Tecnologia

BRIDGE FIREWALL – UMA SOLUÇÃO BASEADA EM *SOFTWARE* LIVRE PARA A SEGURANÇA DA EBNET

Evaldo Galvão Mendonça[1]

Resumo. Este artigo apresenta uma proposta para a segurança da EBNet baseada em *Software* Livre. Esta iniciativa consiste em utilizar um computador pessoal (PC) de baixo poder de processamento com um Sistema Operacional robusto, voltado para a segurança, o *OpenBSD.* Instalado em conjunto com ferramentas de gerência e segurança de redes *open source,* deve ser disponibilizada uma unidade por Organização Militar (OM) conectada diretamente à EBNet, por meio do *backbone* da Empresa Brasileira de Telecomunicações (EMBRATEL), garantindo, assim, a otimização na segurança e gerência da EBNet e da Intranet das OM conectadas. O trabalho foi desenvolvido e testado no laboratório de informática da Escola de Administração do Exército (EsAEx), utilizando um PC com três placas de rede *ethernet* 10/100Mbps e *softwares* livres. A abordagem baseia-se num *Firewall* do tipo *Bridge,* conhecido também como invisível por não possuir endereçamento *Internet Protocol* (IP), uma vez que trabalha na camada de enlace de dados (nível 2) do modelo ISO/OSI. A tecnologia implementada possibilita uma solução dita **"caixa-preta"**, de modo que o usuário final não necessite de quaisquer conhecimentos técnicos para instalar a solução na rede de sua OM, sendo administrada e gerenciada remotamente pelo escalão de telemática enquadrante. A solução proporciona suporte para a escalabilidade segura e gerenciada da EBNet, de forma que os projetos do Tecnologia da Informação (TI) do Exército Brasileiro (EB) como a utilização de Voz sobre IP (VOIP) e Videoconferência sobre a EBNet possam ter uma base sustentável.

Palavras-chave: EBNet. Software Livre. Bridge Firewall. Segurança da Informação. Gerência de Redes.

Abstract. This article presents an open source proposal for security in EBNet. This proposal consists of using a Personal Computer (PC) with low processing power with a complete Operational System, turned to security, the OpenBSD. Installed together with management tools and the security of open source networks, a unit connected directly to EBNet must be available for each military organization, through the backbone of the Brazilian Company of Telecommunications (EMBRATEL), as to guarantee the optimization in the security and management of

[1] Graduado em Ciência da Computação. Escola de Adminnistração do Exército(EsAEx), Salvador, Brasil. rsmineiro@gmail.com .

EBNet and the Intranet of the military organization connected. This process was developed and tested in the Computer Laboratory of the “Escola de Administração do Exército” (EsAEx), using a PC with 3 10/100Mbps ethernet cards and open source softwares. The approach is based on a Firewall of the Bridge type, also known as invisible because it doesn’t have an Internet Protocol (IP) Adress, since it works in the layer of data enlace (level 2) of the model ISO/OSI. The technology implemented makes a solution called “Black-Box” possible, so that the final user doesn’t need any technical knowledge to install the solution network at his military organization, as it is administrated and managed remotely by the correspondent telematics team. The solution provides support for safe scalability which is managed by the EBNet, so that the projects of Information Technology (TI) of the Brazilian Army (EB) such as the use of the Voice over IP (VoIP) and Videoconference about the EBNet can have a sustainable base.

Keywords: EBNet. Open Source Software. Bridge Firewall. Information Security. Network Management.

1 Introdução

A EBNet é uma rede de comunicação digital de dados, voz e imagem, tendo como base a Intranet do EB. É interligada pelo *backbone* da Embratel, com acesso direto para as OM incluídas na estrutura principal (Figura 1), valendo-se da *Internet*, por intermédio de uma conexão segura utilizando *Virtual Private Network* (VPN) para as outras OM. É gerenciada pelo Centro Integrado de Telemática do Exército (CITEX), descentralizada por Regiões Militares (RM) sob responsabilidade dos Centros de Telemática e Centros de Telemática de Área (CT e CTA) e visa a tramitação e disponibilização de documentos oficiais do EB, disponibilização de sistemas corporativos, e integração de todas as OM do EB em uma grande rede privada, servindo como porta de saída para a *Internet* com maior segurança e gerenciamento, otimizando os recursos humanos, financeiros e materiais disponíveis nestas instituições. (BRASIL, 2004).

Para garantir que a EBNet cumpra o seu propósito de forma segura,

> os recursos de TI[2] (p. ex.: microcomputadores, “*mainframes*”, servidores, “*notebooks*”, “*palmtops*”, te-

[2] Tecnologia da Informação.

lefones, terminais de fax e equipamentos de radiocomunicação), de propriedade do Exército, são colocados à disposição de seus integrantes – militares ou servidores civis – para uso exclusivo como ferramenta de trabalho (BRASIL, 2007a).

Figura 1: Diagrama da EBNet.
Fonte: Brasil (2004, p. 28).

Conforme pesquisa realizada pela empresa Módulo Security em 2007, 31% das organizações não sabem informar se sofreram ou não tentativas de invasão, das falhas de segurança registradas, 24% são causadas por funcionários da própria organização. Entretanto, o principal obstáculo para a implementação de medidas de segurança preventivas é a falta de conscientização de todos os usuários (55%), que mesmo possuindo bom conhecimento sobre as normas e legislação específicas (Figura 2), resistem em cumprí-las (MÓDULO SECURITY, 2007).

Todo tipo de serviço corporativo de rede de comunicações deve possuir processo de gerência, mecanismos de defesa e de auditabilidade, capazes de garantir o fiel cumprimento das regras de Segurança da Informação, o monitoramento e o registro dos eventos relativos ao funcionamento dos referidos serviços, destinados a garantir a integridade[3], a disponibilidade[4], a confidencialidade[5], e a autenticidade[6] da informação em todo o seu ciclo de vida(BRASIL,2001).

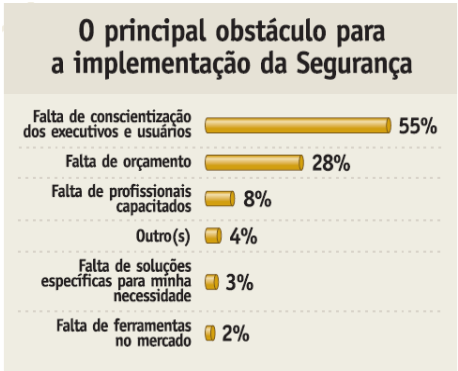

Figura 2 : Obstáculos para implementação da Segurança.
Fonte: Módulo (2007, p. 7).

[3] Garantia de que o conteúdo original da informação não foi modificado indevidamente.
[4] Garantia de que o conteúdo da informação estará disponível para quem tiver autorização para emprego.
[5] Garantia de que o conteúdo da informação só acessível e interpretável por quem possui autorização.
[6] Garantia de que o conteúdo da informação é verdadeiro, como também a fonte geradora da informação e o seu destinatário.

Para Sêmola (2003), **medidas de segurança** são práticas, procedimentos e mecanismos usados para proteger a informação, impedir que ameaças explorem vulnerabilidades e minimizar os riscos. Estas medidas possuem características preventivas, como *firewall;* detectáveis, como Sistema de Detecção de Intrusão (IDS); e corretivas.

A EBNet dispõe de um alto grau de conectividade que é oferecido por meio de uma ampla infra-estrutura de telecomunicações. Entretanto, esta mesma conectividade da qual pode-se dispor é um recurso que corre o risco de perceber comprometida em parte, ou mesmo na totalidade, a qualidade dos serviços que são oferecidos devido a vários tipos de ameaças, tais como ações de militares insatisfeitos, *hackers* e vírus (WEBER, 1997). Sendo assim, faz-se necessária a implantação, em cada OM ligada diretamente ao *backbone* da embratel, uma solução que assegure um elevado nível de segurança durante o uso dos benefícios oferecidos pela EBNet.

A falta de mecanismos que detectem tentativas de ataque contra servidores das OM interligadas pela EBNet dificulta a mensuração de acessos não autorizados aos recursos de TI das OM. Entende-se que quando uma tentativa de ataque obtém sucesso, causa um comprometimento bastante sério de dados, dos escassos recursos computacionais, e, talvez, até mesmo da reputação. Pode-se imaginar as conseqüências de um parecer publicado na *Internet* com informações sigilosas, por exemplo (CHAPMAN; ZWICKY, 1995).

Devido à estrutura de alcance nacional da EBNet, interligando uma grande quantidade de redes de computadores, a detecção, diagnóstico e correção de incidentes fica prejudicada pois grande parte dessas OM não possui pessoal e material especializados para este trabalho, colocando em risco a própria rede e a de outras OM. Cada instituição é como um elo, e a EBNet é como a corrente formada por esses elos, desse modo, deve-se assegurar que todas as OM tenham o mesmo nível de segurança, impedindo assim que toda a corrente seja comprometida pelo elo vulnerável.

Diante do problema exposto, através de uma pesquisa bibliográfica e da utilização de um laboratório de testes, este artigo propõe a implementação de uma solução de baixo custo, tendo em vista o escasso recurso principalmente destinado a informática nas OM, e baseada em Software Livre, em acordo com a Política de Migração para Software Livre do Exército Brasileiro,

que determina a adoção e substituição de softwares proprietários por livres principalmente em servidores (BRASIL, 2007b). A solução pode ser instalada nas OM sem qualquer necessidade de pessoal especializado, sendo gerenciada pelo CITEx e administrada dentro de cada RM por seus respectivos CT ou CTA, seguindo a mesma estrutura da EBNet.

2 Descrição do projeto

Em termos técnicos, a proposta de segurança consiste em instalar em cada OM conectada diretamente ao *backbone* da embratel, uma *Bridge* com *firewall*. Este mecanismo é encarregado de realizar as seguintes funções:

2.1 Segmentação da Rede

A *Bridge Firewall* deve dividir o cenário de cada sub-rede em três partes, assim designadas: rede externa, rede interna e DMZ[7] (CHAPMAN, 1995). A rede externa é composta por tudo o que não pertence à OM, ou seja, é a EBNet. A DMZ contém apenas algumas poucas máquinas com serviços que precisam estar acessíveis pela EBNet, e a rede interna é composta por equipamentos sem necessidade de estarem acessíveis pela EBNet (Figura 3).

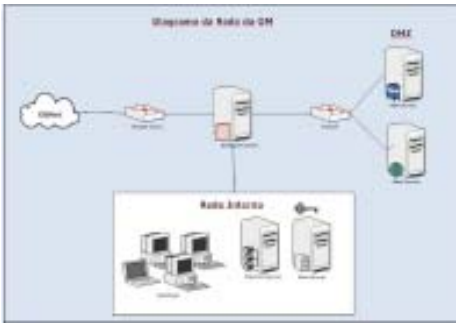

Figura 3: Diagrama da Rede da OM.
Fonte: Do autor.

2.2 *Firewall* do tipo *Bridge*

A implementação de um filtro de pacotes empregando a abordagem de uma bridge (TANENBAUM, 1999) permite-nos criar um *Firewall* do tipo "**caixa preta**", de existência imperceptível e de implantação bastante simples em qualquer ambiente (Figura 4). Isto pode ser feito com o ***OpenBSD,*** que de acordo com Freitas (2005) é um sistema operacional UNIX de código aberto, originalmente desenvolvido na Universidade da Califórnia em Berkley. Foi desenhado para ter uma capacidade de segurança e criptografia extremamente alta e para ser muito resistente a ataques. Um de seus grandes trunfos é a facilidade de implementar *bridges*. É considerado o

[7] Zona Desmilitarizada.

sistema operacional mais seguro do mundo e de acordo com os mantenedores do projeto apresentou: "Somente duas falhas remotas na instalação padrão em mais de 10 anos!" (OPENBSD, 2007).

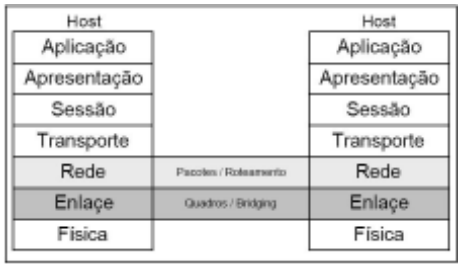

Figura 4: Router e Bridge no modelo ISO/OSI.
Fonte: Tanenbaum (1999, p. 99).

É possível implantar a solução sem a necessidade de qualquer reconfiguração nas máquinas da rede interna e da DMZ com relação ao endereço do *gateway default* (TANENBAUM, 1999). Também é possível estabelecer planos de contingência para falhas neste equipamento, pois não existe a necessidade de alteração na configuração dos equipamentos da rede local. O software utilizado para filtragem de pacotes baseia-se no *Packet Filter (PF)* do OpenBSD, um filtro de pacotes *statefull* (FREITAS, 2005).

2.3 Detecção de Intrusão

Com a utilização do Snort, ferramenta especializada em detecção das tentativas de ataque em rede (SNORT, 2007), é possível manter um banco de dados de todo o território nacional, com informações centralizadas contendo o registro completo de ocorrências deste tipo.

Esta tecnologia possui eficácia comprovada, uma vez que permite detectar inúmeras tentativas de ataque com origem na Internet ou na Intranet das OM contra serviços disponíveis na EBNet.

2.4 *Transparent proxy* para HTTP

O servidor *proxy* atua como procurador do cliente na navegação *Web*, intermediando a conexão entre as máquinas da OM e a EBNet. O emprego de *proxy* tem a grande vantagem de permitir o armazenamento local dos conteúdos mais freqüentemente utilizados, de maneira que quando algum conteúdo for acessado na EBNet, ele também estará disponível por algum tempo para o próximo requisitante desta mesma url (CHAPMAN, 1995). Desta maneira, quando um usuário acessa uma página que ficou armazenada no *proxy*, ele não apenas a recebe com uma velocidade muito superi-

or se comparada com o acesso normal como, também, reduz o tráfego nos canais de comunicação, uma vez que a largura de banda disponível pela EBNet ainda é restrita, propiciando uma utilização "enxuta", ou seja, economizando-se os canais de comunicação, otimizando a banda disponível para outros serviços, tais como envio de documentação oficial das OM ou aplicações corporativas como o envio do pagamento de pessoal.

2.5 Análise de tráfego

Com a instalação da solução, obtém-se um ponto de controle único em cada OM. É possível aos CT e CTA analisarem o tráfego das OM sobre sua administração. Por meio do emprego da ferramenta, pode-se realizar diagnósticos de problemas de tráfego, identificar gargalos de comunicação e, também, ataques do tipo negação de serviço. Para isto é utilizado o NTOP (*Network Traffic Probe*) (NTOP, 2007), que fornece praticamente as mesmas informações que poderiam ser obtidas por um agente de monitoração RMON[8].

2.6 Controle do uso da largura de banda

A largura de banda é um recurso computacional que determina o quanto pode existir de tráfego entre as OM e a EBNet. Pelo modelo *default*, todo o tráfego é tratado da mesma maneira - sem nenhuma distinção, não há Qualidade de Serviço (QOS). Em termos técnicos, por meio da *Bridge Firewall* é possível alterar a disciplina de filas empregada de FIFO[9] para CBQ[10]. No CBQ existe uma definição de classes com base em endereços de origem ou destino, número de portas, protocolos, etc. O PF do OpenBSD já inclui um sistema de gerenciamento de banda completo chamado ALTQ (OPENBSD, 2007).O uso desta ferramenta tem como objetivo realizar uma diferenciação do tráfego para que tarefas envolvendo aplicações corporativas possam ter prioridade, garantindo a qualidade do serviço mesmo quando a EBNet estiver sobrecarregada, garantindo também a reserva de largura de banda para projetos de escalabilidade da EBNet para aplicações como VOIP e

[8] Protocolo de Gerenciamento de Redes.
[9] Primeiro a chegar é o primeiro a ser atendido.
[10] Filas baseadas em classe de prioridade.

Videoconferência. Alterando a disciplina de filas por meio da *Bridge Firewall*, é possível implementar QOS de forma totalmente transparente aos usuários finais.

2.7 Atualizações automáticas

Manter um software sempre atualizado é a premissa número um na área de segurança de redes de computadores (WEBER, 1997). Isto se deve ao fato de que a maioria das vulnerabilidades dos *softwares* de rede é corrigida através de sua atualização. No entanto, o trabalho de se manter atualizado um enorme conjunto de sistemas instalados é uma tarefa hercúlea se realizada de forma manual e esta é a razão pela qual tantas redes são facilmente invadidas por *hackers*: seus gerentes não conseguem ter a agilidade requerida e suas redes ficam perigosamente expostas aos ataques.

3 Administração da solução

As tarefas de identificação dos prováveis problemas, avaliação do grau de seriedade dos mesmos, realização de testes e disponibilização de soluções pode ser feita apenas por um grupo pequeno - mas altamente especializado - de militares integrantes dos CT e CTA dentro das suas RM, e gerenciados pelo CITEx. Esta estrutura facilita o controle de segurança sobre os militares que lidam com essas informações, tendo em vista a sensibilidade das mesmas, para tanto, deve-se considerar na Política de Segurança destes centros, normas de seleção e o controle dos recursos humanos necessários. A vantagem de centralizar a administração e gerência da segurança, reflete uma menor equipe necessária, diminuindo em muito os pontos vulneráveis, e custos com treinamento, facilitando a organização, agilizando o trabalho e assegurando o nível do serviço oferecido.

4 Aspecto inovador

A abordagem do tipo *bridge com Firewall* (TANENBAUM, 1999) apresenta a vantagem de poder ser inserida em qualquer ambiente de um modo absolutamente invisível para o roteamento. Desta maneira, é possível criar um *Firewall* que pode ser utilizado em qualquer cenário. Se fosse utilizada uma abordagem convencional, onde o *Firewall é* o roteador (CHAPMAN, 1995), seria necessário fazer com que todas as máquinas clientes precisassem ter alteradas a referência do seu *gateway* padrão (TANENBAUM, 1999).

Além disso, a instalação da *Brid-*

ge Firewall faz com que exista apenas um único ponto de controle para o acesso à EBNet, o que facilita o gerenciamento e a contabilização de recursos pelas OM, pelos CT ou CTA e finalmente pelo CITEx (Figura 5). Por meio de ferramenta para detecção de intrusão, é possível mensurar a existência de ameaças contra o bom funcionamento do ambiente de rede, e, por este motivo, justifica-se a necessidade de manter cada cenário dividido em rede interna, DMZ e rede externa.

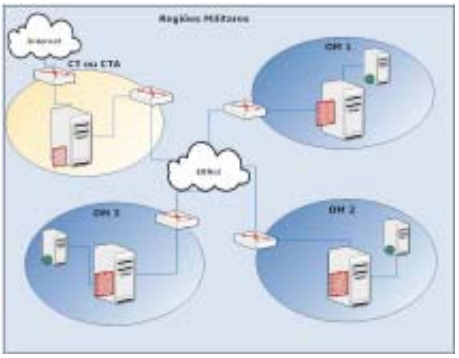

Figura 5: Saída única para a Internet.
Fonte: Do autor.

Com esta solução é possível obter informações centralizadas sobre o uso da rede em todo o país. É possível determinar tanto tentativas de ataque, como os serviços mais utilizados (entre navegação Web, emails e vários outros serviços EBNet disponíveis hoje e no futuro). Isto é algo necessário para a determinação dos perfis a serem traçados para o controle da largura de banda, descrito anteriormente, e o crescimento da EBNet como uma rede privada interligando todas as OM do EB.

5 Recursos Necessários

A solução proposta neste artigo possibilita o reaproveitamento de *hardwares* já existentes e considerados obsoletos. Em termos de capacidade de processamento, cada *Bridge Firewall* necessita de um PC usando sistema operacional OpenBSD 4.1, três placas de rede, disco rígido com pelo menos 2 Gb e memória de no mínimo 64 Mb. Complementando a configuração, são necessários os seguintes *softwares (open source)*:

- Detector de Intrusos **Snort**, versão 2.7;
- Servidor Proxy **Squid**, versão 2.6;
- Ferramenta de Análise de Tráfego **Ntop**, versão 3.3.

5.1 Regras do *Firewall*

De acordo com a ABNT (2002), foi utilizada a regra do menor privilégio, ou seja, tudo que não é devidamente liberado está negado. Com base

nesta organização (Figura 6), é possível controlar o fluxo através da *Bridge* em cada um dos sentidos indicados:

- EBNet ➡ DMZ: Liberado apenas para os serviços disponíveis da OM na EBNet, como servidor *Web, mail*, etc;
- EBNet ➡ Interno: Negado;
- Interno DMZ: Apenas para os serviços disponíveis;
- Interno ➡ EBNet: Apenas para os serviços disponíveis e conhecidos na EBNet, como SiRF, FAP, Web, mail, etc;
- DMZ ➡ Interno: Negado;
- DMZ ➡ EBNet: Negado.

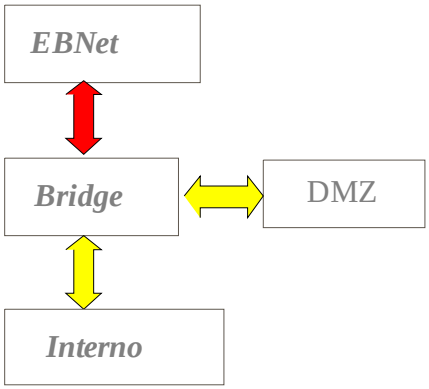

Figura 6 : Regras do Firewall.
Fonte: Do autor.

Para configurar o *Firewall* de acordo com a política adotada basta abrir o arquivo */etc/pf.conf*, adicionar as regras e ativar o *pf* depois de configurado. Isso implica em colocar as regras no ar e ativar a funcionalidade. Se já foi alterado o */etc/rc.conf* e foi reiniciada a máquina, não é necessário ativar novamente a funcionalidade.

5.2 Controle de Banda (QOS)

Desde o OpenBSD 3.0 a implementação de filas *Alternate Queueing* (ALTQ) se tornou parte do sistema base. Desde o OpenBSD 3.3 ALTQ foi integrado ao PF. A implementação ALTQ do OpenBSD suporta os organizadores *Class Based Queueing* (CBQ) e *Priority Queueing* (PRIQ). Ele também suporta *Random Early Detection* (RED) e *Explicit Congestion Notification* (ECN).

Alterando-se a disciplina de filas empregada de FIFO para CBQ, é possível aplicar um tratamento diferenciado para certos tipos de tráfego. Utilizando endereços IP e números de porta TCP/UDP, limitações podem ser impostas de maneira totalmente transparente para usuários finais. É possível fazer uma divisão que priorize determinadas aplicações. Para um link de 256 kbps, normalmente oferecido pela EBNet:

- Navegação www - 150 kbps;
- DNS - 2 Kbps;

- Email - 50 Kbps;
- Sistemas - 54 Kbps.

Havendo ociosidade, a largura de banda excedente em uma dessas classes pode ou não ser compartilhada com as demais.

5.3 *Ports e Packages*

A instalação e remoção de programas no OpenBSD é efetuada através do uso de uma das duas ferramentas, *Ports* ou *Packages* (LUCAS, 2003). Para o desenvolvimento deste projeto, foi adotado o *Ports*, por manter os programas atualizados na árvore CVS[11] do mantenedor do OpenBSD, e pela simplicidade de instalação, uma vez mantido o *Ports* sempre atualizado no sistema.

Após a instalação do sistema, deve ser montado o cdrom de instalação do OpenBSD 4.1, copiado o pacote *ports.tar.gz* para */usr* e descompactado. Uma vez instalado o *ports*, basta procurar o pacote que desejar no diretório */usr/ports* e processar a instalação de acordo com OpenBSD (2003).

5.4 Detector de Intrusos

Snort (SNORT, 2007) é um sistema detector de intrusos em redes (NIDS). Entre outras capacidades, ele pode ler um conjunto de regras e compará-las com o tráfego da rede. Quando um padrão é reconhecido, o programa registra a atividade suspeita e emite um alerta para o administrador, enviando e-mail e registrando em um banco de dados.

5.4.1 Evitando falsos positivos

Falsos positivos são alertas que mostram atividades legítimas e que confundem o administrador dos sistemas. Na maioria das vezes isto ocorre porque o Snort vem preparado para monitorar acesso a alguns scripts de teste de servidores *web*, ou URLs com um padrão suspeito, contendo a palavra "intranet" por exemplo.

O administrador deve realizar testes de acesso aos seus servidores enquanto implanta o *bridging firewall* para garantir que este não venha a bloquear usuários legítimos da rede. Isto pode ser feito observando-se todos

[11] Sistema de Controle de Versões.

arquivos de *log* envolvidos, como o do sistema operacional (/var/log/messages), do Snort (/var/log/snort/alert) e do Guardian (/var/log/snort/guardian).

5.5 Servidor Proxy

A configuração do Proxy transparente é implementada com o **Squid** em conjunto com o ***Packet Filter*** do OpenBSD. O Squid deve ser instalado a partir da árvore de Ports do OpenBSD, e em seguida configurado através do seu arquivo de configuração, localizado em */etc/squid/squid.conf*, este arquivo é melhor documentado em Wessels (2004).

Inicie o squid primeiramente com a opção -z para que sejam criados os diretórios de swap, para reconfigurar as regras após edição é necessário utilizar a opção -k:

Para que o *proxy* trabalhe de modo transparente, é necessário configurar o PF. A configuração do pf fica em */etc/pf.conf*.

5.6 Análise de Tráfego

O software NTOP, auxilia o diagnóstico de problemas na rede, permitindo a identificação de possíveis gargalos no funcionamento. Pode-se também, identificar serviços mais utilizados (TCP e UDP), *hosts* que mais utilizam a rede, tamanho médio de pacotes entre várias outras informações. A instalação pode ser feita pelo *Ports*.

O Ntop não é um software que possui arquivos de configurações editáveis. Alguns parâmetros podem ser setados pela interface web, mas a maioria deles são opções passadas pela linha de comando. No momento da inicialização, a utilização básica é bastante simples, e o acesso é feito através do navegador, acessando o *localhost* na porta 300 (NTOP, 2007).

6 Resultados

A partir da instalação do sistema nas OM pode-se ter como resultado a criação de um Banco de Dados Nacional contendo todos os incidentes de segurança envolvendo a EBNet, a partir de relatórios de atividades de tentativa de roubo de informação, ataques de negação de serviço e exploração de falhas na implementação dos *softwares* servidores. Estas informações podem ser consultadas por meio de uma ferramenta para visualização, o ACID (*Analysis Console for Intruder Detection*) (BEALE; CASWELL, 2004).

Em conjunto com o *Snort*, o *Guardian* pode ser utilizado eficazmente para bloquear as tentativas de

ataques automaticamente agindo nas regras do *Firewall*. Isto torna possível ações reativas em caso de intrusão e prevenção de ataques futuros.

Em cada OM aonde existe uma *Bridge Firewall* instalada, é possível fazer uma monitoração e gerência completas sobre o tráfego de rede por *host*, protocolo, etc. geradas pelo Ntop através de gráficos para interface *Web* (NTOP, 2007).

É possível fazer uma alocação da largura de banda de acordo com o perfil de tráfego em cada lugar, fazendo reservas para aplicações específicas.

7 Conclusão

O projeto *Bridge Firewall* é uma proposta de implantação de segurança e gerência da EBNet. Pode ser instalado em qualquer ambiente sem a necessidade de alterar as regras para roteamento ou o *Gateway* padrão nas máquinas clientes, pois atua de modo transparente, sem causar qualquer impacto no desempenho da rede durante sua instalação ou funcionamento.

O conhecimento e a utilização das ferramentas de auxílio na detecção e bloqueio de intrusos está se tornando um dos fatores críticos de sucesso no cumprimento da política de segurança da informação dentro das organizações, pois fornece recursos para investigar os pacotes de dados antes que estes atinjam os servidores, evitando na maioria das vezes, desde simples *port scannings* até os ataques mais comprometedores, como os *buffer overflows*.

A implementação dessa proposta, de simples instalação e de baixo investimento podem garantir que a EBNet e Intranet das OM tenham suas informações garantidas quanto à integridade, confidencialidade e disponibilidade, contribuindo assim para a preservação da imagem do EB perante toda a sociedade, e também para a soberania nacional, uma vez que todos os softwares utilizados tem código aberto, podendo ser auditados a qualquer momento.

Em acordo com o Sistema de Excelência do EB, através das ferramentas implementadas na solução, a OM e conseqüentemente o EB podem ter acesso a vários relatórios sobre os aspectos de segurança e gerenciamento de sua rede, tendo em mãos uma importante ferramenta para a tomada de decisão com vistas ao melhor direcionamento dos futuros investimentos relacionados com a EBNet. O projeto pode ser expandido com a implementação de um software que integre todos os relatórios das unidades da *Bridge Firewall* em um único

ambiente de administração, necessário para otimizar o gerenciamento pelo CT, CTA e CITEx.

Como recomendação para futuros trabalhos visando desenvolver um modelo completo de segurança da informação para a EBNet, com mecanismos, práticas e normas, é necessário o desenvolvimento de uma Política de Segurança orientada a resultados conforme preconiza a ABNT (2002), envolvendo a segurança em pessoas, processos e recursos, de forma que a **Informação** - recurso mais valioso de uma Organização - esteja sempre preservada.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **Tecnologia da Informação**: código de prática para a gestão da segurança da informação. NBR/ISO/IEC 17799. Rio de janeiro: 2002.

BEALE, J.; CASWELL, B. **Snort 2.1 Intrusion Detection.** Rockland, MA**:** Syngress Publishing, 2004.

BRASIL. Estado Maior do Exército. **Instruções Gerais de Segurança da Informação para o Exército Brasileiro** (IG 20-19)**.** Brasília: Gráfica do Exército, 2001.

_____. Secretaria de Tecnologia da Informação (STI). **EBNet –** Guia do Comandante. Brasília: Gráfica do Exército, 2004.

_____. Departamento de Ciência e Tecnologia (DCT). **Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército (NORTI).** 2.ed. Brasília, DF, 2007a.

_____. Departamento de Ciência e Tecnologia (DCT). **Plano de Migração para Software Livre no Exército Brasileiro.** 3.ed. Brasília, DF, 2007b.

CHAPMAN, D. B.; ZWICKY, E. D. **Building Internet Firewalls.** Sebastopol, CA: O'Reilly & Associates, 1995.

FREITAS, J. H. F. **OpenBSD:** Aspectos e Firewall. 2005. Dissertação (Mestrado em Processamento de Dados) – Faculdade de Tecnologia de Americana, Americana, 2005.

KURTZ, G.; MCCLURE, S.; SCAMBRAY, J. **Hackers Expostos** : Segredos e Soluções para a Segurança de Redes. 2. ed. São Paulo: Makron Books, 2001.

LUCAS, M. W. **Absolute OpenBSD:** Unix for the practical paranoid. San Francisco: No Starch Press, 2003.

MÓDULO SECURITY. **10ª Pesquisa Nacional de Segurança da Informação.** São Paulo**,** 2007.

NTOP – Network Traffic Probe. Disponível em: <http://www.ntop.org/ntop.html>. Acesso em: 25 jun. 2007.

OPENBSD – Free, Functional e Secure. Disponível em: <http://www.openbsd.org/pt/index.html>. Acesso em: 25 jun. 2007.

RITCHEY, R.; FREDERICK, K.; NORTHCUTT, S. **Desvendando Segurança em Redes.** Rio de Janeiro: Campus, 2002.

SÊMOLA, M. **Gestão da Segurança da Informação:** uma visão executiva. São Paulo: Campus, 2003.

SNORT – The Open Source Network Intrusion Detection System. Disponível em: <http://www.snort.org>. Acesso em: 25 jun. 2007.

TANENBAUM, A. S. **Redes de Computadores.** 3. ed. Rio de Janeiro: Campus, 1999.

WEBER, R. F. Segurança na Internet. **RITA – Revista de Informática Teórica e Aplicada.** Instituto de Informática. UFRGS, n. 2, p. 7-46, 1997.

WESSELS, D. **Squid:** the definitive guide. Sebastopol, CA: O'Reilly & Associates, 2004.