UNIVERSIDADE METODISTA DE PIRACICABA

FACULDADE DE CIÊNCIAS EXATAS E DA NATUREZA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

CHECKRULE: UMA FERRAMENTA PARA AUTOMATIZAR A CRIAÇÃO DE REGRAS PARA FIREWALLS SQUID

VANDERLEI IENNE

ORIENTADOR: PROF. DR. PLÍNIO ROBERTO SOUZA VILELA

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação, da Faculdade de Ciências Exatas e da Natureza, da Universidade Metodista de Piracicaba – UNIMEP, como requisito para obtenção do Título de Mestre em Ciência da Computação.

PIRACICABA
2006

CHECKRULE: UMA FERRAMENTA PARA AUTOMATIZAR A CRIAÇÃO DE REGRAS PARA FIREWALLS SQUID

AUTOR: VANDERLEI IENNE

ORIENTADOR: PROF. DR. PLÍNIO ROBERTO SOUZA VILELA

Dissertação de Mestrado defendida e aprovada em 26 de Abril de 2006, pela Banca Examinadora constituída dos Professores:

_____

Prof. Dr. Plínio Roberto Souza Vilela

UNIMEP - Universidade Metodista de Piracicaba

_____

Prof. Dr. Mario Jino

DCA-FEEC-Unicamp

Universidade Estadual de Campinas

_____

Prof. Dr. Marcio Merino Fernandes

UNIMEP - Universidade Metodista de Piracicaba

Ienne, Vanderlei
D219i CheckRule: Uma Ferramenta para Automatizar a Criação de Regras para Firewalls Squid / Vanderlei Ienne – Piracicaba, [S.P.:s.n.], 2006.

Orientador: Plínio Roberto Souza Vilela

Dissertação (Mestrado) – Universidade Metodista de Piracicaba, Faculdade de Ciências Exatas e da Natureza, Programa de Pós-Graduação em Ciência da Computação.

1. Firewall. 2. *Segurança em Redes*. 3. *Squid*. 4. *Linux*. I. Vilela, Plínio Roberto Souza. II. Universidade Metodista de Piracicaba, Faculdade de Ciências Exatas e da Natureza, Programa de Pós-Graduação em Ciência da Computação.

Agradecimentos

O agradecimento é um elemento muito importante para mim, ele tem um significado especial, pois tem um comprometimento com realização e a finalização de um objetivo, que neste caso para mim é a conclusão do Mestrado, acredito ainda que tudo que é feito na vida tem uma finalidade, isso é uma dádiva de Deus, e falando em Deus agradeço a ele hoje e sempre lembrando-o em minhas orações.

Agradeço aos demais integrantes da minha família (tios Plínio, João, Cláudio, Irineu tias Lurdes, Nilva, Isabel aos primos Junior(Juca), César(Cezinha), Cássio(Cassito), Claudinei(Gordo) primas Luciana, Denise, Tânia e também a todos meus priminhos, pois eles foram pessoas que sempre me fortaleceram no meu dia a dia. Meus colegas de sala de aula do Mestrado, pois foram muito importantes para dúvidas que não acabavam mais, aos meus amigos de balada e churrascada, meus colegas da Universidade Anchieta onde trabalho eu agradeço imensamente, principalmente a paciência de meus subordinados que não sei como conseguiram me agüentar.

Outra pessoa que contribuiu muito para esta conquista foi meu orientador Plínio Vilela, um professor que concluiu seus estudos bem cedo que para mim isso significa muita dedicação e perseverança em seu objetivo final que é de ser Professor.

Aos meus irmãos Wagner, Vlamir, Valdecir, Leandro e Rodrigo e por falar nisso meu pai Valdemar Ienne que não deu moleza a minha mãe veja o exemplo da quantidade de filhos que ele fez meus Deus do céu em pai.

Agradeço de forma especial a minha querida mãe, Lídia Lopes de Camargo Ienne, que morreu quando eu tinha 5 anos, nunca vou esquecer de você minha mãezinha, eu sempre vou te amar onde quer que esteja, beijo.

Finalmente, gostaria de dizer o meu muito obrigado e desejar que Deus abençoe a todos os colegas, amigos e familiares que estiveram torcendo por mim ao longo de toda a graduação.

Aos

Meu irmãos pelo ajuda e luta

Aos

Meus pais Waldemar e Lídia (em memória)

“A ferramenta que você sonha, pode já estar em desenvolvimento”

Linus Benedict Torvalds (born December 28, 1969)

RESUMO

Com o compartilhamento de recursos em rede tornou-se importante assegurar que as informações que nela trafegam estejam protegidas. Inúmeros esforços têm sido empregados para conter o crescente aumento de ataques às redes de computadores que ocorrem no mundo todo. A maior parte desses ataques ocorre por problemas nos mecanismos de proteção. Nesse trabalho, são apresentados os problemas levantados durante o estudo desses mecanismos de proteção, resultando na criação e implementação de uma ferramenta chamada Check Rule. A finalidade dessa ferramenta é a de auxiliar o administrador a reduzir o tempo gasto na criação de regras de segurança e também diminuir as chances de se cometer erros durante o processo de criação, tentando assim melhorar a eficiência da segurança da rede. Como resultado foi verificado que houve realmente uma diminuição nos erros de codificação das regras e uma maior eficiência nos bloqueios. A expectativa referente à diminuição do tempo gasto para configuração das regras não se comprovou nos testes, já que alguns usuários não tinham habilidade suficiente para manusear a nova ferramenta comprometendo assim a sua eficácia.

PALAVRAS-CHAVE: Firewall, Segurança em Rede, Squid, Linux

CHECKRULE: A TOLL TO AUTOMATIZE THE CREATION OF FIREWALLS SQUID RULES

ABSTRACT

The increasing popularity of network shared resources, especially through the use of the Internet, has motivated the research on security aspects related to this field. Much effort has been done to control the increasing number of attacks which occur in the computer networks all over the world. The majority of these attacks happen due to problems in the protection mechanisms. In this research, we intend to present the problems aroused in the studies of these security mechanisms, resulting in the creation and implementation of a security tool named Check Rule. The aim of this tool is to help the administrator to reduce not only the time spent in the process of security rules creation but the chances of mistakes in the process as well, trying to improve the efficiency of network security. A decreasing number of mistakes in the rules codification and greater efficiency in the blockings were verified. The expectancy referring to time reduction in the rules configuration has not been proved in the tests since some users weren't qualified enough to use the new tool, compromising its efficiency.

Key words: firewall , net safety , squid, linux

SUMÁRIO

SUMÁRIO (CONTINUAÇÃO)

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ACL	ACCESS CONTROL LIST
ADSL	ASYMMETRIC DIGITAL SUBSCRIBER LINE
FTP	FILE TRANSFER PROTOCOL
HTTP_ACCESS	HYPER TEXT TRANSFER PROTOCOL ACCESS
LDAP	Lightweight Directory Access Protocol
MRTG	MULTI ROUTER TRAFFIC GRAPHER
RPM	REDHAT PACKAGE MANAGER
UDP	USER DATAGRAM PROTOCOL
URL	UNIVERSAL RESOURCE LOCATOR
VNC	VIRTUAL NETWORK COMPUTING

LISTA DE TABELAS

1. INTRODUÇÃO

A interligação entre organizações atinge proporções globais graças à Internet. A facilidade e agilidade no intercâmbio de informações melhoraram significativamente a eficiência e a competitividade de comércios, indústrias e corporações, afetando positivamente inclusive áreas como ensino e governo. Termos como E-Business, E-Commerce e E-Learning são forjados na literatura internacional e se tornam presentes no cotidiano, dando forma a uma "Sociedade da Informação". NAKAMURA (2002).

Entretanto, conjuntamente com as vantagens provenientes do uso cada vez mais difundido da Internet, emergiu uma crescente preocupação com a segurança de informações. O acesso por pessoas não autorizadas a informações sigilosas pode causar enormes prejuízos a uma empresa ou usuário, o que tem direcionado diversos esforços no sentido de melhorar a segurança dos sistemas computacionais envolvidos, visando impedir, ou pelo menos limitar, o acesso não autorizado. Para garantir a segurança de sistemas computacionais, esses esforços têm sido direcionados a três focos principais de aplicação: segurança de redes, segurança de aplicações e segurança de sistemas operacionais.

A segurança de redes constitui a primeira barreira contra ataques remotos e visa restringir tanto o acesso às informações trafegando pela rede quanto a subversão de algum serviço que dê acesso ao computador em si. No primeiro caso, um atacante poderia obter as informações simplesmente acessando os pacotes que trafegam pela rede e, no segundo, obter as informações diretamente de uma máquina comprometida. Segundo GARFINKEL e SPAFFORD (1996), o uso de firewalls, filtros de pacotes, detectores de intrusão e a criptografia são alguns dos mecanismos utilizados com a finalidade de limitar o acesso externo.

Por sua vez, a segurança de aplicações constitui a segunda linha de defesa para ataques remotos. A grande maioria dos ataques que resultam em

comprometimento de um computador e, por vezes, de uma rede inteira, utiliza-se de defeitos nas aplicações servidoras ou clientes de serviços de rede, permitindo ao atacante obter acesso às informações diretamente. Para minimizar os defeitos presentes nas aplicações, existem técnicas de programação segura VIEGA e MCGRAW (2003) e mecanismos que visam detectar tentativas de subversão de uma aplicação COWAN et al.(1998).

Uma técnica consiste em um conjunto de regras que bloqueiam possíveis tentativas de invasão, as regras são incluídas nas linhas de programação, verificando se os código programadas estão realmente de acordo com as especificações anteriormente elaboradas. Outra técnica consiste em incluir marcadores dentro do código da programação, na tentativa de identificar os ataques que podem ser burlados, são estes marcadores que irão informar aos programadores onde ocorreram as tentativas de invasão e que com isso sejam novamente programadas novas regras, para tentar assim diminuir essas invasões. No terceiro foco, segurança de sistemas operacionais, foi negligenciado nos primórdios dos sistemas operacionais; muitos sistemas operacionais modernos apresentam problemas de segurança cujas soluções não foram implementadas para manter a compatibilidade com sistemas mais antigos (nestes, incluem-se o Linux e o Windows) LOCOCCO et al. (1998).

Nesse contexto verifica-se que a idéia principal de segurança é restringir ao máximo cada aplicação e habilitar o acesso somente às informações de que necessita e tentar impedir qualquer acesso fora deste escopo; com isso, mesmo que um atacante consiga passar pela segurança de rede e comprometer uma aplicação, ele teria um acesso restrito que o impediria de acessar informações não autorizadas.

Umas das alternativas mais utilizadas pelas empresas como medida de proteção contra ataques é o *firewall;* ele é caracterizado por ser uma barreira de segurança entre duas redes e sua principal característica é bloquear todo o tráfego não autorizado oriundo de uma rede à outra CUPERTINO (2003). Em sua composição convencional, podem ser encontradas outras características como filtragem de pacotes, serviço de *proxy* e NAT *(Network Address*

Translation). Porém, não é raro encontrar modelos de *firewall* com antivírus e filtragem de conteúdo, que permite bloquear o acesso de usuários internos a assuntos como *hackers* e pornografia TAYLOR (2002). Os principais firewalls existentes no mercado são: Firewall Squid CHADD et al. (2003) Iptables, Microsoft Antispyware, Symantec Enterprise Firewall. CUPERTINO (2003).

A estratégia de utilização do firewall como mecanismo de segurança, permite a centralização das regras em um só ponto, facilitando assim um melhor controle em seu gerenciamento. Neste ponto de controle, todo pacote (HTTP, FTP, SMTP, SSH, IMAP, POP3, TELNET) que entra e sai é inspecionado, podendo ser autorizado ou rejeitado, conforme as regras de segurança estabelecidas.

1.1. MOTIVAÇÃO

Ao passar dos anos, o acesso remoto foi tipicamente caracterizado por usuários remotos acessando recursos privados de uma organização através de uma rede pública, com a conexão discada terminando em um servidor de acesso a rede localizada na rede da organização. É importante notar que para tal acesso, freqüentemente assume-se que a infra-estrutura de comunicação utilizada para acessar o servidor, neste caso a rede pública, é relativamente segura, não apresentando nenhuma ameaça significativa à confidencialidade e à integridade da comunicação.

Com base nesta suposição, a segurança da conexão se limitava a um controle de acesso ao servidor de acesso à rede, baseado em um par usuário/senha. Contudo, na realidade, as comunicações sobre uma rede pública nunca foram invioláveis a um atacante. A enorme difusão da Internet e a crescente disponibilidade do acesso de banda larga, em conjunto com o desejo de redução dos altos custos do acesso discado, têm conduzido ao desenvolvimento de mecanismos de acesso à Internet.

Esse tipo de comunicação, comumente chamado de acesso remoto, utiliza a tecnologia de Redes Privadas Virtuais (VPN), possibilitando que uma infra-estrutura de rede pública, como a Internet, seja utilizada como canal de

comunicação entre o usuário remoto e a rede privada. Em alguns casos, o usuário remoto acessa primeiramente um Provedor de Acesso à Internet e em seguida estabelece uma conexão virtual adicional sobre a Internet até a rede privada.

A facilidade de acesso e o alcance global da Internet, no entanto, possibilitam a existência de vários outros cenários de acesso remoto. Contudo, a tarefa de satisfazer os requisitos de segurança das várias classes de usuários de acesso remoto apresenta vários desafios. Junto aos inúmeros benefícios trazidos pelo acesso remoto, surge também uma série de implicações, principalmente quanto à segurança das informações, que passam a correr riscos com relação a sua confidencialidade e a sua integridade, já que passam a trafegar através de uma rede pública. Além disso, a extensão do perímetro de segurança da rede privada, que passa a englobar a máquina remota, pode expor a rede da organização a novas ameaças que devem ser avaliadas e solucionadas.

Como a segurança é um fator crucial, o profundo conhecimento dessas novas ameaças e a adoção de um conjunto de mecanismos de segurança capazes de atender aos requisitos impostos nestes cenários torna-se vital para o desenvolvimento de uma solução de acesso remoto seguro e viável. Com base em tudo isso a melhoria da segurança é muito importante e a motivação para esse trabalho se destaca em dois pontos: o primeiro ponto é que existem dificuldades em se entender as regras que serão criadas fazendo com que, às vezes, sejam incluídas regras antigas ou obsoletas que não são totalmente eficazes no contexto de segurança de hoje; o segundo ponto é que falta uma padronização efetiva nas regras, podendo assim ocorrer uma falta de consenso na hora de se criar às novas regras, ocasionando uma grande diversidade de conceitos e podendo assim aumentar a quantidade de erros de compatibilidade.

1.2. OBJETIVO

Considerando que um dos problemas que têm dificultado uma adoção mais ampla de mecanismos de segurança está relacionado à dificuldade de

configurar corretamente as políticas de segurança, dada a complexidade de especificar estas regras que são descritas em forma textual mediante linhas de comandos e garantir que elas sejam condizentes com as finalidades de segurança a que se propõe.

O objetivo deste trabalho é minimizar a ocorrência de erros na codificação das regras do firewall e facilitar a sua confecção, criando uma ferramenta que auxilie no processo de especificação. Uma grande limitação do modelo textual de especificação é a dificuldade de compreender o impacto que uma regra tem em relação aos usuários e aos aplicativos que eles utilizam, o que pode ensejar a inserção não intencional de brechas de segurança.

O projeto de criação de uma ferramenta de visualização gráfica para regras de segurança foi elaborado com a finalidade de melhorar a compreensão, análise e validação das estruturas das regras, auxiliando na configuração correta do comportamento do firewall em relação à segurança e permitindo identificar problemas existentes na política de regras especificadas.

Além do desenvolvimento do projeto, foi realizada a implementação parcial da ferramenta, tendo por base uma das representações criadas para apresentar a política, permitindo a leitura dos arquivos e a interação do usuário com a estrutura visual utilizada.

1.3. ORGANIZAÇÃO

Baseado nas etapas do desenvolvimento deste trabalho, os diversos aspectos envolvidos na elaboração de uma solução de segurança ao acesso Internet, foram agrupados e, são discutidos a seguir.

A organização deste trabalho foi dividida, para uma melhor compreensão, como será demonstrado a seguir, Capítulo 1, identificação do problema, onde são abordados quais as dificuldades atuais na criação das novas regras; Capítulo 2, verificação de ferramentas equivalentes no mercado, onde serão discutidas algumas ferramentas que já estão em uso Apêndice, introdução ao

firewall Squid, onde será discutido qual é a funcionalidade de um firewall abrangendo principalmente a ferramenta Squid; Capítulo 4, criação de regras feitas manualmente, onde serão demonstradas as reais dificuldades da criação das regras feitas manualmente; Capítulo 5, criação da ferramenta Check Rule, onde será abordada a criação da nova Ferramenta para tentar solucionar os erros encontrados nas regras feitas manualmente; Capítulo 6, estudo de caso, irá ser demonstrada como a ferramenta ajudará a diminuir o tempo gasto com a criação das novas regras e como conseqüência a diminuição nas requisições de acesso ao link de dados; Capítulo 7, uma conclusão geral do projeto, foi adicionado também um capitulo onde é abordada a possibilidade de trabalhos futuros para uma continuidade do trabalho aqui realizado.

2. SEGURANÇA DE REDES

2.1. TECNOLOGIA DE SEGURANÇA

Apesar dos problemas, podemos afirmar que o uso adequado da Tecnologia de Segurança é um dos mecanismos de proteção e controle na Internet que permite realizar operações comerciais em condições mais seguras do que os meios de transações e comunicações convencionais.

De nada valem os conceitos e preocupações deste problema se a organização não tem a intenção de formar ou adotar uma "cultura" voltada para a segurança. A segurança não é um ato isolado em um dado momento ou de competência de apenas algumas pessoas, e sim algo que deverá ser verificado diariamente. Serão apresentadas algumas aplicações que estão diretamente relacionadas com a manipulação destas regras de segurança:

2.1.1. SQUID

O Squid é uma ferramenta para a criação de proxy e cache de web e ftp, permitindo que as máquinas compartilhem o acesso à internet controlado por um servidor central, mesmo que elas não tenham acesso direto à Internet. Entre os recursos do Squid, estão as possibilidades de definir listas de regras de controle de acesso a Internet.

Geralmente este controle de acesso é feito por máquina / IP. Entretanto, o Squid tem acesso a permissões por usuário, onde cada pessoa que tentar acessar a web é obrigada a fornecer um login e uma senha para verificação. Esta verificação pode ser feita através de um arquivo passwd tradicional, ou ainda através de um servidor LDAP.

2.1.2. ACL

A ACL (Access Control Lists) ou listas de controle de acesso, constituem-se na grande flexibilidade e eficiência do Squid, é através delas que podemos criar regras para controlar o acesso à internet das mais diferentes formas. Praticamente todo o processo de controle do Squid é feito com o seu uso.
O uso das listas de controle de acesso é a parte mais importante da configuração de um servidor proxy Squid, pois se bem configuradas podem trazer um nível de segurança muito bom para a rede, entretanto se mau configuradas podem ter resultado oposto, já que além da falsa sensação de segurança não será aproveitada a grande capacidade e funcionalidade do Squid. A declaração de ACLs (Access Control List) ou Lista de Controle de Acesso, define a combinação de permissão (allow) e negação (deny) de acesso HTTP (http_access), implementa a política e controle de acesso à web.

Tipos de ACL's

As ACL's são definidas da seguinte forma: acl nome tipo string | ``arquivo''

Abaixo os tipos mais comuns:

src - tipo utilizado para indicar endereços IP de origem. Pode-se especificar um endereço de rede, como 192.168.16.0/24, um endereço de um determinado host, como 192.168.16.10/24 ou uma faixa de endereços, como 192.168.16.10-192.168.16.20/24;

dst - semelhante ao tipo anterior, mas está relacionada ao endereço de destino;

srcdomain - tipo indicado para verificar o domínio da máquina cliente. Os domínios serão obtidos por resolução reversa de IP, o que pode causar atrasos para a resposta da requisição. A definição do domínio deve ser feita da seguinte forma: ``.meudominio.com.br'', não podendo ser esquecido o ``.'' (ponto) no início;

dstdomain - usado da mesma forma que srcdomain, entretanto com relação ao destino;

srcdom_regex - avalia o domínio usando expressões regulares. Seu uso é semelhante as duas anteriores, acrescentando a flexibilidade do uso da expressão regular;

dstdom_regex - usado da mesma forma que srcdom_regex, entretanto com relação ao destino;

time - usado para especificar dias da semana e horários. Os dias da semana são definidos através de letras que os representam, e os horários;

url_regex - Este tipo percorre a URL a procura da expressão regular especificada. Deve ser observado que a expressão é case-sensitive, para que seja case-insensitive deve ser usada a opção -i. É o tipo mais comum de ACL dada a flexibilidade proporcionada pelo uso de expressões regulares;

urpath_regex - Tipo semelhante a url_regex, mas procura a expressão regular na URL sem levar em conta o nome do servidor e o protocolo, isto quer dizer que a procura vai ser feita apenas na parte da URL após o nome do servidor, como por exemplo, na URL http://www.servidor.com.br/pasta/sexo.html a procura será realizada apenas na parte /pasta/sexo.html. Ela é também case-sensitive, para que seja case-insensitive deve ser usada a opção -i;

port - Realiza o controle pela porta de destino do servidor, neste tipo deve ser especificado o número da porta;

proto - Serve para especificar o protocolo, como por exemplo FTP ou HTTP;

proxy_auth - Tipo usado para implementar autenticação de usuários no proxy. A autenticação é feita com uso de softwares externos, podem ser passados os nomes dos usuários ou usada a opção REQUIRED para que seja autenticado qualquer usuário válido;

2.1.3. FILTRAGEM DE PACOTES

É o processo que permite ou bloqueia o tráfego de pacotes entre duas redes, baseando-se nas informações obtidas nos cabeçalhos dos pacotes e em um conjunto de regras de filtragem. Esse processo usa geralmente informações dos cabeçalhos IP da origem e do destino e as informações dos cabeçalhos TCP ou UDP são os números de portas usados na origem e no destino. Os filtros de pacotes protegem o sistema operacional por serem implementados no kernel evitando que certos pacotes nocivos cheguem ao sistema operacional. LIMA (2000).

2.1.4. PROXY

O termo servidor Proxy vem da palavra em inglês que significa procuração. Em termos técnicos, servidor de Proxy é um software que tem a "procuração" de um ou mais hosts para buscar na Internet uma informação solicitada. Muitos integradores instalam um servidor proxy e configuram os hosts clientes para acessar o proxy. O proxy atua como um cache que em certos casos se torna uma vantagem por diminuir o tempo de acesso ao sites já visitados.

2.1.5. REDE DE PERÍMETRO

Uma rede acrescentada entre uma rede protegida e uma rede externa, a fim de fornecer uma camada adicional de segurança. Uma rede de perímetro é às vezes chamada de uma DMZ que significa Zona Desmilitarizada. (FILADORO, Ricardo, maio 2004)

2.2. TECNOLOGIA DE VISUALIZAÇÃO

A seguir são apresentadas algumas ferramentas que auxiliaram na visualização das novas regras que foram incorporadas, fazendo com que elas sejam bem mais fáceis de se compreender

2.2.1. MRTG - MULTI ROUTER TRAFFIC GRAPHER

É uma ferramenta para análise e monitoramento do tráfego dos dados da rede, que cria páginas HTML com relatório baseado em dados obtidos de roteadores e hosts dessa rede via SNMP[1], com gráficos GIF/PNG e apresentando uma visão real desses dados coletados; estes dados são captados através de um script, que é inserido em uma tabela variando de cinco em cinco minutos, cada vez que é iniciado, ele obtém os dados pré-estabelecidos e gera gráficos no formato .png (Portable Network Graphic) para posterior análise e sua utilidade é indiscutível na avaliação das condições da rede.

Pode-se verificar a diferença entre dois pontos, o estágio da leitura foi dividido pela decorrência do tempo, então foi possível determinar os dados comuns da taxa de transição durante os últimos cinco minutos.
Notou-se nestes dados, que foi gerado um Gráfico disponibilizado na Web, onde foi possível visualizar o estado do acesso à Internet.

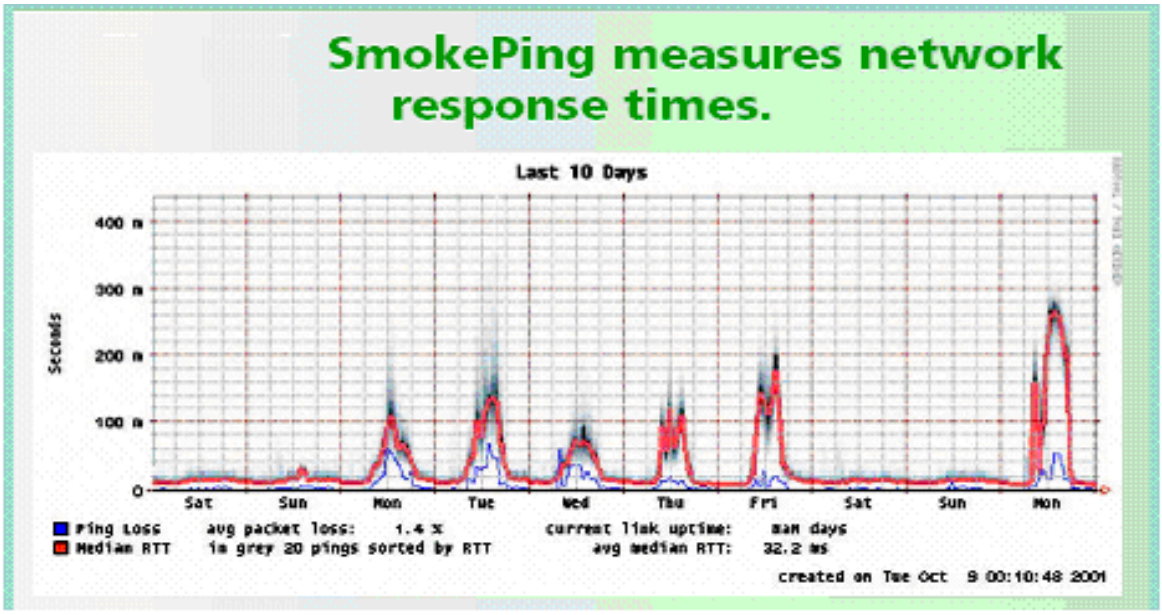


FIGURA 1 – MRTG SMOKEPING / MEDE O TEMPO DE RESPOSTA DA REDE

Conforme a Figura 1, o MRTG SmokePing, transmite a cada cinco minutos um sinal de envio na rede estipulada, para obter uma resposta do dispositivo; os

[1] **SNMP** *Simple Network Management Protocol* É um protocolo para monitorar informações de hosts na rede, possibilita ao Administrador gerir o desempenho da rede, encontrar e resolver problemas de rede, e planejar seu crescimento.

valores dos pings médios aparecem em vermelho e os pings restantes são visualizados na cor cinza do gráfico. Este gráfico indica um provável problema com a largura da banda da rede.

2.2.2. SARGE

O Sarge é um interpretador de logs para o Squid. Sempre que ele é executado cria-se um conjunto de páginas, divididas por dia, com uma lista de todas as URLS que foram acessadas a partir de uma máquina específica. Ele também mostra os usuários, caso o Squid esteja configurado para exigir autenticação; pode-se também acompanhar as páginas que estão sendo acessadas, mesmo que não exista nenhum filtro de conteúdo e tomar as medidas cabíveis em casos de abuso. Alguns exemplos de relatório gerado pelo Sarge da Universidade Padre Anchieta, Figuras 2 e 3, mostrando os sites acessados por IPs. CHADD et al. (2003).

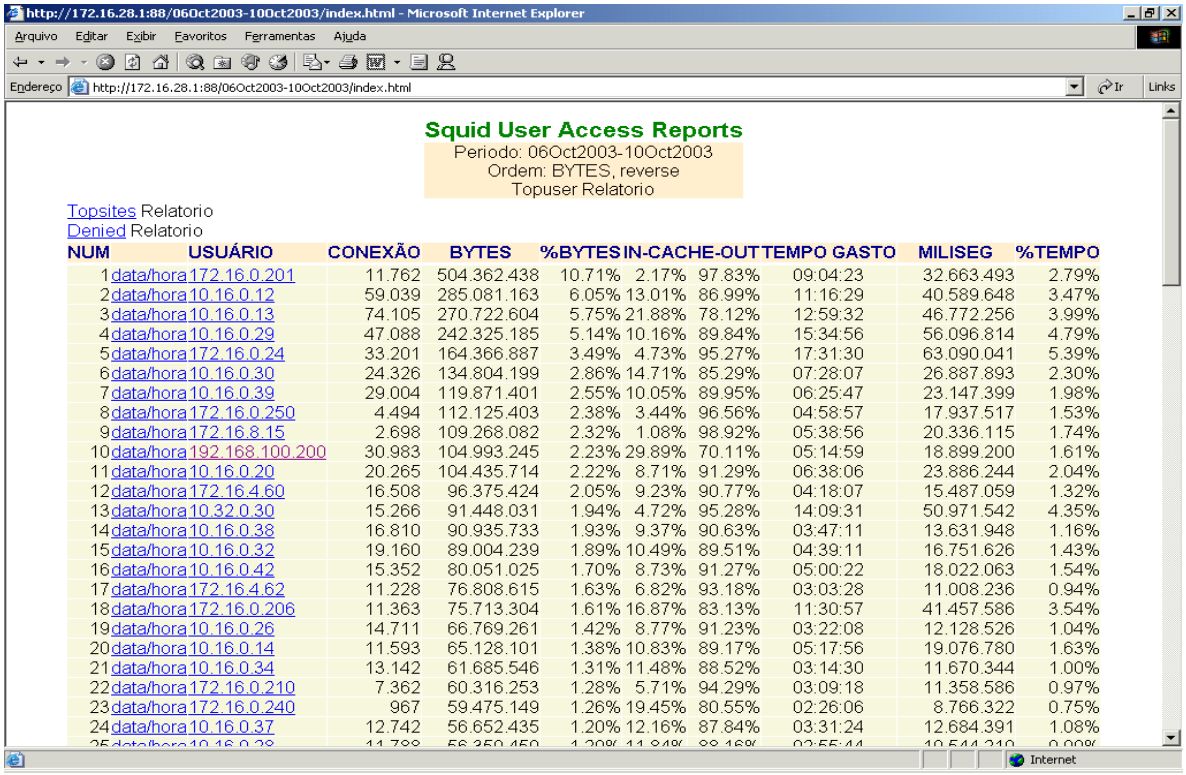
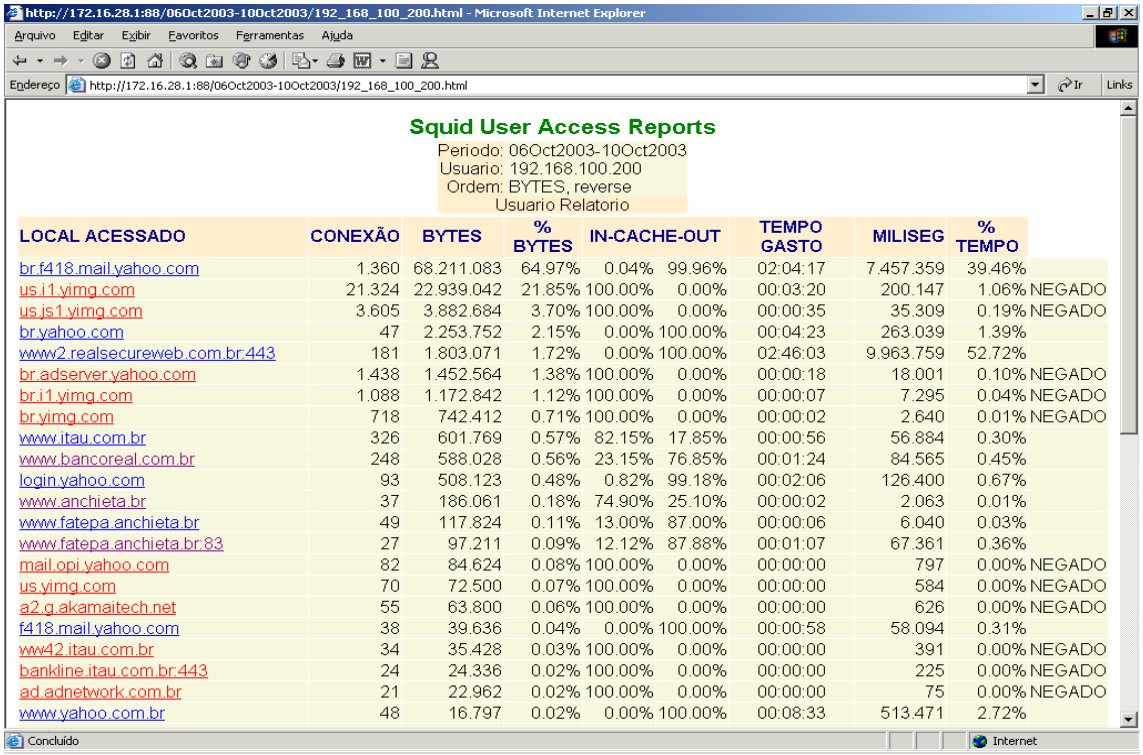


FIGURA 2 - SARGE / RELATÓRIOS DE UTILIZAÇÃO NA INTERNET - POR IP



LOCAL ACESSADO	CONEXÃO	BYTES	% BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	% TEMPO	
br.f418.mail.yahoo.com	1.360	68.211.083	64.97%	0.04%	99.96%	02:04:17	7.457.359	39.46%	
us.i1.yimg.com	21.324	22.939.042	21.85%	100.00%	0.00%	00:03:20	200.147	1.06%	NEGADO
us.js1.yimg.com	3.605	3.882.684	3.70%	100.00%	0.00%	00:00:35	35.309	0.19%	NEGADO
br.yahoo.com	47	2.253.752	2.15%	0.00%	100.00%	00:04:23	263.039	1.39%	
www2.realsecureweb.com.br:443	181	1.803.071	1.72%	0.00%	100.00%	02:46:03	9.963.759	52.72%	
br.adserver.yahoo.com	1.438	1.452.564	1.38%	100.00%	0.00%	00:00:18	18.001	0.10%	NEGADO
br.i1.yimg.com	1.088	1.172.842	1.12%	100.00%	0.00%	00:00:07	7.295	0.04%	NEGADO
br.yimg.com	718	742.412	0.71%	100.00%	0.00%	00:00:02	2.640	0.01%	NEGADO
www.itau.com.br	326	601.769	0.57%	82.15%	17.85%	00:00:56	56.884	0.30%	
www.bancoreal.com.br	248	588.028	0.56%	23.15%	76.85%	00:01:24	84.565	0.45%	
login.yahoo.com	93	508.123	0.48%	0.82%	99.18%	00:02:06	126.400	0.67%	
www.anchieta.br	37	186.061	0.18%	74.90%	25.10%	00:00:02	2.063	0.01%	
www.fatepa.anchieta.br	49	117.824	0.11%	13.00%	87.00%	00:00:06	6.040	0.03%	
www.fatepa.anchieta.br:83	27	97.211	0.09%	12.12%	87.88%	00:01:07	67.361	0.36%	
mail.opi.yahoo.com	82	84.624	0.08%	100.00%	0.00%	00:00:00	797	0.00%	NEGADO
us.yimg.com	70	72.500	0.07%	100.00%	0.00%	00:00:00	584	0.00%	NEGADO
a2.g.akamaitech.net	55	63.800	0.06%	100.00%	0.00%	00:00:00	626	0.00%	NEGADO
f418.mail.yahoo.com	38	39.636	0.04%	0.00%	100.00%	00:00:58	58.094	0.31%	
ww42.itau.com.br	34	35.428	0.03%	100.00%	0.00%	00:00:00	391	0.00%	NEGADO
bankline.itau.com.br:443	24	24.336	0.02%	100.00%	0.00%	00:00:00	225	0.00%	NEGADO
ad.adnetwork.com.br	21	22.962	0.02%	100.00%	0.00%	00:00:00	75	0.00%	NEGADO
www.yahoo.com.br	48	16.797	0.02%	0.00%	100.00%	00:08:33	513.471	2.72%	

FIGURA 3 - SARGE / RELATÓRIO DE ACESSO A INTERNET POR URL – BLOQUEADO

2.2.3. NAGIOS

O NagiosTM é uma poderoso Aplicativo Open Source que monitora Micros, Switchs, Impressoras e tudo mais o que estiver ligado na rede. Ele verifica constantemente toda a disponibilidade dos equipamentos configurados de sistemas e de redes, conforme Figuras 4 e 5, ele checa também clientes e serviços, que foram especificados anteriormente, alertando ao Administrador possíveis falhas nos servidores.

Ele foi originalmente projetado para rodar em Linux, mas hoje ele funciona na maioria das plataformas. GALSTAD (2004).

Alguma ferramentas do Nagios:

- Monitoramento de rede e serviços (SMTP, POP3, HTTP, NNTP, PING);
- Monitoramento dos recursos de clientes (carga de processador, uso de disco);

- Organização simples de plugins que permite aos usuários facilmente desenvolverem seus próprios serviços de checagem;

- Checagem paralela de serviços;

- Habilidade para definir hierarquia de redes de clientes usando clientes pais (parent hosts), permitindo a detecção e distinção entre clientes que estão desativados e aqueles que estão inalcançáveis;

- Notificação de contatos quando problemas em serviços e clientes ocorrerem ou forem resolvidos (via email, pager, ou métodos definidos pelo usuário);

- Habilidade para definir tratadores de eventos (event handlers) que serão executados durante eventos de serviços ou clientes na tentativa de resolução de problemas;

- Rotatividade automática de arquivos de logs;

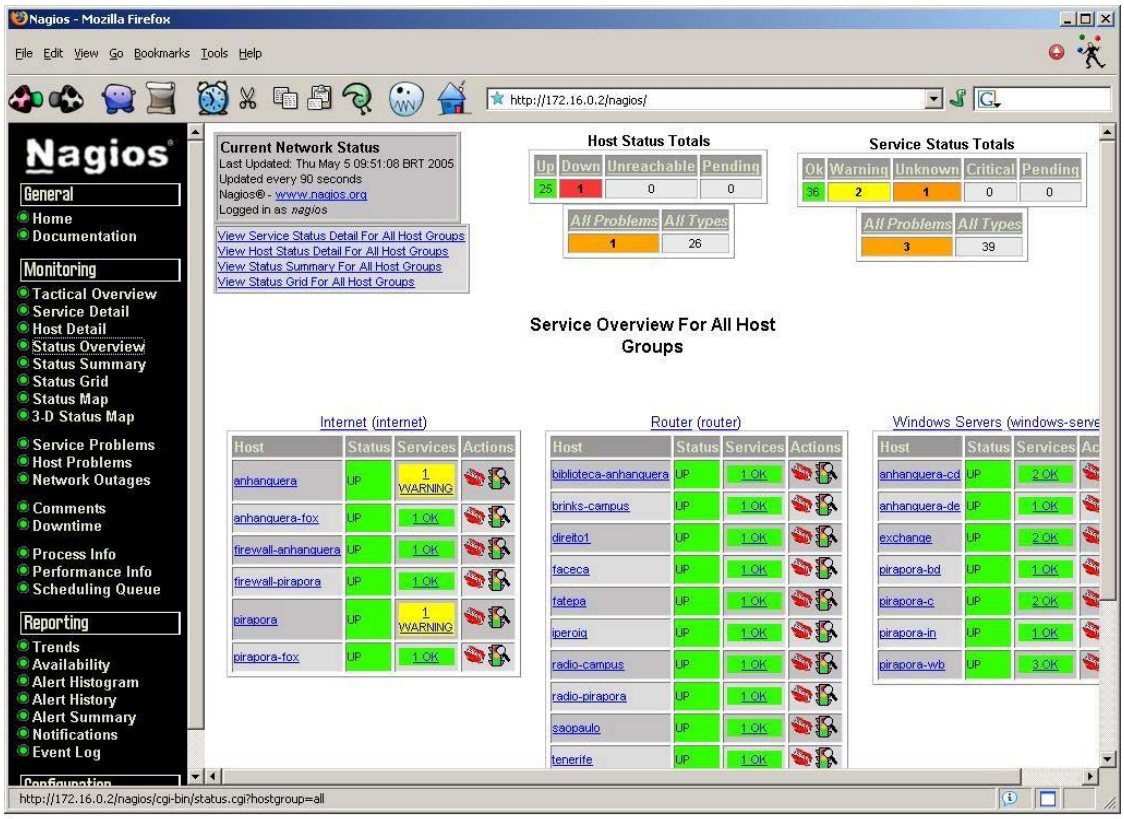


FIGURA 4 – NAGIOS / LINKS DE ACESSO

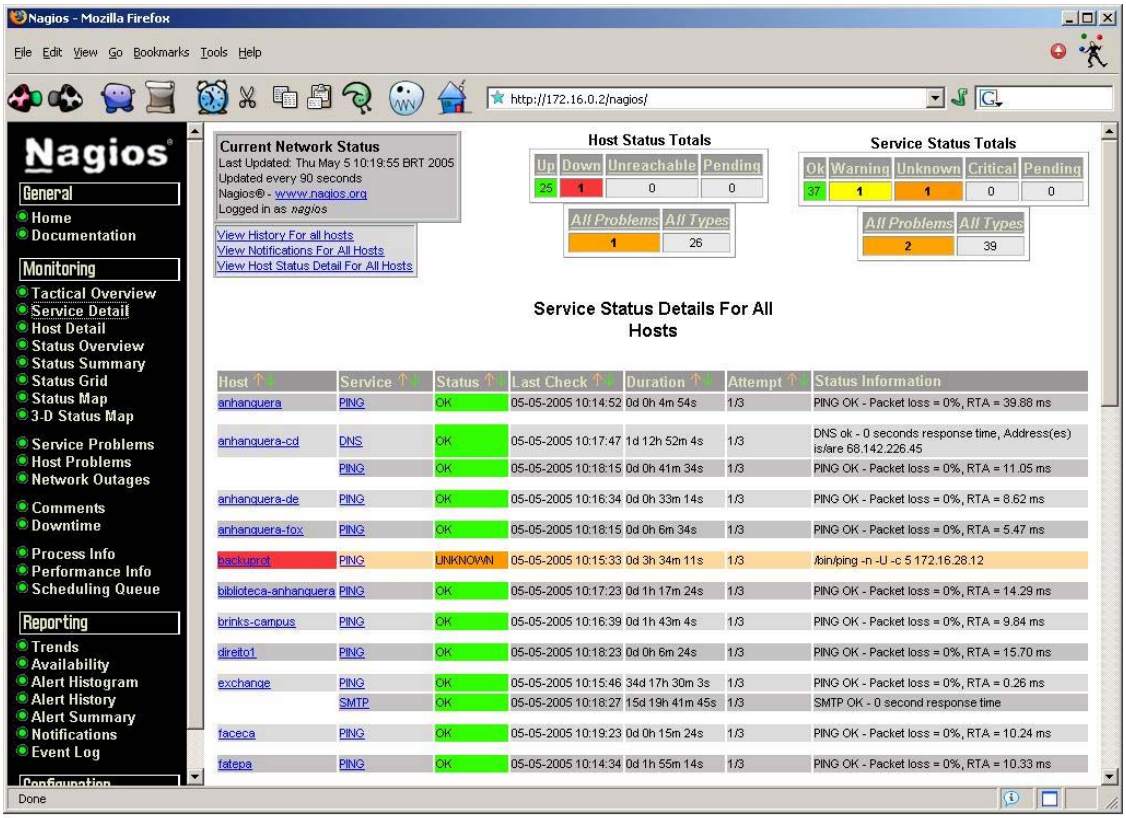


FIGURA 5 – NAGIOS / ACESSO AOS SERVIDORES

2.2.4. NTOP - NETWORK TRAFFIC PROBE

Conforme Deri (2004) o NTOP é um aplicativo em Linux capaz de mostrar a utilização da rede detalhando a utilização por host ou protocolo ele possui uma interface web e é capaz de gerar gráficos que facilitam a interpretação de estatística de uso, conforme demonstrados nas Figuras 6 e 7.

O NTOP não possui um arquivo de configuração; então para utilizar alguma configuração diferente dos valores padrões é necessário incluir argumentos via linha de comando ou criar um pequeno script. A utilização básica é bastante simples, e opções mais avançadas requerem uma experiência mais apurada do Administrador de Rede. O acompanhamento do fluxo chega a ele de forma simplificada e é normal consumir uma grande quantidade de memória, lembrando que quanto maior a rede, maior será a utilização de memória; pode-se evitar que esse problema ocorra, desabilitando o acompanhamento de sessões TCP (parâmetro -z) e diminuindo o tempo que uma sessão deve permanecer inativa.

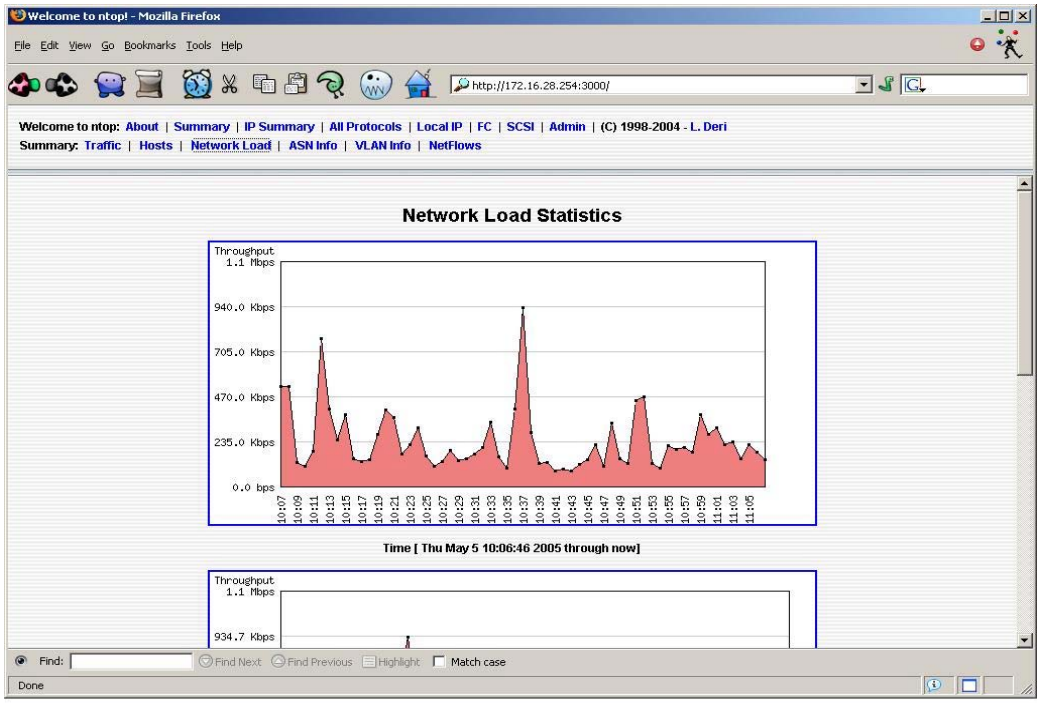


FIGURA 6 – NTOP / TRÁFEGO BANDA DE DADOS

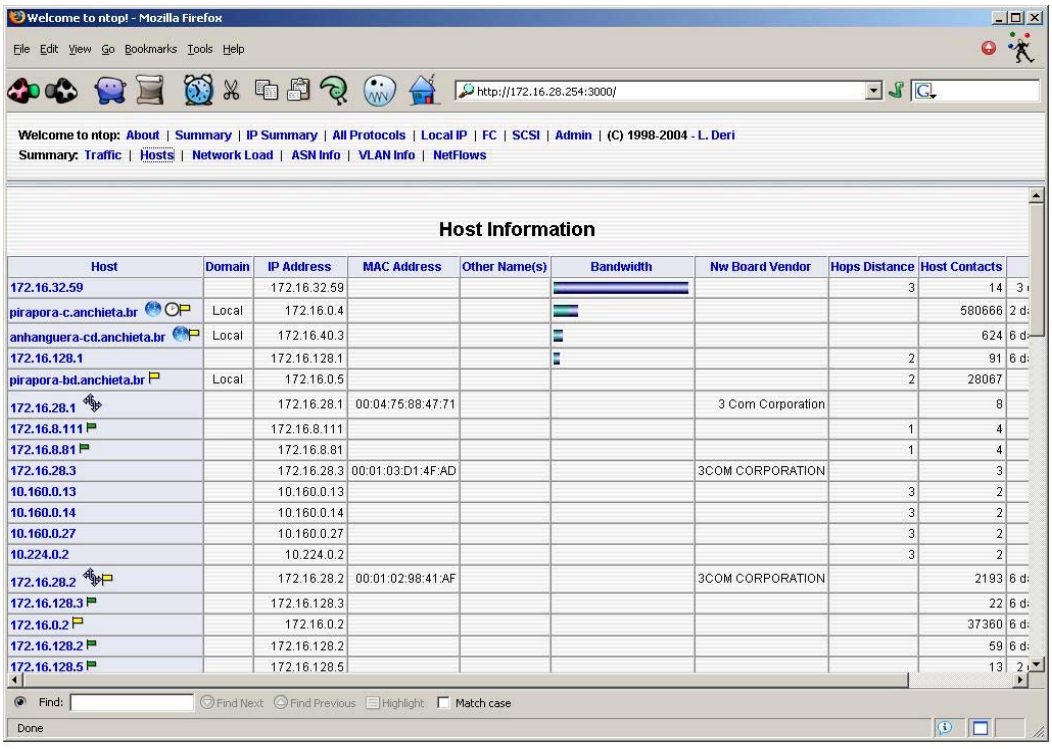


FIGURA 7 - NTOP / ACESSO TCP/IP

2.2.5. WEBMIN

É uma ferramenta de Administração Gráfica que utiliza linguagem Perl. Ela foi projetada para ser uma ferramenta de administração leve, funcional, e que possa ser facilmente estendida. A ferramenta está disponível hoje em mais de vinte idiomas, e está sendo considerada a ferramenta oficial de administração em vários sistemas operacionais e distribuições *Linux*.

O Webmin funciona como um centralizador de configurações do sistema, monitoração dos serviços e de servidores, fornecendo uma interface amigável e que, quando configurado com um servidor web, pode ser acessado de qualquer local através de um Browser, conforme Figuras 8, 9 e 10. A maioria das interfaces de administração possui uma interface fixa que só pode ser acessada de um ambiente local. O Webmin, entretanto, trabalha com uma interface *web*, ou seja, a possibilidade de se configurar uma máquina através de uma rede é totalmente cômoda, pois basta ter acesso a um navegador. Com isto, é possível configurar uma máquina através de praticamente qualquer plataforma de *hardware* e *software*. CAMERON (2005).

Os módulos do Webmin no *Linux* estão divididos em vários pacotes, cada um com uma função:

- *task-webmin*: Meta-pacote que instala o Webmin completamente;
- *task-webmin-desktop:* Meta-pacote que instala o Webmin para configurações em um *desktop;*
- *task-webmin-server:* Meta-pacote que instala o Webmin para as configurações de um servidor;
- *webmin-core:* instala apenas a parte principal do Webmin, ou seja, nenhum módulo além do módulo *acl*. É o mínimo necessário para se ter o Webmin funcionando;
- *webmin-desktop*: Possui os módulos que são referentes a configuração de um desktop, como, por exemplo, conexão ADSL;

- *webmin-server:* Possui os módulos que são referentes a configuração de um servidor como, por exemplo, o Postfix;

- *webmin-theme-conectiva*: Tema Conectiva para o Webmin (tema padrão).

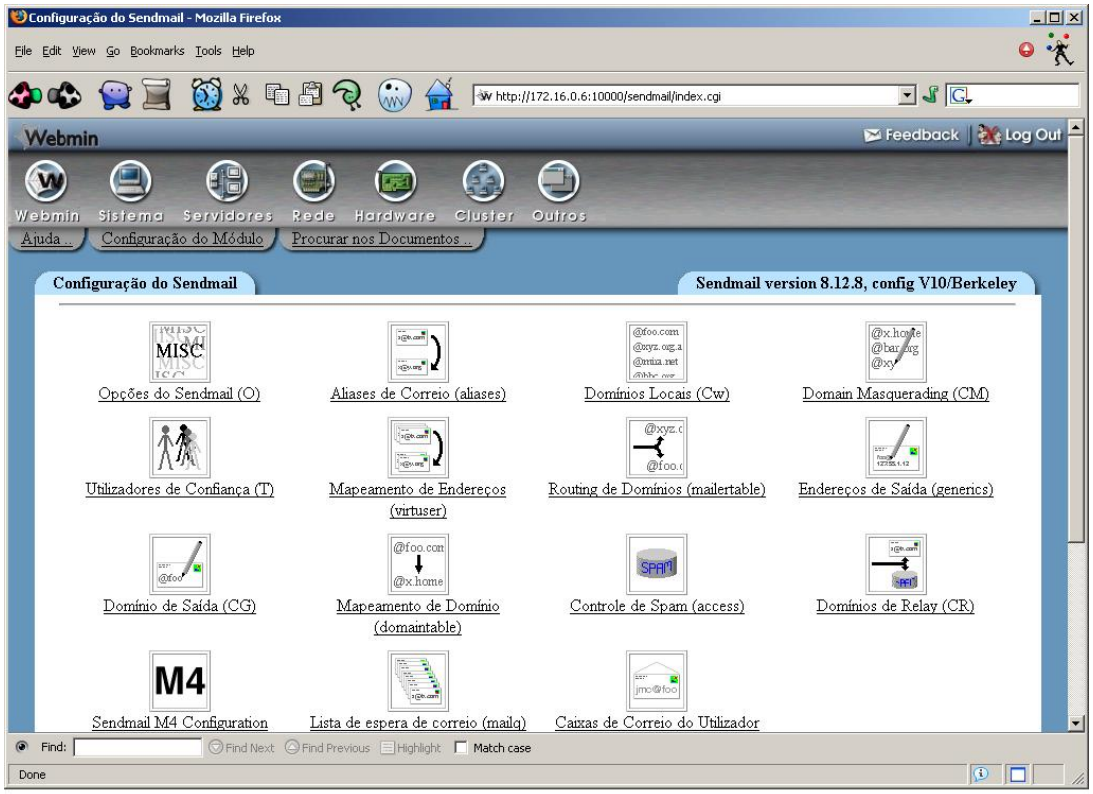


FIGURA 8 – WEBMIN / CONFIGURAÇÃO E-MAIL

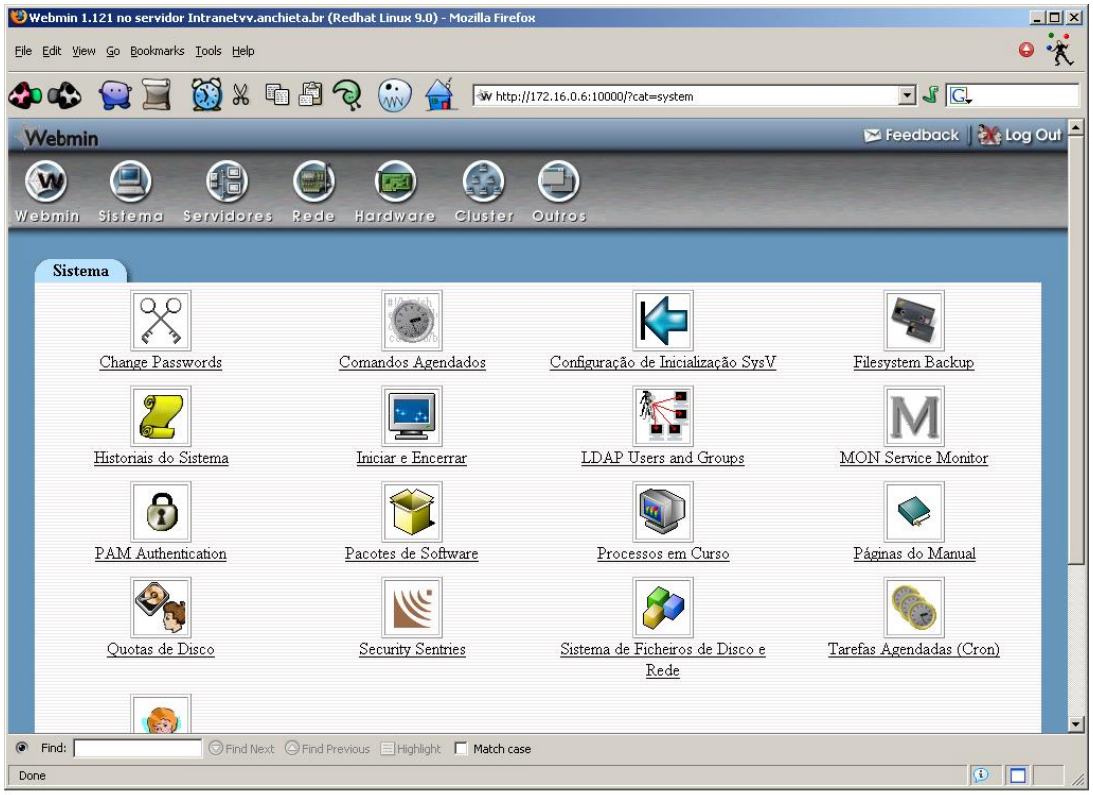


FIGURA 9 – WEBMIN / GERENCIAMENTO DO SISTEMA

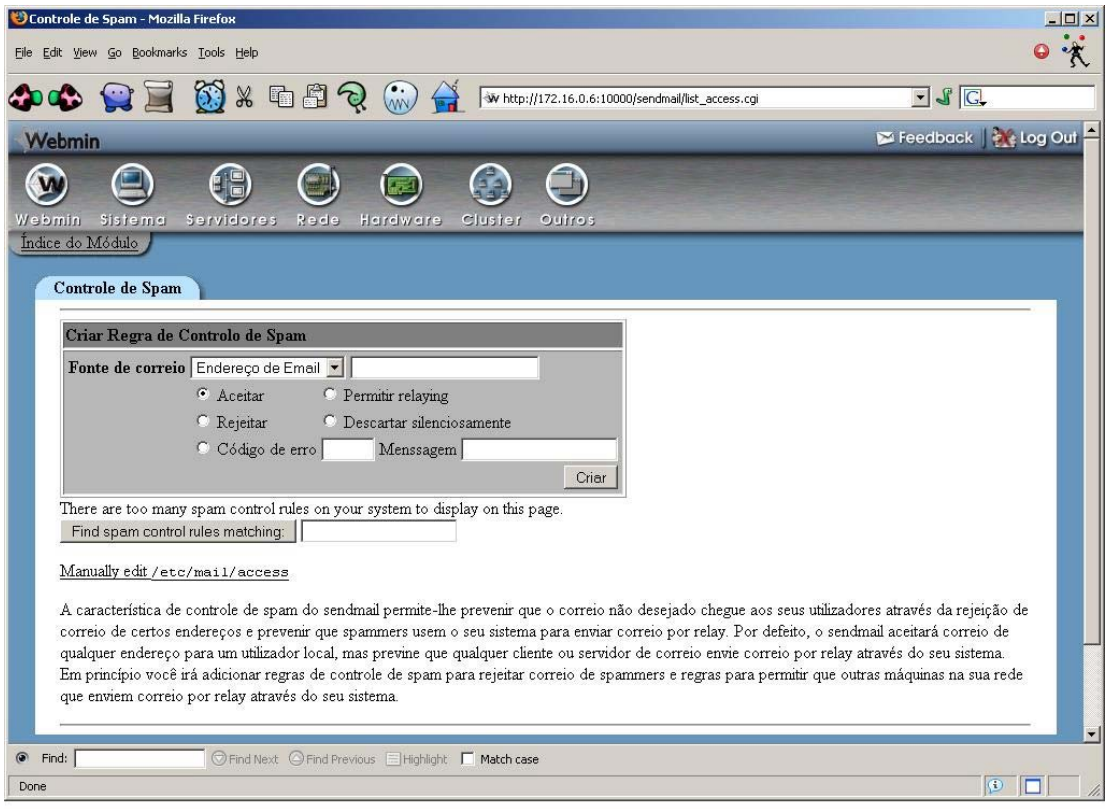


FIGURA 10 – WEBMIN / CONTROLE DE SPAM

3. SCRIPT SQUID

Neste capítulo, será apresentada a estrutura Squid tendo como base o Sistema Operacional Linux. Será descrito, em seguida, o subconjunto das linhas programadas que foram escolhidas para fazer parte da implantação da Ferramenta Check Rule. É bom lembrar que no Squid somente são verificados três pontos: o primeiro é se tudo o que foi iniciado na regra foi finalizado; o segundo é se existem erros de digitação nos comandos, pois na grande maioria das vezes esta verificação é conferida logo após a programação pelo próprio programador; e o terceiro ponto é saber se o serviço do Squid analisou somente o que foi digitado ou se realmente todas as regras que foram solicitadas; estão incorporadas na programação. Sendo estes os pontos discutidos, serão demonstradas a seguir as possibilidades de correlação entre as regras em modo *Shell* usados anteriormente e os gerados pela ferramenta Check Rule.

3.1. ESTRUTURA GERAL DO ARQUIVO SCRIPT SQUID LINUX

O arquivo script Squid registra informações detalhadas dos parâmetros das regras que serão usadas para implementar liberações ou bloqueios de acesso as funções requisitadas. A ilustração abaixo mostra os comandos que são executados linha a linha de acordo com as especificações impostas pelo programador.

Alteração do arquivo squid.conf

Exemplo de script para habilitar as linhas de comando:

```
http_port 80
cache_mem 64 MB
cache_access_log /var/log/squid/access.log
pid_filename /var/run/squid.pid
refresh_pattern ^ftp:1440  20% 10080
refresh_pattern  ^gopher: 1440  0% 1440
httpd_accel_with_proxy on
```

store_avg_object_size 5 KB

Conforme a ilustração acima mencionada, os comandos podem ser divididos em sete campos:

- Liberação da porta de acesso onde serão desviadas as conexões (port 80).
- Quantidade de cachê em memória que será disponibilizada para arquivamento de informações dos acessos visitados, quando o espaçamento é aumentado é criado um novo arquivo que segue a mesma nomenclatura sendo subdividida em números crescentes em seu nome.
- Redirecionamento do arquivo ao caminho de diretório específico para onde serão enviadas as informações de acesso.
- Registro numérico que se dá ao serviço registrado *PID*.
- Liberação de acesso ao proxy de armazenamento na opção squid.
- Arquivamento de objetos de tamanhos pré-definidos 5KB.

3.2. LINHAS DE SCRIPTS ESCOLHIDAS PARA IMPLANTAÇÃO DA FERRAMENTA

Esta linhas de script são importantes para se verificar a atividade de sua utilização. O arquivo script Squid.conf é responsável pelas regras de bloqueio ou liberação de acesso a Internet; todas as suas configurações são inseridas diretamente neste arquivo, que se comunica com alguns outros arquivos que normalmente têm a descrição de seu nome com as características referentes a sua função.

Para arquivos de bloqueios de sites de sexo, poderia ter como sugestão um nome sexo_url.txt ou palavras que seriam bloqueadas com descrições de jogos poderia ter como sugestão o nome jogos_word.txt, vale lembrar que no script são mencionados quais serão os bloqueios e quais serão os arquivos que terão estas instruções.

Depois destas regras serem adicionadas ao arquivo, é feita uma verificação parcial se todas as entradas foram finalizadas, pois toda acl tem que possuir sua http, podemos entender como se fosse um begin end, sendo que a acl informa qual é a máquina ou qual o usuário que será cadastrado, e a http fornece quais são as restrições ou liberações de acesso que o usuário ou a máquina irá possuir. Os erros de interpretação são alterados e posteriormente é dado um restart no serviço para sincronizar com as novas regras, com o comando service squid restart e também são reiniciado os arquivos *.txt para atualizar qualquer tipo de alteração com o comando squid –k reconfigure.

Foi selecionado um conjunto de regras de script que são especificadas para liberação (Acls access) ou restrição (Access deny) a rede. O primeiro critério foi observar quais são as linhas de mensagens que apareciam com maior freqüência no arquivo e quais delas poderiam fornecer informações gerenciais para o Administrador. E o segundo critério utilizado foi priorizar as mensagens que, embora não sejam muito frequentes, apresentam um nível de importância relativamente alta na área de segurança de rede.

3.2.1. ACESSO AOS USUÁRIOS

Neste conjunto de regras são demonstrados os comandos principais de ACL e Http_access, lembrando que os ACLs são incluídos para criar um novo usuário ou um novo grupo, e as Http_access são informações de quais liberações ou bloqueios o usuário ou grupo terão, sendo que primeiro se cria os usuários e depois existe a finalização das regras que foram adotadas.

Script de liberação de acesso exclusivo a um determinado usuário

TABELA 1 – SQUID / LIBERAÇÃO DE ACESSO AO USUÁRIO

Liberação de acesso /por IPs acl labinternet src 192.168.0.5-192.168.0.35 #por IPs de grupo especifico acl usuario1 src 192.168.0.1 #por IP de usuario acl usuario2 src 192.168.0.40 #por IP de usuario
Liberação de acesso / regra por site de um usuario especifico acl usuario2lib dstdomain "/etc/squid/usuario2lib"
Habilita o acesso a Internet aos usuarios cadastrados na acl http_access allow usuario1 # permitindo acesso total aos usuarios
Habilita o bloqueio total ao usuario2, menos o que estiver no arq usuario2lib http_access deny usuario2 !usuario2lib

3.2.2. ACESSO AOS PARÁMETROS

Os scripts são demonstrados por quais palavras ou quais sites serão bloqueados e também onde será armazenado o arquivo com as referidas informações.

TABELA 2 – SQUID / LIBERAÇÃO DE REGRAS DE SEGURANÇA

Liberação de acesso /regra por site especifico acl unblock url_regex -i "/etc/squid/unblock"
Bloqueio de acesso /regra por palavra especifica acl palavraquente url_regex -i "/etc/squid/palavraquente"
Bloqueio de acesso / regra por site especifico acl labnegado dstdomain "/etc/squid/labnegado"
Bloqueio de acesso a arquivos de sons e imagens acl nega_mp3 urlpath_regex \.mp3$ acl nega_avi urlpath_regex \.avi$ acl nega_ram urlpath_regex \.ram$
Habilita o acesso a Internet menos o conteudo dos arqs. palavra??? e lab??? http_access allow labinternet !palavraquente #por palavras http_access allow laboratorio1 !labnegado #por site
Habilita o bloqueio do arq. palavraquente, menos o conteudo do arq. unblock http_access deny palavraquente !unblock
Habilita o bloqueio das acl´s de sons e imagens http_access deny nega_mp3 http_access deny nega_avi

4. ASPECTOS GERAIS DA FERRAMENTA CHECK RULE

4.1. ANÁLISE DE REQUISITOS

O arquivo de especificação da política de segurança do Squid definiu os serviços básicos de que os usuários irão dispor. Na tentativa de compreender a política de segurança padrão do Squid, percebeu-se a necessidade de uma ferramenta para visualização de políticas que auxiliassem em sua compreensão, o que desencadeou uma pesquisa para identificar as ferramentas disponíveis. As ferramentas encontradas e seu foco em sistemas distribuídos demonstraram a necessidade de desenvolver uma ferramenta que objetivasse auxiliar os administradores em sua compreensão, análise e também uma verificação de quais seriam as novas política de segurança implantadas. Com isso em mente, surgiu a idéia de projetar uma ferramenta que exibisse de maneira clara e independente do conhecimento de cada um, uma forma de se fazer uma relação mais clara entre as programações das especificações de cada usuário e suas respectivas regras de acesso.

Neste capítulo serão apresentadas as atividades realizadas para identificar a necessidade da ferramenta, modelos que poderiam ser utilizados, e quais as questões importantes a serem consideradas no projeto, desenvolvimento e utilização da ferramenta. Primeiramente, são apresentados os trabalhos correlatos estudados. Em seguida, são apresentados os objetivos do sistema e o ambiente de desenvolvimento, que darão base à análise de requisitos apresentada em seguida e finalmente será apresentado a ferramenta desenvolvida, com o intuito de auxiliar na identificação de estruturas e necessidades do projeto da ferramenta Check Rule.

4.2. AMBIENTE DE DESENVOLVIMENTO

O sistema operacional Windows foi escolhido como plataforma base para o desenvolvimento da ferramenta. Para implementação, decidiu-se pelo uso da linguagem Visual Basic. Esta opção possui um variado conjunto de ferramentas que poderiam ser utilizadas no desenvolvimento, entre as quais destacam-se ferramentas para representação e visualização gráfica, e ferramentas para desenvolvimento de interfaces. Foi escolhida a plataforma .NET para representar a criação desta ferramenta. E finalmente, o ambiente de desenvolvimento foi escolhido como ambiente de programação, pois disponibiliza um framework para desenvolvimento de aplicações em .NET entre outras coisas, ele permite a integração entre código-fonte e interfaces de forma clara e limpa, disponibiliza um editor de interfaces gráficas e permite o gerenciamento centralizado do projeto.

4.3. PROTÓTIPO

Antes de iniciar a etapa de projeto do sistema, foram realizados testes utilizando um protótipo para verificar a viabilidade do mapeamento gráfico e sua utilidade na visualização das políticas. Isso foi feito dado que a transição manual da política de segurança para a nova ferramenta pode ser um processo complicado, tendo em vista a complexidade das regras existentes. O desenvolvimento do protótipo foi essencial para o amadurecimento do projeto, contribuindo com a identificação de estruturas de dados necessárias, de funcionalidades relevantes ao sistema e de uma organização mais elaborada para o projeto.

O protótipo foi desenvolvido utilizando pequenas aplicações desenvolvidas na linguagem Visual Basic, conforme demonstrado no Anexo, em conjunto com o gerenciador de banco de dados Access. Cada aplicação foi criada com uma finalidade específica, utilizando a base de dados Access para armazenar e consultar as regras da política. Por se tratarem de aplicações experimentais, pouco foi feito com relação à simplificação de seu uso para o administrador,

sendo o esforço focado principalmente na funcionalidade e nas estruturas de armazenamento, conforme os objetivos iniciais do desenvolvimento do protótipo.

O gerenciador de banco de dados Access foi utilizado para criar e gerenciar as tabelas para representação das políticas. Ele foi escolhido como repositório por permitir a realização de várias consultas posteriores, pois permite a filtragem e a seleção de dados que possam ser importantes de serem pesquisados. As Figuras 15 e 16 apresentam as tabelas criado para especificar a base de dados a ser utilizada pela aplicação do protótipo.

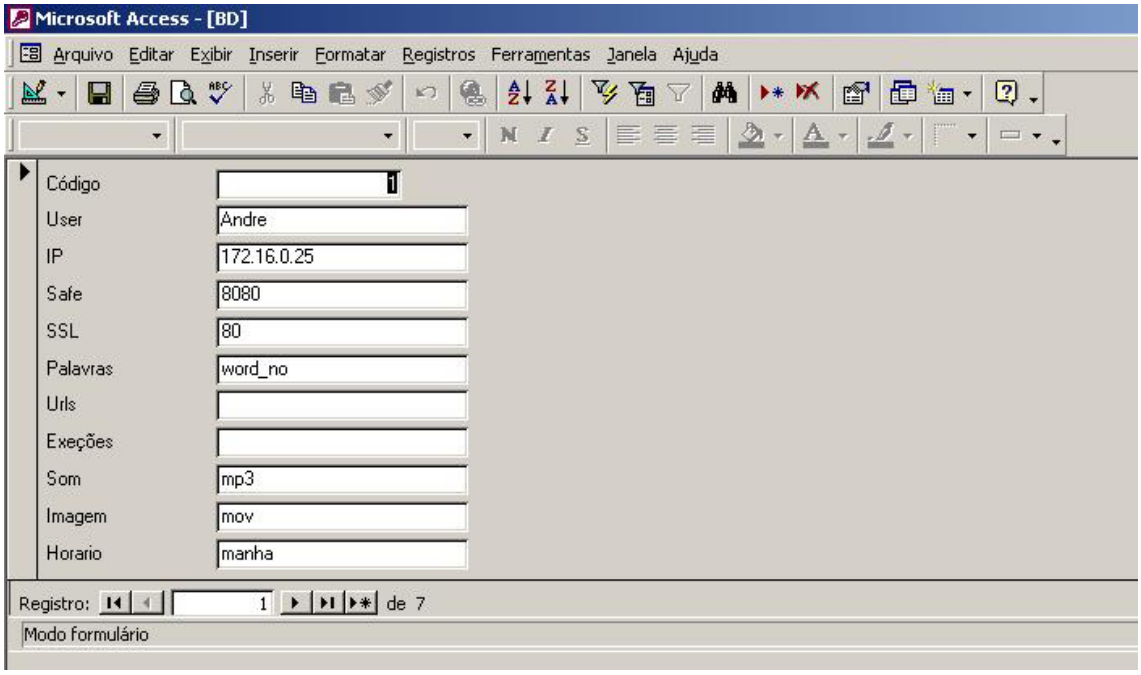


FIGURA 11 – VISUALIZAÇÃO DAS REGRAS DO BANCO DE DADOS

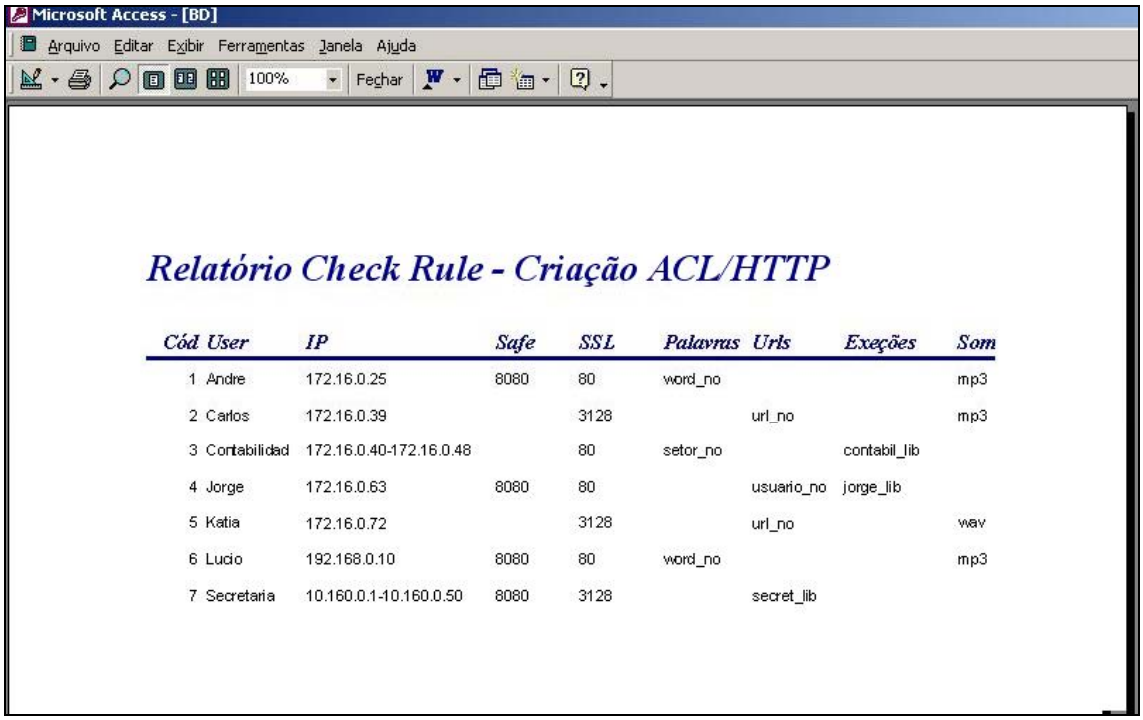


FIGURA 12 – RELATÓRIO DAS REGRAS ACL/HTTP

4.4. FERRAMENTA CHECK RULE

Concluída a etapa de análise e protótipo da ferramenta, iniciou-se a elaboração do projeto mediante ao guia no desenvolvimento da ferramenta Check Rule. Os resultados obtidos nas etapas anteriores foram essenciais na definição das representações, arquitetura e estruturas de dados utilizados na ferramenta.

A partir do projeto, pretendia-se a implementação completa da ferramenta; porém, o pouco tempo disponível tornou inviável tal implementação, motivo pelo qual decidiu-se pela implementação parcial da ferramenta, considerando apenas alguns aspectos do projeto, porém de tal forma que fossem possíveis inclusões incrementais para o desenvolvimento posterior de todas as funcionalidades e representações previstas no projeto. A partir da ferramenta desenvolvida, foram elaboradas análises de determinados aspectos da política de segurança padrão do Squid, para comprovar sua utilidade e eficácia com relação às novas regras, evitando que alguns erros que eram cometidos manualmente não sejam cometidos com a utilização da ferramenta. Foram apresentados o projeto da ferramenta Check Rule, os detalhes da

implementação da ferramenta desenvolvidos a partir do projeto e alguns exemplos de uso da ferramenta.

4.5. DETALHAMENTO DA IMPLEMENTAÇÃO DA FERRAMENTA

A ferramenta foi implementada seguindo a estrutura prevista pelo projeto; porém algumas experiências obtidas durante o desenvolvimento da ferramenta serviram para realimentar o projeto e algumas modificações no mesmo foram derivadas de necessidades identificadas durante a implementação. Algumas regras e estruturas diferem entre o projeto e a ferramenta devido a essa realimentação; porém, tendo em vista o isolamento entre componentes obtido, a modificação para adaptação ao projeto pôde ser realizada sem grandes impactos no código. Para implementação parcial da ferramenta, foram escolhidos alguns conjuntos de regras a serem mapeados e um conjunto de funcionalidades essenciais relacionadas a estas regras. Decidiu-se por iniciar a implementação da ferramenta pelas regras relacionadas ao modelo previsto pelo projeto conforme demonstrados na Figura 13. A primeira fase foi o planejamento onde se verificou como seria feito o Projeto desta nova ferramenta e quais seriam as dificuldades que poderiam ocorrer. Na segunda fase foi elaborada uma análise que mostrou as características da ferramenta e também as especificações técnica dos envolvidos na criação e também os planos de teste que seriam usados no final para a verificação se a ferramenta está de acordo com as especificações.

Na fase do desenvolvimento foi abordada a criação da ferramenta em si, e os procedimentos de sua instalação; já na fase de Implementação foi elaborado um experimento que foi conduzido e executado por alguns profissionais da área que auxiliaram as novas inclusões das regras dos usuários. No final dos testes foi elaborado um estudo de caso, verificando se a implantação desta nova ferramenta proporcionou ou não um ganho de performance na requisição dos acessos ao link Internet.

Estrutura de Implantação				
Planejamento	**Análise**	**Desenvolvimento**	**Implementação**	**Testes**
Projeto	Especificação da Ferrament	Ferramenta Check Rule	Experimento	Estudo de Caso
Dificuldades	Especificação Técnica	Procedimento de Instalação		
	Planos de Testes			

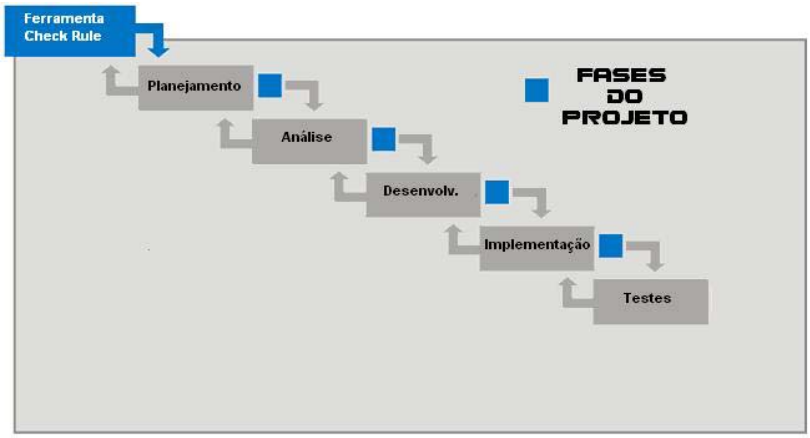


FIGURA 13 – ESTRUTURA DE IMPLANTAÇÃO DA FERRAMENTA

4.6. INTERFACE DE VISUALIZAÇÃO COM O USUÁRIO

A interface com o usuário foi projetada visando à simplificação e à interatividade do usuário provendo um maior conjunto de recursos possíveis para auxiliar o usuário na visualização e análise da política de segurança. A Figura 14 apresenta a interface básica de uma da telas da ferramenta. Estão destacadas na tela as seguintes opções: Acesso Liberado ou Bloqueado, Sites, Palavras, Horários, Sons e Imagens.

A tela de visualização do menu principal permite ao Administrador o preenchimento das novas regras nos campos solicitados; neste exemplo existem as opções de se criar um usuário incluindo as suas características de bloqueio ou liberação de acesso a Internet; também será disponibilizado ao Administrador a função de escolher ou criar novas categorias de bloqueio ou inclusões de horários específicos ou até de incluir novas extensões de músicas ou imagem. Este mecanismo, além de ser responsável pela produção e visualização de relatórios dos históricos, fornecerá informações detalhadas referentes a uma ou várias regras específicas. A ferramenta utiliza o banco do Access para fornecer ao Administrador uma visualização diferenciada. Além disso, a interface de visualização é favorável em uma melhor compreensão das regras criadas.

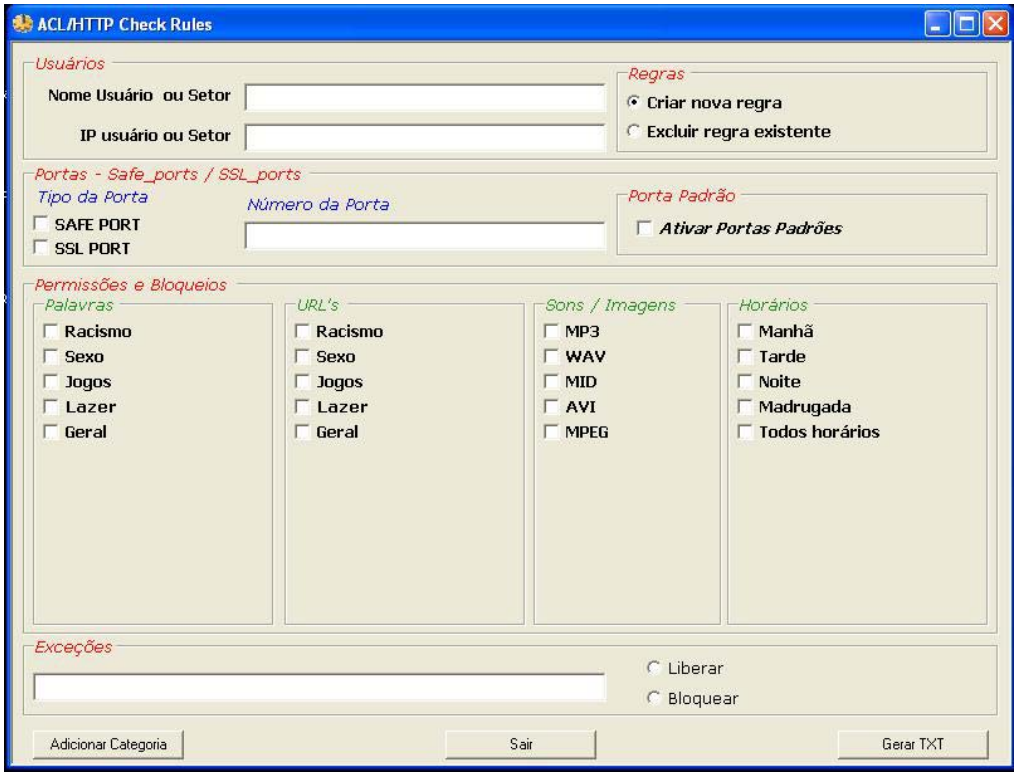


FIGURA 14 – INTERFACE DE VISUALIZAÇÃO DA FERRAMENTA

4.7. ASPECTOS DE VALIDAÇÃO (EXECUÇÃO E TESTES)

O propósito deste teste é a de verificar se a Ferramenta em questão possuía algum tipo de erro na programação ou se a interpretação dos profissionais estava de acordo com as características de funcionalidade que seriam utilizadas para a criação das novas regras. Foi elaborado e executado durante três semanas, com o auxílio de alguns profissionais.

Na primeira parte a Ferramenta foi testada em um pequeno Teste de Mesa, e foram verificados alguns erros de programação e também alguns erros de interpretação do código; após esta verificação foram feitas as devidas correções e posteriormente elaborados novos testes. Então foram verificados que os erros cometidos anteriormente tinham sido eliminados após atualização da ferramenta. Estes testes foram divididos em duas fases: na primeira fase foi elaborada um teste de criação das novas regras com os profissionais que possuíam uma menor experiência em programação e na segunda fase para os

profissionais que tinham um melhor conhecimento em criação, conforme demonstrados na Figura 15.

Após a criação das primeiras regras foi elaborado um levantamento de quais foram os erros cometidos, tanto pelos profissionais de melhor qualificação como pelo de menor conhecimento, após a criação foi elaborado um pequeno treinamento para os profissionais com menor conhecimento. O que foi notado é que após este treinamento os erros cometidos na criação foram reduzidos, com isso foi verificado conforme o andamento do experimento que a quantidade de erros foi menor quando utilizado a ferramenta, assim ficou demonstrado que as pessoas que tinham um maior conhecimento em programação, tiveram menos erros na hora da criação das novas regras e também um menor tempo de execução na criação das novas regras.

Treinamento Ferramenta Check Rule

	DIFICULDADE DE CRIAÇÃO DAS REGRAS		Situação1 Dúvidas Criação Antes Treinamento	Situação2 Dúvidas Criação Após Treinamento
	Nome do Analista	**Função**		
A	André Jose da Silva	Analista Programador	4	3
B	Cristian Rodrigo Dalcico	Analista de Sistemas SR	2	1
C	Denis Henrique de Melo	Analista de Sistemas JR	4	2
D	Eduardo Borriero	Analista Controle de Qualidade	3	2
E	Rafael Rubim da Silva Matos	Analista Controle de Qualidade	4	3
F	Ricardo Augusto Mean	Analista de Sistemas SR	1	1
G	Thiago Raphael Milan	Analista Programador	4	3

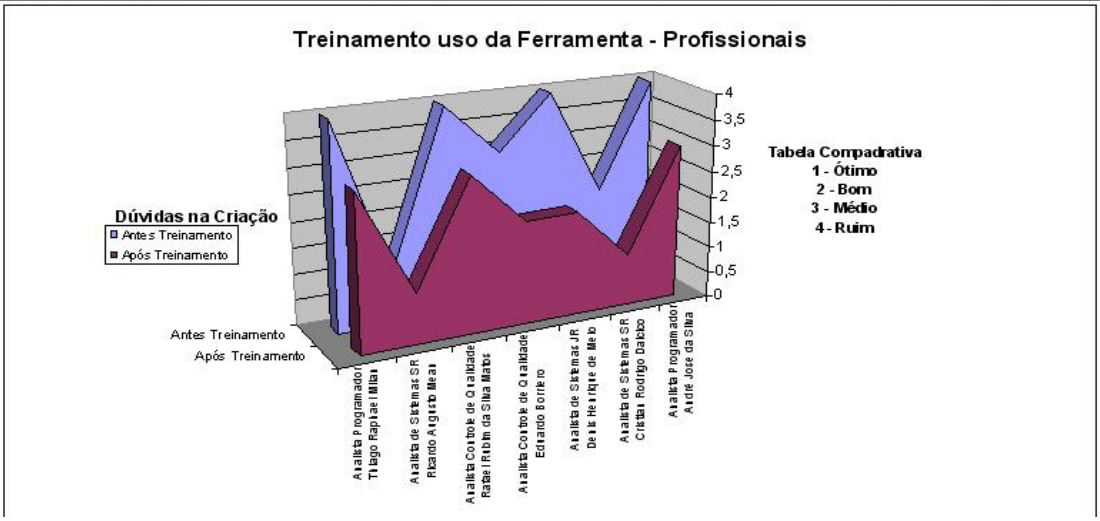


FIGURA 15 – LEVANTAMENTO DAS DIFICULDADES NA CRIAÇÃO DAS REGRAS

5. EXPERIMENTO DA FERRAMENTA CHECK RULE

O principal objetivo desse experimento foi verificar se a utilização da CheckRule facilita a elaboração das regras; observa-se que normalmente as regras eram criadas de forma manual via script diretamente no arquivo texto. Espera-se que ao se desenvolver um visualizador gráfico de políticas de segurança permite ao Administrador uma melhor compreensão da estrutura de segurança especificada pela da visualização do relacionamento entre os elementos da política de segurança ou a interação entre os usuários; outro aspecto é que o uso de representações visuais poderá contribuir para a identificação de possíveis erros de segurança das regras especificadas, que não seriam identificados pela análise direta pelo administrador de segurança ou pelo uso de verificadores de restrições baseado em regras.
Este experimento pretende colher informações que poderão ser posteriormente utilizadas para criação de novas formas de manipular regras de segurança, objetivando uma forma mais segura de diminuir os problemas encontrados de acesso indevido ou tentativas de invasão na rede.

5.1. MÓDULO DE CRIAÇÃO ARQUIVO TEXTO SQUID.CONF - MANUALMENTE

O módulo de criação de regras consiste em acrescentar novos comandos script no arquivo Squid.conf, para poder formatar informações básicas que são essenciais para a implantação das regras que serão inseridas no Squid.

Pode se verificar anteriormente quais são as opções disponíveis de restrições e também, se estas regras estão sendo acrescentadas de forma correta, pois o Squid lê e executa todas as suas informações de forma seqüencial.

Neste experimento os profissionais da área de Desenvolvimento de Software, sendo dois Analistas de Controle de Qualidade, dois Analistas Programadores e três Analistas de Sistemas. Esses profissionais foram submetidos à criação de novas regras de scripts diretamente no arquivo texto (squid.conf), isto tudo

de forma manual, então foram fornecidos a cada um deles uma planilha chamada **Tabela de Criação Usuários e Grupos**, contendo dados com características diferenciadas. O resultado deste experimento foi incorporado em uma outra planilha denominada **Tabela de Análise do Experimento** como será demonstrado a seguir.

5.2. MÓDULO CRIAÇÃO ARQUIVO TEXTO SQUID.CONF - FERRAMENTA CHECK RULE

5.2.1. FASES DO EXPERIMENTO

A arquitetura da ferramenta está dividida em dois módulos um deles é o Módulo de Criação das Regras Acls Https e o outro Módulo de Criação de Categorias. Com base nesta arquitetura o experimento foi subdividido em 3 fases:

- Planejamento
- Condução
- Análise dos resultados

5.2.2. PLANEJAMENTO

Nesta fase foi elaborada uma rotina de criação de regras, sendo criada uma planilha denominada Tabela de Criação de Usuários e Grupos, conforme Tabela 3, que compõem os dados do Analista que é a pessoa responsável pelo teste de criação das novas regras de usuários e também de grupos. Podendo verificar, qual é o tempo de inicio e o tempo final do experimento, sendo calculado a quantidade de tempo gasto, sendo utilizado dois tipos de criação, as de regras feitas manualmente diretamente no arquivo texto squid.conf e a outra feita com o auxílio da ferramenta Check Rule.

TABELA 3 - CRIAÇÃO USUÁRIOS E GRUPOS

Dados do Criador
Nome: André José da Silva
Setor: Desenvolvimento
Função: Analista Programador
Data: 05/09/2005 Segunda-feira

	Manualmente		Ferramenta Check Rule		
	Tempo Início: 13:15	Total	Tempo Início: 14:12	Total	Dif.
	Tempo Final: 13:47	32 minutos	Tempo Final: 14:22	10 minutos	22 minutos

	Usuários	Login	Setor	Nr. Equip.	Nr. IP	URL	Word	Horário	Som	Imagem	SSL_ports	Safe_ports
Incl.	Alfred Hitchcock	ahitchcock	Direito	micro308	172.16.0.13	users_url_no		T-N	não	sim	443 563	3128
1	Alexandre Graham Bel	abell	Telecomunicações	micro320	172.16.4.3		word_no	M-T-N	sim	sim	443 563	21 25 80 110
2	Issac Newton	inewton	Contabilidade	micro427	172.16.8.4		word_no	M-T	não	não	443 563	3128
3	Sigmund Freud	sfreud	Psicologia	micro749	192.168.0.5	url_no		M-T	não	não	443 563	80
4	Von Neumann	vneumann	Informática	micro236	192.168.2.9	url_no		M-T-N	sim	sim	443 563	21 25 80 110

Incl.	Grupos	Login	Setor	Nr. Equip.	Nr. IP	URL	Word	Horário	Som	Imagem	SSL_ports	Safe_ports
1	Laboratório1	lab1	Laboratório	micro400-425	10.16.0.1-25	setor_url_no		M-T-N	não	não	443 563	25 80 100
2	Biblioteca1	bibli1	Biblioteca	micro500-512	10.19.0.1 e 12	setor_url_no		M-T-N	não	não	443 563	25 80 100
7												

Apoio Tabela Auxiliar		
URL		dstdomain
Word		url_regex -i
Som		urlpath_regex -ex \.mp3$ \.wav$
Imagem		urlpath_regex -ex \.mov$ \.avi$ \.mpg$ \.mpeg$ \.wmv$
Horário		horario_no time 07:00-23:00
		manha_no time 07:01-12:00
		tarde_no time 12:01-18:00
		noite_no time 18:01-24:00
		madru_no time 00:01-07:00

Os usuários e grupos que foram criados estão divididos da seguinte forma:

Nome do Usuário: fornece o nome do usuário que será adicionado na nova regra. Ex: Alexandre Graham Bell

Nome do Grupo: fornece o nome do grupo que será adicionado na nova regra. Ex: Laboratorio1

Login: fornece qual será o login de acesso do usuário, sendo que a regra de criação do login é composto da primeira letra do nome + a última palavra do sobrenome, quando ocorre do nome do usuário ter mais de um sobrenome é utilizado o último, salvo quando ocorrer duplicidade de login e quando isso ocorre é utilizado o sobrenome anterior. Ex: abell

Setor: fornece qual o setor que o usuário pertence. Ex.: Telecomunicações

Nr. do Equipamento: fornece qual é o número da máquina que será utilizada pelo usuário. Ex: micro320

Nr. de IP: fornece qual é o número de IP que a máquina possui. Ex: 172.16.4.3

Word: fornece qual é o arquivo que o usuário irá utilizar como bloqueio, este arquivo é armazenado no diretório linux “/etc/squid/”, palavras que não podem ser acessadas na Internet. Ex: sexo, jogos, guerra

URL: fornece qual é o arquivo que o usuário irá utilizar como bloqueio, pode ocorrer do campo estar em branco o que significa que o usuário não possui restrições de URLS, mas quando ocorre o bloqueio é feito via URL, o arquivo é armazenado no diretório do linux “/etc/squid/”, URL proibidas.. Ex: www.sexo.com.br; www.racismo.com.br

Horário: fornece qual é o horário que o usuário ou o grupo poderá acessar a Internet, sendo que se não for informado nenhum horário, por padrão é liberado o acesso a todos os horários. Ex: manha_no time 07:01-12:00 (horário liberado das 07:01 até as 12:00)

Som: fornece qual é a extensão de som que pode ou não ser acessado, caso não seja acrescentado nenhum, por padrão ficam liberadas todas as extensões de sons. Ex: urlpath_regex \.mp3$

Imagem: fornece qual é a extensão de imagem que pode ou não ser acessada, caso não seja acrescentada nenhuma por padrão ficam liberadas todas as extensões de imagens. Ex: urlpath_regex \.mov$

SSL_ports: fornece quais serão as portas SSL que serão liberadas, por padrão são fornecidas as portas de número 443 e 563.

Safe_ports: fornece quais serão as portas Safe que serão liberadas. Ex: portas 21 FTP, 22 SSH, 25 SMTP, 80 HTTP, 110 POP3, HTTP 3128

Como apoio à criação destas novas regras foi disponibilizado uma Tabela Auxiliar contendo algumas informações importantes na criação, exemplos de opções URL, Word, Som, Imagem, Horário. Uma outra observação que informa quando o Analista pode criar regras de users ele terá que trocar o campo users pelo nome específico do usuário e para também o campo setor pelo nome especifico do grupo que será utilizado.

5.2.3. CONDUÇÃO DO EXPERIMENTO

Nesta fase do experimento foram demonstrados em detalhes os erros e acertos cometidos pelos Analistas na criação das regras. O experimento foi conduzido em duas partes, a primeira parte corresponde as regras feitas manualmente diretamente no arquivo texto squid.conf e a segunda parte utilizando o auxílio da Ferramenta Check Rule na criação das novas regras, verificando se com este segundo processo ocorre ou não a diminuição dos erros ocorridos na criação das regras anteriormente. Cada Analista recebeu uma planilha individual que fornecia os dados que foram importantes para a criação das novas regras (Planejamento), com a planilha em mãos o Analista foi elaborando as regras que foram fornecidas e o Administrador fez a Análise das regras que foram elaboradas visualizando quais os erros cometidos na criação; abaixo a relação está dividida por Analista, *Erros ocorridos (manualmente)* e *Erros ocorridos (Ferramenta Check Rule)* e também uma análise do Total de erros e a porcentagem de erros ocorridos.

A - USUÁRIO A

Erros ocorridos (manualmente)

- ACLS, Usuários, Setores
  1 – O Analista errou ao inserir o range de IPs 10.16.0.1-25 do usuário lab1, não inserindo o caractere específico “-” entre os IPs.
- ACLS Palavras, URLs
  2 – O Analista teve dificuldade em localizar onde iria inserir o arquivo etc do usuário ahitchcock, das respectivas urls (“etc/squid/ahitchcock_url_no”)
- Configuração ACLS, HTTP – Portas Padrão
  3 – O Analista demorou um tempo para distinguir a diferença entre SSL_ports e Safe_ports na criação das portas
- ACLs Sons, Imagem
  4 – O Analista se confundiu ao inserir a regra url_regex e urlpath, o correto seria url-regex para poder incluir o usuário sfreud com opção de url_no

Total de erros: 4 / Porcentagem de erro=57%

Erros ocorridos (Ferramenta Check Rule)

- ACLS Usuário, Setores
  1 - A ferramenta inclui os caracteres especiais automaticamente quando o Analista escolhe a opção de range
- ACLS Palavras, URLs
  2 – A ferramenta insere automaticamente o caminho do arquivo que será acrescentado
- 3 – A ferramenta está preparada para inserir a opção de portas, pois possui regras fixas na criação de uma nova
- 4 – A ferramenta inclui a regra correta por não possuir opção dupla

B - USUÁRIO B

Erros ocorridos (manualmente)

- ACLS, Palavras, URLs
  1 – O Analista trocou a opção da regra do usuário inewton que seria url_regex pela dstdomain sendo que url_regex é para bloqueio por palavras específicas como exemplo “sexo” e dstdomain para bloqueio de site como exemplo “//www.anchieta.br”
- HTTP_Access Usuários, Setores, Horários
  2 – O Analista trocou a regra allow por deny do usuário abell, ocasionando a liberação das palavras cadastradas no arquivo Word_no
  ex: http_access deny usuario! word_no

Total de erros: 2 / Porcentagem de erro=29%

Erros ocorridos (Ferramenta Check Rule)

- ACLS, Palavras, URLs
  1 – A ferramenta possui opção para bloqueio por palavras ou URLs, o Analista não necessariamente precisa saber qual é o script que será implantado
- HTTP_Access Usuários, Setores, Horários
  2 – As regras são atualizadas automaticamente não sendo necessária a consulta de acesso negado ou liberado

C - USUÁRIO C

Erros ocorridos (manualmente)

- ACLS Usuários, Setores
  1 – O Analista errou na criação da regra do usuário lab1, na opção de IP range com IP randômico, sendo que não utilizou o traço e sim o espaço ex.: 10.16.0.1-10.16.0.25
- Configuração ACLS, HTTP_portas padrão
  2 – O Analista trocou a acl SSL_ports por Safe_ports, ocasionando o bloqueio da porta 80 do usuário vnewmann
- ACLS Palavras, URLs

3 – O Analista não colocou a opção “-i” na url_regex do usuário sfreud, ocasionalmente erros nas palavras que possuem letras maiúsculas

Total de erros: 3 / Porcentagem de erro=71%

Erros ocorridos (Ferramenta Check Rule)

- ACLS Usuários, Setores
  1 – Na seleção de IP a ferramenta fornece a opção de IP randômico ou IP range e quando se escolhe a opçãp o script é gerado automaticamente
- Configuração ACLS, HTTP_portas padrão
  2 – Na ferramenta o Analista escolhe qual o tipo de porta e assim é liberada ou bloqueada automaticamente
- ACLS, Palavras, URLs
  3 – A ferramenta inclui a opção-i diretamente nas novas regras url_regex

D – USUÁRIO D

Erros ocorridos (manualmente)

- ACLS Palavras, URLs
  1 – O Analista trocou o comando url_regex pelo dstdomain do usuário abell, ocasionando um erro de interpretação das regras de acesso as palavras bloqueadas
- ACLS Sons, Imagens
  2 – O Analista trocou o comando urlpath_regex pelo url_regex do usuário sfreud, ocasionando a liberação de imagens que o usuário não poderia ter acesso

Total de erros: 2 / Porcentagem de erro=29%

Erros ocorridos (Ferramenta Check Rule)

- ACLS Palavras, URLs
  1 – A ferramenta inclui automaticamente o comando correto dstdomain para bloqueio de URLs.
- ACLS Sons, Imagens
  2 – Quando o Analista escolhe o bloqueio da música “MP3” a ferramenta cria as regras com a opção de comando correta urlpath_regex

E - USUÁRIO E

Erros ocorridos (manualmente)

- ACLS, Usuários, Setores
  1 – O Analista errou a inserção dos IPs randômicos, pois ele inseriu o caracter “-“ entre os IPs do usuário bibli1, ocasionando o range de IP

10.19.0.1 até 10.19.0.12 sendo que o correto seria IP 10.19.0.1 e o IP 10.19.0.12

- ACLS, Palavras, URLs
  2 – O Analista trocou a opção da regra url_regex pela dstdomain do usuário inewton, sendo que url_regex é para bloqueio de palavras específicas e dstdomain para URLs

Total de erros: 2 / Porcentagem de erro=29%

Erros ocorridos (Ferramenta Check Rule)

- ACLS, Usuários, Setores
  1 – A ferramenta inclui os caracteres especiais automaticamente, quando o Analista escolhe a opção de range
- ACLS, Palavras, URLs
  2 – A ferramenta possui opção para bloqueio por palavras ou URLs, o Analista não necessariamente precisa saber qual é o script que será implantado

F - USUÁRIO F

Erros ocorridos (manualmente)

- Configuração ACLS, HTTP_portas padrão
  1 – O Analista trocou o comando SSL_ports pelo Safe_ports na inclusão de bloqueio na porta 3128 do usuário inewton, ocasionando o bloqueio desta porta para acesso a Internet

Total de erros: 1 / Porcentagem de erro=14%

Erros ocorridos (Ferramenta Check Rule)

- Configuração ACLS, HTTP_portas padrão
  1 – A ferramenta esta preparada para inserir a opção de portas, pois possui auxílio na criação da nova regra escolhida

G - USUÁRIO G

Erros ocorridos (manualmente)

- ACLS Usuários, Setores
  1 – O Analista errou ao inserir IPs randômicos, não inserindo o caracter específico “-” entre os IPs do usuário lab1, sendo assim as regras de IPs ficaram como range 10.16.0.1 até 10.16.0.25 e não IP 10.16.0.1 e IP 10.16.0.25
- ACLS Palavras, URLs
  2 – O Analista inseriu errado o nome do arquivo onde continha as URLs bloqueadas, causando o bloqueio em sites que seriam para ter a sua opção liberada

- ACLS Sons, Imagens
  3 – O Analista errou a opção da regra de bloqueio de imagem do comando url_pathregex, colocando incorretamente o comando urlpath_regex do usuário inewton, ocasionando a liberação das imagens ao invés dos bloqueios

Total de erros: 3 / Porcentagem de erro=43%

Erros ocorridos (Ferramenta Check Rule)

- ACLS Usuários, Setores
  1 – A ferramenta inclui os caracteres especiais automaticamente, quando o Analista escolhe a opção de range
- ACLS Palavras, URLs
  2 – Quando se insere uma URL ou palavra na ferramenta é incluído corretamente o caminho onde o arquivo deve ser armazenado
- ACLS Sons, Imagens
  3 – A ferramenta fornece uma única opção de escolha para fazer o bloqueio exclusivo de sons ou imagens específicas

5.2.4. ANÁLISE DOS RESULTADOS

Nesta fase foram analisados os resultados ocorridos ao final da fase da *Condução do Experimento*, conforme demonstrado na Tabela 4, sendo divididos em duas partes: a primeira são as dificuldades na criação das novas regras e a segunda a eficácia em sua criação, levando em conta que cada parte é subdividida em duas opções, sendo que a primeira opção são as regras elaboradas manualmente chamado neste caso de *Situação1* e a segunda são as regras elaboradas com o auxílio da Ferramenta Check Rule chamado neste caso de *Situação2*

TABELA 4 – ANÁLISE DO EXPERIMENTO – FINAL

ANÁLISE DO EXPERIMENTO - FINAL

			Manualmente Situação1 Total de Inclusões = 7		Ferramenta Check Rule Situação2 Total de Inclusões = 7	
	DIFICULDADE DE CRIAÇÃO DAS REGRAS		**Tempo Gasto**		**Tempo Gasto**	**Diferença Horas**
	Nome do Analista	**Função**				
A	André Jose da Silva	Analista Programador	00:32		00:10	**00:22**
B	Cristian Rodrigo Dalcico	Analista de Sistemas SR	00:12		00:05	**00:07**
C	Denis Henrique de Melo	Analista de Sistemas JR	00:26		00:08	**00:18**
D	Eduardo Borriero	Analista Controle de Qualidade	00:20		00:07	**00:13**
E	Rafael Rubim da Silva Matos	Analista Controle de Qualidade	00:25		00:09	**00:16**
F	Ricardo Augusto Mean	Analista de Sistemas SR	00:08		00:05	**00:03**
G	Thiago Raphael Milan	Analista Programador	00:23		00:10	**00:13**
		Total de Horas	**02:26**		**00:54**	**01:32**

			Manualmente Situação1 Total de Inclusões = 7		Ferramenta Check Rule Situação2 Total de Inclusões = 7	
	EFICÁCIA		**Erros Ocorridos**	**Err. %**	**Erros Ocorridos**	**Dif. %**
	Nome do Analista	**Função**				
A	André Jose da Silva	Analista Programador	4	57%	0	0%
B	Cristian Rodrigo Dalcico	Analista de Sistemas SR	2	29%	0	0%
C	Denis Henrique de Melo	Analista de Sistemas JR	5	71%	0	0%
D	Eduardo Borriero	Analista Controle de Qualidade	2	29%	0	0%
E	Rafael Rubim da Silva Matos	Analista Controle de Qualidade	2	29%	0	0%
F	Ricardo Augusto Mean	Analista de Sistemas SR	1	14%	0	0%
G	Thiago Raphael Milan	Analista Programador	3	43%	0	0%
		Total de Erros	**19**		**0**	**0%**

Na Figura 16 foi demonstrado que o tempo gasto usado para a criação das novas regras de forma manual foram superiores ao criados com o auxílio da Ferramenta Check Rule, verificando-se que a diferença de horas tem intervalo de três minutos até vinte e dois minutos. Foi detectado com isso que quanto maior a experiência do criador menor o tempo gasto para a finalização das novas regras, o tempo gasto dos scripts feitos manualmente tiveram uma variação de oito até trinta e dois minutos e o tempo gasto com o auxílio da Ferramenta teve variação de cinco até dez minutos um tempo bem inferior ao feito manual. A automatização das regras serão elaboradas mais facilmente tendo um ganho substancial em relação ao tempo gasto para a criação destas novas regras.

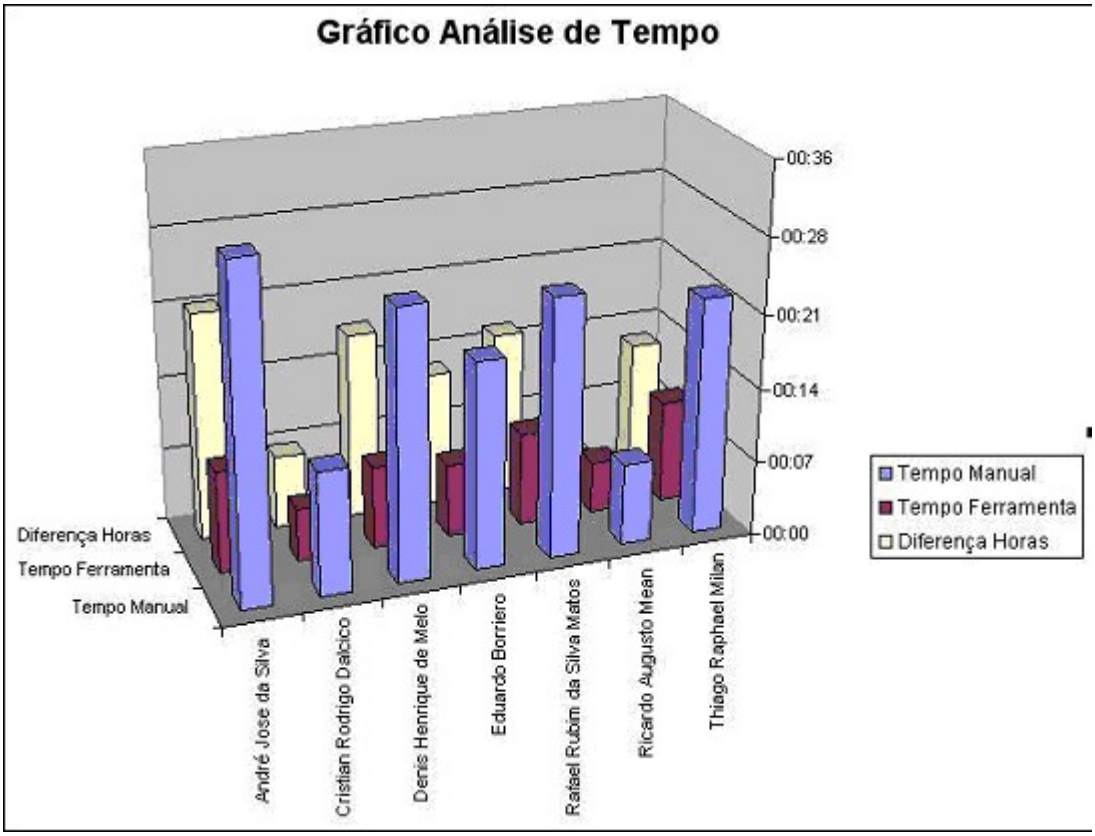


FIGURA 16 – GRÁFICO DE ANÁLISE DE TEMPO

A Figura 17 ilustra que a Ferramenta contribuiu para a diminuição dos erros que eram ocorridos durante a programação dos scripts de forma manual, este teste apresentou em sua visualização uma melhor Eficácia durante a programação executada com o auxílio da Ferramenta Check Rule, demonstrando que o intervalo de erros variou de um até cinco, e utilizando uma porcentagem de erros variando de 14% até 71%, lembrando que os criadores que tinham uma maior experiência em programação, foram os que menos ocasionaram erros nos scripts.

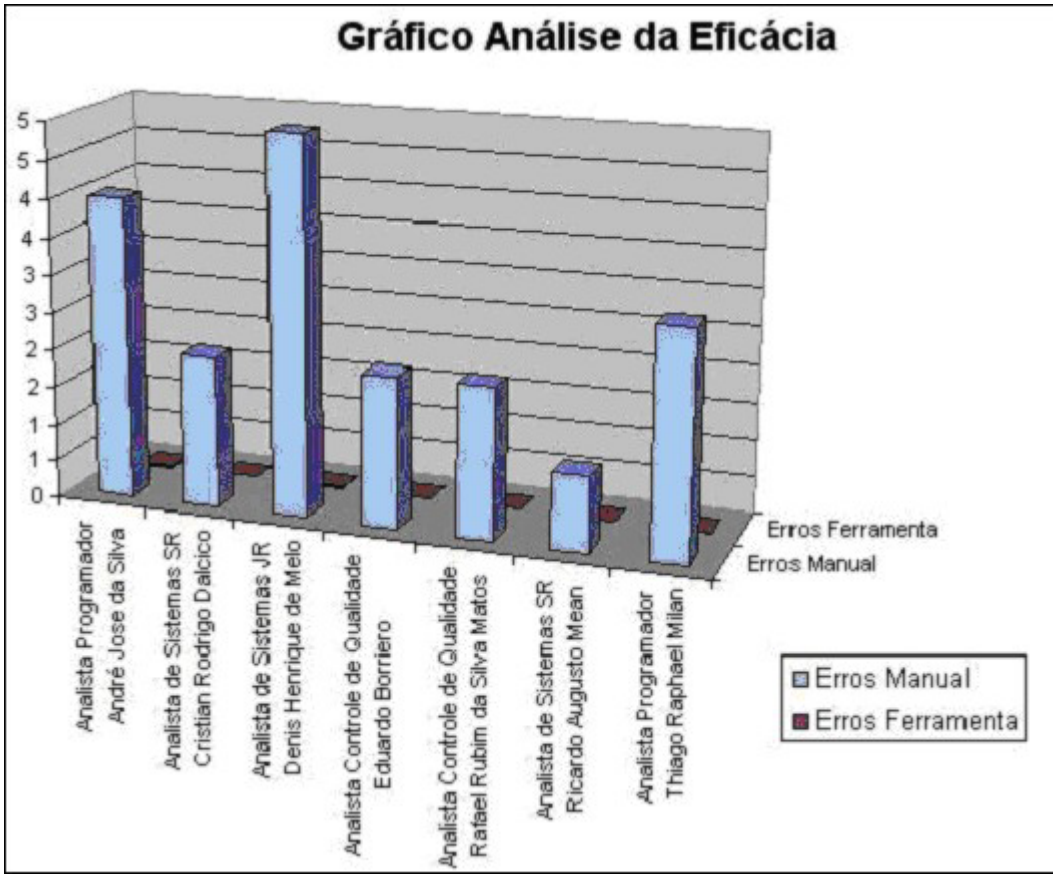


FIGURA 17 – GRÁFICO DE ANÁLISE DE EFICÁCIA

Parte1 - Dificuldades na criação das regras

Situação1

Nome do Analista: onde são fornecidos os nomes dos Analistas que serão as pessoas responsáveis pela criação das novas regras, neste experimento foi elaborado em um total de sete Analistas colaboradores, sendo fornecido a identificação da letra A até a letra G

Função: onde é fornecido qual é a função que o Analista exerce dentro da instituição

Total de Inclusões: onde é fornecido qual é o total de regras que serão criadas, neste experimento foi num total de sete novas regras, sendo fornecido a identificação do número um até o número sete

Tempo Gasto: onde é demonstrado qual é o tempo gasto pelos Analistas na finalização das novas regras, tendo como base um horário inicial e um horário

final, e a diferença entre esses horários foram anotados individualmente, neste caso o Analista Usuário A teve um tempo de trinta e dois minutos muito mais elevado do que o Analista Usuário B que obteve o tempo de apenas doze minutos, os horários variaram de acordo com a capacidade de cada Analista, os horários foram anotados oito minutos até trinta e dois minutos, tendo um valor de diferença muito grande, demonstrando uma enorme diferença de capacidade entre os Analistas

Situação2

Nome do Analista: onde são fornecidos os nomes dos Analistas que serão as pessoas responsáveis na criação das novas regras, neste experimento foi elaborado em um total de sete Analistas colaboradores, sendo fornecido a identificação da letra A até a letra G

Função: onde é fornecido qual é a função que o Analista exerce dentro da instituição

Total de Inclusões: onde é fornecido qual é o total de regras que serão criadas, neste experimento foi num total de sete novas regras, sendo fornecido a identificação do número um até o número sete

Tempo Gasto: onde é demonstrado qual é o tempo gasto pelos Analistas na finalização das novas regras, tendo como base um horário inicial e um horário final, e a diferença entre eles foram anotados os horários individualmente, os horários variaram de acordo com a capacidade de cada Analista, os horários variaram de cinco minutos até dez minutos, tendo um valor de diferença não muito elevado tem como base a fase anterior que a diferença chegava até vinte e quatro minutos, mas podemos supor também que tendo como base os valores exclusivos utilizando a ferramenta ocorreu uma variação de até 100% de diferença demonstrando que cada Analista tem um tipo de conhecimento, mas com o auxílio da ferramenta os erros foram nulos, demonstrando o Analista não precisava ter um conhecimento profundo nos comandos do squid apenas selecionar a opções corretas desejadas

Total de Horas: o total de tempo gasto feita de forma manual foi de 2 horas e 26 minutos entre todos os Analistas envolvidos, verificando uma média de 2:26 / 7 = 32 minutos, já o total de tempo gasto feito com o auxílio da ferramenta foi de 54 minutos entre todos os Analistas envolvidos, verificando uma média de 00:54 / 7 = 7 minutos e 71 segundos, e quanto à diferença entre eles foi de uma diminuição de 1 hora e 32 minutos ocasionando um ganho no tempo na criação das novas regras

Parte2 - Eficácia na criação das regras

Situação1

Nome do Analista: onde são fornecidos os nomes dos Analistas que serão as pessoas responsáveis pela criação das novas regras, neste experimento foi elaborado um total de sete Analistas colaboradores, sendo fornecido a eles uma identificação da letra A até a letra G

Função: onde é fornecido qual é a função que o Analista exerce dentro da instituição

Total de Inclusões: onde é fornecido qual é o total de regras que serão criadas, neste experimento foi num total de sete novas regras, sendo fornecido a identificação do número um até o número sete

Erros Ocorridos: onde é demonstrada a quantidade de erros ocorridos durante a criação das novas regras, neste caso os erros variaram de 1 até 5, demonstrando assim que os Analistas que mais tinham conhecimento das regras Squid foram o que menos erraram e conseqüentemente os Analistas que não tinham muito conhecimento nos comandos de script foram o que mais erraram, neste caso o Analista Usuário C cometeu 5 erros, e o Analista Usuário F, que possui um maior domínio errou somente 1 regra

Situação2

Nome do Analista: onde são fornecidos os nomes dos Analistas que serão as pessoas responsáveis pela criação das novas regras, neste experimento foi elaborado um total de sete Analistas colaboradores, sendo fornecido a eles uma identificação da letra A até a letra G

Função: onde é fornecido qual é a função que o Analista exerce dentro da instituição

Total de Inclusões: onde é fornecido qual é o total de regras que serão criadas, neste experimento foi num total de sete novas regras, sendo fornecido a identificação do número um até o número sete

Erros Ocorridos: onde é demonstrada a quantidade de erros ocorridos durante a criação das novas regras mas desta vez com o auxílio da Ferramenta Check Rule, neste experimento foi verificado que os erros foram nulos, demonstrando que o Analista não precisa necessariamente de ser conhecedor dos comandos scripts para a criação destas.regras mas sim de fazer a escolha correta na hora de selecionar as opções que a Ferramenta oferece.

Diferença em Porcentagens %: foram disponibilizados quais foram às porcentagens entre os erros ocorridos de forma manualmente e os erros ocorridos utilizando a ferramenta, sendo que manualmente os erros variaram de 14% até 71%, mostrando uma grande diferença entre a criação das regras, e as regras utilizadas com a ferramenta a porcentagem de erros foi nula, demonstrando que independente do conhecimento dos comandos de script do linux, todos os Analistas tiveram % zero, já que com o auxílio da ferramenta o Analista não necessariamente precisa ser conhecer dos comandos e sim escolher corretamente quais as opções fornecidas pela ferramenta será selecionado, sendo que com a opção escolhida a ferramenta disponibiliza automaticamente um arquivo texto com as novas regras selecionadas

Total de Erros: no total foram encontrados 19 erros somados entre todos os Analistas envolvidos, verificando uma média de 19 / 7 = **2,714**

5.3. MÓDULO DE CRIAÇÃO UTILIZADO – FERRAMENTA CHECK RULE

5.3.1. MÓDULO DE CRIAÇÃO DAS REGRAS ACLS HTTPS – USUÁRIOS E SETORES

Com o auxílio da Ferramenta Check Rule, conforme *Figura 18* as novas regras são elaboradas em interfase gráfica, visando auxiliar e direcionar o Administrador na criação das novas regras tendo com base duas metas: a primeira é de se gastar um menor tempo possível em sua criação e a segunda de se ter um menor número de ocorrências de erros cabíveis, tendo como parâmetro as regras criadas manualmente diretamente no arquivo texto, conforme demonstrado anteriormente na Tabela 4 – Análise do Experimento – Final.

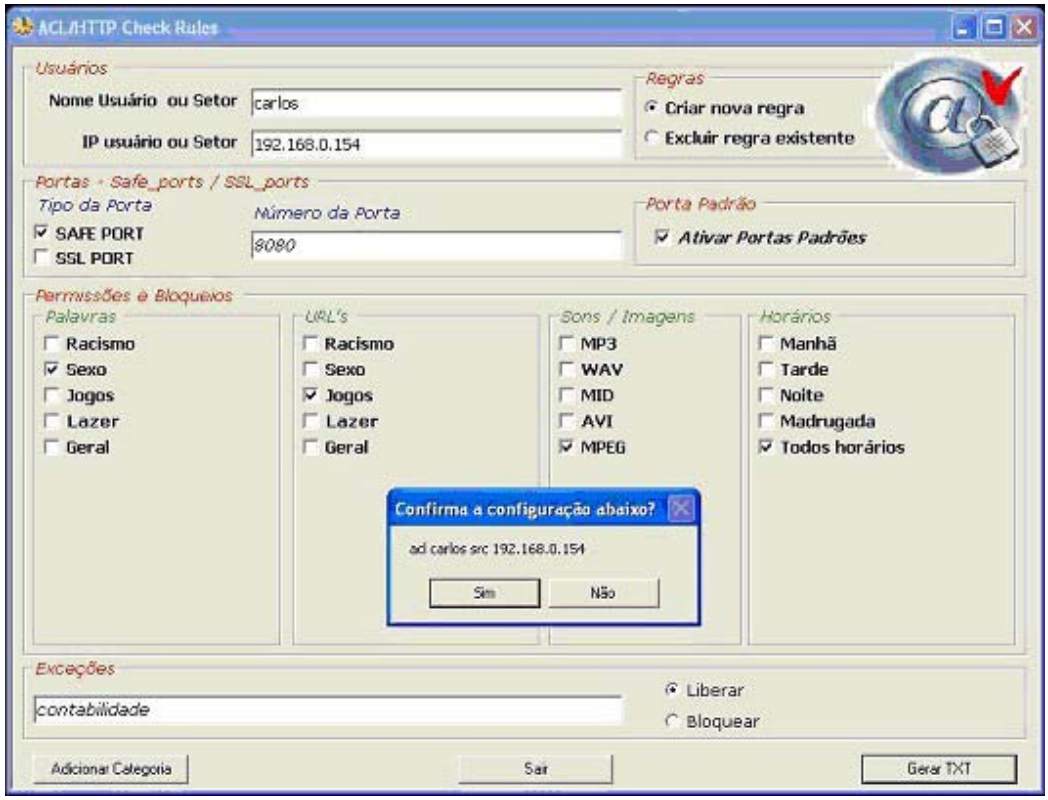


Figura 18 - Módulo Criação de Acls e Https (Usuários e Setores)

5.3.2. MÓDULO DE CRIAÇÃO DAS NOVAS CATEGORIAS

Neste módulo a Ferramenta proporciona algumas opções que podem ser demonstrada na Figura 19, a primeira é de criar novas categorias de bloqueio

ou liberação, a segunda de acrescentar ou excluir novas palavras que são incluídas no arquivo word_no ou acrescentar ou excluir novas Urls no arquivo URL_no, a terceira de incluir novos horários ou utilizar os já cadastrados, a quarta opção de criar novos arquivos de Sons ou Imagens ou utilizar os já adicionados anteriormente.

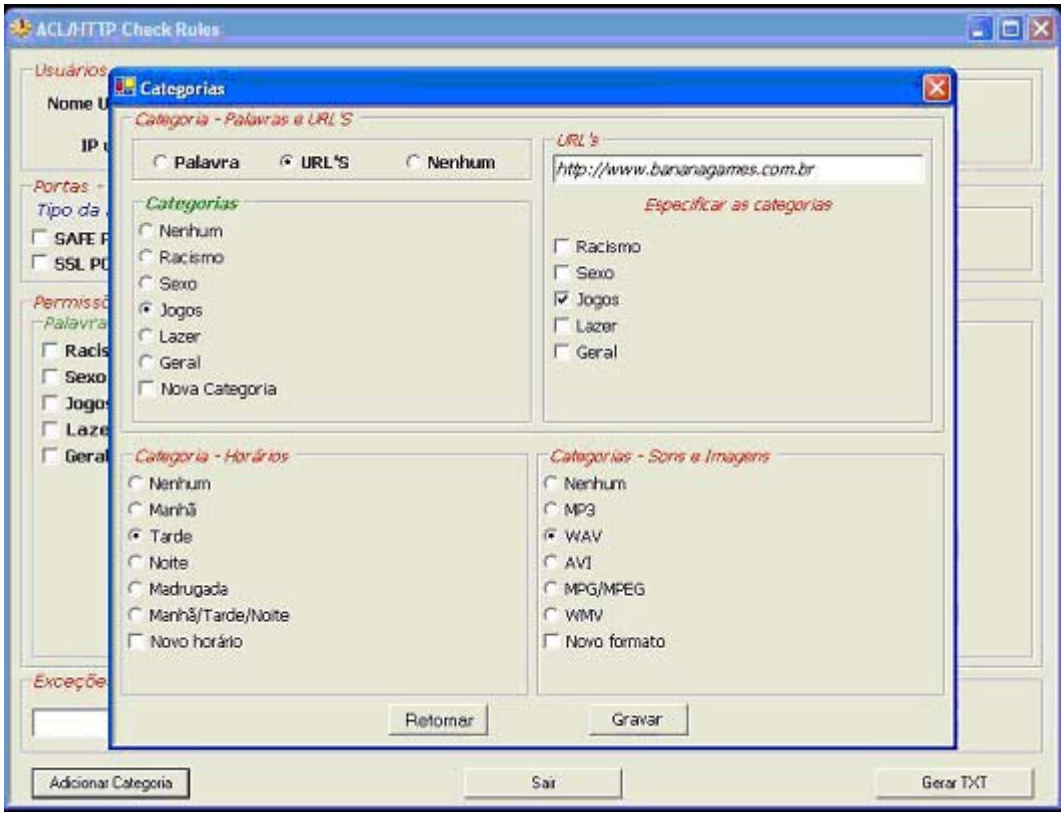


FIGURA 19 - MÓDULO CRIAÇÃO DE CATEGORIAS - URLS, HORÁRIOS, SONS, IMAGENS

5.4. CARACTERÍSTICAS DA FERRAMENTA AO USO DA REDE

O objetivo aqui foi demonstrar através de testes, que a ferramenta Check Rule realizou suas funções com eficiência, ao diminuir os erros de interpretação e de padronização que eram encontrados anteriormente. Como local de testes foi utilizada a rede acadêmica da Universidade Anchieta de Jundiaí – São Paulo – EMPRESA A, cuja infra-estrutura possui aproximadamente 800 computadores ligados em rede e com acesso a internet via rádio em dois pontos cada um com 2Mbps somando o total de 4Mbps full. Sendo quatro firewalls que se encontra em pontos distintos um no Campus Pirapora e outro no Campus Anhanguera. A ferramenta CHECK RULE foi inserida no período aproximado de três semanas totalizando dez dias de utilização e através desta ferramenta ficou identificada à queda na média de tempo na criação das regras em aproximadamente 25% a menos.

O processo de inclusão de regras na ferramenta pode ser solicitado mediante relatório do que foi incluído no arquivo de script. Por exemplo, haverá a possibilidade de ver informações das ocorrências de um determinado atributo incluso em um usuário, isso fornece um melhor gerenciamento das regras que foram inseridas, e com isso pode-se verificar os abusos nas liberações de acesso a Internet ou também informações mais detalhadas das restrições que foram atribuídas ao um usuário específico.

5.4.1. INFLUÊNCIA DAS REGRAS NO CONSUMO DE BANDA INTERNET

Através das linhas de regras criadas pela ferramenta é demonstrada na Figura 20 uma diminuição no tráfego de acesso a Internet das 12:00 as 18:00hs. Note que os maiores acessos são gerados de segunda a sexta das 19:00 até as 22:20 com um tamanho aproximado de 900 a 980Kbps, isso porque são nestes horários que as regras do squid são liberados para acesso aos laboratório de aulas e também aos laboratórios de pesquisa.

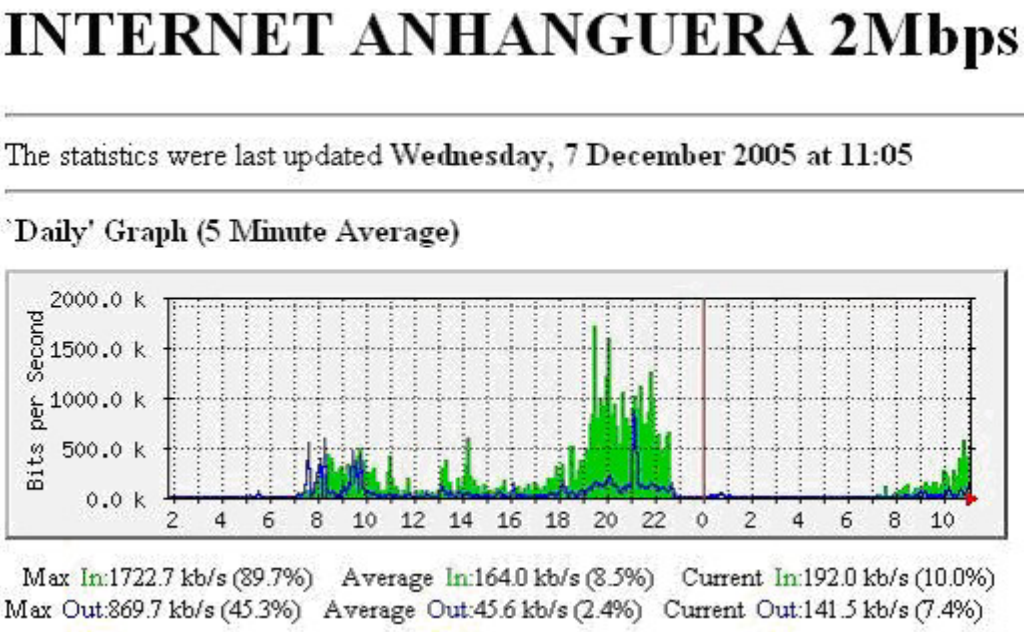


FIGURA 20 – MRTG / RELATÓRIO DE UTILIZAÇÃO DA INTERNET

Sabendo-se que com regras ativadas o fluxo de dados é reduzido e com isso há uma melhora no acesso aos dados da Internet. Neste horário toda e qualquer página que foi criada anteriormente e alertada em forma de mensagem na tela do usuário que tem no seu conhecimento que o site que foi tentado abrir possui regra de bloqueio *Acesso Negado,* mostrado na Figura 21.

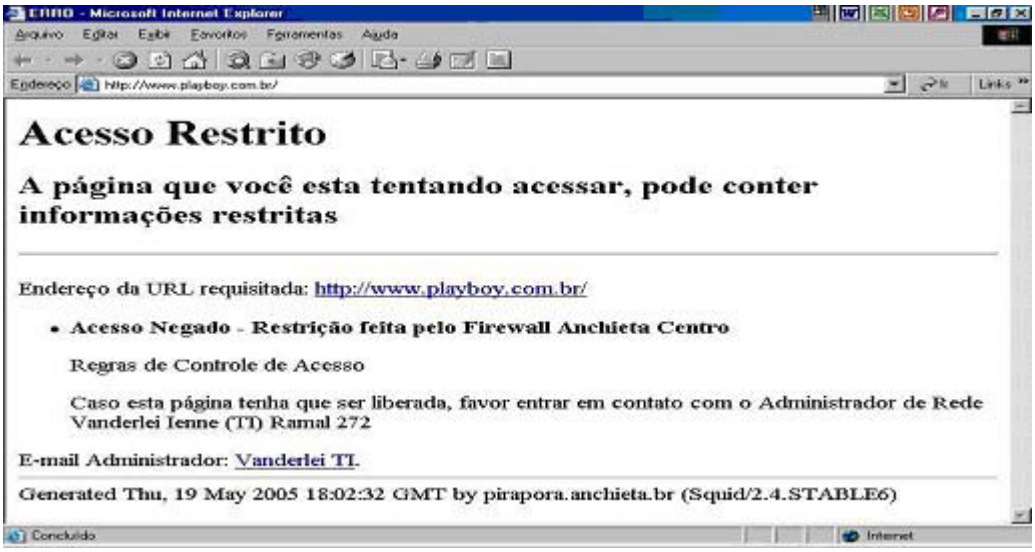


FIGURA 21 – SQUID / BLOQUEIO DE ACESSO URL

Quando se cria regra de bloqueio, os acessos indevidos são bloqueados e informados ao Administrador que pode verificar quais são as *Url* que estão sofrendo maior bloqueio no acesso conforme Figura 22, podendo também ser

disponibilizado quais são os horários Figura 23 que estas Url estão sendo acessadas, podendo assim verificar se estes acessos estão no horário de almoço do funcionário ou fora de seu horário normal de trabalho; com estas informações o Administrador pode alterar as regras ou enviar os relatórios conforme Figura 24 para os responsáveis de cada departamento para que ele possa tomar medidas cabíveis ao usuário infrator. Foi verificado que quando se envia este tipo de relatório ao responsável do departamento o acesso diminui consideravelmente, no caso do Empresa A este relatório é enviado toda quarta-feira e posteriormente nas reuniões que são feitas nas quintas os usuários são advertidos verbalmente e se isso continuar a ocorrer é formulada uma advertência por escrito que tem assinatura do usuário com dia e hora de sua infração, e contanto três advertências por escrito o funcionário é dispensado.

SARG Squid Analysis Report Generator

Squid User Access Report

Periodo: 2005Nov21-2005Nov23
Usuario: 172.16.32.52
Ordem: BYTES, reverse
Usuario Relatorio

LOCAL ACESSADO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO	
jundiai.bifgv.com.br	52	173.46K	18.10%	2.33%	97.67%	00:00:33	33.88K	14.56%	
www.bifgv.com.br	21	160.97K	16.79%	0.00%	100.00%	00:00:08	8.67K	3.73%	
ultimosegundo.ig.com.br	10	157.56K	16.44%	0.00%	100.00%	00:00:08	8.42K	3.62%	
image.ig.com.br	58	123.53K	12.89%	16.68%	83.32%	00:00:10	10.38K	4.46%	
adserver.ig.com.br	12	94.44K	9.85%	15.28%	84.72%	00:00:06	6.64K	2.86%	
message.real.com	5	89.31K	9.32%	0.00%	100.00%	00:00:27	27.26K	11.72%	
www.bimd.com.br	6	56.39K	5.88%	0.00%	100.00%	00:00:34	34.71K	14.92%	
www.adserver.com.br	2	31.99K	3.34%	46.83%	53.17%	00:00:06	6.80K	2.93%	
cache.unicast.com	1	17.87K	1.86%	100.00%	0.00%	00:00:00	15	0.01%	
ads1.mediaops.com.br	1	10.85K	1.13%	0.00%	100.00%	00:00:00	74	0.03%	
www.anchieta.br	18	10.36K	1.08%	32.35%	67.65%	00:00:00	583	0.25%	
ad.adnetwork.com.br	3	7.80K	0.81%	0.00%	100.00%	00:00:04	4.68K	2.01%	
www.ig.com.br	23	5.99K	0.63%	55.39%	44.61%	00:00:12	12.65K	5.44%	
www.google.com.br	1	4.05K	0.42%	0.00%	100.00%	00:00:01	1.00K	0.43%	
igshopping.ig.com.br	3	3.47K	0.36%	100.00%	0.00%	00:00:00	44	0.02%	NEGADO
images.ig.com.br	6	3.02K	0.32%	100.00%	0.00%	00:00:00	184	0.08%	
www.americanas.com.br	1	1.48K	0.15%	0.00%	100.00%	00:00:12	12.01K	5.16%	
promos.hotbar.com	4	1.39K	0.15%	0.00%	100.00%	00:00:02	2.09K	0.90%	
loginnet.passport.com	1	1.10K	0.12%	100.00%	0.00%	00:00:00	60	0.03%	NEGADO
www.hotmail.com	1	803	0.08%	0.00%	100.00%	00:00:11	11.73K	5.04%	
www.americanas.com	1	653	0.07%	0.00%	100.00%	00:00:12	12.43K	5.34%	

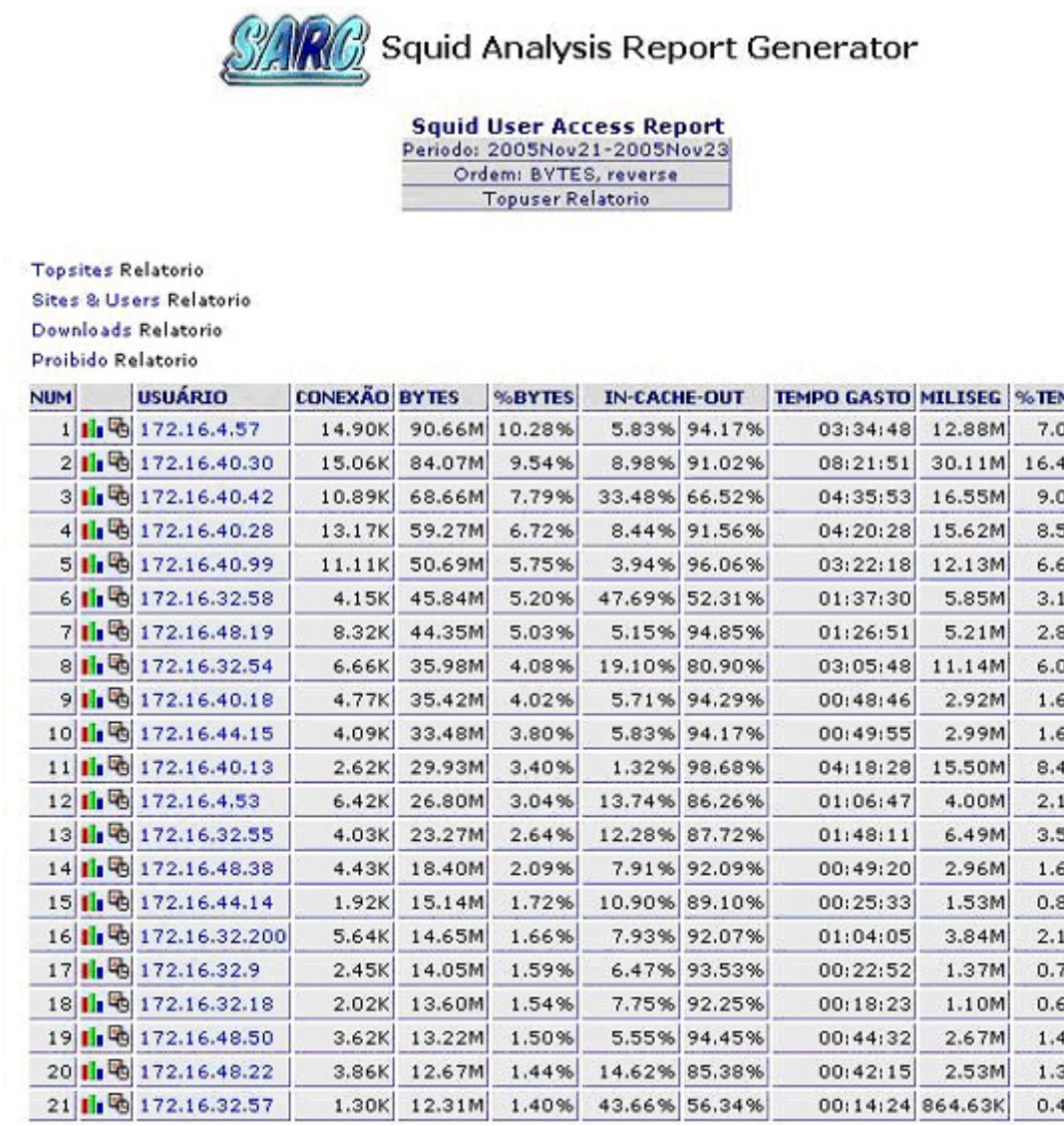
FIGURA 22 – SQUID / RELATÓRIO DE UTILIZAÇÃO - URLS BLOQUEADAS

Squid Analysis Report Generator

Squid User Access Report

ARQUIVO/PERÍODO	DATA CRIAÇÃO	USUÁRIOS	BYTES	MÉDIA
2005Dec04-2005Dec04	Mon Dec 5 04:03:42 BRST 2005	5	16.53M	3.30M
2005Dec04-2005Dec05	Tue Dec 6 04:04:06 BRST 2005	65	281.55M	4.33M
2005Dec04-2005Dec06	Wed Dec 7 04:04:00 BRST 2005	85	455.47M	5.35M
2005Nov28-2005Nov28	Tue Nov 29 04:03:52 BRST 2005	84	209.69M	2.49M
2005Nov28-2005Nov29	Wed Nov 30 04:04:07 BRST 2005	111	519.44M	4.67M
2005Nov28-2005Nov30	Thu Dec 1 04:04:09 BRST 2005	116	664.18M	5.72M
2005Nov28-2005Dec02.1	Fri Dec 2 04:04:30 BRST 2005	119	925.84M	7.78M
2005Nov28-2005Dec02	Sat Dec 3 04:04:28 BRST 2005	125	1.09G	8.74M
2005Nov21-2005Nov21	Tue Nov 22 04:04:02 BRST 2005	115	281.27M	2.44M
2005Nov21-2005Nov22	Wed Nov 23 04:04:22 BRST 2005	126	603.22M	4.78M
2005Nov21-2005Nov23	Thu Nov 24 04:04:23 BRST 2005	128	881.65M	6.88M
2005Nov21-2005Nov24	Fri Nov 25 04:04:28 BRST 2005	131	1.10G	8.43M
2005Nov21-2005Nov25	Sat Nov 26 04:06:21 BRST 2005	132	1.34G	10.21M
2005Nov14-2005Nov14	Tue Nov 15 04:04:28 BRST 2005	81	1.17G	14.50M
2005Nov14-2005Nov15	Wed Nov 16 04:04:19 BRST 2005	81	1.17G	14.50M
2005Nov14-2005Nov16	Thu Nov 17 04:05:32 BRST 2005	132	2.06G	15.61M
2005Nov14-2005Nov17	Fri Nov 18 04:06:45 BRST 2005	139	3.29G	23.73M
2005Nov14-2005Nov18	Sat Nov 19 04:07:24 BRST 2005	141	3.97G	28.22M
2005Nov09-2005Nov09	Thu Nov 10 04:04:20 BRST 2005	122	453.60M	3.71M
2005Nov09-2005Nov11.1	Fri Nov 11 04:06:27 BRST 2005	135	1.34G	9.99M
2005Nov09-2005Nov11	Sat Nov 12 04:06:11 BRST 2005	140	2.44G	17.46M
2005Nov07-2005Nov07	Tue Nov 8 04:04:26 BRST 2005	127	922.59M	7.26M
2005Nov07-2005Nov08	Wed Nov 9 04:04:53 BRST 2005	133	1.61G	12.15M

FIGURA 23 – SQUID / RELATÓRIO DE UTILIZAÇÃO – DATA E HORA



Squid Analysis Report Generator

Squid User Access Report
Periodo: 2005Nov21-2005Nov23
Ordem: BYTES, reverse
Topuser Relatorio

Topsites Relatorio
Sites & Users Relatorio
Downloads Relatorio
Proibido Relatorio

NUM		USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO
1		172.16.4.57	14.90K	90.66M	10.28%	5.83%	94.17%	03:34:48	12.88M	7.03%
2		172.16.40.30	15.06K	84.07M	9.54%	8.98%	91.02%	08:21:51	30.11M	16.43%
3		172.16.40.42	10.89K	68.66M	7.79%	33.48%	66.52%	04:35:53	16.55M	9.03%
4		172.16.40.28	13.17K	59.27M	6.72%	8.44%	91.56%	04:20:28	15.62M	8.53%
5		172.16.40.99	11.11K	50.69M	5.75%	3.94%	96.06%	03:22:18	12.13M	6.62%
6		172.16.32.58	4.15K	45.84M	5.20%	47.69%	52.31%	01:37:30	5.85M	3.19%
7		172.16.48.19	8.32K	44.35M	5.03%	5.15%	94.85%	01:26:51	5.21M	2.84%
8		172.16.32.54	6.66K	35.98M	4.08%	19.10%	80.90%	03:05:48	11.14M	6.08%
9		172.16.40.18	4.77K	35.42M	4.02%	5.71%	94.29%	00:48:46	2.92M	1.60%
10		172.16.44.15	4.09K	33.48M	3.80%	5.83%	94.17%	00:49:55	2.99M	1.63%
11		172.16.40.13	2.62K	29.93M	3.40%	1.32%	98.68%	04:18:28	15.50M	8.46%
12		172.16.4.53	6.42K	26.80M	3.04%	13.74%	86.26%	01:06:47	4.00M	2.19%
13		172.16.32.55	4.03K	23.27M	2.64%	12.28%	87.72%	01:48:11	6.49M	3.54%
14		172.16.48.38	4.43K	18.40M	2.09%	7.91%	92.09%	00:49:20	2.96M	1.62%
15		172.16.44.14	1.92K	15.14M	1.72%	10.90%	89.10%	00:25:33	1.53M	0.84%
16		172.16.32.200	5.64K	14.65M	1.66%	7.93%	92.07%	01:04:05	3.84M	2.10%
17		172.16.32.9	2.45K	14.05M	1.59%	6.47%	93.53%	00:22:52	1.37M	0.75%
18		172.16.32.18	2.02K	13.60M	1.54%	7.75%	92.25%	00:18:23	1.10M	0.60%
19		172.16.48.50	3.62K	13.22M	1.50%	5.55%	94.45%	00:44:32	2.67M	1.46%
20		172.16.48.22	3.86K	12.67M	1.44%	14.62%	85.38%	00:42:15	2.53M	1.38%
21		172.16.32.57	1.30K	12.31M	1.40%	43.66%	56.34%	00:14:24	864.63K	0.47%

FIGURA 24 – SQUID / RELATÓRIO DE UTILIZAÇÃO - PERÍODO POR IP

Foram apresentados alguns recursos de visualização mediante ao acesso de utilização na internet. Embora estes recursos forneçam indícios que medem a utilização da Internet. Os eventos estatísticos, como visto anteriormente, armazenam a quantidade de acessos enviados e recebidos por intermédio de um *firewall*. Em virtude desta análise dos dados obtém-se o real tráfego que passou pelas regras do *firewall.*

A Figura 25 mostra o volume de dados que são trafegados na rede de interligação via rádio do campus Centro e campus Anhanguera nos horários de maior movimento. Vale esclarecer que em cada lado da rede se encontra hosts de origem e destino. Os dados, desta forma, podem ser enviados ou recebidos

da rede privada ou também da Internet, sendo que a área em azul corresponde a saída dos dados e a verde a entrada de dados, é bom verificar que a área em verde e superior a área em azul , pois a comunicação de informações com o banco de dados é remoto, sendo assim qualquer requisição que é feita pelo usuário do campus Anhanguera é totalmente desviado para o campus Centro onde esta requisição é processada e posteriormente enviada com o resultado obtido, já a área de cor azul corresponde as requisições de download sobre atualizações de versões do sistema, sendo que quando ocorre um grande volume de alterações no sistema interno a porcentagem e aumentada consideravelmente.

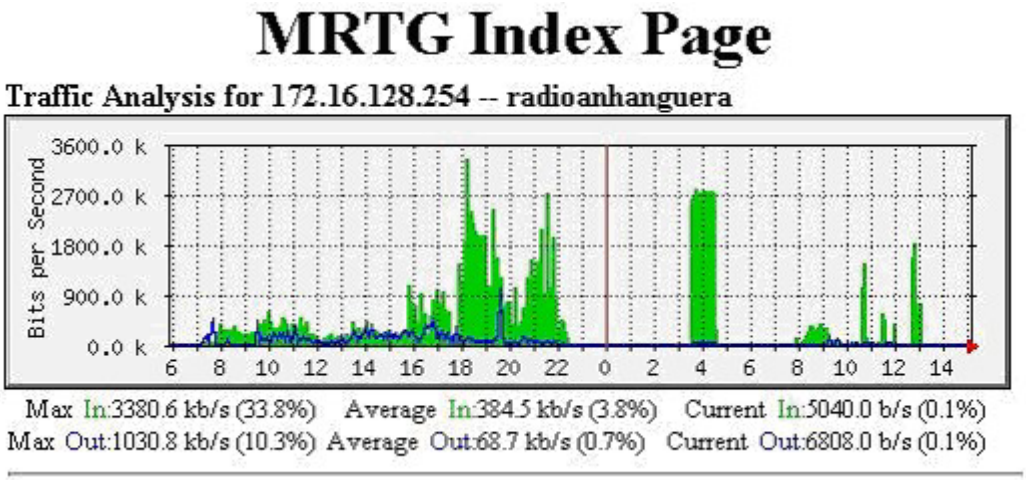


FIGURA 25 – MRTG / RELATÓRIO DE UTILIZAÇÃO DA INTERNET

6. CONCLUSÃO

Este trabalho apresentou uma ferramenta chamada CHECK RULE, voltada à criação de novas regras de segurança em redes ou validação e atualização de regras antigas para minimizar futuros problemas de segurança na rede computacional.

As antigas regras de segurança do firewall eram criadas de forma manual via script acrescentada diretamente no arquivo texto que ocasionava problemas de erros de digitação e interpretação dos comandos usados, isto porque nem sempre a pessoa responsável pela criação destas regras tinham total domínio destes comandos e também havia o problema dos bloqueios dos usuários e grupos que desprendia um tempo muito elevado na hora da criação.

Foi verificado que estes erros encontrados poderiam ser solucionados, então surgiu a idéia de ser projetar uma ferramenta que exibisse de maneira clara e objetiva as políticas de segurança, com opções pré-definidas que seriam mostradas com disponibilidade visual para facilitar e encaminhar o programador na hora de se criar estas novas regras.

Com a implantação deste novo recurso foi constatado que os erro de codificação das regras foram sanadas e também houve uma diminuição significativa no tempo gasto que antes eram desprendidos.

A ferramenta proposta neste trabalho, entretanto, apresenta algumas limitações no que se refere ao desempenho, embora elas não comprometem o funcionamento da ferramenta. É importante em uma outra face, a possibilidade de enriquecer a Ferramenta CHECK RULE, possibilitando maiores facilidades aos Administradores (para melhorar o entendimento e a avaliação dos resultados), cuja finalidade foi apresentar novas técnicas para o fortalecimento da ferramenta.

7. TRABALHOS FUTUROS

Diversos aspectos de segurança foram abordados neste trabalho, com o intuito de garantir um nível de segurança aceitável no acesso remoto. Contudo, apesar da segurança ser um fator obrigatório em uma solução, diversos outros aspectos também necessitam de um estudo aprofundado para uma solução que seja realmente escalonável e ao mesmo tempo gerenciável.

Dessa forma, seria indispensável uma melhoria da Ferramenta nos seguintes aspectos: maior integração das novas categorias criadas com as já existentes, um “print-view” das mudanças que estão sendo criadas antes de concretizá-las, melhorar as opções de exceções dos usuários/setores e também uma melhoria no relatório final que disponibilizada o resultado de todos os novos usuários que foram criados, alterados ou excluídos, é importante que sejam estudadas estas melhorias para que facilite este crescimento.

A atualização destes novos mecanismos que permitam impor restrições e configurações a sistemas remotos é um tópico que deve ser alvo de uma pesquisa ainda maior.

Além desses, diversos outros fatores envolvidos em um cenário de acesso remoto ainda permanecem em aberto. Desde uma interatividade mais amigável com o usuário final até a integração com tecnologias de rede amplamente difundidas, muitas das barreiras impostas ao acesso remoto ainda precisam ser superadas, necessitando do desenvolvimento de trabalhos que apresentem alternativas viáveis para a efetiva disseminação e popularização desta ferramenta.

REFERÊNCIAS BIBLIOGRÁFICAS

CAMERON, Jamie – **Webmin Open Country Inc** - obtido através da Internet. http://www.webmin.com, Fev, 2005

CHADD, Adrian; COLLINS, Robert; NORDSTROM, et al - **SQUID Web Proxy Cache** - index.html,v 1.69 2003 18:46:06 wessels Exp - Site Oficial: www.squid-cache.org - Novembro 2003

COWAN, C., CALTON P., and BAKKE, P. **Stackguard: Automatic adaptive detection and prevention of bu_er-overow attacks.** In Proceedings of the 7th USENIX Security Conference, 1998

CUPERTINO, Cristoffer - **Symantec Corporation Interprise Firewall** – Reference Guide, Symantec, 2003

DERI, Luca – **Generated NTOP SourceForge** - Version 3.0 Documentation Copyright © 1998-2004

FILADORO, Ricardo – **Segurança na Estrutura de Rede, Restrições contra Invasões de Hackers e Spam** http://www.brasil-info.com.br/Prod_brma.jsp, Maio, 2004

GALSTAD, Ethan – **NAGIOS Network Monitor** - Version 1.0 Documentation Copyright © 1999-2003

GARFINKEL, Simson and SPAFFORD, Gene. **Pratical Unix & Internet Security.** O'Reilly & Associates, Inc., USA, 2nd edition, 1996. 971 p.

LIMA, Marcelo Barbosa - **Provisão de Serviços Inseguros Usando Filtros de Pacotes com Estados** - Dissertação apresentada ao Instituto de Computação, UNICAMP, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação – Campinas – São Paulo - Outubro, 2000

LOCOCCO, P. A., Smalley, S. D., MUCKELBAUER, A., TURNER, S. J. and FARREL, J. F. **The inevitability of failure: The awed assumption of security in modern computing environment.** In Proceedings of the 21st National Information Systems Security Conference, pages 303-314, October 1998

NAKAMURA, Emílio Tissato and GEUS, Paulo Lício de – **Segurança de Redes em Ambientes Cooperativos** – Editora Berkeley 2002

OETIKER, Tobias - **Monitoring Your ITGear: The MRTG Story** - 1520-9202/01 © 2001 IEEE - November - December 2001 IT Pro

RAND, Dave and OETIKER, Tobias - **MRTG Multi RouterTraffic Grapher** – Latest Release: MRTG 2.10.5 - Site Oficial: www.mrtg.org - Novembro 2003

ROEDIG, U., GÖRTZ, M. and STEINMETZ, R. - **RSVP as Firewall Signalling Protocol** - Proceedings of the Sixth IEEE Symposium on Computers and Communications ISCC'01 1530-1346/01 © 2001 IEEE

SINNAPPAN, Scott Hazelhurst Adi Attar Raymond - **Algorithms for Improving the Dependability of Firewall and Filter Rule Lists** - 0-7695-0707-7/00 2000 IEEE

SMITH, Robert N. and HARYA, Sourav Bhattac - **Firewall Placement In A Large Network Topology** - Proceedings of the 6th IEEE Workshop on Future Trends of Distributed Computing Systems FTDCS '97 0-8186-8153-5/97 © 1997 IEEE

SPAFFORD, Christoph L. Schuba and Eugene H. - **A Reference Model for Firewall Technology** - Proceedings of the 13th Annual Computer Security Applications Conference ACSAC '97 1063-9527/97 © 1997 IEEE

TAYLOR, Tiffany – **Security Complete** - 2. ed. Alameda, CA: Sybex, 2002

VIEGA, J. and MCGRAW, G. **Building Secure Software: How to Avoid Security Problems the Right Way**. Addison-Wesley, 3rd edition, 2003

YING-DAR Lin; HUAN Yunwei, and SHAO-TANG Yu - **Building an Integrated Security Gateway: Mechanisms, Performance Evaluations, Implementations, and Research Issues** - IEEE Communications Surveys http://www.comsoc.org/pubs/surveys - Outubro 2003

ZWICKY, Elizabeth D., and CHAPMAN, Brent D. – **Building Internet Firewalls** Editora Campus – Rio de Janeiro 2001 Tradução da 2 ed. Original

APÊNCICE A - INSTALAÇÃO DA FERRAMENTA

A instalação da Ferramenta foi feita através de um aplicativo executável chamado setup.exe, que pode ser iniciado com dois click do mouse ou executado no comando Shell pelo comando Abrir: setup.exe conforme demonstrado na Figura 26.

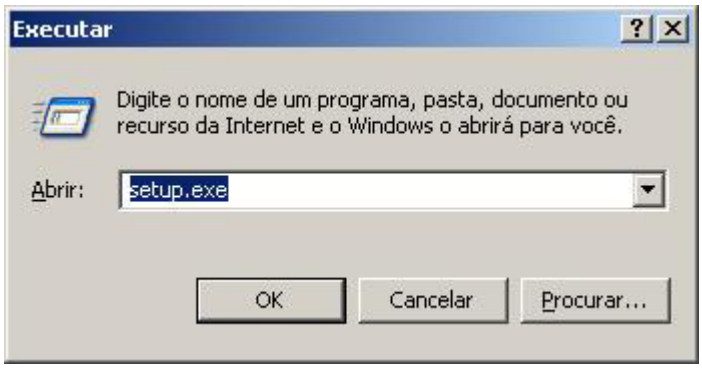


FIGURA 26 - TELA DO COMANDO DE INSTALAÇÃO EM MODO SHELL

A Figura 27 mostra a tela de confirmação da instalação onde o instalador irá escolher o botão OK para prosseguir com a instalação da Ferramenta ou o botão Exit Setup para sair da instalação.

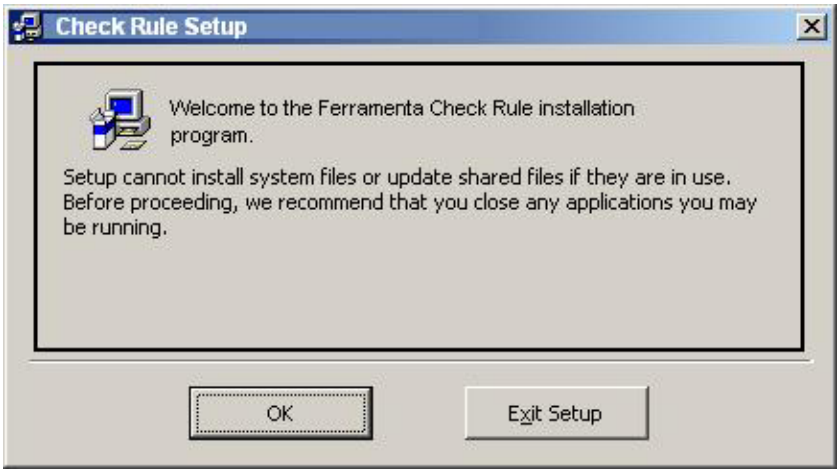


FIGURA 27 – TELA DE SETUP DE INSTALAÇÃO DA FERRAMENTA

Já a Figura 28, mostra qual será o diretório que a ferramenta será armazenada sendo possível acessar diretamente no diretório mencionado ou no caminho

Iniciar/Programas/Check Rule, neste caminho será visualizado também uma outra função que é a de poder desinstalar a ferramenta pela opção uninstall.

FIGURA 28 - TELA DE CRIAÇÃO DO DIRETÓRIO DA FERRAMENTA

1) Seqüência do código fonte Ferramenta Check Rule:

Parte do Código Fonte da Ferramenta Check Rule

```
Private Sub frm_tela_conf_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
Tooltip_CS.SetToolTip(Me.txt_ip_usuario, "Ex.: Único 172.16.0.1" & vbCr & " " & _
                                         " Range: 172.16.0.9 - 172.16.0.255" & vbCr & " " & _
                                         " Random: 172.16.0.12 172.16.0.40 172.16.0.52")

Tooltip_CS.SetToolTip(Me.txt_num_porta, "Ex.: Único 80" & vbCr & " " & _
                                                 " Range: 3100 - 3128" & vbCr & " " & _
                                                 " Random: 495 21 25 110")

Tooltip_CS.SetToolTip(Me.chk_all_ports, "Ex.: ACL all src 0.0.0.0 / 0.0.0.0")
...

Private Function mostraword()
Dim i As Byte
i = 1

Try

While DRword.Read

Select Case i
        Case 1
            If DRword.HasRows = False Then
                chk_cat_1.Visible = False
            Else
                chk_cat_1.Visible = True
                chk_cat_1.Text = DRword("categoria").ToString
            End If
        Case 2
```

```
            If DRword.HasRows = False Then
                chk_cat_2.Visible = False
            Else
                chk_cat_2.Visible = True
                chk_cat_2.Text = DRword("categoria").ToString
            End If
        Case 3
            If DRword.HasRows = False Then
                chk_cat_3.Visible = False
            Else
                chk_cat_3.Visible = True
                chk_cat_3.Text = DRword("categoria").ToString
            End If
```

...

```
Private Sub btn_gravar_som_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btn_gravar_som.Click
Dim Cnn As New OleDbConnection("Provider=Microsoft.JET.OLEDB.4.0; Data
Source=C:\Conf_Squid\base\squid.mdb")
Dim Cmd As New OleDbCommand

If rd_csi_none.Checked = True Then
    MsgBox("Você não selecionou nenhuma opção. Categoria não será gravada.",
MsgBoxStyle.Information)
Else

Try

Cnn.Open()

With Cmd

        .Connection = Cnn
        .CommandTimeout = 0
        .CommandText = "INSERT INTO som(som, dia, hora)" & _
                       "VALUES (@som, @dia, @hora)"
        .CommandType = CommandType.Text

End With

Cmd.Parameters.Add(New OleDbParameter("@som", OleDbType.VarChar))
Cmd.Parameters("@som").Value = txt_cc_imgsom.Text

Cmd.Parameters.Add(New OleDbParameter("@dia", OleDbType.Date))
Cmd.Parameters("@dia").Value = Date.Today

Cmd.Parameters.Add(New OleDbParameter("@hora", OleDbType.Date))
Cmd.Parameters("@hora").Value = Format(Date.Now, "HH:mm:ss")

Cmd.ExecuteNonQuery()


Private components As System.ComponentModel.IContainer

Friend WithEvents btn_voltar As System.Windows.Forms.Button
Friend WithEvents grp_cat_word_url As System.Windows.Forms.GroupBox
Friend WithEvents tooltip_cat As System.Windows.Forms.ToolTip
Friend WithEvents GroupBox1 As System.Windows.Forms.GroupBox
Friend WithEvents GroupBox2 As System.Windows.Forms.GroupBox
Friend WithEvents grp_cp_word As System.Windows.Forms.GroupBox
```

```
Friend WithEvents Label1 As System.Windows.Forms.Label
Friend WithEvents txt_cp_word As System.Windows.Forms.TextBox
Friend WithEvents rd_cct_url As System.Windows.Forms.RadioButton
Friend WithEvents rd_cct_word As System.Windows.Forms.RadioButton
Friend WithEvents Label2 As System.Windows.Forms.Label
Friend WithEvents grp_cp_url As System.Windows.Forms.GroupBox
Friend WithEvents rd_cct_none As System.Windows.Forms.RadioButton
Friend WithEvents chk_curl_racismo As System.Windows.Forms.CheckBox
Friend WithEvents chk_curl_geral As System.Windows.Forms.CheckBox
Friend WithEvents chk_curl_lazer As System.Windows.Forms.CheckBox
Friend WithEvents chk_curl_jogos As System.Windows.Forms.CheckBox
Friend WithEvents chk_curl_sexo As System.Windows.Forms.CheckBox
Friend WithEvents chk_cw_geral As System.Windows.Forms.CheckBox
Friend WithEvents chk_cw_lazer As System.Windows.Forms.CheckBox
Friend WithEvents chk_cw_jogos As System.Windows.Forms.CheckBox
Friend WithEvents chk_cw_sexo As System.Windows.Forms.CheckBox
Friend WithEvents chk_cw_racismo As System.Windows.Forms.CheckBox
Friend WithEvents chk_curl_1 As System.Windows.Forms.CheckBox
Friend WithEvents txt_cat_new As System.Windows.Forms.TextBox
Friend WithEvents chk_cw_1 As System.Windows.Forms.CheckBox
Friend WithEvents lbl_cat_new As System.Windows.Forms.Label
Friend WithEvents rd_ccat_none As System.Windows.Forms.RadioButton
Friend WithEvents rd_ccat_racismo As System.Windows.Forms.RadioButton
Friend WithEvents rd_ccat_sexo As System.Windows.Forms.RadioButton
Friend WithEvents rd_ccat_jogos As System.Windows.Forms.RadioButton
Friend WithEvents rd_ccat_lazer As System.Windows.Forms.RadioButton
Friend WithEvents rd_ccat_geral As System.Windows.Forms.RadioButton
Friend WithEvents txt_url_url As System.Windows.Forms.TextBox
Friend WithEvents pn_url_1 As System.Windows.Forms.Panel
Friend WithEvents chk_url_4 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_3 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_2 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_1 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_8 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_7 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_6 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_5 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_9 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_10 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_11 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_12 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_13 As System.Windows.Forms.CheckBox
Friend WithEvents chk_url_14 As System.Windows.Forms.CheckBox
...
```

2) COMO INSTALAR E CONFIGURAR O PACOTE SQUID

Para usufruir os recursos que o Squid oferece, primeiramente é preciso fazer a instalação e posteriormente configuração, abaixo uma relação de passos que devem ser seguidos para a implantação desta ferramenta:

Passo1: Instalação do pacote squid
rpm –ivh squid-???.rpm
Passo2: Verificação da instalação
Verifique se o pacote foi instalado corretamente pelo comando rpm –qa |grep squid
Verifique se a pasta /etc/squid e o arquivo squid.conf foram instalados

Passo2: Configuração e Alteração do arquivo squid.conf
Obs: para habilitar linha comentada é só tirar o #

Habilite as seguintes linhas de comando, caso ainda não estejam liberadas:
http_port 80
cache_mem 64 MB
cache_access_log /var/log/squid/access.log
pid_filename /var/run/squid.pid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern . 0 20% 4320
icp_access allow all
miss_access allow all
httpd_accel_with_proxy on
store_avg_object_size 5 KB

Passo 3: Inclusão das regras dentro do arquivo /etc/squid/squid.conf

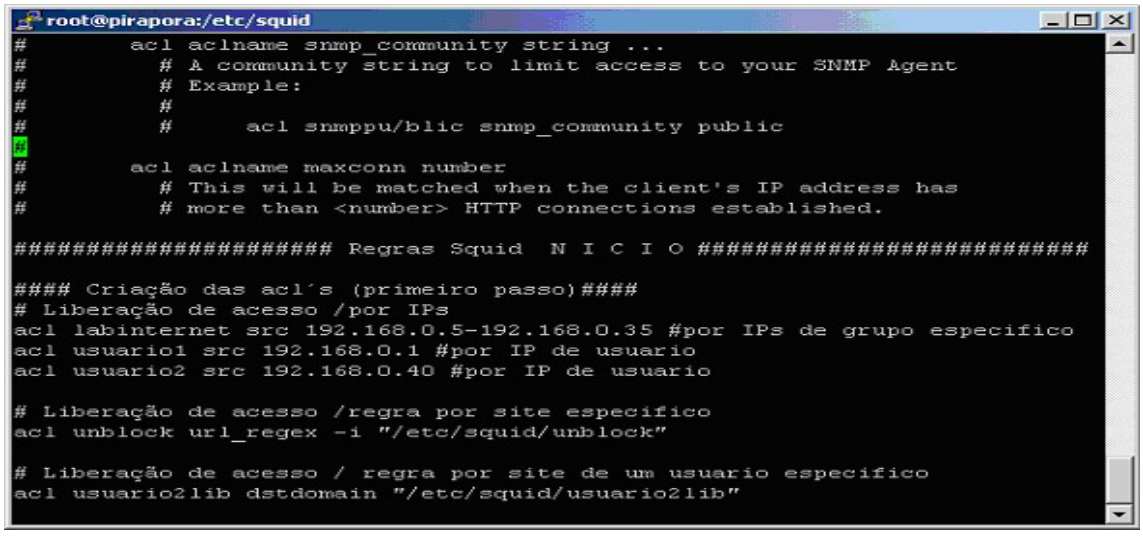


FIGURA 29 - EXEMPLO DE PROGRAMAÇÃO MANUAL NO SQUID

```
#####################################################
################## REGRAS SQUID #####################
#####################################################
################## I N I C I O #####################
#####################################################

# ACLS Usuarios, Setores
acl ana src 172.16.0.203
acl biblioteca src 172.16.0.230-172.16.0.250
acl contabilidade src 172.16.4.12
acl laboratorio src 10.160.0.1-10.160.0.255
acl marcel src 172.16.36.14
acl secetraria src 172.16.4.11 172.16.4.13 172.16.4.15 172.16.4.17

# Configuracao ACLS, HTTP - Portas Padrao(liberacao/bloqueio)
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 21 25 70 80 110 210 280 488 563 591 777
acl Safe_ports port 88 # Sarg
acl Safe_ports port 89 # Webmail
acl Safe_ports port 1080 1214 # Kazaa Lite
acl Safe_ports port 7003 # Vivo
acl Safe_ports port 8080 # OAB
acl Safe_ports port 1025-65535
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny  manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
# ACLS Palavras, Urls
acl word_no url_regex -i "/etc/squid/word_no"
acl url_no dstdomain -i "/etc/squid/url_no"
acl users_url_no dstdomain "/etc/squid/users_url_no"
acl setor_word_no url_regex -i "/etc/squid/setor_word_no"
acl sexo_word_no url_regex -i "/etc/squid/sexo_word_no"

# ACLS Horarios
acl horario_no time 07:00-23:00
acl manha_no time 07:01-12:00
acl tarde_no time 12:01-18:00
acl noite_no time 18:01-24:00
acl madru_no time 00:01-07:00

# ACLS Sons,Imagens
acl mp3_no urlpath_regex \.mp3$
acl wav_no urlpath_regex \.wav$
acl avi_no urlpath_regex \.avi$
acl mpg_no urlpath_regex \.mpg$
acl mpeg_no urlpath_regex \.mpeg$
acl mov_no urlpath_regex \.mov$
acl wmv_no urlpath_regex \.wmv$

#####################################################

# HTTP_ACCESS Usuarios, Setores, horarios
http_access deny ana !users_url_no
http_access allow biblioteca
```

```
http_access deny contabilidade !url_no
http_access allow laboratorio horario_no
http_access allow laboratorio !setor_word_no
http_access allow marcel !sexo_word_no
http_access allow secretaria !word_no

# HTTP_ACCESS Sons,Imagens
http_access deny mp3_no
http_access deny wav_no
http_access deny avi_no
http_access deny mpg_no
http_access deny mpeg_no
http_access deny mov_no
http_access deny wmv_no

##########################################################
#################### F I M ###############################
##########################################################
```

Passo 4: Reiniciar o serviço squid:
service squid Restart
ou
service squid stop
Service squid start # iniciar service

APÊNDICE B - OUTRAS FERRAMENTAS

Partindo da necessidade de encontrar ferramentas que auxiliassem na compreensão de políticas de segurança, foram pesquisadas ferramentas que utilizassem representações de políticas não baseadas em arquivos textuais, visto que a linearidade imposta pelo formato textual é um dos fatores que dificultam a análise das políticas. Com relação à modelagem em estruturas gráficas, foram encontradas três ferramentas; BRMultiaccess, Aker Web Content Analyzer e Websense Enterprise, envolvendo o mapeamento de políticas de segurança em uma estrutura gráfica, e com objetivos aparentemente ligados a esta dissertação.

Estas ferramentas visam identificar quais são as estruturas utilizadas para obter um maior formalismo em sua especificação e tentar implementar novas estruturas de segurança para auxiliar na identificação dos problemas de segurança. As ferramentas também levam em conta questões de usabilidade para auxiliar o usuário a navegar entre os domínios do sistema, incluindo menus de contexto e integração com outras ferramentas, e utiliza um algoritmo de mapeamento em árvores, para disposição dos nós da árvore, o que garante uma melhor navegação na hierarquia.

BRMULTIACCESS

Segundo FILADORO (2004), as empresas que possuem Speedy, Virtua, Multi-Link ou outro tipo de conexão à Internet de banda larga e precisam compartilhá-la com todos os micros de sua rede, devem também se preocupar em proteger seus dados contra hackers, vírus, etc, assim como evitar o mau uso da web por parte de seus funcionários. A solução para estas questões é o BRmultiaccess, um software que compartilha uma única conexão à Internet para todos os micros de uma empresa, protegê-los de ações danosas e, principalmente, controlar o tempo e o tipo de acesso, o que afasta os prejuízos altíssimos com a perda de produtividade.

Os recursos do BRmultiaccess incluem:

Compartilhamento - uma única conexão com a Internet (linha discada, conexões dedicadas, Multi-*Link*, DVI, Speedy, Velox, @jato, Virtua, WLL, *etc*), é compartilhada por todos os microcomputadores da rede.

Interface *web* de fácil utilização - o administrador da rede pode gerenciar todos os recursos do BRmultiaccess através de qualquer microcomputador que esteja conectado à rede interna ou à Internet.

Gerenciamento e política de acesso – por meio de um *browser*, o administrador poderá verificar como os usuários estão usando a conexão e criar regras, combinando usuários, grupos, horários, serviços, portas e palavras-chaves para personalizar o uso de acordo com as reais necessidades da empresa.

Relatórios, estatísticas e gráficos - o administrador do BRmultiaccess tem à sua disposição uma série de relatórios, estatísticas e gráficos para poder avaliar o uso da conexão em sua empresa.

***Firewall* com alarmes** - minimiza ao extremo o risco de invasão e vazamento de dados confidenciais.

DMZ - barramento de rede independente, para servidores que serão acessados através da Internet.

Mascaramento de IP - todas as estações de trabalho da rede local utilizam endereços de IP falsos, que não podem ser acessados diretamente via Internet, garantindo maior segurança às estações.

Proxy transparente - agiliza o acesso à *web* e proporciona melhor aproveitamento da conexão. Não precisa ser configurado nas estações.

DHCP Server - fornece automaticamente endereços de IP para as estações no momento de sua conexão à rede.

Controle de banda - com o controle de banda, é possível fracionar seu *link*, de modo que serviços essenciais à empresa sejam priorizados. Em um *link* de 64 Kbps, é possível determinar que 56 Kbps serão destinados ao acesso *web* e os

8 Kbps restantes atenderão os outros serviços (ICQ, *e-mail*, FTP, *etc*)

Web-mail - verificação de *e-mails* com total privacidade através de qualquer micro conectado à Internet.

Multiplataforma - o BRlinux, sistema operacional criado pela BRconnection especificamente para o BRmultiaccess, é requerido somente no micro onde o BRmultiaccess será instalado. Os demais micros continuarão com seus sistemas operacionais (Windows, OS/2, Mac OS, Unix, Linux

Cluster **de redundância** - muitas empresas não podem ficar sem acesso à Internet porque o servidor parou de funcionar repentinamente. Oferecendo uma solução a esse problema, a BRconnection desenvolveu o módulo de redundância para o BRmultiaccess. Com esse módulo, a empresa conta com dois servidores de acesso à Internet. Dessa forma, se o servidor primário parar de funcionar por qualquer motivo, o secundário o substituirá, passando a ser o servidor primário em questão de segundos. A sincronização dos dados entre os servidores é feita a cada 24 horas.

AKER WEB CONTENT ANALYZER

A Aker Web Content Analyzer é um avançado sistema de análise e filtragem de páginas Web por contexto, através dessa ferramenta de controle de URL, com mais de 500.000 sites na Internet classificados e atualizados diariamente, permite bloquear ICQ, Mensseger e sites de relacionamentos diversos e com o auxílio da Aker Web Control uma ferramenta gratuita, que cria perfis individuais, onde usuário tem acesso personalizado pelo administrador da rede, aumentando sua produtividade e utilizando de forma racional os recursos de rede.

O Web Content Analyzer bloqueia ICQ e MSN, indo até a origem.(nome, extensão, endereço de e-mail) mesmo que seja executável ou seja renomeado.

A filtragem é feita a partir da pesquisa do endereço a ser acessado.

O produto é atualizado diariamente por uma equipe especializada e é reaplicada para todos os clientes automaticamente.

O produto faz toda a filtragem a partir da pesquisa do endereço a ser acessado, essa pesquisa é feita previamente por uma equipe que classifica milhares de sites novos por dia distribuídos em vinte e quatro categorias, oferecendo uma base de dados de sites brasileiros.

Cabe ao administrador escolher os usuários/grupos autorizados ou não a ter acesso a determinados sites.

Produzido no Brasil, o Analisador de URL, conta com uma quantidade muito maior de sites nacionais, possibilitando um nível de abrangência muito grande.

Algumas categorias presentes no Aker Web Content Analyzer:

Sexo Explícito, Drogas e Álcool, Jogos de Azar, Violência,Diversão e Entretenimento, Jogos Eletrônicos, Bancos e Instituições Financeiras, Procura de Empregos, Viagem, Veículos e Motores, Notícias, Namoro e Paquera, Compras, Esportes, Conversação, Hackers, Música e MP3, Webmail.

A cada conexão requerida, o sistema identifica a classificação do site na base de dados do Analisador de URLs, conforme a Figura 30 e determina se o usuário está apto a acessá-lo ou não com base em seu perfil.

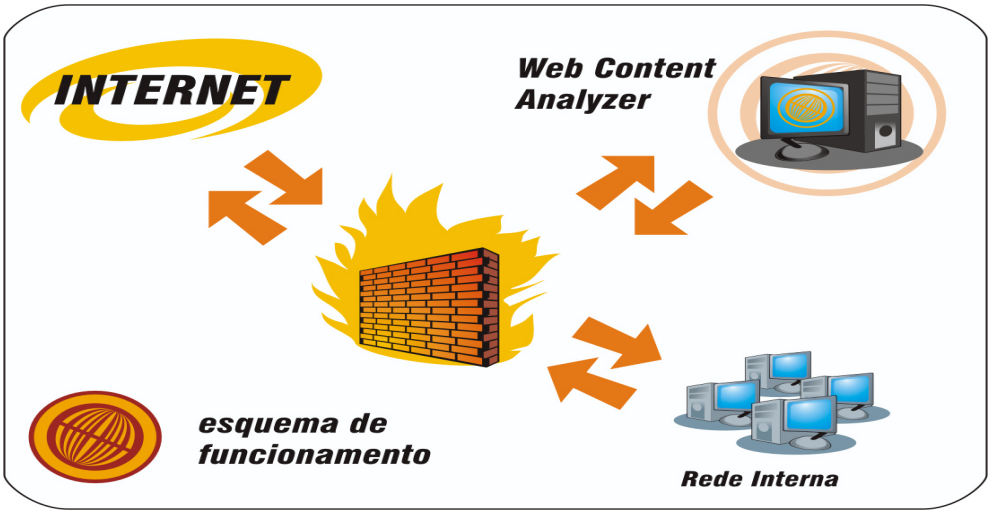


FIGURA 30 – ANALISADOR WEB ANALYZER

WEBSENSE ENTERPRISE

Websense é baseado na tecnologia de filtragem “pass-through” (“passe-através”), o método mais preciso, confiável e escalável de filtragem de acesso à Internet. A filtragem Pass-Through força todas as requisições a páginas da Web iaô passar através de um ponto de controle de Internet, como um firewall, servidor Proxy ou dispositivo de cache. Websense é integrado a esses pontos de controle e verifica cada requisição para determinar se ela deve ser permitida ou recusada. Todas as ações são armazenadas em log para a geração de relatórios.

Base de Dados

O Banco de Dados de URLs possui mais de onze milhões de sites, representando dois e meio bilhões de páginas web, divididas em mais de noventa categorias (maior granularidade de categorias, evitando bloqueio excessivo ou insuficiente) com as quais é possível aplicar políticas de acesso (Permitir, Bloquear, Continuar, Cotas de Tempo e Configuração de Horário) por usuário, grupos, etc, em qualquer das integrações possíveis (Firewalls, Cache, Proxy, Stand-Alone, Roteadores e Switches Cisco).

Contém ainda mais de sessenta protocolos de rede/ aplicação cadastrados (MSN, Yahoo, FTP, Kazaa, Telnet, Skype, Hopster, Windows Media Player, etc) divididos em sessenta categorias (I.M., P2P, Transferência de Arquivos, Streaming Media, etc) e atualizados automaticamente (sem a necessidade de intervenção do administrador) com a base de URLs, visando oferecer controle do tráfego e utilização através do Network Agent, implementando políticas de utilização destes protocolos por usuários, grupos em qualquer das integrações disponíveis para o produto. O Network Agent é integrado ao Websense Enterprise, sem custo adicional e gerenciado pela mesma console do Websense Enterprise.

Base de dados de extensão de arquivo atualizados automaticamente e de forma incremental durante a atualização da Websense Master Database.

Permite, por exemplo, liberar o acesso a Webmail, sem que se possa baixar nenhum arquivo, ou determinadas extensões de arquivo.

Atualização diária, automática e incremental da base de dados e protocolos, através da Console de Gerenciamento, via Web.

A identificação de URLs não cadastradas é feita pelo WebCatcher que envia ao fabricante as devidas Urls para categorização, recurso que pode ser ativado ou não pelo administrador. Este recurso é integrado ao Websense Enterprise, sem custo adicional, categorizando websites em mais de cincoenta idiomas, entre eles o português.

O sistema permite ao administrador criar novas categorias de URLs (Categorias Customizáveis) e implementar políticas de acesso da mesma forma que as categorias pré-existentes. Desta forma, o administrador pode mover páginas cadastradas numa categoria específica para as categorias criadas manualmente, sendo que o Websense manterá estas alterações mesmo após as atualizações da base de dados.

Para cada categoria (ou grupos de categoria) é possível especificar o bloqueio de downloads de arquivo por extensão. É possível ainda especificar-se diferentes extensões para cada categoria, de forma independente.

Qualquer usuário que não esteja autenticado no domínio pode ser autenticado pelo Websense, recebendo uma tela de Login (usuário e senha). Caso este não se autentique manualmente no Websense, seu acesso será bloqueado, visando permitir o acesso à Web apenas de usuários cadastrados no domínio da empresa. Isto permite ao administrador criar perfis de acesso para visitantes ou usuários temporários, com acessos específicos.

Aplicação de filtragem mesmo em páginas do tipo “embedded URLs”, ou seja, opção “Cache” presente normalmente em sites de busca como Google, Yahoo, etc, que visam “enganar” produtos de controle de acesso web, 14. Implementação de políticas mesmo para protocolos de aplicações que façam uso do tunelamento HTTP. Muitas destas tecnologias fazem uso deste recurso para enganar ferramentas como Proxies e Firewalls e obter acesso à Web,

comprometendo a segurança e consumindo banda. O Network Agent oferece este gerenciamento, permitindo ao administrador implementar políticas de acesso para Instant Messaging (MSN, Yahoo, ICQ, etc), Peer-to-Peer (Kazaa, Morpheus, etc), FTP, POP3, etc por usuário ou grupos. O Network Agent é integrado ao Websense Enterprise, sem custo adicional e gerencia mais de 68 protocolos de rede divididos em 60 categorias.

Você pode rodar o Websense sobre os sistemas operacionais Microsoft Windows NT, Windows 2000, Sun Solaris ou Linux (Red Hat Linux.)

O Websense integra-se facilmente com Base de usuários e grupo: Active Directoy, Windows NT, Novell, LDAP, RADIUS.

Ferramentas de relatórios do Websense Enterprise

As ferramentas de relatórios do Websense Enterprise ajudam a identificar problemas potenciais com exibições em tempo real e históricos dos riscos associados ao uso da Internet por funcionários. Com essas informações, os administradores de TI podem ajustar as políticas de acesso à Internet e reduzir com eficiência os riscos associados ao uso da informática por funcionários na organização.

Todos os acessos realizados pelos usuários são registrados em base de dados SQL Server (Enterprise e Standard Editions), possuindo ainda uma console para gerenciamento da base SQL, oferecendo gerenciamento SQL de modo fácil e simples mesmo ao administrador que não possui conhecimento neste banco de dados.

O **Websense Enterprise** traz inclusas três ferramentas de relatório que atuam em diferentes segmentos, que são:

Websense Reporter: gerador de relatórios baseado em Crystal Reports conforme Figura 31, que compõem mais de oitenta modelos configuráveis, como: Top “n” Usuários por Consumo de Banda, Top “n” Sites ou Categorias mais Acessados, etc. Gera relatórios nas extensões: HTML, Word, Excel, CSV, PDF. Permite ainda que os relatórios, uma vez devidamente configurados,

possam ser agendados pelo administrador para horários específicos e configuráveis; uma vez configurados, o administrador não precisará mais gerar os relatórios manualmente, podendo salvar os mesmos em diretórios de rede, envio por e-mail, etc. Esta ferramenta permite ainda ao pessoal de TI gerar e distribuir informações relavantes para outros departamentos da empresa, como RH (número de acessos a sites de emprego, estatísticas de uso da web, etc), Financeiro (bilhetagem do uso da Web baseado em grupos, filiais, etc) e Gerentes de Negócio (produtividade, tempo de acesso, etc), além do departamento de TI como o exclusivo relatório de Classes de Risco, etc.

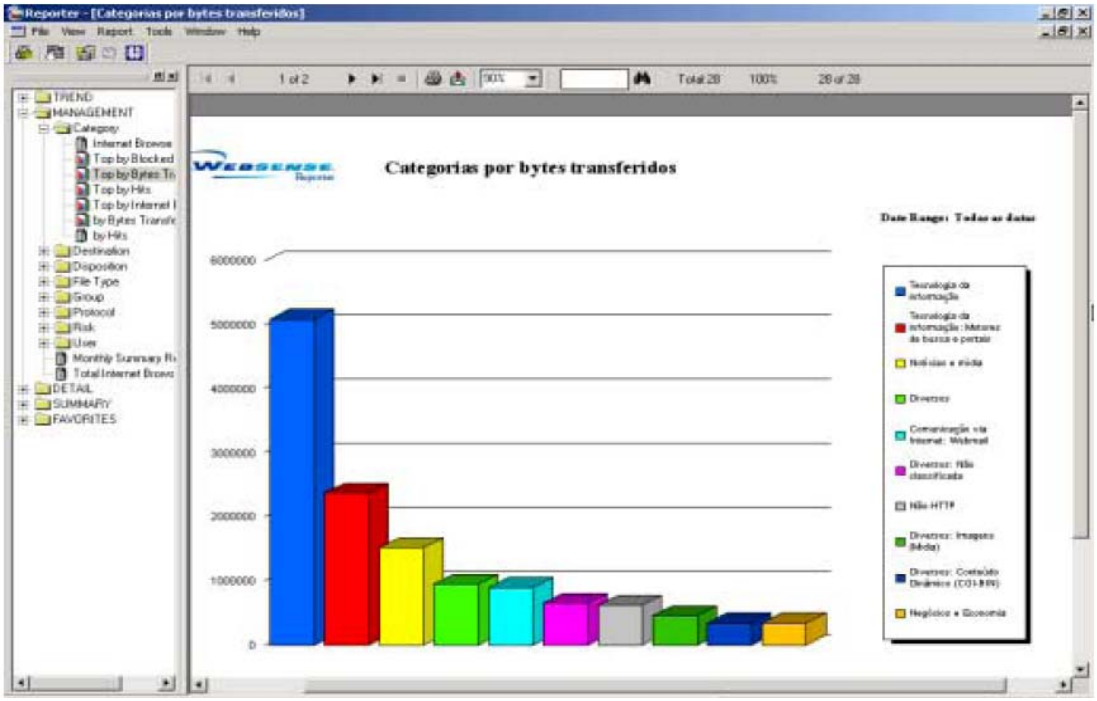


FIGURA 31 - WEBSENSE REPORTER

Websense Explorer: ferramenta Analítica do Websense Enterprise, conforme Figura 32, em modo browser e protegida por senha, permitindo a “navegação” através dos logs, extraindo informações em tempo real sem a necessidade de gerar novos relatórios. Atualiza os dados recebidos a cada trinta segundos, mostrando ao administrador os principais riscos no acesso realizado (Perda de Produtividade, Consumo de Banda, Problemas Legais e Risco à Segurança), permitindo ainda que o administrador “explore” cada um destes resumos através de Usuário, Grupo, Categoria, Sites, Tempo de Conexão, Hits, Bytes, etc. Permite ainda identificar qual ação o usuário tomou mesmo após ser

advertido através de tela de bloqueio, para fins forenses. Possibilita ainda evitar a exposição dos funcionários, possibilitando a omissão de nomes dos usuários para relatórios ou apresentações onde os dados possam ser de natureza sensível ou sigilosa.

FIGURA 32 - WEBSENSE EXPLORER

Websense Real-Time Analyser: ferramenta baseada em browser, conforme Figura 33, atua em tempo real e é protegida por senha, voltada a analisar a situação do segmento de rede em análise. Identifica os protocolos que estão em uso, gerando ainda informações dos usuários, categorias e sites acessados, permitindo ao administrador a rápida tomada de decisão para corrigir eventuais abusos ou situações que possam estar comprometendo os recursos da empresa, como congestionamento de links, etc.

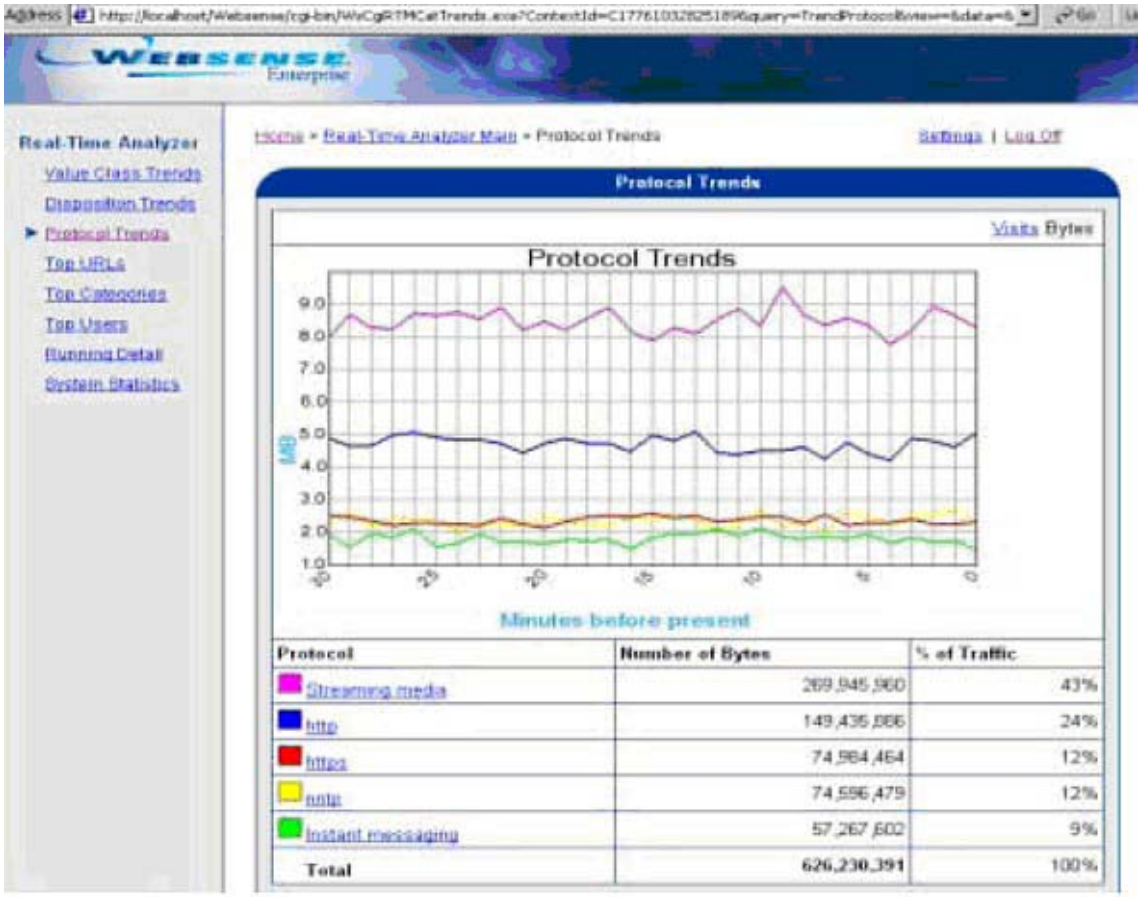


FIGURA 33 - WEBSENSE REAL-TIME ANALYSER