NETACT – ATUADOR EM GERÊNCIA DE REDES

Rogério Carvalho Schneider, Antônio Rodrigo Delepiane de Vit, Fábio Roberto Pillatt, Luís Cassiano Goularte Rista
UNICRUZ – Universidade de Crua Alta, Departamento de Informática,
Cruz Alta – RS – Brasil
[stockrt, arodrigo, pillatt, rista]@unicruz.edu.br

Liane Margarida Rockenbach Tarouco
UFRGS – Universidade Federal do Rio Grande do Sul, Departamento de Informática,
Porto Alegre – RS – Brasil
liane@penta.ufrgs.br

Resumo

No processo de gerência de redes, a tomada de medidas administrativas normalmente é auxiliada pelo uso de ferramentas de gerência. Através da geração de relatórios com estatísticas do uso de rede torna-se possível identificar os pontos falhos de um sistema e, a partir destes dados, tomar medidas corretivas embasadas. Sendo assim, o objetivo deste trabalho é integrar essa geração de relatórios, a partir de ferramentas já existentes, com uma base de dados histórica com a finalidade de gerar padrões de rede e utilizar técnicas de identificação de desvios para diagnosticar, de forma automática, as anomalias de rede. O NetAct é uma ferramenta que auxilia na gerência de rede e que tem esta proposta, a de identificar um ponto falho e realizar um processo curativo, de forma autônoma e constante.

Palavras-chave: Gerenciamento, Redes de Computador, Monitoramento, Análise de Padrão Comportamental

Abstract

In the process of network management, the taking of administrative measures normally is assisted by the use of management tools. Through the generation of reports with statisticians of the net use one becomes possible to identify the defective points on a system and, from these data, to take based corrective measures. Being thus, the objective of this work is to integrate this generation of reports, from already existing tools, with a historical database with the purpose to generate network standards and to use techniques of shunting line identification to diagnosis, of automatic form, the network anomalies. The NetAct is a tool that assists in the network management and that it has this proposal, to identify a defective point and to carry through a dressing process, by an independent and constant form.

Keywords: Management, Computer Networks, Monitoring, Pattern Behavior Analysis

1. Introdução

O uso de redes de computadores em ambientes corporativos e educacionais se faz cada vez mais presente. Esta tecnologia possibilita a comunicação entre os seus participantes dentro de um ambiente de forma prática e com baixo custo, e ainda fornece a possibilidade de se aplicar as mesmas facilidades de comunicação a longas distâncias.

Assim como o aumento do uso de redes, também se expande com velocidade a procura por implantação de qualidade de serviço e a correta manutenção da conectividade. Em contrapartida, a facilidade de comunicação também gera problemas, como a facilitação para a entrada de vírus e *worms* nos computadores pertencentes à rede, chamados, então, de intrusores. Também se considera o ataque de *crackers*. Os serviços convergem todos para o uso de redes locais e internet visando à diminuição dos custos de comunicação e fazendo uso de estruturas já existentes. Esta convergência torna a disponibilidade da conectividade um fator importante e decisivo, tanto na área educacional como corporativa.

Para que se mantenha a produção em funcionamento, é preciso monitorar a rede, fazer o seu gerenciamento e administração, e para isso uma equipe tecnicamente especializada torna-se necessária. Contudo, muitas vezes, não existe a possibilidade de se efetuar revezamento para monitoria do estado da rede 24 horas por dia. A maioria dos

softwares livres disponibilizados para a gerência de redes apenas trata do fornecimento de gráficos para análise humana do estado da rede, sendo este – o operador humano - o responsável pelas tomadas de decisão na administração/gerência da rede. A proposta deste trabalho é a criação de um sistema baseado em plataformas de *software* livre que se valha das informações fornecidas por *softwares* reconhecidos de monitoria de rede e faça ele mesmo a análise das informações recebidas e tome por si próprio as decisões necessárias (agindo com um atuador), fazendo com que a correção dos problemas de gerenciamento (a eliminação de uma intrusão, por exemplo) seja feita no menor tempo possível, garantindo a manutenção e a estabilidade do acesso para os usuários e informando os acontecimentos ao administrador/gerente da rede.

Uma grande rede não pode ser gerenciada somente por esforços humanos. É necessária a utilização de ferramentas para seu auxílio. Conclui-se, daí, que uma rede que não pode ser gerenciada corretamente possui pouco valor [WAN03].

2. Gerência de Redes

Gerenciar qualquer sistema consiste, basicamente, nas atividades de monitorar os elementos - tais como roteadores, *switches*, aplicações, entre outros - analisá-los à luz de uma política previamente estabelecida, e atuar sobre esses elementos, de modo a manter o sistema funcionando dentro de padrões aceitáveis [FIL03].

O que caracteriza a gerência de redes é, sem dúvida, a utilização de ferramentas, aplicativos e dispositivos, para auxiliar o elemento humano na monitoria e manutenção da rede.

No processo de gerenciamento, uma separação funcional de necessidades foi apresentada pela *International Organization for Standardization* (ISO), como parte de sua especificação de gerenciamento de sistemas OSI (*Open System Interconnection*). A maioria dos fornecedores de sistemas de gerenciamento de redes adotou esta divisão funcional para descrever as necessidades de gerenciamento: falhas, desempenho, configuração, contabilização e segurança [GUB02].

O modelo ISO propõe a divisão da gerência de redes em cinco categorias, sendo essa divisão chamada de FCAPS (*Fault, Configuration, Accounting, Performance, Security*).

- **Falhas**: A gerência de falhas é o processo de localizar problemas, ou falhas, em uma rede de dados. Envolve as tarefas de descobrir o problema, isolá-lo e solucioná-lo quando possível. Entre as causas mais prováveis para falhas em uma rede estão: erros de projeto e implementação da rede, erros de sobrecarga, distúrbios externos, tempo de vida útil de equipamentos expirado e má implementação de *softwares* [FRA02].

- **Configuração**: O gerenciamento de configuração está relacionado com a inicialização da rede e também com as tarefas de manutenção, adição, atualização e estado dos componentes durante a operação da rede [ALM05].

- **Contabilização**: Pode-se usar o gerenciamento de contabilidade para determinar se a utilização dos recursos da rede está aumentando com o crescimento, o que deve indicar a necessidade de adições e reajustamentos em um futuro próximo [PER01].

- **Desempenho**: Estatísticas de desempenho podem ajudar no planejamento, administração e manutenção de grandes redes. Essas informações podem ser utilizadas para reconhecer situações de gargalo antes que elas causem problemas para o usuário final. Ações corretivas podem ser executadas, tais como trocar tabelas de roteamento para balancear ou redistribuir a carga de tráfego durante horários de pico, ou, ainda, a longo prazo, indicar a necessidade de expansão de linhas para uma determinada área [GUB02].

- **Segurança**: O objetivo do gerenciamento de segurança é o de dar subsídios à aplicação de políticas de segurança, que são os aspectos essenciais para que uma rede baseada no modelo OSI seja operada corretamente, protegendo os objetos gerenciados e o sistema de acessos indevidos de intrusos. Deve providenciar um alarme ao gerente da rede sempre que se detectarem eventos relativos à segurança do sistema [SZT96].

3. Fluxos de rede e conversações

Existem várias definições para fluxos de rede, contudo a mais utilizada é a definida na versão 5 do *NetFlow* [CIS06] da Cisco, chamado de *NetFlow v5* [CIS06a].

Um fluxo de rede pode ser encarado como a metadata de uma comunicação de rede, comunicação esta que envolveria conexão, tráfego de dados e finalização de conexão. A metadata é um resumo deste volume todo de informações, extraindo de uma comunicação somente a informação realmente importante sobre este tráfego, ou seja, não é preciso armazenar e processar todo o tráfego de rede mas apenas o seu resumo.

O *NetFlow v5* define uma tupla com os seguintes dados para cada fluxo:

- IP (*Internet Protocol*) origem e destino;
- Porta origem e destino;
- Protocolo IP;
- TOS (*type of service*);
- A união das *flags* TCP (*Transmission Control Protocol*) observadas durante todo o fluxo.

Uma conversação de rede se assemelha a um fluxo de rede, contudo, no fluxo de rede, para cada comunicação seriam obtidas duas tuplas, uma referente ao IP originador da comunicação e outra para o IP que aceitou o estabelecimento desta, pois um fluxo de rede é sempre considerado como unidirecional, um fluxo no sentido servidor-cliente e outro no sentido cliente-servidor, conforme descrito por Yiming Gong [GON04].

Nas conversações, o que se resume é uma conexão de dados, com seu início e fim, gerando uma tupla para cada conexão que envolva dois pontos A e B. Esta tupla contém dados, tais como ambos IPs envolvidos, quantia de *bytes* (dados) trafegados *in/out* para cada um dos IPs e quantia de *frames* (pacotes) trafegados *in/out* para cada um dos IPs, conforme descrito por Gerald Combs [COM05].

4. Uso de *baseline* em análise de tráfego de rede

Uma *baseline* é um modelo que descreve que atividade de rede é considerada “normal”, de acordo com algum teste padrão de tráfego histórico, e todo tráfego que cair fora do escopo deste padrão será considerado como anômalo. Os relatórios de análise de tendência e de *baseline*, comumente referidos como *Top N* e *Análise de Baseline*, são os métodos mais simples, e comumente utilizados, de se fazer análise baseada em fluxos de rede. Dessa maneira, a atenção é dispensada sobre os registros de fluxos que têm "características especiais de volume elevado", especialmente o valor daqueles campos do fluxo que desviam significativamente de uma *baseline* histórica estabelecida [GON04].

O modelo de cálculo de *baseline* utilizado na versão corrente do NetAct é baseado na média de conversações originadas por cada *host*, individualmente, em seu histórico. O procedimento consiste em descartar as tuplas com valores nulos no campo avaliado (o campo de conversações originadas) e então é gerada a média dos N últimos valores históricos coletados para cada *host*. O valor de N serve para descartar dados muito antigos e pode ser configurado pelo usuário do sistema.

5. Implementação

A proposta do NetAct é a de utilizar-se um coletor de informações estatísticas de uso de rede já reconhecido (tal como o *tethereal* [COM05]) e montar uma base histórica de coletas para a definição de *baseline* de padrão comportamental das estações de rede. Algumas ferramentas de coleta foram testadas e serão apresentadas no item 5.1.

A partir da geração do padrão de uso de rede, por cada estação identificada, entraria em ação o módulo de atuação, cruzando informações de coletas atuais com a *baseline* gerada em banco de dados. Neste ponto, se uma máquina da rede interna, num determinado momento, saísse de seu padrão comportamental, ela seria isolada da rede com a finalidade de auditoria do *host* e da manutenção do acesso aos recursos de rede, tais como *link* internet e *link* entre segmentos, aos demais *hosts*.

O objetivo principal do NetAct é criar perfis individuais de uso estatístico de rede por parte dos *hosts* integrantes e, com isso, criar um mecanismo capaz de identificar desvios muito intensos de comportamento. Com esta finalidade, o NetAct objetiva principalmente a manutenção do acesso aos recursos de rede por parte dos demais integrantes do sistema sob controle, tendo como foco a proteção e manutenção da conectividade inter-redes, seja entre redes *LANs* (*Local Area Networks*) segmentadas internamente ou acesso ao *link* de internet.

Dentre os objetivos principais do gerenciamento de redes, os seguintes se destacam [ALM05]:

- Aumentar a disponibilidade da rede: essa tarefa surge da necessidade de se fornecer um ambiente rápido e seguro para o usuário. Nesse sentido, quaisquer problemas na rede devem ser resolvidos da forma mais rápida possível;

- Diminuir os custos de operação da rede: com o aumento da heterogeneidade das *LANs*, aumentou também a necessidade de se fornecer um ambiente de gerenciamento heterogêneo que desse suporte à manutenção de equipamentos de vários fornecedores.

5.1 Coleta de informações de uso de rede

O modelo de coleta de informações sobre o uso de rede foi implementado para atuar de modo passivo. O modo passivo compreende a coleta de informação sem a necessidade de instalação ou configuração de *software* adicional nas estações monitoradas. Na realidade, as estações monitoradas não precisam saber que estão sendo monitoradas, por isso não se adotou o uso de SNMP (*Simple Network Management Protocol*) [SNM06] para a coleta de dados de uso de rede.

Para tal modo de coleta torna-se necessário o uso de um sistema de captura de pacotes em modo promíscuo, ou *dump*. A escolha do *software* para a captura dos pacotes de rede foi feita levando em consideração a informação disponibilizada pelo aplicativo. Dentre os testes feitos, duas opções se destacaram: *NetFlow (flow-tools, softflowd)* e *tethereal*.

O *tethereal* foi o escolhido por fornecer um relatório mais compacto e pré-processado, levando em consideração a visão de conversações e não apenas fluxos. Uma visão geral do processo de coleta, geração de histórico e comparação com definição prévia de *baseline*, pode ser vista na figura 1.

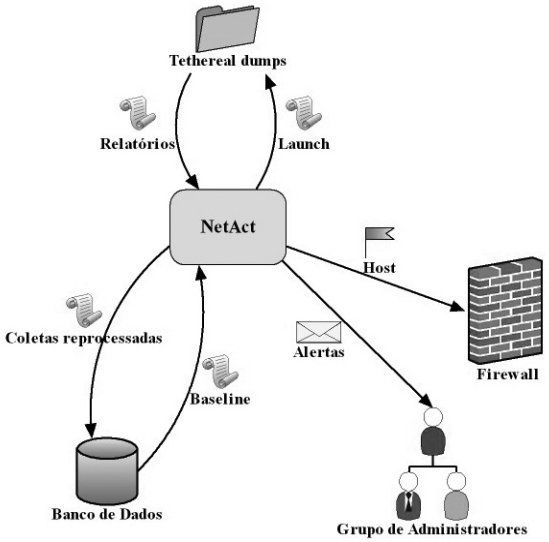

Figura 1. Esquema de funcionamento do NetAct

Após a execução do *tethereal* para captura de estatísticas de uso de rede, em modo passivo, individual por *host* identificado, o relatório pré-processado do *tethereal* é novamente reprocessado pelo NetAct. Esta etapa consiste em uma interpretação que o NetAct faz em cima do relatório gerado, agrupando os resumos de conversações identificadas para esta iteração, e gerando o valor total de conversações originadas, conversações recebidas, *bytes* enviados e recebidos em todas as conversações, bem como *frames* enviados e recebidos em todas as conversações, para cada *host*, em forma de somatório.

5.2 Aplicação de *baseline*

A aplicação de *baseline* só é possível quando se monta uma base histórica do funcionamento do que se quer analisar. Para a construção da *baseline* usou-se o banco de dados *MySQL*, já que este foi o que ofereceu a melhor interface de comunicação com a linguagem de programação utilizada na implementação do NetAct, o *ANSI C*.

Depois de cada iteração de coleta das informações de rede, os valores finais são armazenados em uma base de dados. A cada intervalo regular de tempo, o volume de dados armazenado é então processado para a geração da *baseline*, que será utilizada como parâmetro para constatação de anomalias de rede nos próximos processos de coleta e avaliação.

A geração da *baseline* é feita levando em consideração os ajustes históricos de mudança de comportamento, permitindo que um *host* mude, com o passar do tempo, a sua *baseline*, podendo variar seu padrão de comportamento sem comprometer a flexibilidade da rede e de seus usuários. Para que essa variação pudesse ocorrer, foi necessária a inserção de *thresholds* (sistema de tolerâncias para permitir variações de limites) no cruzamento de atividade atual do *host* com sua base histórica, criando assim uma pequena margem para crescimento ou decrescimento de atividade por estação monitorada sem gerar alertas.

O modelo utilizado para a determinação da linha de base do NetAct é o seguinte: para cada *host* monitorado na rede é criado um padrão individual, um valor simples, que é comparado, após cada iteração de monitoria, com o valor simples da leitura atual de conversações originadas pela máquina monitorada. Esse valor simples, que é a *baseline* individual do *host*, é gerado através do cálculo da média das últimas iterações registradas para aquele *host*. As iterações cujo valor de conversações originadas seja nulo (sem atividade na rede) são descartadas para não prejudicar o cálculo da média, pois podem ocorrer situações nas quais somente se capturam os pacotes entrantes

(requisições recebidas) e não os pacotes de saída, que seriam as conversações originadas, as que interessam neste ponto. A geração do valor médio de conversações originadas por *host* é efetuada a cada hora de monitoria do NetAct na rede, atualizando os valores referentes a cada *host* na rede, ajustando o seu padrão comportamental. No momento em que se percebe que uma determinada máquina está muito acima de sua média de conversações originadas, um alerta é disparado, e o bloqueio é efetuado.

Consideram-se ainda mais três pontos importantes na geração de *baseline*: 1) Somente é gerada a média de conversações originadas por um *host* caso este tenha um registro mínimo de monitorias realizadas. O valor mínimo é fixado em 100 iterações e, conforme explicado anteriormente, com o uso de *thresholds*, as iterações de monitoria seguintes poderão fazer com que a média gerada a partir destes 100 registros iniciais seja alterada, variando para cima ou para baixo; 2) Os registros muito antigos (valor de N definido pelo usuário) são descartados no cálculo da média; 3) Os registros identificados pelo NetAct como sendo "anormais", ou seja, aqueles muito acima do padrão previamente definido são marcados para não serem levados em consideração nas gerações seguintes de *baseline*, evitando assim que uma máquina já identificada como comprometida, venha a elevar a sua média, conseguindo escapar da marcação de máquina comprometida.

Quanto ao sistema de tolerância adotado, pode-se dizer que ele permite a variação da média gerada para cima ou para baixo. A partir do momento em que se tem um valor definido como média de conversações, com um mínimo de registros avaliados, aplica-se o sistema de *thresholds*, que funciona definindo que variações com até 100% de incremento no valor da média atual são permitidos, possibilitando a *baseline* variar para cima. Os valores registrados acima desse limite de tolerância são marcados como sendo comportamento anormal na base histórica do NetAct para o *host* em questão e não serão levados em consideração nas próximas gerações de média de conversações originadas. Qualquer valor abaixo ou igual ao valor atual da média de conversações originadas (e diferente de zero) é aceito, permitindo assim que a *baseline* possa também decrescer o seu valor, sempre individualmente, para cada máquina monitorada na rede.

A monitoração de *baseline* é um conceito simples que se aplica a muitas áreas onde há necessidade de monitorar e analisar quantidades grandes de dados. Reprocessar os dados todos, por inteiro, e de tempo em tempo, não é eficaz. A monitoração da linha de base é útil quando se analisa a mudança nos dados ao invés dos dados como um todo [RAC05].

5.3 Atuação

A atuação do NetAct na rede se resume em identificação do problema, isolamento e alerta. A identificação de *hosts* problemáticos é feita através da avaliação do seu estado atual em comparação ao seu histórico, caso o *host* em questão esteja saindo do padrão e excedendo os limites estabelecidos, este *host* é marcado.

Dos dados coletados e armazenados em banco de dados, para a geração da *baseline*, o mais importante para o NetAct é o de conversações originadas. Quando se identifica algum distúrbio no número de conversações que um dado *host* origina, a cada intervalo de coleta, a máquina em questão pode ser considerada como tendo um comportamento anormal, podendo estar comprometida. Quando uma máquina apresenta muitas iniciativas de conexão para diversos *hosts* diferentes ou para um *host* em específico, isso pode caracterizar uma tentativa de *spread* (disseminação) de vírus/*worm* ou ataque.

O isolamento do problema vem depois da identificação. Cada *host* marcado como tendo comportamento anormal é bloqueado junto ao servidor em questão, através

da alteração *on-the-fly* (flutuação, alteração de regras durante seu período de execução, bloqueando e liberando *hosts* ao decorrer do tempo) das regras de *firewall*. O passo seguinte é a notificação do grupo de administradores registrados sobre o desvio de comportamento do *host* identificado, bem como a notificação de seu devido bloqueio junto às regras de *firewall* da máquina.

No sentido de proteção do *link* de internet e segmentos, o NetAct precisa estar posicionado de forma correta dentro da rede. Para que o programa consiga efetuar a monitoração dos integrantes (*hosts*) de uma rede, ele precisa ser instalado em uma máquina com características de posicionamento geográfico privilegiado. A recomendação é de que ele seja posicionado em máquinas *Gateway* ou *Bridge*, quando da proteção e monitoração do link de segmentos de rede, ou então junto ao *Firewall* da rede, para a proteção e monitoramento do link de internet, conforme demonstrado na figura 2 e figura 3.

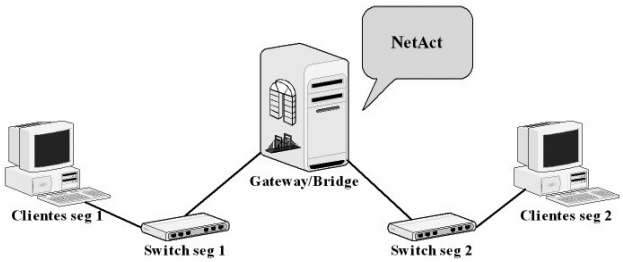

Figura 2. Posicionamento em rede: Protegendo segmentos de rede em *Gateway* ou *Bridge*

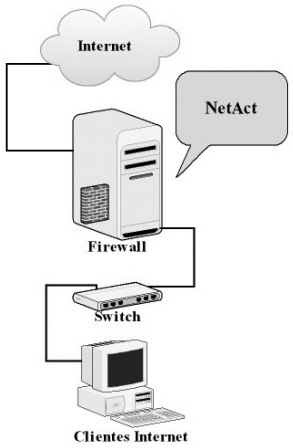

Figura 3. Posicionamento em rede: Protegendo *link* de internet no *Firewall*

Ressalta-se a importância de se posicionar o NetAct em uma máquina centralizadora de tráfego a fim de poder exercer, com sucesso, as suas funções de análise/coleta passiva de estatísticas de uso de rede, bem como a atuação efetiva em regras de bloqueio de *hosts* comprometidos, junto às regras de *firewall* da máquina responsável pelo setor de rede em questão.

O melhor a se esperar seria que as falhas que possam vir a ocorrer em um sistema fossem detectadas antes que os efeitos mais significativos decorrentes dessa falha fossem percebidos. Pode-se conseguir este ideal através da monitoração das taxas de erro do sistema e da evolução do nível de severidade gerado pelos alarmes, que permite emitir as notificações de alarme ao gerente, que pode definir as ações necessárias para corrigir o problema e evitar as situações mais críticas [ALM05].

6. Resultados parciais e trabalhos futuros

Os sistemas de gerenciamento de redes podem ser montados desde o uso simples de ferramentas ou protocolos específicos a um propósito no auxílio da manutenção de uma rede isolada até sistemas complexos, que cruzam informações de bases de dados distribuídas, ferramentas e protocolos diferentes para geração de relatórios e gráficos em tempo real do uso e estado de uma rede heterogênea e complexa.

O NetAct faz uso de ferramentas prontas, tais como o coletor de estatísticas de rede e o banco de dados escolhidos, e se caracteriza por fazer o reprocessamento, análise e intermédio das informações fornecidas com a finalidade de identificação de desvios comportamentais de tráfego dentro de uma rede de computadores, com o objetivo de efetuar bloqueios e gerar alertas.

Os objetivos iniciais do trabalho podem ser considerados atingidos, pois o *software* NetAct respondeu às expectativas, sendo capaz de identificar máquinas com comportamento anormal, que podem denotar características de máquinas comprometidas, ou por vírus ou por intrusores. O bloqueio dos *hosts* comprometidos e os alertas para grupos de administradores também estão implementados em sua versão atual.

Para trabalhos futuros verificam-se necessidades de alguns ajustes da implementação, podendo ser citados:

- Cruzar as informações de desempenho da rede com o comportamento individual e geral dos *hosts* e verificar se o nível de desempenho corrente da rede foi prejudicado, através de parâmetros como atrasos, vazão, disponibilidade, e o número de retransmissões realizadas. Isto teria a finalidade de constatar se um desvio de padrão comportamental foi realmente prejudicial à rede ou não.

- Desenvolver uma interface gráfica web para acesso a relatórios e interação com as regras de *firewall* alteradas/inseridas pelo NetAct.

- Implementar a geração de gráficos para demonstrativo do uso de rede pelos *hosts*, usando as informações coletadas na monitoria.

- Estudo e implementação de um novo método de geração de *baseline* mais elaborado, levando em consideração as informações de desempenho da rede contra as taxas de utilização da rede pelos *hosts*, e não somente a média de conversações por *host*.

- Inserção da avaliação de taxa de transferência em *bytes*, além da atual avaliação de conversações originadas.

- Avaliação das conversações não somente de origem por *host*, mas avaliação também das conversações por *host* como destino, a fim de estabelecer se determinada máquina está sendo alvo de tentativa de ataque por negação de serviço ou *portscan* (varredura de portas), eliminando assim falsos positivos. Quando uma máquina recebe requisições, ela também responde a estas, gerando conversações dessa máquina para outras, como sendo de origem sua, na visão de conversação, podendo causar falsos positivos. Num caso desses, a máquina não estaria originando várias requisições e sim apenas respondendo a um possível atacante.

7. Referências

[ALM05] ALMEIDA, Rodrigo Hermann. ***MTAS: Uma Ferramenta para Gerenciamento de Servidores de Aplicação***. Trabalho de Conclusão de Curso, Graduação. UNICRUZ, Universidade de Cruz Alta, Cruz Alta, RS. 2005.

[CIS06] Cisco NetFlow. ***Cisco IOS NetFlow Overview***. 2006. Disponível em: <http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00805e7c53.html>. Acesso em: <22 Jun.

2006>.

[CIS06a] Cisco NetFlow. ***Netflow***. 2006. Disponível em: <http://en.wikipedia.org/wiki/Netflow>. Acesso em: <22 Jun. 2006>.

[COM05] COMBS, Gerald. ***Tethereal ManPages***. 2005. Disponível em: <http://www.ethereal.com/docs/man-pages/tethereal.1.html>. Acesso em: <29 Set. 2005>.

[FIL03] FILHO, Raimir Holanda. ***AGRES Um Sistema Baseado em Conhecimento para Apoio à Gerência de Falhas em Redes de Computadores***. Dissertação de Mestrado. UFC, Universidade Federal do Ceará, CE, 2003. p. 153.

[FRA02] FRANCESCHI, Ana S. M.; BARRETO, Jorge M.; ROISENBERG, Mauro. ***Desenvolvendo Agentes de Software Para Gerência de Redes Utilizando Técnicas de Inteligência Artificial***. UFSC, Universidade Federal de Santa Catarina, Florianópolis, SC, 2002. p. 11.

[GON04] GONG, Yiming. ***Detecting Worms and Abnormal Activities with NetFlow, Part 1***. 2004. Disponível em: <http://www.securityfocus.com/infocus/1796>. Acesso em: <21 Abr. 2006>.

[GUB02] GUBERT, Luiz Cláudio. ***Utilizando o padrão de gerenciamento SNMP para gerenciar tráfego multicast: A ferramenta Multicast Monitor***. Dissertação de Mestrado. UFSC, Universidade Federal de Santa Catarina, Florianópolis, SC, 2002.

[PER01] PEREIRA, Mateus Casanova. ***Adminstração e Gerência de Redes de Computadores***. UFSC, Universidade Federal de Santa Catarina, Florianópolis, SC, 2001.

[RAC05] RACHMAN, Ophir. ***Baseline Analysis of Security Data***. 2005. Disponível em: <http://www.securitydocs.com/library/3018>. Acesso em: <21 Abr. 2006>.

[SNM06] SNMP. ***Simple Network Management Protocol***. Disponível em: <http://en.wikipedia.org/wiki/Simple_network_management_protocol>. Acesso em: <22 Jun. 2006>.

[SZT96] SZTAJNBERG, Alexandre. ***Gerenciamento de Redes - Versão Resumida Conceitos Básicos sobre os Protocolos SNMP e CMIP***. 1996. Disponível em: <http://www.gta.ufrj.br/~alexszt/ger/compact.html>. Acesso em: <20 Abr. 2006>.

[WAN03] WANDARTI, Daniel Francisco. ***Proposta de um Framework para Gerência de Clusters***. Dissertação de Mestrado. PUC-PR, Pontifícia Universidade Católica do Paraná, Curitba, PR. 2003. p. 79.