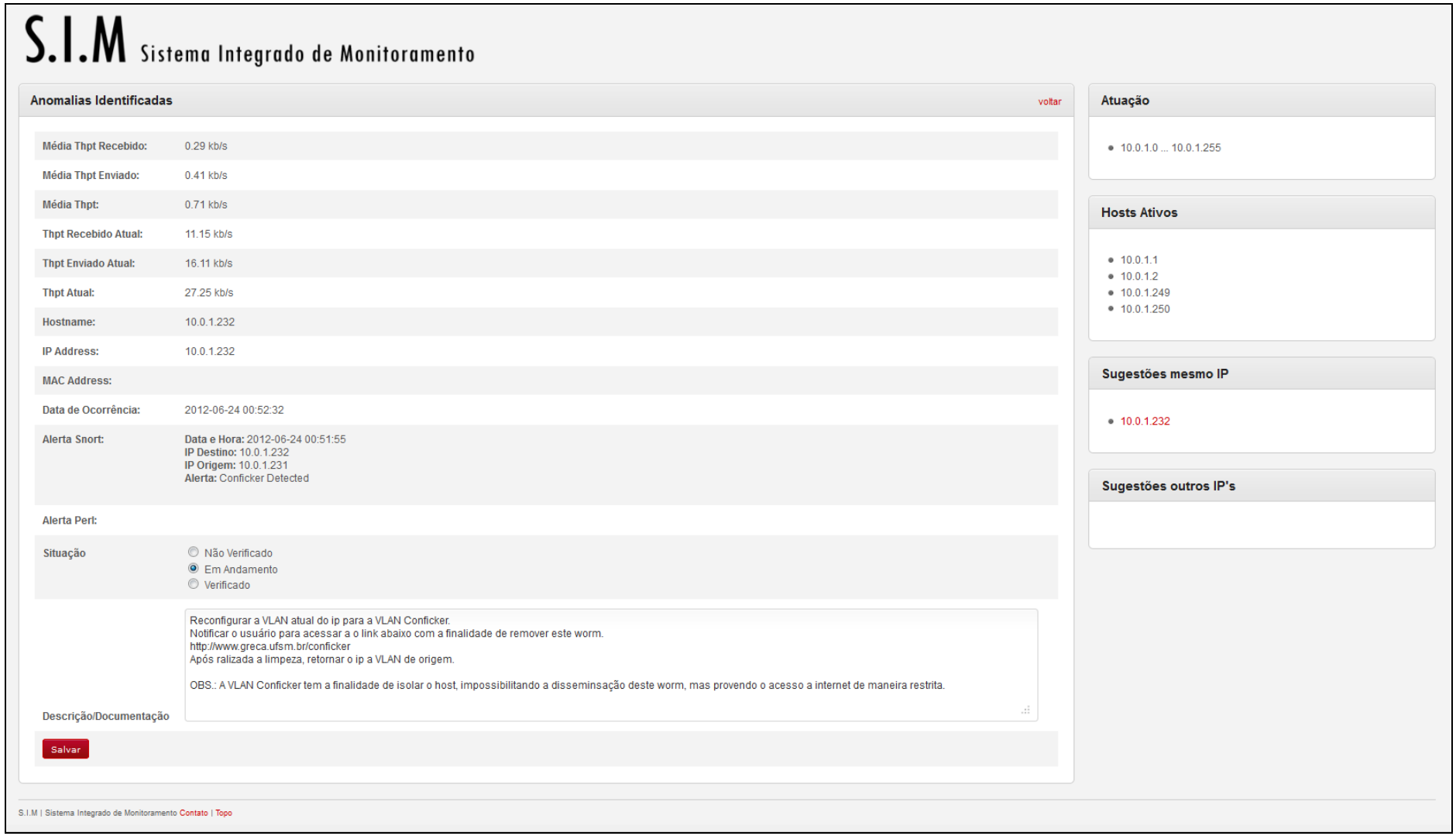

Figura 21 - Documentação de mudança de configuração de rede para solucionar incidentes proposto pelo MREG.

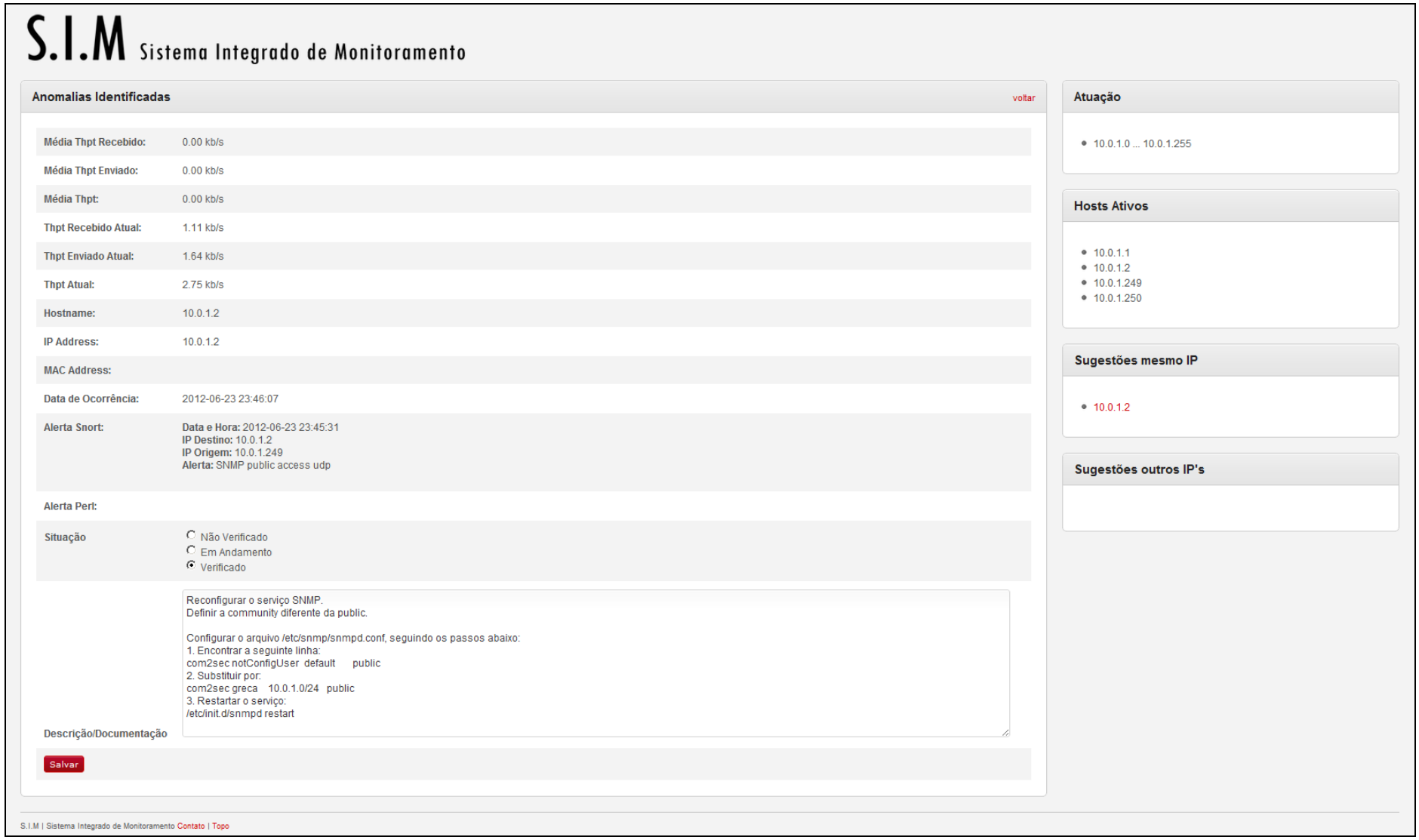

Figura 22 - Documentação de modificações no serviço de SNMP no servidor.

5 CONSIDERAÇÕES FINAIS

Com a conclusão da presente pesquisa faz-se necessário revisitar os objetivos propostos inicialmente. O objetivo geral consistiu em "*Reter parte da expertise do administrador de redes no Sistema Integrado de Monitoramento (S.I.M.)*". Este objetivo foi atingido, pois a base principal da pesquisa: coleta de dados de atendimentos e correlação de atendimentos correntes com anteriores foram realizadas com sucesso e proporcionaram a documentação comportamental e de reações por parte do administrador de redes. Através desta, o S.I.M. tornou-se uma ferramenta que propicia/facilita a retenção de parte de conhecimento da expertise gerencial e capaz de propor soluções na interface que possuíam correlação com os incidentes.

Na sequência são retomados os objetivos específicos, bem como os principais resultados e comentários relativos a cada um deles, juntamente com as sugestões e recomendações identificadas.

- 1º Objetivo específico: *Criar uma base de informação*.

A transformação da base de atendimentos em uma base de informação foi viabilizada com a adição das entradas na interface de "Descrição/Documentação" e "Processos Responsáveis". Deste modo, o banco passou a ser dotado de informações significativas que possibilita a reutilização destas como propostas de futuras soluções a casos semelhantes.

- 2º Objetivo específico: *Tornar o aplicativo capaz de relacionar eventos.*

Com o banco de informações em constante formação objetiva-se uma nova tarefa de trazer estes dados como benefício para o gestor da rede. Sendo assim, foram codificadas funções de relacionamento de eventos de ocorrência atual com os presentes no banco, como descrito na seção 3.2.

Como dificuldade encontrada para construção destas relações, refere-se a eventos criados através de taxas altas de tráfego, pois, este parâmetro não possibilita relacionamentos com eventos. Deste modo, necessitou-se criar mais um parâmetro a ser armazenado em banco, chamado de "Processos Relacionados". Através deste possibilitou-se selecionar do banco os dados a serem apresentados na interface ao gerente.

- 3º Objetivo específico: *Reduzir o tempo de respostas aos incidentes.*

Juntamente à criação do banco de informação, relacionamento de eventos e apresentação de soluções conseguiu-se atingir o terceiro objetivo, o qual tem a finalidade de auxiliar o administrador na sua tarefa de gestão da rede. Com as ocorrências documentadas e propostas é possível inferir que o tempo de atendimento pode ser reduzido, pois as documentações de atendimentos passados podem ser utilizadas para solucionar o problemas em questão. Desta maneira evita repetidas análises do mesmo incidente por parte do gestor e relembra casos que foram atendidos em um longo prazo de tempo anterior.

Com a conclusão deste trabalho foi possível desenvolver novos conhecimentos na área de gerência de redes, sistema de atendimento a bilhetes, banco de dados e relacionamento lógico de eventos.

Para definir diretivas de trabalhos futuros pode-se propor:

- Detecção de problemas: Realizar monitoramento constante do ambiente de rede do GRECA, tanto interno como externo, tendo como finalidade analisar o funcionamento.

- Dispositivos móveis: Tornar o sistema capaz de ser acessado através de dispositivos móveis. Assim, implementando uma interface apropriada para visualização dos dados no ambiente de monitoramento, através destes.

- Ampliar escopo de monitoramento: Aumentar o número de ferramentas que compõem o S.I.M., buscando assim maior capacidade de correlação de eventos. Através destes, tornar o MREG capaz de reter uma gama maior de expertise gerencial, tendo como finalidade de desassociar a dependência da instituição com o gestor ou equipe de TI.

- Criar uma gerência especificamente para a nuvem: Possibilitando obter conhecimento e descrição comportamental de atividades ocorridas neste ambiente e consequentemente maior segurança no tráfego e processamento dos dados.

- Transformação de informação textual em regras de IA: Utilizar técnicas de inteligência artificial para realizar um melhoramento no filtro de soluções a propor, tornando mais eficiente o processo de sugestões de soluções ao gerente de redes.

REFERÊNCIAS

CACTI. **Cacti:** The Complete RRDTool-based Graphing Solution. [S. I.], 2012. Disponível em: <http://www.cacti.net/>. Acesso em: 27 maio 2012.

CRUZ, H. F. da. **Implantação de um IT Service Desk com a Ferramenta Livre OTRS alinhado aos Processos de Incident e Problem Management of the Framework ITIL**: Exemplo de Aplicação na Eletronorte. 2008. 112f. Trabalho de Graduação (Graduação em Engenharia da Computação) - Instituto de Tecnologia, da Faculdade de Engenharia da Computação, Belém, 2008. Disponível em: <http://pt.scribd.com/doc/36757709/38/CICLO-DE-VIDA-DE-UMA-REQUISICAO-TICKET>. Acesso em: 26 maio 2012.

DEERING, S. **RFC 1256**, [S. l.], Set. 1991. Disponível em: <http://datatracker.ietf.org/doc/rfc1256/>. Acesso em: 10 maio 2012.

DINGDING, W.; T. Li, S. Zhu, Y. Gong "**iHelp: An Intelligent Online Helpdesk System**". In: IEEE transactions on systems, man, and cybernetics, vol. 41, issue 1, p. 173-182, 2011.

ESCOLA SUPERIOR DE TECNOLOGIA SETÚBAL (EST). **Trouble Tickets**. Disponível em: <http://moodle.ests.ips.pt/IPS/CI-IPS/Manual_Trouble_Tickets.pdf>. Acesso em: 20 fev. 2012.

FONG, A. C. M.; HUI, S. C., "**An intelligent online machine fault diagnosis system**", 2001, Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=962673&tag=1>. Acesso em: 10 ago. 2012

HEWLETT-PACKARD (HP). **HP System Mananger**. São Paulo, SP, 2012. Disponível em: <http://h20331.www2.hp.com/hpsub/cache/284133-0-0-225-121.html?jumpid=ex_R2845_vanityim/gossm/ka011106>. Acesso em: 26 maio 2012.

INTERNATIONAL BUSINESS MACHINES (IBM). **IBM TIVOLI**. São Paulo, SP, 2012. Disponível em: <http://www-01.ibm.com/software/br/tivoli>. Acesso em: 26 maio 2012.

INTERNATIONAL STANDARD ORGANIZATION (ISO). **ISO/IEC 7498-4**: Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management framework, [S. l.], Nov. 1989. Disponível em: <http://www.cin.ufpe.br/~redis/intranet/bibliography/standards/s014258e.pdf>. Acesso em: 29 maio 2012.

JOHNSON, D. **RFC 1297**, [S. l.], Jan. 1992. Disponível em: <http://datatracker.ietf.org/doc/rfc1297/>. Acesso em: 30 abr. 2012.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet**: uma abordagem top-down. [S. l.]: Pearson Education, 2006.

LUCENA, S. C. de. Ferramentas de Domínio Público para Gerenciamento de Chamados a Suporte. **Rede Nacional de Ensino e Pesquisa**, [S. l.], v. 5, n. 5, out. 2001. Disponível em: <http://www.rnp.br/newsgen/0109/RT.html>. Acesso em: 10 maio 2012.

MELCHIORS C., TAROUCO L. M. R., "**Troubleshooting Network Faults Using Past Experience**", 2000, Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=830413>. Acesso em: 18 Julho. 2012

MYSQL. **MySQL 5.0 Reference Manual.** [S. l.], 2012. Disponível em: <**http:**// http://dev.mysql.com/doc/refman/5.0/en/index.html/>. Acesso em: 06 julho. 2012.

NAGIOS. **NAGIOS: The Industry Standard in IT Infrastructure Monitoring**. [S. l.], 2012. Disponível em: <http://www.nagios.org/>. Acesso em: 10 mai. 2012.

JOHNSON, D. **RFC 1297**, [S. l.], Jan. 1992. Disponível em: <http://datatracker.ietf.org/doc/rfc1297/>. Acesso em: 30 abr. 2012.

NMAP. **NMAP:** Reference Guide. [S. l.], 2012. Disponível em: <http://nmap.org/book/man.html/>. Acesso em: 05 ago. 2012.

NTOP. **NTOP**: An Overview. [S. l.], 1998. Disponível em: <http://www.ntop.org/products/ntop/>. Acesso em: 10 jun. 2012.

PEDROSO, H. S. et. al. Uma proposta de Sistema Integrado para a Gerência da Segurança em Redes de Computadores nas Organizações - Estudo e Implementação. In: VII Congresso Nacional de Excelência em Gestão, ago. 2011, Rio de Janeiro. **Anais eletrônicos**... Disponível em: < http://www.excelenciaemgestao.org/Portals/2/documents/cneg7/anais/T11_0364_1989.pdf >. Acesso em: 20 maio 2012.

REDE NACIONAL DE ENSINO E PESQUISA (RNP). **RNP**. Botafogo, RJ, 2012. Disponível em: <http://www.rnp.br/index.php>. Acesso em: 03 jun. 2012.

SAYDAM, T.; MAGEDANZ, T. From Networks and Network Management Into Service and Services Management. **Journal of Networks and System Management**, [S. l.], v. 4, n. 4, p. 345-348, dez. 1996. Disponível em: <http://www.springerlink.com/content/n91v5h83387m05m8/>. Acesso em: 15 abr. 2012.

SEIFRIED, K. Monitoramento Eficiente. **Linux Magazine**, São Paulo, v. 1, n. 76, p. 42-47, nov. 2011.

SNORT. **Snort Uses Manual**. [S. l.], 2010. Disponível em: <http://www.snort.org/>. Acesso em: 29 maio 2012.

WGET. **GNU WGET**. [S. l.], 2010. Disponível em: <http://www.gnu.org/software/wget/>. Acesso em: 15 maio 2012.

ZENMAP. **Zenmap Reference Guide**. [S. l.], 2012. Disponível em: <http://nmap.org/zenmap/>. Acesso em: 29 maio 2012.