Rogério Carvalho Schneider

NETACT - ATUADOR EM GERÊNCIA DE REDES

Trabalho de Conclusão de Curso

CRUZ ALTA-RS, 2006.

Rogério Carvalho Schneider

NETACT - ATUADOR EM GERÊNCIA DE REDES

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Ciência da Computação, da Universidade de Cruz Alta-RS, como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. MSc. Antônio Rodrigo Delepiane de Vit

CRUZ ALTA-RS, JULHO 2006.

UNIVERSIDADE DE CRUZ ALTA - UNICRUZ
CURSO DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

A COMISSÃO EXAMINADORA, ABAIXO ASSINADA, APROVA O TRABALHO DE CONCLUSÃO DE CURSO INTITULADO

NETACT - ATUADOR EM GERÊNCIA DE REDES

Elaborado por

Rogério Carvalho Schneider

Como requisito parcial para obtenção do Grau de Bacharel em Ciência da Computação

Comissão Examinadora

Prof. MSc. Antônio Rodrigo Delepiane de Vit - Orientador _____/UNICRUZ-RS

Prof. MSc. Fábio Roberto Pillatt _____/UNICRUZ-RS

Prof. MSc. Luís Cassiano Goularte Rista _____/UNICRUZ-RS

CRUZ ALTA-RS, 15 DE JULHO 2006.

DEDICATÓRIA

Dedico este trabalho à minha família, responsável maior por eu ter chegado até aqui.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais, Dílson e Tadjane Schneider, pela força, incentivo e confiança depositados em mim e pela ajuda financeira.

À minha irmã Andréia e à minha namorada Cláudia, por me incentivarem a seguir em frente.

Ao meu orientador, professor Rodrigo, pela atenção dispensada e pelas cobranças feitas, ponto fundamental para a conclusão deste trabalho.

À professora Liane Margarida Rockenbach Tarouco, por aceitar co-orientar este trabalho e pelos materiais fornecidos.

Aos professores Copetti, Fábio e João Carlos, pelo convívio, confiança, reconhecimento e amizade.

A todos os mestres ao longo da minha formação, que souberam fazer despertar o meu interesse pelo conhecimento.

Ao meu amigo e colega Lucas "Scorfell" Schneider, pelo layout web desenvolvido para o NetAct.

E finalmente aos meus colegas de curso, dos quais guardarei somente lembranças boas, pela nossa amizade e confidência. Em especial aos amigos Jeferson, Maurício e Tiago.

RESUMO

NETACT - ATUADOR EM GERÊNCIA DE REDES

Autor: Rogério Carvalho Schneider

Orientador: Prof. MSc. Antônio Rodrigo Delepiane de Vit

O objetivo deste trabalho é apresentar o NetAct, uma ferramenta de auxílio no gerenciamento de redes de computadores. Esta ferramenta é capaz de identificar desvios no comportamento das máquinas internas à rede e tem a finalidade de realizar tarefas administrativas de forma autônoma, tomando decisões baseadas no histórico comportamental da rede.

Foram estudadas algumas ferramentas de gerência existentes, com a finalidade de identificar suas capacidades e realizar a escolha de uma ferramenta de geração de relatórios que pudesse ser utilizada em conjunto com o NetAct. Para a determinação do padrão comportamental da rede, os dados gerados pelos relatórios de uma ferramenta reconhecida em gerência de redes seriam então utilizados pelo NetAct em sua base histórica, auxiliando na tomada de decisão deste *software*. Como resultado deste trabalho obteve-se conhecimento sobre diversas ferramentas de gerência existentes, habilidades em gerenciamento de regras de *firewall*, banco de dados e, também, conhecimento sobre técnicas de detecção de intrusão e de programação. O resultado maior deste trabalho foi a produção de uma ferramenta de gerência de redes.

Deste conjunto de técnicas, estudos e ferramentas surgiu o NetAct, um atuador em gerência de redes, capaz de monitorar o comportamento de máquinas, em uma rede, e de avaliar seus padrões, determinando se a máquina está dentro ou não de seu funcionamento normal, realizando tarefas administrativas (bloqueios e alertas) de forma automática. Com isso, o objetivo proposto foi alcançado, o de produzir uma ferramenta capaz de atuar ativamente na monitoria e segurança da rede, fornecendo relatórios e gráficos de uso de rede e de padrão comportamental individuais para cada *host*.

PALAVRAS-CHAVE: Gerência de Redes, Análise de Padrão Comportamental, Monitoramento, Detecção de Intrusão.

ABSTRACT

NETACT - ATUADOR EM GERÊNCIA DE REDES

Author: Rogério Carvalho Schneider

Advisor: Prof. MSc. Antônio Rodrigo Delepiane de Vit

The objective of this work is to present the NetAct, a tool to aid in the management of computer networks. This tool is capable to identify shunting lines in the behavior of the internal network machines and it has the purpose to carry through administrative tasks of an independent form, taking decisions based on the mannering description of the network.

Some existing tools of management had been studied, with the purpose of identify its capacities and to carry through the choice of a tool of report generation that could be used in set with the NetAct. For the determination of the mannering standard of the network, the data generated for the reports of a recognized tool in network management then would be used by the NetAct in its historical base, assisting in the taking of decision of this software. As result of this work got knowledge on diverse existing tools of management, abilities in management of firewall rules, data base and, also, knowledge on techniques of programming and intrusion detection. The greater result of this work was the production of a network management tool.

Of this set of techniques, studies and tools appeared the NetAct, an actuator in network management, capable to monitor the behavior of machines, in a computer network, and to evaluate its standards, determining if the machine is inside or not of its normal functioning, carrying through administrative tasks (blocks and alerts) of automatic form. With this, the considered objective was reached, to produce a tool capable to actively act in the monitoring and network security, supplying reports and graphs of individual use of the network and mannering standard for each host.

KEY-WORDS: Network Management, Pattern Behavior Analysis, Monitoring, Intrusion Detection.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ISO	International Organization for Standardization ou Organização Internacional de Padronização
OSI	Open System Interconnection ou Sistema Aberto de Interconexão
SNMP	Simple Network Management Protocol ou Protocolo Simples de Gerência de Redes
IDS	Intrusion Detection System ou Sistema de Detecção de Intrusão
MRTG	Multi Router Traffic Grapher ou Traçador Gráfico Múltiplo de Tráfego de Roteadores
RRD	Round Robin Database ou Banco de Dados Round Robin
FCAPS	Fault, Configuration, Accounting, Performance and Security ou Falha, Configuração, Contabilizacão, Desempenho e Segurança
POP – RS	Ponto de Presença da RNP no Estado do Rio Grande do Sul
RNP	Rede Nacional de Pesquisa
TCHE	Integrantes da Rede do POP-RS, Universidades e Instituições de Ensino que utilizam recursos de Internet do POP-RS
TCP	Transmission Control Protocol ou Protocolo de Controle de Transmissão
IP	Internet Protocol ou Protocolo Internet
SYN	SYNchronize ou Sinalização de requisição de conexão em TCP
ACK	ACKnowledgement ou Confirmação de recebimento de pacote em TCP
LAN	Local Area Network ou Rede de Área Local
HTML	Hyper Text Markup Language ou Linguagem de Marcação de Hipertexto
PHP	Hypertext Preprocessor ou Pré-processador de Hipertexto
GNU	Acrônimo de: GNU's not UNIX ou GNU não é UNIX
BSD	Berkeley Software Distribution ou Distribuição de Software de Berkeley

SCSI Small Computer System Interface ou Interface de Sistemas Computacionais Pequenos

GB GigaByte, unidade de medida que representa aproximadamente 1 bilhão de bytes

RAM Random Access Memory ou Memória de Acesso Randômico

MHZ MegaHertz, frequência de trabalho de um processador em milhões de pulsos por segundo

PORTS Sistema de distribuição de pacotes utilizado nos sistemas operacionais da família BSD

API Application Programming Interface ou Interface de Programação de Aplicação

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 de comunicação convergem para o ambiente 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. À medida que o tempo passa, essas ferramentas têm ficado cada vez mais complexas e também se evidencia o aumento do número de revendedores de equipamentos. Conclui-se, daí, que uma rede que não pode ser gerenciada corretamente possui pouco valor (WANDARTI, 2003).

O objetivo deste trabalho é apresentar a ferramenta de auxílio na gerência de redes chamada NetAct. Essa ferramenta baseia-se em uma coleta de tráfego de rede em modo passivo, armazenamento de padrões de fluxos de rede para cada *host* e avaliação, a cada iteração de coleta, dos fluxos atuais contra os fluxos históricos, definindo se uma máquina está ou não fora do seu padrão normal de comportamento. A finalidade de se criar essa base histórica e avaliar o padrão de comportamento é identificar desvios e gerar alertas e bloqueios automáticos.

Por se tratar de uma ferramenta que será executada em uma máquina centralizadora de tráfego e por ter capturas de tráfego em modo passivo e local, o uso de SNMP não se fez necessário neste estudo de caso. Partindo do princípio que não se está fazendo coleta de tráfego e nem atuando em equipamentos remotos, o NetAct utiliza o Tethereal para captura em modo passivo dos pacotes de rede, dispesando a coleta de fluxos remotos oferecida pelo SNMP. A proposta é gerenciar a rede monitorando as máquinas que a compõem sem a necessidade de instalação de *software* adicional nos clientes.

No capítulo 2, a gerência de redes é apresentada com uma descrição de cada uma de suas categorias, conforme a divisão de modelos ISO de gerência. Também são apresentadas algumas ferramentas existentes para a gerência de redes e as ferramentas que foram utilizadas como base para o desenvolvimento do NetAct, sejam como trabalhos prévios ou correlatos. As teorias de fluxos de rede e de uso de *baseline* para criação de padrão histórico também são apresentadas nesse capítulo.

A descrição da ferramenta desenvolvida é feita no capítulo 3, bem como sua forma detalhada de instalação, funcionamento e uso.

No capítulo 4, os resultados do trabalho são expostos, e trabalhos futuros são propostos como forma de continuidade deste estudo.

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 (FILHO, 2003).

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. 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 (GUBERT, 2002).

O modelo ISO propõe a divisão da gerência de redes em cinco categorias. Essa divisão é chamada de FCAPS.

2.1 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* (FRANCESCHI; BARRETO; ROISENBERG, 2002).

O gerenciamento de faltas envolve a detecção, gravação, notificação e correção automatizada (na medida do possível) de problemas de rede. Este elemento é o mais largamente explorado no modelo ISO pelo fato de que falhas podem trazer *downtime* ou grande degradação às redes, tornando-as impraticáveis em determinados cenários.

2.2 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 (ALMEIDA, 2005).

A categoria de gerência de configuração explora o armazenamento histórico de versões utilizadas em sistemas da rede. Através de uma base de dados alimentada com a situação histórica de equipamentos, versões e distribuição destes na rede é possível se criar um *snapshot* do cenário atual da rede e efetuar o *backtracking* de problemas originados por conta de alteração de equipamentos em sua configuração, versão de *software* ou disposição na rede. A base citada serve como ponto de referência dos sucessivos cenários assumidos pela rede, podendo ainda servir como modelo para a implantação de novos cenários, por exemplos, que reproduzam uma configuração atual de rede já catalogada. O repositório desta base é formado por informações coletadas dos sistemas operantes na rede bem como de seus arquivos de configuração.

2.3 Contabilização

O objetivo da contabilização é medir os parâmetros de utilização da rede e criar meios de garantir que os usuários somente tenham acesso ao recurso a eles disponibilizado. Mensurando a utilização dos recursos de rede pelos usuários ou grupos, é possível criarem-se mecanismos que possam assegurar cotas de recursos, como banda de *link* ou espaço em disco, para os usuários catalogados. Regular o acesso aos recursos pode evitar problemas, pois, a partir desse procedimento, se está dando garantias aos demais usuários da rede de que, quando necessitarem, a sua porção de recurso estará disponível.

Pode-se também usar o gerenciamento de contabilidade para determinar se a utilização dos recursos da rede estão aumentando com o crescimento, o que deve indicar a necessidade de adições e reajustamentos em um futuro próximo (PEREIRA, 2001).

2.4 Desempenho

Relativamente ao gerenciamento de desempenho, busca-se medir e tornar disponíveis vários elementos relativos ao desempenho da rede. O objetivo dessas medições é manter os níveis de desempenho da rede em valores aceitáveis. Algumas das variáveis

avaliadas, quando se fala em desempenho da rede, estão relacionadas com tempo de resposta ao usuário e utilização do *link*.

Os passos envolvidos na gerência de desempenho são três, basicamente: primeiro, coleta de dados das variáveis a serem avaliadas; segundo, análise dos dados coletados para definição do funcionamento normal, a *baseline*; terceiro, cruzamento dos novos dados coletados com a *baseline* criada. Neste ponto, adotando um sistema de *thresholds* (tolerância a limites de variação), pode-se determinar se a variação do valor coletado para uma variável excedeu ou não os limites, e a partir disso alertas podem ser gerados.

O esquema proposto se caracteriza como sendo reativo. No momento em que um limite definido pelo administrador da rede é excedido, o alerta é gerado. Também se poderia adotar, em alguns casos, um esquema pró-ativo, que, através de simulações de crescimento de rede, poderia alertar com antecedência sobre perdas em desempenho na rede.

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 (GUBERT, 2002).

2.5 Segurança

O gerenciamento de segurança envolve o controle de pontos de acesso às informações sensíveis em uma rede. Essas informações armazenadas nos equipamentos de rede, as quais a organização deseja manter em segurança, não devem estar disponíveis para todos os usuários. O gerenciamento de segurança é responsável pela proteção dessas informações e pela detecção e relato das tentativas de intrusão na rede, ocorridas com sucesso ou não, incluindo facilidades para procedimentos de controle, tais como estabelecer políticas para o uso da rede, estabelecer e manter chaves criptografadas e códigos de autorização, manter um registro (*log*) do acesso à rede, prevenir e relatar acessos não autorizados, iniciar procedimentos de investigação em resposta a acessos não autorizados, detectar e prevenir vírus de computadores (LEWIS, 1995).

Quando se fala em gerenciamento com foco na segurança, fala-se sobre controle de acesso. Uma política interna a uma determinada rede é criada, e sobre esta política são liberados ou restringidos os acessos de determinados usuários ou grupos a certos recursos de rede. Utilizando mecanismos de autenticação, os recursos restritos são então liberados aos usuários aos quais a política de rede libera acesso ao recurso requerido.

Ainda no campo da gerência de segurança, a detecção de intrusão também é um assunto importante. A partir do uso de ferramentas que visam monitorar a rede, com a finalidade de detectar a presença de vírus. *worms* ou até mesmo atacantes, é possível garantir uma qualidade de acesso melhor aos recursos de rede, evitando o uso abusivo por parte das máquinas comprometidas ou com comportamento suspeito. Tais ferramentas são chamadas de IDS (*Intrusion Detection System*), e é nesta categoria de gerenciamento de redes em que o NetAct se enquadra, já que ele visa a detecção de anomalias na rede por meio da monitoração do uso de recursos, gerando os devidos bloqueios e alertas. No início da seção 2.8, as duas categorias mais conhecidas de IDS serão apresentadas.

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 (SZTAJNBERG, 1996).

2.6 Ferramentas de Gerência de Redes

Nesta seção, serão citadas algumas ferramentas de auxílio no gerenciamento de redes, as quais foram estudadas e utilizadas no processo de elaboração deste trabalho, com uma breve descrição de suas funcionalidades. Outras ferramentas, também aplicadas ao gerenciamento de redes, e diretamente relacionadas ao NetAct, serão apresentadas nas seções 2.8 e 2.9, em momento oportuno.

2.6.1 MRTG

O MRTG (*Multi Router Traffic Grapher*) (OETIKER, 2005) objetiva gerar uma página *web* com gráficos e taxas de utilização dos recursos monitorados. Os gráficos do MRTG

são previamente definidos, e fornecem uma visão do estado atual e histórico do uso do recurso monitorado.

Fazendo uso do protocolo SNMP (*Simple Network Management Protocol*) (SNMP, 2006), o MRTG captura as informações fornecidas pelos equipamentos configurados com o SNMP, e monta gráficos que demonstram o uso do recurso monitorado. Uso diário, semanal, mensal e anual são listados na tela de gráficos.

O MRTG pode ser aplicado à monitoria de qualquer tipo de recurso, mas é normalmente utilizado na monitoria do *link* de rede ou internet em roteadores ou *gateways*. O equipamento monitorado precisa estar habilitado para fornecer acesso aos objetos SNMP gerenciados.

2.6.2 Cacti

O Cacti (GROUP, 2005) tem o objetivo de fornecer uma interface amigável ao uso do poderoso pacote RRDtools (OETIKER, 2006).

Ao usuário são fornecidos modelos de geração de gráficos e sistemas básicos de coleta de informação e alimentação de bases RRD (*Round Robin Database*), tudo através de uma interface *web*, facilitando o uso deste recurso na monitoria de objetos.

Por ser capaz de gerenciar gráficos de praticamente qualquer coisa, o Cacti não é usado somente em gerência de redes, apesar de este ser o seu uso mais comum. O fornecimento de uma interface *web* para criação de novos gráficos, e acesso a estes, tornou o Cacti muito popular no processo de visualização gráfica de recursos computacionais diversos.

2.6.3 Nagios

O Nagios (GALSTAD, 2005) é um *software* monitorador de máquinas e serviços. Ele é capaz de identificar se os servidores e serviços remotos, configurados para serem monitorados, estão ou não rodando satisfatoriamente.

O administrador da estação gerencial (onde o Nagios está instalado e rodando) deve configurar os grupos de administradores, grupos de servidores e grupos de serviços no Nagios. Essa máquina onde o Nagios se encontra instalado deve ter acesso às máquinas e serviços gerenciados e, a partir deste cenário, a monitoria começa.

Ao perceber que alguma máquina ou serviço se encontra fora de operação ou com

atrasos muito elevados nas respostas, o Nagios emite notificações, via *e-mail*, *sms* ou sistema de mensagens instantâneas, aos grupos de administradores responsáveis pelo setores que apresentam defeito. Da mesma forma, quando um serviço é restabelecido, o Nagios também informa aos grupos de contatos que a situação voltou ao normal.

Além dos alertas por *e-mail* e *sms*, o Nagios oferece uma interface *web*, onde se pode ter acesso a relatórios de disponibilidade dos servidores e serviços monitorados, e onde se pode, também, visualizar a situação atual dos grupos monitorados. Virtualmente, é possível se monitorar qualquer coisa com o Nagios, basta que exista um *plugin* disponível para o que se quer monitorar.

2.6.4 NTop

O NTop (DERI, 2006) é uma ferramenta de gerência de redes que possui uma interface gráfica *web* completa. A idéia do NTop é baseada no comando *top* do Unix, que mostra o uso de recursos de cpu e memória pelos processos de um sistema operacional Unix. Contudo, o NTop objetiva mostrar o uso de recursos de rede, não de cpu.

A interface gráfica do NTop é o seu grande atrativo, pois ela informa os *Top Users* de maneira que se possa navegar pelas páginas de relatórios clicando nos links gerados para cada host ativo na rede. Os gráficos são gerados em tempo de acesso à interface, portanto, são gráficos atualizados. O nível de detalhamento das informações é grande, mostrando protocolos, portas, conexões e tráfego para cada host ativo na rede.

A ferramenta somente possui módulos de visualização de estatísticas de uso de rede, não oferece nenhuma forma de interação com o *firewall*.

2.6.5 Portsentry

O Portsentry (PSIONIC, 2006) tem a finalidade de identificar tentativas de ataque baseadas em *portscan* (varredura de portas em busca de vulnerabilidades). Através da detecção da ocorrência de espécies de assinaturas de *scanners*, o Portsentry consegue identificar tentativas de varreduras, e pode tomar ações a partir destes fatos.

As ações podem ser avisos por *e-mail* aos administradores da rede, informando o que está acontecendo, ou até mesmo o bloqueio da máquina que está apresentando o comportamento não desejado.

O Portsentry não oferece interface gráfica *web* e nem relatórios, e não possui um

sistema de *whitelist* (lista de *hosts* que nunca devem ser bloqueados).

2.6.6 Snort

O Snort (ROESCH, 2006) é um poderoso IDS, programado em linguagem C e que age de modo passivo na coleta de pacotes de rede. Ele coleta, analisa e armazena registros (*logs*) de pacotes, com a finalidade de efetuar uma grande variedade de operações sobre estes dados.

Algumas das operações possíveis em cima dos dados que o Snort é capaz de capturar são: a detecção de *portscan*; detecção de ataques dos mais variads tipos; detecção de presença de virus ou worms na rede, dentre outros. Todas as análises são baseadas em assinaturas de *softwares* mal intencionados, que são cruzadas em sua base de dados, permitindo a identificação de grande variedade de problemas de rede.

Tais análises somente são possíveis de serem feitas pelo Snort por ele ser capaz de fazer a análise de conteúdo dos pacotes capturados na rede e por ter a sua base de assinaturas constatemete atualizada pela internet.

O Snort não oferece interface gráfica *web* nativa e não provê recursos de bloqueios automáticos ou relatórios, mas possui sistema de alertas de variados tipos, dentre eles o *e-mail*, para os alertas mais graves.

2.7 Tabela comparativa

A tabela 1 mostra algumas das funcionalidades das ferramentas estudadas, comparadas entre si, quanto às suas funções, tipo de interface, geração de gráficos e atuação.

FERRAM.	**FUNÇÃO**	**INTERF.**	**GRÁF.**	**ATUA**
MRTG	Gráficos de utilização de recursos	Web	Sim	Não
Cacti	Criação a alimentação de RRDs	Web	Sim	Não
Nagios	Gerência de falhas em estações e serviços	Web	Sim	Alertas
NTop	Gráficos de utilização de rede	Web	Sim	Não
PortSentry	Detectar varreduras de portas	Não	Não	Bloqueios
Snort	Detectar máquinas comprometidas	Não	Não	Alertas

Tabela 1: Comparativo de ferramentas de Gerência

As ferramentas previamente citadas foram importantes na elaboração deste trabalho, pois serviram como base para o desenvolvimento das diversas características do NetAct. O MRTG e Cacti serviram de exemplo na geração de gráficos, usando RRDtools. Das ferramentas Nagios e NTop foi retirada a idéia de uma interface *web* para

o gerenciamento da ferramenta. Do Portsentry e Snort veio a idéia de se fazer uma ferramenta que pudesse identificar a intrusão e gerar bloqueios e alertas de forma automática, porém contando com uma interface em modo *web* e que não fosse baseada em assinaturas, e sim em padrões de rede.

2.8 Trabalhos prévios considerados

Nesta seção, apresenta-se uma breve descrição sobre os trabalhos prévios considerados para a elaboração deste. O estudo das ferramentas citadas possibilitou a escolha de um gerador de relatórios de uso de rede para ser utilizado em conjunto com o NetAct.

Manter a qualidade de serviço durante o maior período de tempo possível é o ideal para qualquer administrador de redes. A procura pela manutenção da conectividade envolve o uso de ferramentas de gerência, visando à visualização da situação em que uma rede de computadores se encontra, com a finalidade de identificar possíveis sinais que indiquem queda de desempenho ou quebra de segurança.

Para a identificação de quebras de segurança em redes, utilizam-se técnicas e ferramentas de IDS (*Intrusion Detection System*), que têm a finalidade de identificar tentativas de quebra de segurança a partir de máquinas comprometidas na rede.

A detecção de intrusão é definida como "o processo de identificação e resposta à atividade mal intencionada dirigida a recursos de computação e rede" (AMORSO, 1999). Os sistemas de detecção de intrusão tentam rastrear tentativas de ataques contra recursos de computação e rede através da monitoração do comportamento de máquinas e pessoas. Tais sistemas fazem uso de duas categorias principais de monitoramento: detecção de uso indevido e detecção de anomalias.

A detecção de uso indevido de recursos baseia-se na análise de padrões reconhecidos de atividades mal intencionadas. Cruzando-se a atividade atual com assinaturas de atividades sabidamente mal intencionadas, é possível identificar tentativas de intrusão.

A detecção de anomalias baseia-se na definição de padrões comportamentais. O comportamento que estiver fora do escopo do padrão comportamental previamente definido é considerado como anormal, e fica marcado como possivelmente uma tentativa de intrusão.

A busca por um sistema de automatização de tomadas de decisão e atuação no

gerenciamento de redes, a partir da análise estatística dos padrões de uso de rede, fez com que se propusesse a criação do NetAct.

2.8.1 Gerência de Segurança Através do Uso de Netflow

No artigo (BERTHOLDO; ANDREOLI; TAROUCO, 2003) é feita uma demonstração de como utilizar o NetFlow para coletar fluxos de rede a partir de roteadores CISCO e gerar relatórios gráficos com a finalidade de facilitar a identificação de ataques de *worms* na rede.

O ambiente montado no referido trabalho envolvia a captura de fluxos de rede a partir dos roteadores da rede do POP-RS com a finalidade de gerenciar a segurança envolvendo os clientes da rede TCHE. O cenário do sistema de gerência foi montado com a utilização das ferramentas de geração, captura e análise de fluxos de rede.

As ferramentas utilizadas foram:

- A habilitação da exportação de fluxos de rede nos roteadores da rede POP-RS no formato NetFlow;
- A instalação de um coletor desses fluxos exportados, o CFlowd (CAIDA, 2005a), que coleta os dados enviados do roteador e os armazena em disco para posterior processamento;
- O uso de um conjunto de ferramentas para manipular tais dados armazenados em arquivos, o flow-tools (FULLMER, 2005);
- E, por fim, um gerador de relatórios gráficos, o FlowScan (PLONKA, 2005).

Através da análise dos gráficos gerados, pôde-se chegar à identificação de anomalias na rede, e com uma visão mais detalhada do histórico de fluxos foi possível identificar os blocos IP ou máquinas que apresentavam sintomas de infecção por *worm*.

2.8.2 O NetFlow

O NetFlow (CISCO, 2006a) é um padrão de exportação de fluxos de rede utilizado em roteadores, tais como CISCO, Junniper e Extreme. Esta exportação de fluxos também pode ser emulada em máquinas roteadoras que utilizem sistemas operacionais em plataforma Unix, tais como as distribuições Linux ou o FreeBSD.

A partir da coleta de fluxos de rede, pode-se traçar gráficos detalhados da utilização da recursos de rede, e com diferentes visões da rede, é possível se chegar, com precisão, ao ponto que pode estar gerando queda de desempenho ou tentativa de quebra de segurança.

Para a geração, coleta, armazenamento e análise dos fluxos, algumas ferramentas estão disponíveis em formato de código aberto. São elas:

- softflowd (MILLER, 2005): Permite a geração e exportação da informação sobre os fluxos de rede correntes;
- flow-tools: Conjunto de ferramentas que permitem a coleta, armazenamento, manipulação e análise das informações de fluxos de rede exportadas pelo softflowd ou por roteadores configurados para a exportação de fluxos.
- FlowScan. Utilizado na geração de gráficos para facilitação da visualização da informação gerada pelos fluxos de rede no formato do NetFlow.

Na seção 2.10, os fluxos de rede serão explicados em detalhes.

2.8.3 A ferramenta Tethereal

O Tethereal (COMBS, 2005) é uma ferramenta que oferece a possibilidade de coleta e análise do tráfego de rede em modo texto, em terminais de sistemas baseados na plataforma Unix. Ele permite a captura e análise de pacotes de rede próximo do tempo real, gerando relatórios da utilização da rede em formato texto simples.

Os tipos de relatórios gerados pelo Tethereal são variados, mas o mais interessante deles para este trabalho é o relatório de conversações por IP, que dá uma visão do número de conexões, *bytes* e pacotes que uma máquina gera durante um certo período de avaliação da rede.

Na seção 2.10, as conversações serão explicadas em detalhes.

2.8.4 Comparação

Enquanto o NetFlow permite a geração, coleta e análise dos fluxos de rede a partir de uma máquina ou roteador configurados para a exportação desses dados, o Tethereal permite a geração de dados semelhantes aos fluxos de rede, que seriam as conversa-

ções, de uma forma mais direta, capturando os dados necessários diretamente das interfaces de rede da máquina centralizadora de tráfego.

O NetFLow exige a habilitação da exportação de fluxos, por um lado, e a coleta e processamento destes fluxos por outro. O Tethereal é mais direto, possibilitando uma instalação do cenário de forma mais simplificada, pois, para o seu funcionamento, ao contrário do sistema NetFLow, não é preciso fazer uso de mais do que um único comando.

Os relatórios gerados pelo NetFlow são salvos em arquivos binários, e é necessária a utilização de ferramentas do pacote flow-tools para decodificá-los a fim de poder utilizá-los, já o Tethereal tem a possibilidade de salvar os relatórios gerados diretamente em formato texto, facilitando a interação desta ferramenta com o NetAct.

Pelos motivos anteriormente descritos, optou-se por utilizar o Tethereal em conjunto com o NetAct para a geração de relatórios de carga de utilização de rede.

Em relação ao trabalho de (BERTHOLDO; ANDREOLI; TAROUCO, 2003), pode-se perceber a diferença da proposta do NetAct quanto à atuação na rede. Enquanto no trabalho citado o cenário é montado para fornecer ao adminstrador uma visão geral da situação atual e histórica da rede, no NetAct a proposta é de manter alguns gráficos e relatórios para controle do adminstrador da rede, mas principalmente atuar nas regras de *firewall* e emitir alertas ao detectar anomalias.

2.9 Trabalhos relacionados

A seguir são apresentados de forma breve alguns trabalhos que abordam temas relacionados com a proposta deste.

2.9.1 A ferramenta flow-host-profile

Na proposta descrita em (ROMIG; FULLMER; RAMACHANDRAN, 1999), foi utilizado o conjunto NetFlow+flow-tools para a definição de padrões de comunicação individuais para as máquinas componentes da rede.

O flow-host-profile cria uma listagem de IPs e portas normalmente utilizadas na rede em que atua. A taxa de utilização para cada IP em cada porta listada é gerada e armazenada como sendo o padrão comportamental esperado para aquela máquina. Quando se percebe uma atividade muito acima da considerada normal para uma deter-

minada porta em um IP em específico, um alerta é gerado. A ocorrência de atividade em novas portas (antes não utilizadas pelo *host*) também gera alertas no flow-host-profile.

2.9.2 A ferramenta Net-Watcher

Através da análise de cabeçalhos de pacotes TCP (*Transmission Control Protocol*) com o Net-Watcher (PARK, 2001) é possível gerarem-se perfis de comportamento dos IPs que compõem a rede monitorada, perfis individuais e perfis de comportamento padrão de rede.

A maneira utilizada, no referido trabalho, para a detecção de anomalias, foi gerar um perfil diário de comportamento dos *hosts* a partir da coleta de dados, tais como pares de IP origem/destino, portas de entrada e saída e *flags* TCP SYN/ACK, e comparar estes dados com um perfil de comportamento padrão de rede, também gerado pelo Net-Watcher.

Toda a coleta de fluxos de rede é gerada durante 24 horas e armazenada em disco. Após este passo, as ferramentas de geração de perfil diário e de anomalias devem ser executadas manualmente pelo adminstrador da rede. Após estes procedimentos tem-se a possibilidade de leitura dos relatórios gerados e identificação dos *hosts* possivelmente comprometidos na rede, além da identificação de ocorrências de *portscan* (varredura de portas em busca de vulnerabilidades) a partir de *hosts* externos à rede com destino a servidores internos. Utilizando-se então as ferramentas componentes do pacote fornecido na instalação do Net-Watcher consegue-se extrair relatórios que indicam quais *hosts* na rede têm demonstrado um comportamento anormal. A partir destes relatórios, poder-se-iam identificar os pontos problemáticos na rede.

2.9.3 Comparação

Comparando-se a proposta dos dois trabalhos correlatos apresentados anteriormente ao NetAct, pode-se notar algumas diferenças.

No que diz respeito ao conteúdo avaliado por cada proposta para a detecção de anomalias, nota-se que a proposta do flow-host-profile é criar um perfil de uso de serviços de rede por *host*, definindo quais são as portas comumente acessadas por um determinado *host* e disparando alertas ao perceber atividade em novas portas. O Net-Watcher, por sua vez, preocupa-se em analisar os cabeçalhos IP e guardar informações

relativas ao uso de portas e *flags* TCP para cada *host*, interno ou exteno à rede, e, ao final do dia, gerar relatórios do comportamento diário das máquinas, sendo capaz de identificar comportamentos estranhos, comparando a atividade diária com o padrão de comportamento normal de rede, o qual também é gerado pelo Net-Watcher e salvo em arquivo.

Quanto ao procedimento adotado por cada ferramenta ao identificar problemas, não se percebe diferença alguma entre o flow-host-profile e o Net-Watcher. Ambos geram relatórios de anomalias, em modo texto, e deixam que o adminstrador da rede decida o que fazer após ler os relatórios gerados. O Net-Watcher faz mais ainda: deixa que o próprio adminstrador gere manualmente os relatórios desejados.

A diferença do NetAct para as ferramentas citadas anteriormente é que ele se preocupa em analisar e armazenar os dados referentes ao tráfego de saída dos *hosts* da rede interna (conversações originadas) e, baseado nisso, cria uma linha de base que define qual o limite aceitável de tráfego de saída para cada *host*, disparando rotinas de bloqueio imediato e alertas via *e-mail* ao identificar um *host* muito acima de seu padrão de tráfego de saída. O NetAct ainda é capaz de mostrar ao adminstrador, em modo gráfico, através de sua interface *web*, quais os *hosts* que têm demonstrado maior atividade na rede, quais os atuais bloqueados e gráficos de comportamento individual das máquinas que compõem a rede monitorada.

2.10 Fluxos de rede e conversações

Existem várias definições para fluxos de rede, contudo a mais utilizada é a definida na versão 5 do NetFlow da Cisco, chamado de NetFlow v5 (CISCO, 2006b).

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 origem e destino;
- Porta origem e destino;

- Protocolo IP;
- TOS (type of service).
- A união das *flags* TCP 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 (GONG, 2004).

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* 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 (COMBS, 2005).

2.11 Uso de *baseline* na 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* (hosts mais ativos) e *Análise de Baseline* (hosts com atividade acima do normal), 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 (GONG, 2004).

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 (conversações originadas) e então gerar 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. Na seção 3.5.3, a aplicação de *baseline* será explicada em detalhes.

No próximo capítulo, a descrição da implementação do NetAct será feita em detalhes, mostrando quais ferramentas e linguagens foram utilizadas para a composição deste trabalho. Um detalhamento sobre os processos de instalação, uso e funcionamento do NetAct também será apresentado no capítulo seguinte.

3 DESCRIÇÃO DA FERRAMENTA DESENVOLVIDA

A proposta do NetAct é a de utilizar-se um coletor de informações estatísticas de uso de rede já reconhecido (tal como o Tethereal) 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 3.5.1.

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 internas segmentadas ou acesso ao *link* de internet.

Dentre os objetivos principais do gerenciamento de redes, os seguintes se destacam (ALMEIDA, 2005):

- 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.

Nas seções a seguir, o NetAct terá todas as suas funcionalidades explicadas em detalhes.

3.1 O NetAct na Gerência de Redes

A ferramenta NetAct, que será apresentada neste capítulo em detalhes, é direcionada ao auxílio no gerenciamento de redes. Por se tratar de um analisador de estatísticas de uso de rede, e por interargir com as regras de *firewall* do servidor, o NetAct se caracteriza como um atuador em gerência, capaz de tomar decisões baseadas em históricos e de agir controlando o bloqueio e liberação de *hosts* dentro de uma rede.

Das cinco categorias de gerenciamento de redes apresentadas no capítulo 2, a categoria na qual o NetAct melhor se enquadra é a de gerência de segurança de redes. Por se tratar de um *software* que identifica possíveis intrusores na rede, os bloqueia e gera alertas, o NetAct pode ser considerado uma ferramenta de IDS voltada à detecção de anomalias, fazendo assim parte da categoria de ferramentas de gerenciamento de segurança, assim como no exemplo apresentado na seção 2.8.1.

3.2 Implementação da ferramenta desenvolvida

Para a implementação da ferramenta desenvolvida foi utilizada a linguagem de programacão C, em ambiente Unix, para a camada funcional da aplicação. Para a camada de interface com o usuário foi utilizado o conjunto HTML+PHP.

A linguagem C foi a utilizada devido a sua velocidade de execução, já que o número de registros processados pode ser elevado, dependendo do cenário em que o sistema estiver instalado.

O compilador utilizado foi o gcc 3.4.4 (GNU Compiler Collection) (FOUNDATION, 2005), no sistema operacional FreeBSD 6.0-STABLE (DISTRIBUTION, 2006).

O banco de dados escolhido para armazenagem histórica e processamento estatístico dos dados foi o MySQL 5.0.22 (MYSQL, 2006).

Para a geração do gráficos utilizou-se a ferramenta RRDtools 1.2.11.

A máquina utilizada na implementação possui quatro processadores Intel de 550MHz, três discos SCSI de 9GB cada, cinco interfaces de rede para os diversos segmentos monitorados e 1GB de memória RAM.

A interface *web* do sistema rodou sob um servidor Apache 2.2.2 (FOUNDATION, 2006) com PHP 4.4.2 (TECHNOLOGIES, 2006) habilitado, com módulo php4-mysql instalado via Ports (PORTS, 2006).

O NetAct teve seu ambiente de testes montado sobre o sistema operacional FreeBSD, contudo, o NetAct também oferece compatibilidade com sistemas Linux (LINUX, 2006). Além do módulo de interação com o *firewall* do FreeBSD, o IPFW (IPFW, 2005) o NetAct possui um módulo de interação com o IPtables (PROJECT, 2006), o *firewall* do Linux. Todo o código fonte do projeto foi montado de forma que se possa compilá-lo tanto em distribuições BSD como em distribuições Linux, e as dependências do NetAct, tais como banco de dados MySQL, RRDtools e demais citados, tem, da mesma forma, portabilidade para Linux.

3.3 Visão Geral

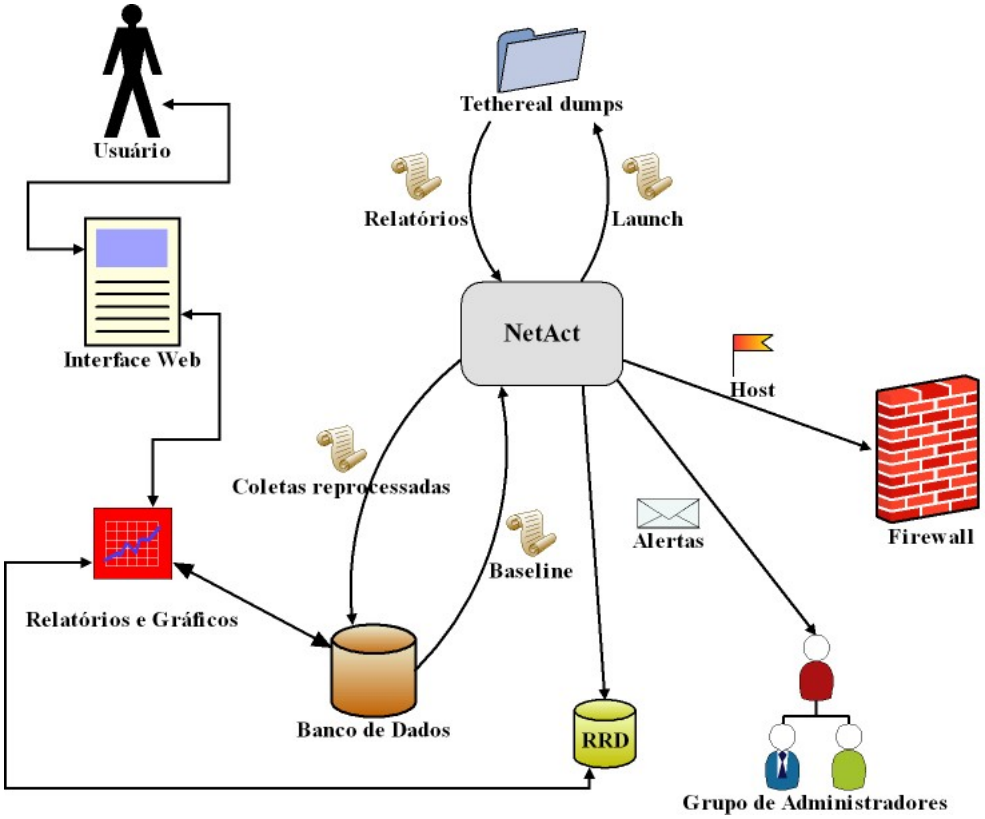

Figura 1: Esquema de funcionamento do NetAct

A figura 1 mostra uma visão geral do funcionamento do NetAct.

- O usuário (administrador) acessa a interface *web* do sistema para mudar parâmetros de configuração, acessar relatórios de *Top Users* ou visualizar gráficos de comportamento de *hosts*;
- A interface *web* se comunica com o banco de dados e registros de bases RRD para mostrar os relatórios de *Top Users* e gráficos de comportamento;

- O NetAct executa o Tethereal para a coleta de informações do uso de rede pelos *hosts*;
- Ao receber o retorno do Tethereal, o NetAct interpreta os relatórios gerados e grava as informações resumidas no banco de dados e bases RRD;
- As novas imagens gráficas de acesso são geradas a partir dos novos dados encontrados nas bases RRD;
- Os dados interpretados dos relatórios fornecidos pelo Tethereal são cruzados em teste contra as informações de *baseline*, mantidas em banco de dados;
- Caso seja notada alguma anomalia comportamental para um determinado *host*, este é bloqueado junto às regras de *firewall* da rede e um alerta é enviado por *e-mail* ao grupo de adminstradores cadastrados;
- Caso não seja notada nenhuma anomalia, os valores coletados são levados em consideração para a alteração da *baseline* pertinente a cada *host* monitorado na rede.

Dessa maneira, o adminstrador pode acompanhar graficamente o estado de sua rede e o comportamento de tráfego das máquinas. Um acesso *web* é fornecido para facilitar a interação humana com o *software*, em suas configurações, relatórios e atividades de bloqueio e desbloqueio de *hosts*.

3.4 Preparação do Ambiente e Instalação

Para a validação do trabalho proposto foi montado o seguinte cenário:

- Instalação do sistema operacional FreeBSD 6.0 em um servidor de *Firewall*;
- Criação da base de dados em MySQL no mesmo servidor;
- Habilitação do serviço *web* com Apache dando suporte a PHP;
- Habilitação do PHP para suporte a conexão com MySQL;
- Instalação do Tethereal na máquina de *Firewall*;
- Instalação do pacote RRDtools;
- Instalação do sistema NetAct no mesmo servidor.

Como o sistema operacional escolhido foi o FreeBSD, que oferece a facilidade de ter o gerenciador de pacotes chamado Ports, todos os pacotes necessários para o funcionamento correto do NetAct foram instalados utilizando-se o Ports, nos seguintes procedimentos:

```
# cd /usr/ports/databases/mysql50-server

# cd /usr/ports/databases/mysql50-client

# cd /usr/ports/databases/mysql50-scripts

# cd /usr/ports/www/apache22

# cd /usr/ports/lang/php4

# cd /usr/ports/databases/php4-mysql

# cd /usr/ports/net/tethereal

# cd /usr/ports/net/rrdtool
```

Para cada diretório citado o comando "make install" foi executado, a fim de instalar o pacote selecionado via Ports.

Após a instalação desses pacotes, é necessário, antes da compilação e instalação do NetAct, fazer alguns ajustes simples no sistema. Como o NetAct se utiliza, em tempo de compilação e execução, da biblioteca forncecida pelo MySQL para conexão da linguagem C ao banco de dados, é preciso ajustar o sistema da seguinte maneira, a fim de que o compilador gcc seja capaz de encontrar a biblioteca requerida:

```
# cd /usr/local/lib

# ln -s /usr/local/lib/mysql/libmysqlclient.so.15

# ldconfig
```

Com estes passos o sistema está pronto para receber o NetAct, através do "make all" e "make instalar", dentro do pacote descompactado da ferramenta proposta:

```
# tar xzvf netact.tar.gz

# cd netact

# make all

# make instalar
```

Concluído este passo, os arquivos seguintes serão instalados no sistema:

- "/usr/local/bin/netact": Este é o programa em si, o binário, que será executado para a monitoria da rede;
- "/usr/local/etc/netact/netact.conf-dist": Este é o arquivo original de configuração do NetAct quanto à sua conexão com o banco de dados. Este arquivo deve ser editado (caso o usuário deseje customizar a conexão com o banco) e salvo com as novas configurações (ou com as suas próprias configurações originais) em "/usr/local/etc/netact/netact.conf". Este arquivo contém somente os dados de conexão com o banco, todas as outras configurações do NetAct serão alteradas pela sua interface gráfica *web*.

Após isso, é necessário criar o banco de dados e usuário no MySQL, do qual o NetAct fará uso através do programa principal, em C, e da interface *web*:

```
# mysql < sql/netact_db.sql
```

Com isso, a estrutura completa do banco de dados será criada automaticamente, e o NetAct estará pronto para ser executado através dos scripts fornecidos em seu diretório:

```
# ./start.sh

# ./stop.sh
```

O NetAct é um processo que roda no sistema o tempo todo, monitorando a geração de relatórios do Tethereal e as requisicões, via banco de dados MySQL, da interface *web*. Ao rodar o comando "./start.sh", o usuário será devolvido ao prompt de comando, mas o NetAct estará sendo executado em *background* até que seja parado, novamente, pelo administrador do sistema.

3.5 Processamento

A seguir será explicado, passo a passo, o funcionamento do NetAct no que diz respeito ao processo de coleta de dados de uso de rede, interpretação de relatórios, ajustes de *baseline* e atuação através de bloqueios e alertas.

3.5.1 Coleta de informações de uso de rede

O modelo de coleta de informações sobre o uso de rede foi implementado para atuar em 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 essa razão não se adotou o uso de SNMP para a coleta de dados de uso de rede. Contudo, uma maneira de se utilizar o SNMP, centralizando a captura dos fluxos, seria implantar a coleta, armazenamento e análise de fluxos de rede na máquina em que o NetAct estivesse instalado, centralizando o tráfego, e com isso utilizar-se do softflowd e flow-tools para coleta e decodificação dos dados armazenados, para posterior processamento pelo NetAct. Caso este modelo fosse utilizado um parâmetro importante de configuração do NetAct ficaria prejudicado, o tempo máximo de coleta ("flow_capture_time_min"), que é definido pelo adminstrador da rede, e explicado na subseção 3.7.1. Por se tratar de um conjunto de *daemon* (softflowd), que captura os fluxos de rede e os exporta, via SNMP, e ferramentas de decodificação (flow-tools, flow-captute), que são capazes de receber estes fluxos por SNMP, armazená-los em disco e processar os arquivos gerados, a configuração do tempo máximo de captura ficaria prejudicada pelo fato de que o *daemon* teria de ser reiniciado, a cada alteração de configuração, com o novo tempo máximo estabelecido pelo usuário. O Tethereal neste ponto é muito mais flexível, pois ele é lançado a cada iteração pelo NetAct já com o seu tempo máximo de coleta estipulado e, ao terminar a sua execução, retorna os relatórios em modo texto, não necessitando de reprocessamento por ferramentas externas em cima dos *logs* gerados. A cada iteração o tempo máximo pode ser alterado com facilidade, pois não é preciso alterar parâmetros de um *daemon* e sim apenas lançar a ferramenta (Tethereal) com um novo parâmetro de tempo máximo de execução. Dessa forma, pelo tipo de coleta escolhida, pela necessidade de flexibilidade na configuração do tempo máximo de coleta e por não ser necessário coletar dados de estações gerenciáveis remotas, o NetAct não faz uso do SNMP.

Para o modo de coleta passiva 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 e seu modo de uso. 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, por fornecer relatórios em modo texto, não necessitando de reprocessamento de decodificação, em cima dos *logs* gerados, por ferramentas externas e por ter maior flexibilidade na configuracão do tempo máximo de coleta a realizar em cada iteração. Uma visão geral do processo de coleta, geração de histórico e comparação com definição prévia de

baseline pode ser vista na figura 2.

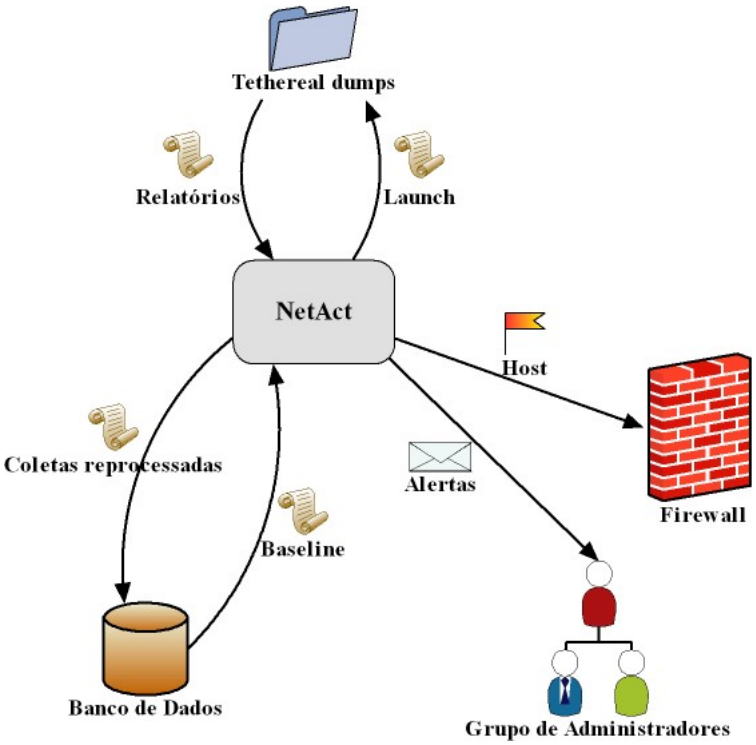

Figura 2: Esquema de funcionamento simples do NetAct

3.5.2 Interpretação

Após a execução do Tethereal para captura de estatísticas de uso de rede, em modo passivo, individual por hosr identificado, o relatório pré-processado do Tethereal é novamente reprocessado pelo NetAct.

Esta etapa consiste de uma interpretação que o NetAct faz sobre o 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.

A finalidade deste processamento é a avaliação de *baseline* e a inserção dos novos dados de coleta, refinados, no banco de dados.

3.5.3 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 da 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 sistema de tolerância será explicado em seguida.

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 pelo 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. A utilização de um método avançado de geração de *baseline* ficou fora do escopo deste trabalho, o cálculo utilizado é baseado em média simples.

Consideram-se ainda mais alguns pontos importantes na geração de *baseline* do NetAct: 1) Somente é gerada a *baseline* de um *host* caso este tenha um registro mínimo de monitorias realizadas. O valor mínimo é definido pelo administrador do sistema nas configurações do NetAct e, conforme explicado anteriormente, com o uso de *th-*

resholds, as iterações de monitoria seguintes poderão fazer com que a média gerada a partir dos X registros iniciais seja alterada, variando para cima ou para baixo. A utilização de um método matemático específico para este passo da criação de *baseline* ficou fora do escopo deste trabalho, e o administrador deverá configurar este valor mínimo de monitorias a serem realizadas antes da geração da *baseline* de acordo com o seu conhecimento em relação a rede, de forma empírica. Este valor mínimo pode ser ser encarado como o tempo mínimo de aprendizagem do NetAct sobre a rede, antes de começar a agir; 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 Y% (também definido nas configurações do NetAct, pelo administrador da rede) de incremento no valor da média atual são permitidos, possibilitando a *baseline* variar para cima. Esta porcentagem poderia ser encarada como o nível de sensibilidade do NetAct às anomalias. 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. O sistema de tolerância adotado é baseado no conhecimento do administrador quanto ao comportamento de sua rede, e a utilização de um modelo matemático específico de *thresholds* também ficou fora do escopo deste trabalho.

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 (RACHMAN, 2005).

3.5.4 Atuação e alertas

A atuação do NetAct na rede se resume em identificação do problema, isolamento e alerta. A identificação de *hosts* problemáticos é feita pela 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 3 e figura 4.

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.

A figura 5 ilustra o que seria um *host* comprometido em comparação com o com-

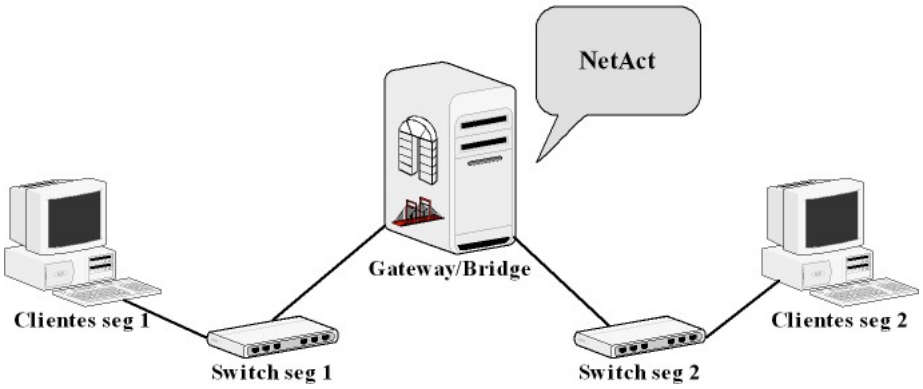

Figura 3: Posicionamento em rede: Protegendo segmentos de rede em *Gateway* ou *Bridge*

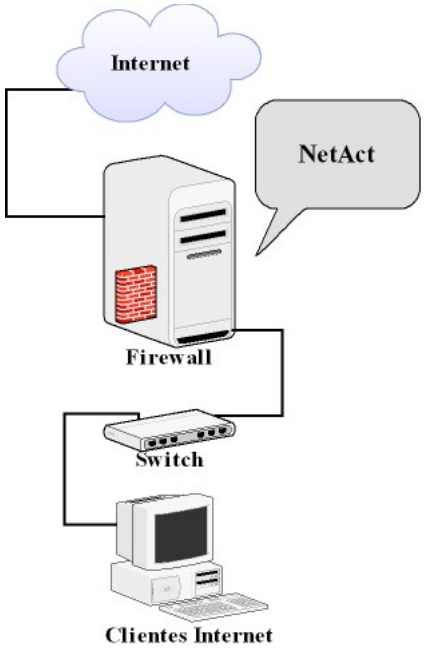

Figura 4: Posicionamento em rede: Protegendo *link* de internet no *Firewall*

portamento de *hosts* em stuação normal de operação:

Após a identificação de anomalia comportamental, para um determinado *host*, o NetAct envia um *e-mail*, conforme o anexo A, para cada um dos contatos cadastrados no sistema. O *e-mail* enviado contém a informação do horário em que ocorreu o problema, o *host* em questão e o número de conversações geradas pelo *host* naquele momento de monitoração.

O melhor a se esperar seria que as falhas que possam vir a ocorrer em um sistema pudessem ser 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 (ALMEIDA, 2005).

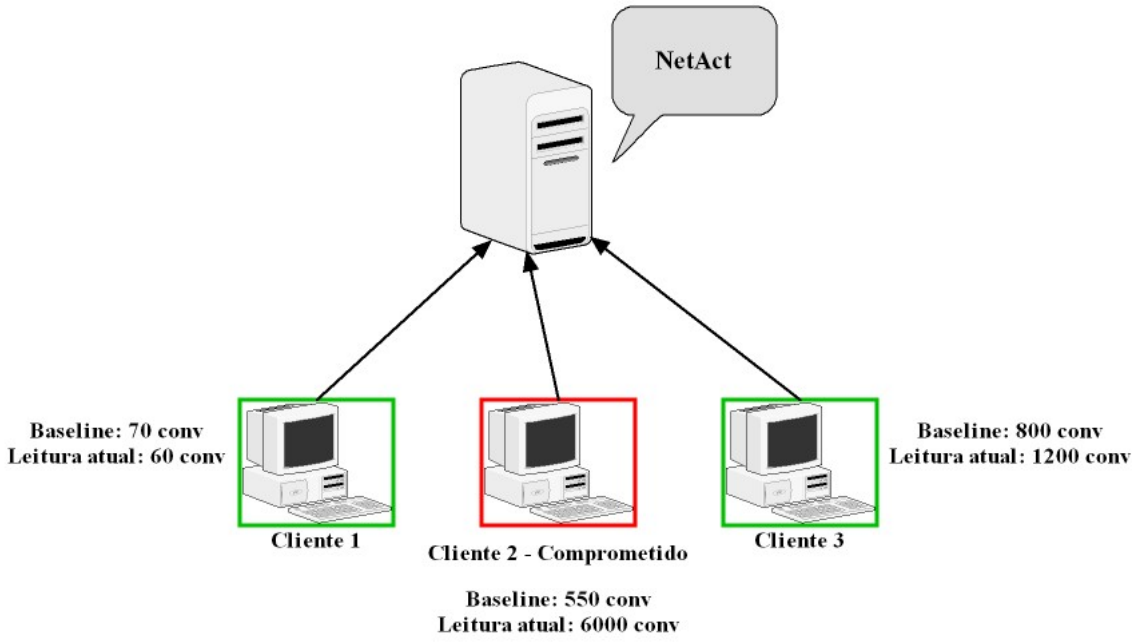

Figura 5: *Hosts* em operação normal e comprometidos: Ilustração da avaliação de *baseline*

3.6 Integração com banco de dados

Por necessitar de um sistema confiável de armazenamento de dados, e que pudesse dar suporte no processamento desses dados na geração de estatísticas, o NetAct foi construido de maneira a se conectar com o banco de dados relacional MySQL. Para a geração de gráficos foi utilizado um banco de dados específico, e muito bem divulgado para gerência de redes, o RRD (Round Robin Database). Ambos serão apresentados a seguir.

3.6.1 API MySQL para C

A API fornecida pelo MySQL para conexão através da linguagem C oferece algumas funções para a manipulação da informação armazenada e para a inserção, naturalmente, de novas informações.

As funções utilizadas pelo NetAct são descritas a seguir:

- mysql_init(): Utilizada para inicializar uma conexão com o MySQL. Caso retorne erro, quer dizer que não deve haver memória suficiente disponível no sistema para tal operação;
- mysql_real_connect(): Função que conecta efetivamente ao banco de dados. Utilizando a área de memória reservada pelo mysql_init(), cria-se um socket com o

banco de dados, passando parâmetros, tais como usuário, senha, banco e *host* desejados para a conexão;

- mysql_real_query(): Executa uma *query* no banco de dados. O parâmetro a ser passado a esta função é a própria string com o SQL a ser executado e a conexão retornada por mysql_init() e mysql_real_connect();
- mysql_use_result(): Depois da *query* executada com sucesso, esta função retorna um ponteiro para os dados retornados pela *query* em memória;
- mysql_fetch_row(): Com esta função, pode-se capturar os valores, linha a linha, do resultado retornado em memória pela *query* executada;
- mysql_free_result(): Ao se concluir a utilização dos resultados desejados, pode-se liberar a memória alocada com esta função;
- mysql_close(): Fecha uma conexão previamente estabelecida com o MySQL.

3.6.2 API RRD para C

Para a geração de gráficos, foi utilizada a API fornecida pelo RRDtools à linguagem C. Com esta API, pode-se criar, alimentar e gerar gráficos a partir de bases RRD. As principais funções utilizadas foram:

- rrd_create(): Função utilizada para a criação de novas bases RRD. Para cada IP de *host* encontrado como ativo na rede é criada uma base RRD para que se possa criar gráficos individuais;
- rrd_update(): Com esta função é possível alimentar as bases RRD existentes com novas informações;
- rrd_graph(): A criação dos gráficos em arquivos no formato png é feita com a utilização desta função.

3.7 Integração com interface *Web*

Para uma mehor interação do adminstrador de redes com o NetAct, foi criada uma interface *web*, que permite operações, tais como configurar parâmetros de execução do NetAct, acessar relatórios de *Top Users*, visualizar gráficos e lista de IPs bloqueados, podendo ainda interagir com o *Firewall*, bloqueando e desbloqueando IPs.

3.7.1 Configurando os parâmetros do NetAct via *browser*

Na figura 6, é mostrada a interface *web*. Os menus listados a seguir são referentes à configuração do NetAct:

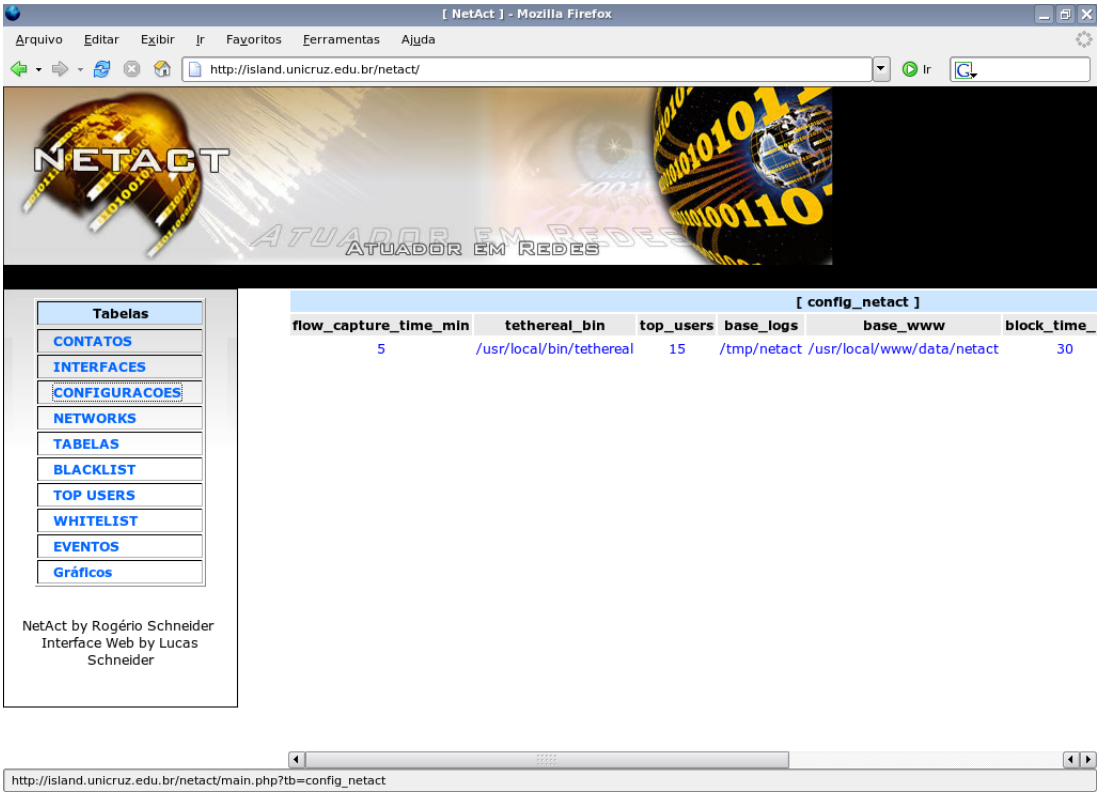

Figura 6: Menu principal da interface *web* do NetAct

- CONTATOS: Neste menu devem ser inseridos os contatos adminstrativos do sistema. Para cada contato aqui cadastrado, será enviado um *e-mail* na ocorrência de alertas e bloqueios;
- INTERFACES: Aqui devem ser inseridas as interfaces a serem monitoradas pelo NetAct;
- CONFIGURAÇÕES: Neste menu, pode-se configurar parâmetros de execução do NetAct, tais como:
    1. "flow_capture_time_min": É o tempo, em minutos, que cada coleta deve durar. A cada intervalo desses, um relatório é gerado pelo Tethereal e avaliado pelo NetAct para ter seus dados inseridos em banco de dados, gráficos são gerados e o comportamento dos *hosts* é avaliado. O valor inicial e recomendado é de cinco minutos;

2. "tethereal_bin": É o caminho completo ao binário do Tethereal no sistema em que o NetAct é executado;
3. "top_users": Define o número de *Top Users* a serem considerados na geração de relatórios. Para cada categoria de *Top Users* serão listados os primeiros N "top_users" aqui definidos;
4. "base_logs": É o diretório onde os logs temporários do NetAct e Tethereal serão armazenados para processamento, em cada iteração;
5. "base_www": Define o dretório raiz da página *web* do NetAct. É dentro deste diretório que serão gerados os gráficos de uso de rede;
6. "block_time_min": Configuração do tempo máximo, em minutos, que um *host* deverá ficar bloqueado;
7. "days_to_keep": Valor, em dias, dos dados históricos a manter em base de dados. Os dados mais antigos que este valor serão excluídos do cálculo de *baseline*, porém não afeta a base RRD de histórico comportamental da rede, mantendo o histórico nos gráficos;
8. "days_to_learn": Tempo de aprendizado do NetAct sobre o comportamento da rede antes de começar a agir, definido em dias;
9. "threshold": Valor da sensibilidade do NetAct, definido em porcentagem aceita para variação acima do limite estabelecido pela *baseline*.

- NETWORKS: Definição de quais redes IP devem ser monitoradas (padrão comportamental e geração de gráficos) pelo NetAct;
- BLACKLIST: São os IPs bloqueados pelo sistema;
- TOP USERS: Acesso aos relatórios de *Top Users* da rede;
- WHITELIST: Listagem de IPs locais a serem desconsiderados da análise de tráfego. Normalmente aqui são inseridos os IPs do próprio servidor de Internet e de outros servidores, que nunca devem ser bloqueados;
- EVENTOS: Acesso aos relatórios de eventos. Os alertas de bloqueios e desbloqueios podem ser visualizados neste menu;
- GRÁFICOS: Acesso aos gráficos de histórico comportamental dos *hosts* da rede.

3.7.2 Relatórios de *Top Users*

O relatório de *Top Users* mostra, em ordem decresente, a listagem de *hosts* mais ativos na rede, de acordo com as leituras da última iteração. A figura 7 ilustra esse menu.

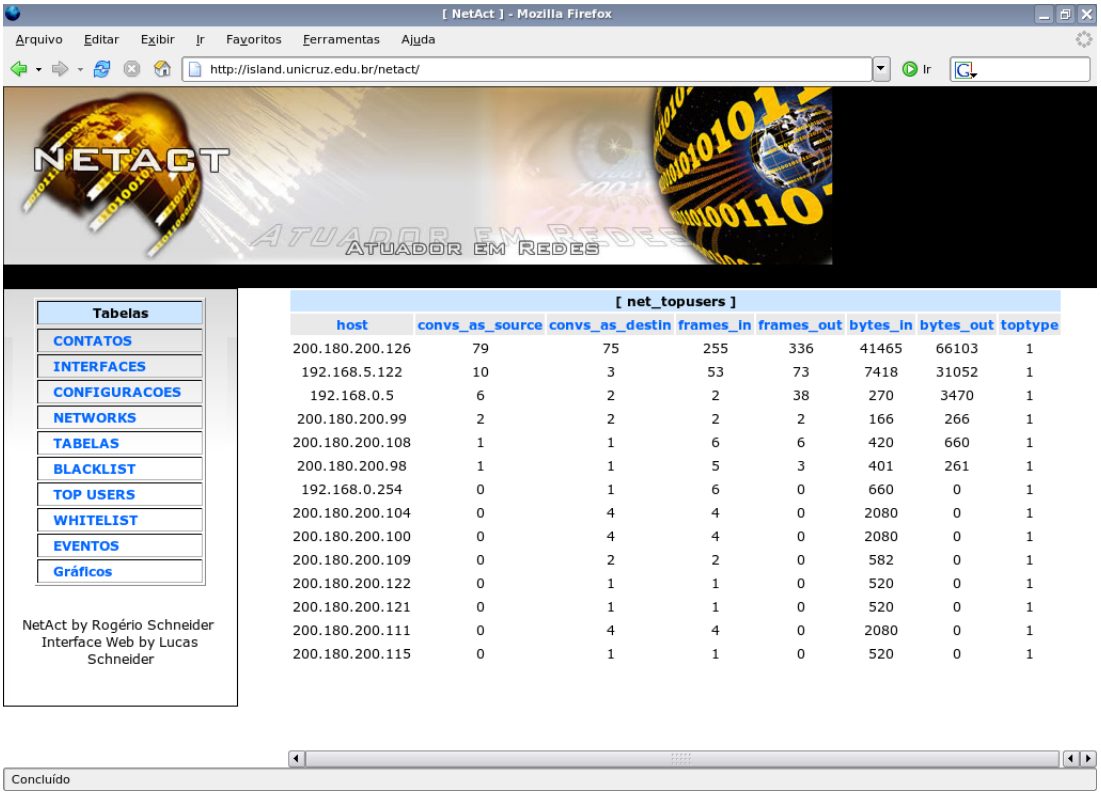

Figura 7: Relatório de *Top Users*

Este relatório é dividido em seis categorias, sendo elas:

- Maior atividade em conversações originadas;
- Maior atividade em conversações recebidas;
- Maior atividade em *frames* recebidos;
- Maior atividade em *frames* enviados;
- Maior atividade em *bytes* recebidos;
- Maior atividade em *bytes* enviados.

O objetivo desses relatórios é mostrar ao administrador da rede a situação de tráfego nos *hosts* mais ativos da rede.

3.7.3 Visualizando os gráficos

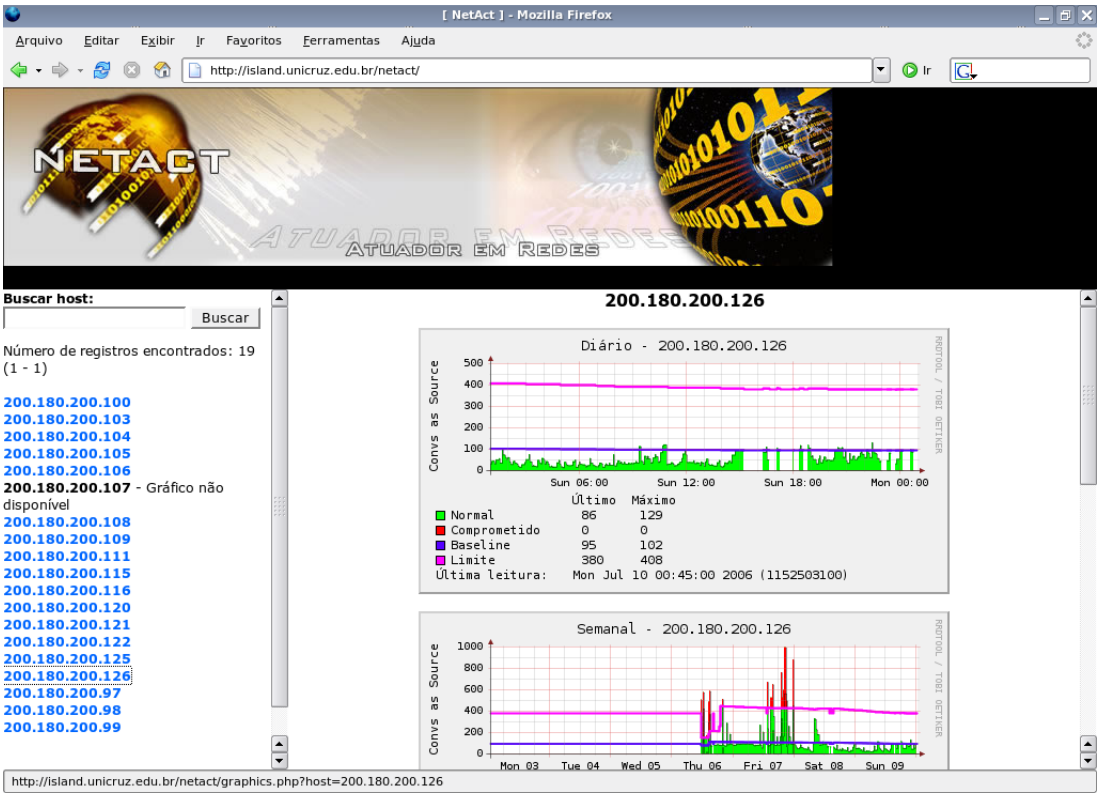

Figura 8: Relatório de histórico de comportamento através de gráficos

O NetAct gera gráficos do comportamento histórico dos *hosts* e os mostra na interface *web*. Para a geração dos gráficos, foi utilizado o pacote RRDtools, que gera arquivos no formato *png* contendo os gráficos desejados pelo programador. A figura 8 ilustra a visualização dos gráficos gerados.

Ao acessar o menu *Gráficos*, o adminstrador recebe uma caixa de entrada onde vai digitar o IP que deseja procurar. Caso o IP escolhido tenha os arquivos de gráficos gerados, o NetAct irá fornecer um *link* na interface para esses gráficos; caso ainda não existam as entradas desejadas, o usuário da interface será notificado.

3.7.4 Visualizando os *hosts* bloqueados

A visualização dos *hosts* atualmente bloqueados pelo NetAct (figura 9) é feita através do menu *Black List*. Ao abrir este menu o usuário receberá a listagem de IPs bloqueados, e poderá efetuar o seu desbloqueio, caso deseje.

Ao usuário é oferecida a opção, nesse menu, de se inserir um novo registro. A inserção de um novo registro, em *Black List*, causa o bloqueio imediato do IP especifi-

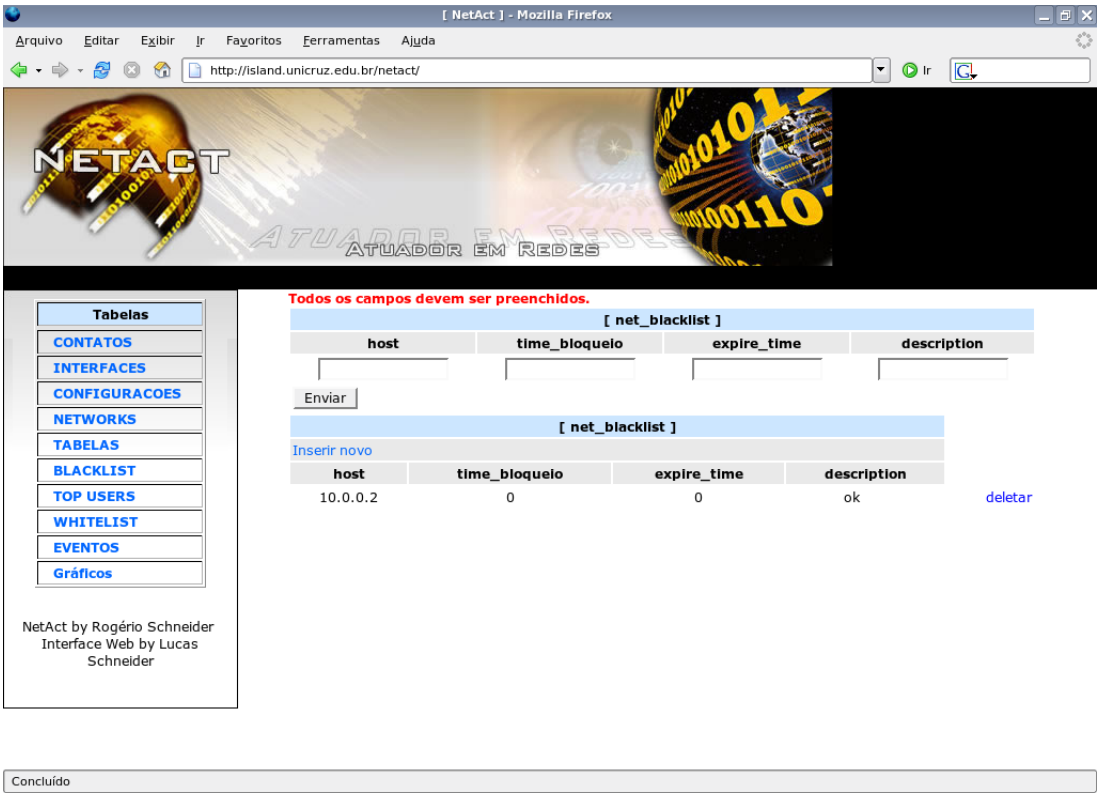

Figura 9: Relatório de *hosts* bloqueados

cado junto às regras de *firewall*, seja IPFW ou IPtables, identificado automaticamente pelo NetAct para os sistemas FreeBSD ou Linux, respectivamente.

No capítulo final, os resultados obtidos e as sugestões de continuidade deste estudo serão apresentadas.

4 CONCLUSÃO

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 automáticos e gerar alertas. Conforme a importância das redes de computadores tende a crescer dentro das instituições, a demanda por atuação automática tende a crescer, projetando um cenário onde as tarefas automatizadas de gerência auxiliam na manutenção da qualidade e disponibilidade dos recursos de rede. A convergência dos serviços de comunicação e sua centralização em redes de computadores compete com o aumento na incidência de vírus e *worms*, gerando uma demanda por atuação imediata na administração de redes.

Os objetivos gerais do trabalho, que compreendem o exercício de técnicas de programação, técnicas de *firewall*, exercício de habilidades de utilização de banco de dados e levantamento sobre as principais ferramentas de gerência de redes foi atingido. No processo de elaboração do NetAct uma pesquisa foi realizada, procurando listar as principais ferramentas existentes, em *software* livre, para o gerenciamento de redes, nas diversas categorias de gerência, tais como segurança de redes, desempenho e falhas. As técnicas de programação foram exercitadas, utilizando-se as linguagens de programação C e PHP para a composição do sistema do NetAct. O banco de dados MySQL foi utilizado para o armazenamento de históricos de tráfego e geração de médias de conversações originadas por cada *host* na rede, criando um perfil de utilização, e possibilitando a identificação de desvios comportamentais a partir deste perfil histórico. Para que o NetAct pudesse atuar na rede, os sistemas de *firewall* mais utilizados em servidores de rede foram estudados, identificando-se como interagir com os sistemas IPFW e IPtables, utilizados respectivamente em FreeBSD e distribuições Linux. Outro ponto importante a se destacar deste trabalho foi a utilização de uma ferramenta específica de geração de gráficos personalizados, o RRDtools, que possibi-

litou a visualização gráfica do estado da rede, tanto do estado atual como de estados históricos, sendo muito flexível na customização do armazenamento de informação e geração gráfica de relatórios, permitindo que se armazene a informação por um longo período de tempo com baixo uso de recurso, devido às suas caracteristicas internas de consolidação dos dados armazenados através de valores médios, máximos, mínimos ou computados por outros tipos, personalizados, de cálculo.

Os objetivos específicos do trabalho também 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. A compatibilidade do NetAct com os sistemas mais utilizados em ambientes de rede, no que diz respeito a *firewalls* e *gateways*, tais como os sistemas operacionais Linux e BSD, é um fator importante do *software* criado, pois garante a sua flexibilidade e portabilidade, não ficando restrito a uma determinada versão ou distribuição de sistema operacional.

O NetAct oferece um diferencial, se comparado a outras ferramentas de gerência, pois ele é um sistema de detecção de intrusão por anomalias que oferece uma interface gráfica acessível pela *web* e atua de forma autônoma sobre as regras de *firewall* da rede. Fazendo-se uso desta interface, todas as configurações relativas ao funcionamento do NetAct podem ser alteradas, tais como interfaces de rede a monitorar, redes de IP (blocos) a monitorar, tempo máximo de coleta de tráfego a cada iteração, etc. Ainda na interface *web* se pode ter acesso a relatórios de eventos, alterar as regras de bloqueio, liberando ou bloqueando manualmente, via *browser*, as máquinas que se desejar, dentro da rede. O NetAct se diferencia ainda das demais ferramentas apresentadas por ser capaz de identificar os desvios comportamentais de *hosts* internos à rede e os bloquear de forma automática, enviando relatórios por *e-mail* das ações tomadas e registrando eventos para acesso via *web*. Uma outra forma de acompanhamento da atividade da rede é proposta pelo NetAct, sendo que, como o programa foi criado para monitorar cada máquina individualmente na rede, gera-se gráficos de tráfego individuais para cada máquina, podendo-se ter uma visão mais detalhada de como os *hosts* integrantes de uma rede tem se comportado, ao longo do tempo, quanto ao número de conexões originadas, dando uma visão da atividade de rede de forma individual.

4.1 Trabalhos Futuros

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, através de parâmetros como atrasos, vazão, disponibilidade e número de retransmissões realizadas, se o nível de desempenho corrente da rede foi prejudicado. Isto teria a finalidade de constatar se um desvio de padrão comportamental foi realmente prejudicial à rede ou não;
- Estudo e implementação de um novo método de geração de *baseline*, mais elaborado, que leve 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*;
- Utilização de um método específico de *thresholds* bem como de tempo mínimo de aprendizagem dos padrões de rede;
- 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*, eliminando assim falsos positivos. Quando uma máquina recebe requisições, ela também responde a estas, gerando conversações dessa máquina para outras como se fossem de origem sua, na visão de conversação, podendo causar falsos positivos. Num caso desses, a máquina não estaria originando várias requisições mas apenas respondendo a um possível atacante;
- A coleta dos dados estatísticos do uso de rede poderia ser feita utiizando-se SNMP em *switches* gerenciáveis ou máquinas centralizadoras de tráfego que exportem relatórios de fluxos de rede, com a finalidade de compatibilizar a ferramenta com redes *Gigabit* e com o protocolo padrão de gerência de redes.

REFERÊNCIAS

ALMEIDA, R. H. *MTAS: Uma Ferramenta para Gerenciamento de Servidores de Aplicação*. Trabalho de Conclusão de Curso — UNICRUZ, Universidade de Cruz Alta, Cruz Alta, RS, 2005.

AMORSO, E. *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, and Response*. [S.l.]: Intrusion.Net Books, 1999.

BERTHOLDO, L. M.; ANDREOLI, A. V.; TAROUCO, L. M. R. *Gerência de Segurança Através do Uso de Netflow*. 2003. Capturado em 22 de Jun. 2006. Online. Disponível na Internet `http://www.rnp.br/_arquivo/wrnp2/2003/gsaun01a.pdf`.

CAIDA. *cflowd: Traffic Flow Analysis Tool*. 2005. Capturado em 12 de Out. 2005. Online. Disponível na Internet `http://www.caida.org/tools/measurement/cflowd`.

CAIDA. *FlowScan - Network Traffic Flow Visualization and Reporting Tool*. 2005. Capturado em 22 de Out. 2005. Online. Disponível na Internet `http://www.caida.org/tools/utilities/flowscan`.

CHAPMAN, D. B.; ZWICKY, E. D. *Building Internet Firewalls*. [S.l.]: O'Reilly Associates Inc, 1995.

CISCO. *Cisco NetFlow*. 2006. Capturado em 22 de Jun. 2006. Online. Disponível na Internet `http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00805e7c53.html`.

CISCO. *Cisco NetFlow*. 2006. Capturado em 22 de Jun. 2006. Online. Disponível na Internet `http://en.wikipedia.org/wiki/Netflow`.

COMBS, G. *Tethereal ManPages*. 2005. Capturado em 29 de Set. 2005. Online. Disponível na Internet `http://www.ethereal.com/docs/man-pages/tethereal.1.html`.

DERI, L. *NTop*. 2006. Capturado em 19 de Fev. 2006. Online. Disponível na Internet `http://www.ntop.org`.

DISTRIBUTION, B. S. *FreeBSD. The Power to Serve*. 2006. Capturado em 23 de Jun. 2006. Online. Disponível na Internet `http://www.freebsd.org`.

FILHO, R. H. *AGRES Um Sistema Baseado em Conhecimento para Apoio à Gerência de Falhas em Redes de Computadores*. Dissertação (Dissertação de Mestrado) — UFC, Universidade Federal do Ceará, CE, 2003.

FOUNDATION, F. S. *GCC, the GNU Compiler Collection*. 2005. Capturado em 22 de Out. 2005. Online. Disponível na Internet `http://gcc.gnu.org`.

FOUNDATION, T. A. S. *Apache HTTP Server Project*. 2006. Capturado em 23 de Jun. 2006. Online. Disponível na Internet `http://httpd.apache.org`.

FRANCESCHI, A. S. M.; BARRETO, J. M.; ROISENBERG, M. Desenvolvendo agentes de software para gerência de redes utilizando técnicas de inteligência artificial. p. 11, 2002.

FULLMER, M. *Flow-Tools*. 2005. Capturado em 27 de Ago. 2005. Online. Disponível na Internet `http://www.splintered.net/sw/flow-tools`.

GALSTAD, E. *Nagios - Network Monitoring Software*. 2005. Capturado em 26 de Ago. 2005. Online. Disponível na Internet `http://www.nagios.org`.

GARFINKEL, S.; SPAFFORD, G. *Practical Unix Security*. [S.l.]: O'Reilly Associates Inc, 1994.

GONG, Y. *Detecting Worms and Abnormal Activities with NetFlow, Part 1*. 2004. Capturado em 21 de Abr. 2006. Online. Disponível na Internet `http://www.securityfocus.com/infocus/1796`.

GROUP, T. C. *Cacti: The Complete RRDtool-based Graphing Solution*. 2005. Capturado em 18 de Set. 2005. Online. Disponível na Internet `http://www.cacti.net`.

GUBERT, L. C. *Utilizando o padrão de gerenciamento SNMP para gerenciar tráfego multicast: A ferramenta Multicast Monitor*. Dissertação (Dissertação de Mestrado) — UFSC, Universidade Federal de Santa Catarina, Florianópolis, SC, 2002.

IPFW. *IPFW ManPages*. 2005. Capturado em 30 de Ago. 2005. Online. Disponível na Internet `http://www.freebsd.org/cgi/man.cgi?query=ipfw&apropos=0&sektion=0&manpath=FreeBSD+6.0-RELEASE+and+Ports&format=html`.

KNUTH, D. E. *The art of computer programming: sorting and searching*. New York, NY: Addison-Wesley, 1998.

LEWIS, L. *Managing Computer Networks: A Case-Based Reasoning Approach*. Norwood: Artech House, 1995.

LINUX. *Linux*. 2006. Capturado em 12 de Jul. 2006. Online. Disponível na Internet `http://pt.wikipedia.org/wiki/Linux`.

MILLER, D. *SoftFlowd ManPages*. 2005. Capturado em 26 de Ago. 2005. Online. Disponível na Internet http://www.mindrot.org/softflowd.html.

MYSQL. *MySQL*. 2006. Capturado em 23 de Jun. 2006. Online. Disponível na Internet http://www.mysql.com.

OETIKER, T. *MRTG - The Multi Router Traffic Grapher*. 2005. Capturado em 15 de Set. 2005. Online. Disponível na Internet http://oss.oetiker.ch/mrtg.

OETIKER, T. *Round Robin Database*. 2006. Capturado em 13 de Jun. 2006. Online. Disponível na Internet http://oss.oetiker.ch/rrdtool.

PARK, B. I. *Net-Watcher - An anomaly Intrusion Detection System tool*. 2001. Capturado em 22 de Jun. 2006. Online. Disponível na Internet http://www.cs.utk.edu/~park/net_watcher/net_watcher.html.

PEREIRA, M. C. Adminstração e gerência de redes de computadores. 2001.

PFAFF, B. *GNU libavl 2.0.2*. 2005. Capturado em 12 de Out. 2005. Online. Disponível na Internet http://www.stanford.edu/~blp/avl/libavl.html.

PLONKA, D. *FlowScan*. 2005. Capturado em 22 de Out. 2005. Online. Disponível na Internet http://net.doit.wisc.edu/~plonka/FlowScan/.

PORTS. *Ports*. 2006. Capturado em 23 de Jun. 2006. Online. Disponível na Internet http://www.freebsd.org/ports.

PROJECT, T. netfilter.org iptables. *IPtables*. 2006. Capturado em 11 de Jul. 2006. Online. Disponível na Internet http://www.netfilter.org/projects/iptables/index.html.

PSIONIC. *Portsentry*. 2006. Capturado em 19 de Fev. 2006. Online. Disponível na Internet http://sourceforge.net/projects/sentrytools.

RACHMAN, O. *Baseline Analysis of Security Data*. 2005. Capturado em 21 de Abr. 2006. Online. Disponível na Internet http://www.securitydocs.com/library/3018.

RANUM, M. J. *A Taxonomy of Internet Attacks: What you can expect*. [S.l.]: Information Warehouse Inc, 1995.

ROESCH, M. *Snort*. 2006. Capturado em 30 de Jan. 2006. Online. Disponível na Internet http://www.snort.org.

ROMIG, S.; FULLMER, M.; RAMACHANDRAN, S. *Cisco Flow Logs and Intrusion Detection at the Ohio State University*. 1999. Capturado em 22 de Jun. 2006. Online. Disponível na Internet `https://db.usenix.org/publications/login/1999-9/osu.html`.

SIYAN, K.; HARE, C. *Internet Firewalls and Network Security*. [S.l.]: New Riders Publishing, 1995.

SNMP. *Simple Network Management Protocol*. 2006. Capturado em 22 de Jun. 2006. Online. Disponível na Internet `http://en.wikipedia.org/wiki/Simple_network_management_protocol`.

SOARES, L. F. G.; LEMOS, G.; COLCHER, S. *Redes de Computadores. Das LANs, MANs e WANs às Redes ATM*. Rio de Janeiro, RJ: Campus. 623-624 p.

SZTAJNBERG, A. *Gerenciamento de Redes - Versão Resumida Conceitos Básicos sobre os Protocolos SNMP e CMIP*. 1996. Capturado em 20 de Abr. 2006. Online. Disponível na Internet `http://www.gta.ufrj.br/~alexszt/ger/compact.html`.

TANEMBAUM, A. S. *Redes de Computadores*. 3. ed. Rio de Janeiro: Campus, 1997.

TECHNOLOGIES, Z. *PHP: Hypertext Preprocessor*. 2006. Capturado em 23 de Jun. 2006. Online. Disponível na Internet `http://www.php.net`.

WANDARTI, D. F. *Proposta de um Framework para Gerência de Clusters*. Dissertação (Dissertação de Mestrado) — PUC-PR, Pontifícia Universidade Católica do Paraná, Curitba, PR, 2003.

APÊNDICE A – ALERTA ENVIADO POR E-MAIL

Date: Wed, 12 Jul 2006 18:25:05 -0300 (BRT)
From: ISLAND Root <root@island.unicruz.edu.br>
To: stockrt@unicruz.edu.br
Subject: NetAct - Alerta Host "10.0.1.5"

Host "10.0.1.5" com "28207" conversações como origem foi bloqueado pelo NetAct.
Baseline: 1263
Limite: 5052