WHATWALL: UM SISTEMA PARA ANÁLISE ATIVA DO COMPORTAMENTO DE FIREWALLS

Ákio Nogueira Barbosa, Pedro Luís. P. Sanchez, Vonys B. Bernal
Departamento de Engenharia Eletrônica
Escola Politécnica da Universidade de São Paulo
05508-900 São Paulo - SP
{akio.barbosa, pedro.sanchez, volnys.bernal}@poli.usp.br

Adilson Eduardo Guelfi, Silvio L. Marangon
Departamento de Engenharia Eletrônica
Escola Politécnica da Universidade de São Paulo
05508-900 São Paulo - SP
{guelfi, marangon}@lsi.usp.br

RESUMO

Atualmente, as tecnologias de firewall representam elementos de segurança vitais aplicados na proteção do perímetro de um ambiente de rede. Entretanto, criar uma estrutura de proteção baseando-se nas tecnologias de firewall pode ser uma tarefa complexa devido a diversos fatores, como por exemplo, quantidade excessiva de regras de acesso, manutenção da base de regras, definição da topologia adequada etc. Portanto, após ser implementado, a análise da eficiência de um firewall torna-se igualmente importante para que seja possível verificar e avaliar se o cumprimento da política de segurança está sendo efetuado. O objetivo deste artigo é apresentar o sistema para análise ativa de firewalls chamado "WHATWALL", o qual se baseia na injeção e observação supervisionada de pacotes. Nesta fase, a análise ativa de regras de filtragem UDP se mostrou viável desde que sejam empregados mecanismos que minimizem o problema da explosão combinatória.

ABSTRACT

Currently, firewall technologies are vital security elements applied in the protection of network perimeters. However, the generation of a protection structure based on the firewall technologies could be a complex task due to several factors, for example, extreme amount of access rules, maintenance of the rule base, definition of the proper topology etc. Therefore, after firewall implementation, the analysis of its efficiency becomes equally important so that it is possible to verify and evaluate if the security policy is being followed. The goal of this paper is to present the system for active analysis of firewalls called "WHATWALL", which is based on the injection and visualization of monitored network packets. In this phase, the active analysis of UDP filtering rules it shows viability since that used mechanisms for minimize the combinatory explosion problem.

1. INTRODUÇÃO

Firewall é um conceito importante para proteção de perímetro em redes de computadores ou mesmo, atualmente, computadores individuais. É utilizado principalmente para controle de segurança entre as fronteiras das redes públicas e privadas ou ainda entre redes privadas (CHESWIK, 2005). Quando utilizado para controle de tráfego entre redes é geralmente inserido em pontos de concentração de forma a possibilitar a inspeção de todo o tráfego e, quando necessário, aplicar as restrições definidas em sua configuração.

A configuração do firewall é definida por um operador utilizando sua sintaxe específica. Tal configuração deve ser gerada baseada em uma política de restrição de tráfego definida em uma linguagem de alto nível pela organização.

Firewall é um termo genérico que é utilizado para identificar um conjunto de sistemas e equipamentos que atuam na restrição de tráfego e proteção de perímetro. Geralmente, um firewall pode incorporar diversas funcionalidades (ADI, K. et al, 2003; AL-TAWIL, 1999; PERMPOONTANALARP, 2001; STREBE, 2002), sendo que as principais são:

- Filtragem de pacotes: nas várias camadas de rede TCP/IP, tal funcionalidade, baseando-se em um conjunto de regras definidas, realiza o controle do tráfego por meio da interceptação e análise de pacotes de rede;
- NAT (*Network Address Tranlation*): funcionalidade que atua na tradução de endereços IP e portas. Exemplos: mascaramento e redirecionamento de portas;
- Proxy: representam entidades intermediárias que atuam na camada de aplicação, intermediando a comunicação entre os parceiros de forma transparente. Podem exisitr entidades genéricas de Proxy ou específicas para cada serviço ou protocolo de aplicação. Proxies agregam outras características de segurança importantes, tais como: autenticação de usuários e "proxy reverso";
- Módulo contra "SYN Floods": funcionalidade que permite proteção de servidores contra ataques de inundação de pacotes. Exemplo: "SYN Cookies";
- VPN (Virtual Private Network): funcionalidade que permite acesso remoto seguro ao firewall
- Módulo de Controle de Fragmentação: funcionalidade que permite proteção do ambiente de rede contra ataques de fragmentação maliciosa;
- Módulo contra "ICMP Redirect": funcionalidade que permite controlar o envio de mensagens do tipo "ICMP Redirect".

Basicamente, existem duas classes principais de firewalls: firewalls de rede e firewalls de aplicação. São denominados firewalls de rede aqueles que utilizam filtragem de pacotes. Por sua vez, os firewalls de aplicação controlam o conteúdo dos pacotes trafegados.

2. MOTIVAÇÃO

Conforme Adi et al. (2003) e Woll (2001) a análise do comportamento de um firewall é uma atividade complexa. Uma das grandes dificuldades encontradas nesta análise consiste em validar a configuração dos firewalls para que operem de maneira satisfatória, isto é, seguindo as restrições estabelecidas em uma dada política de segurança.

Portanto, baseando-se na política de segurança definida, os administradores de rede são responsáveis por configurar as regras de restrição de tráfego. Muitas vezes, algumas regras são bastante específicas de tal forma que não é trivial determinar com clareza a atuação efetiva dos firewalls (AL-SHAER, 2004).

Nos firewalls de rede, as configurações de regras de filtragem geralmente são baseadas nas informações presentes nos cabeçalhos dos protocolos IP, ICMP, UDP e TCP, como, por exemplo, endereço IP, porta, tipo de mensagem ICMP e tipo de protocolo. Estas regras de filtragem, dependendo do firewall, podem ser aplicadas nos pacotes recebidos por uma interface específica, enviados por uma interface específica, recebidos pelas interfaces, enviados pelas interfaces, encaminhados pelo elemento de roteamento, encaminhados à camada de aplicação ou recebidos da camada de aplicação. Além do posicionamento do ponto de análise dos pacotes variar a sintaxe utilizada por cada firewall também varia. Estes são alguns motivos que tornam a configuração e manutenção de firewall uma tarefa complexa (WOLL, 2004a).

Na grande maioria dos firewalls, as regras são sensíveis à ordem na qual aparecem. De maneira geral, quando um pacote é recebido pelo firewall, suas regras são analisadas sequencialmente, definindo a ação que deve ser tomada quando uma correspondência ocorre na base de regras. Por exemplo, usando a base apresentada na Tabela 1, ao receber um pacote da rede interna para acesso externo a um serviço HTTPS (fluxo de saída), o firewall faz a verificação perante sua primeira regra, não encontrando correspondência. Na seqüência, o firewall verifica o pacote recebido perante sua segunda regra, encontrando correspondência e, portanto, tomando a ação definida de permitir o encaminhamento do pacote.

Tabela 1 - Modelo de base de regras de um firewall

REGRA Nº	IP DE ORIGEM	PORTA ORIGEM	IP DE DESTINO	PORTA DESTINO	PROTOCOLO	DIREÇÃO	AÇÃO
1	10.0.161.12	>1023	143.107.254.71	110	TCP	saída	permitir
2	10.0.161.0/24	>1023	QUALQUER	443	TCP	saída	permitir
3	143.107.254.71	110	10.0.161.12	>1023	TCP	entrada	permitir
4	192.168.0.0/24	22	10.0.161.12	>1023	TCP	entrada	permitir
5	QUALQUER	80	10.0.161.12	>1023	TCP	entrada	permitir
6	143.107.254.73	143	10.0.161.12	>1023	TCP	entrada	permitir
N							

Assim, para cada regra verifica-se se o pacote satisfaz o critério definido na regra. Se for satisfeito é acionada a ação correspondente, não sendo mais necessário percorrer a base de regras. Caso contrário, a próxima regra é analisada, e assim sucessivamente até que seja definida a ação a ser tomada.

Quando as bases de regras são examinadas, observa-se que o procedimento de implementação destas bases, geralmente, conduz a erros de configuração (WOLL, 2004), que podem ser decorrentes principalmente pelos seguintes motivos:

- Redundância de regras;
- Quantidade excessiva de regras a serem implementadas que podem estar aplicadas em diferentes pontos (interface de entrada, interface de saída, encaminhamento, etc);
- A quantidade e complexidade de regras presentes quando da existência de diversos firewalls que atuam de forma cooperada;

Devido aos motivos citados anteriormente é possível perceber a complexidade da atividade de configuração e manutenção de firewalls. Consequentemente é possível que persistam brechas de segurança na configuração do firewall.

Freqüentemente existe a necessidade de se conhecer o comportamento efetivo do firewall, ou seja, quais são as funcionalidades ativas e que tipo de tráfego está sendo bloqueado por um firewall. Esta necessidade pode partir do próprio administrador de rede para certificar-se de uma configuração aplicada, da equipe de segurança ou da equipe de auditoria a respeito da aderência à política de segurança definida.

3. TÉCNICAS DE ANÁLISE

Existem algumas técnicas de análise de comportamento de firewalls (AL-TAWIL, 1999; BARTAL, 1999). As principais são:

a) Análise manual de regras:

Baseia-se em um agente humano para fazer a análise manual das regras existentes;

b) Análise automática de regras:

Baseia-se na análise da configuração do firewall por uma ferramenta. A configuração do firewall é submetida à ferramenta que deve ser capaz de entender sua sintaxe permitindo identificar e corrigir erros relativos à sintaxe, como também inconsistências entre as regras definidas, conforme Eronen (2001). Algumas destas ferramentas possibilitam também emitir "perguntas" a respeito das restrições definidas.

c) Análise ativa:

Baseia-se na análise por meio da injeção de pacotes e observação do tráfego resultante.

4. OBJETIVO

O principal objetivo deste trabalho é verificar a viabilidade de utilização de técnicas de análise ativa de firewalls. Para isto, foi proposto o sistema WHATWALL e, no âmbito deste sistema, serão realizadas algumas implementações para prova de conceito.

A abrangência da aplicação deste trabalho não está direcionada a descobrir ou apontar erros de sintaxe, confronto de regras e nem definir regras ou conjunto de regras. Portanto estão fora do escopo do sistema:

- Análise da qualidade da política de segurança;
- Confrontação das regras com a política de segurança;
- Análise das inconsistências de regras implementadas em um ou mais firewalls da rede;
- Definição das regras do firewall;
- Verificação e descoberta de problemas relativos a erros de sintaxe;

5. TRABALHOS RELACIONADOS

A aplicação de ferramentas automatizadas utilizadas em testes de firewalls na tentativa de se descobrir o comportamento destes é um assunto cada vez mais explorado e que tem despertado o interesse dos pesquisadores da área de segurança de redes de computadores. Este interesse pode ser justificado principalmente pelo grau de importância que o firewall representa para a proteção dos sistemas de redes de computadores.

Problemas como o alto índice de erros de implementações que ocorrem na configuração de firewalls (WOLL, 2004a), devido às dificuldades encontradas em implementar a política de segurança escrita em uma linguagem de alto nível utilizando uma linguagem de baixo nível, procedimentos/ técnicas de testes eficientes são alguns dos motivos que reforçam a necessidade do aprimoramento das funcionalidades das ferramentas e técnicas de testes existentes.

Gutman (1997) apresenta um sistema, que utiliza uma linguagem simples (lisp-like) para expressar as políticas globais de controle de acesso a serem implementadas no firewall. Com isso procura facilitar a conversão da política de segurança para as regras de firewall utilizando dois algoritmos. O primeiro, dada a topologia de rede, irá gerar um conjunto de regras para o firewall. O segundo algoritmo compara o conjunto de regras geradas com a política de controle de acesso global para determinar todas as violações de política, ou para informar que não existe nenhuma.

A implementação demonstra que os algoritmos são eficientes para responder rapidamente questões em escala realística.

apresenta um sistema, que utiliza uma linguagem própria (lisp-like) para expressar as políticas globais de controle de acesso para serem implementadas nos firewalls. Com isso procura facilitar a conversão da política de segurança para as regras de firewall. Esse sistema possui duas funcionalidades. A primeira, dada a topologia da rede e a política de restrição escritas na linguagem de descrição utilizada (lisp-like) o sistema gera automaticamente as regras para o firewall assegurando, dessa forma, a correta implementação da política de segurança. A segunda possibilita realizar a comparação do resultado do conjunto de regras geradas com a política global de controle de acesso (política de segurança) para determinar se existem violações ou reportar que não existem violações.

Bartal (1999) propõe o sistema FIRMATO (Firewall Management Toolkit), um sistema passivo (não intrusivo) de análise que consiste em um conjunto de ferramentas para gerenciamento de firewalls. Este conjunto de ferramentas possui módulos específicos para interagir com diferentes firewalls .

Os objetivos do sistema podem ser resumidos em:

(a) Ser uma ferramenta capaz de separar a política de segurança das especificidades de cada fabricante de firewall, permitindo assim ao administrador de segurança focar no projeto e política de segurança apropriada sem preocupar-se com a complexidade, ordenação e outras questões de configuração de regras de firewalls;

(b) Poder separar o projeto de política de segurança da topologia da rede em questão, permitindo ao administrador manter a consistência da política em face das alterações de topologia da rede. Esta separação também possibilita ao administrador reutilizar uma política semelhante em múltiplas organizações com diferentes topologias de rede;

(c) Ter capacidade de gerar arquivos de configuração de firewall automaticamente a partir da política de segurança, reduzindo a probabilidade de introduzir brechas de segurança causadas por erros difíceis de descobrir em arquivos de configuração.

Para alcançar estes objetivos o sistema implementa:

(a) Um modelo entidade-relacionamento, que provê uma estrutura para representação tanto da política de segurança quanto da topologia de rede;

(b) Uma Linguagem de Definição de Modelo (MDL) utilizada para definir instâncias de um modelo de entidade-relacionamento e o analisador (parser) associado;

(c) Um compilador de modelos para que traduz uma instância de modelo em arquivos de configuração específicos para cada firewall. O conjunto de tais arquivos inclui informações sobre a topologia e base de regras;

(d) Um visualizador de regras, que transforma arquivos de configurações específicos ao firewall em uma representação gráfica da política e topologia atual. Tal visualização permite uma rápida e prévia avaliação da viabilidade do emprego de uma política escolhida;

Mayer (2000) ratifica os problemas da dificuldade de configurar, manter e testar firewalls, principalmente quando da presença de mais de um firewall de diferentes fabricantes. Para mitigar algumas destas dificuldades propõe o sistema FANG (*Firewall Analysis Engine*), um sistema para análise de firewalls que permite realizar sua análise a partir da observação de seu estado de configuração. Utiliza também uma descrição mínima da topologia de rede.

O sistema interage com o usuário formulando perguntas, em um nível de abstração mais alto que o das regras do firewall. Além disso, o sistema pode ser usado antes que uma política seja de fato empregada.

Os principais objetivos do sistema FANG são:

(a) Usar um nível adequado de abstração: o administrador deverá ser capaz de interagir com o sistema em um nível no qual a política de segurança é definida ou expressa;

(b) Possibilitar realizar análise sem que a configuração utilizada atualmente seja alterada, evitando que esta se torne vulnerável no momento de teste de uma configuração;

(c) Ser passivo: a análise de política não deve envolver o envio de pacotes;

(d) Ser atualizado: a análise deve refletir com precisão a política que é efetivamente aplicada no momento (ou que está a ponto de ser aplicada), e não uma descrição desatualizada disso;

(e) Ser eficiente: o tempo requerido para executar os testes comuns não deve depender do número de máquinas da rede. Deve depender somente da complexidade da topologia, e do número de regras nas várias bases-de-regras;

(f) Ser de fácil utilização: A interface de uso interativo deve permitir executar os testes com alguns cliques de mouse.

Para satisfazer esses objetivos, o sistema FANG coleta e lê os arquivos de configuração relevantes, e constrói uma representação interna da política e topologia da rede. O sistema possui uma interface gráfica na qual o usuário formula perguntas ao sistema. Dada uma questão, o sistema FANG simula o comportamento do firewall, levando em consideração a topologia da rede e disponibiliza a resposta para o usuário.

FANG também pode considerar regras do firewall que executam tradução de endereço de rede NAT (*Network Address Tranlation*).

O software foi desenvolvido como um módulo do conjunto de ferramentas de gerenciamento de firewall FIRMATO (BARTAL, 1999) e utiliza algumas das técnicas de modelamento. Porém, isso pode ser usado independentemente dos outros componentes do conjunto de ferramentas.

A linguagem que o autor utiliza para descrever a topologia é um subconjunto da linguagem MDL do sistema FIRMATO. Eventos como substituição ou adição de um novo dispositivo de rede não invalida o arquivo de topologia existente. Deste modo, espera-se que a escrita ou atualização do arquivo de topologia seja um evento raro.

Woll (2001) apresenta o LFA (*Lumeta Firewall Analyser*), que teve como ponto de partida o sistema FANG (MAYER, 2000). De acordo com o autor, o analisador LFA melhora o sistema FANG em muitos aspectos. Os avanços mais significativos são na iteração humana, resolvendo um importante problema encontrado no uso do sistema FANG cuja utilidade efetiva dependia do usuário saber formular questões úteis para análise (muitas vezes os usuários do sistema não sabiam o que perguntar).

O sistema LFA tem como entrada a tabela de roteamento e arquivos de configuração do firewall. A ferramenta analisa esses dados de baixo nível, e simula o comportamento do firewall contra todos os pacotes que são possíveis de receber. A simulação é realizada completamente off-line, sem enviar nenhum pacote. O administrador recebe um relatório do tráfego que é permitido. O relatório do sistema LFA é apresentado como um conjunto de páginas web, que são ricos em enlaces e referências cruzadas para detalhes adicionais.

O usuário não precisa mais escrever o arquivo de conectividade do firewall. LFA possui um novo módulo que possibilita, a partir da tabela de roteamento criar automaticamente a informação topológica da rede, que é descrita utilizando a linguagem MDL.

LFA abrange um maior número de fabricantes de firewalls. Para este propósito, o sistema LFA usa uma linguagem de configuração intermediária, para a qual é possível converter a configuração de vários fabricantes.

Verma (2005) apresenta o Sistema FACE (*Firewall Analysis and Configuration Engine*), uma ferramenta que ajuda na configuração e análise de firewalls distribuídos. Ao usar o sistema FACE, os administradores de sistema podem automaticamente gerar e analisar configurações para os firewalls da rede, especificando a política de filtragem e o

modelo de ameaça para o qual o firewall deve oferecer defesa.

6. PRINCIPAIS PROBLEMAS

Nas técnicas mencionadas anteriormente é possível identificar alguns aspectos negativos, como por exemplo:

(a) Análise manual das regras: é possível a ocorrência de erros por falhas humanas. Podendo permanecer problemas tais como: redundâncias de regras, erros de sintaxe e parâmetros devidos à quantidade elevada de regras ou bases de regras, inconsistências entre bases de regras;

(b) Análise automática de regras: Necessidade de um módulo de adaptação para cada tipo de firewall existente, devido a diferentes sintaxes utilizadas. Não permite executar análises relacionadas à exaustão de recursos;

(c) Análise ativa: Para alguns tipos de análise como, por exemplo, determinação de datagramas IP filtrados existe o problema da explosão combinatória. Além disso, é necessário equipamentos adicionais que possibilitem a conexão dos agentes de análise aos segmentos de rede conectados ao firewall para possibilitar a injeção e observação do tráfego.

6.1 O problema da explosão combinatória

Para realização de um teste completo, pode ocorrer uma explosão combinatória, o que pode inviabilizar a análise, devido a quantidade excessiva de datagramas IPs gerados.

Para exemplificar o problema da explosão combinatória, considere a geração de datagramas IPs para todas as combinações possíveis de endereços IPs de origem, endereços IPs de destino, tipos de protocolo, portas de origem e portas de destino. Neste caso existem 2^{104} combinações possíveis, sendo:

Endereço IP de origem: 2^{32}
Endereço IP de destino: 2^{32}
Porta TCP de origem: 2^{16}
Porta TCP de destino: 2^{16}
Protocolos: 2^{8}

Observando que o valor 2^{104} é apenas para uma interface. A análise também pode ser efetuada nas outras interfaces.

7. O SISTEMA WHATWALL

Para verificar a viabilidade da análise ativa de firewalls foi proposto o sistema WHATWALL cuja arquitetura geral está apresentada na Figura 1. Estão sendo desenvolvidos alguns módulos do sistema como prova de conceito.

O sistema WHATWALL é composto por um controlador e diversos agentes. O controlador é o

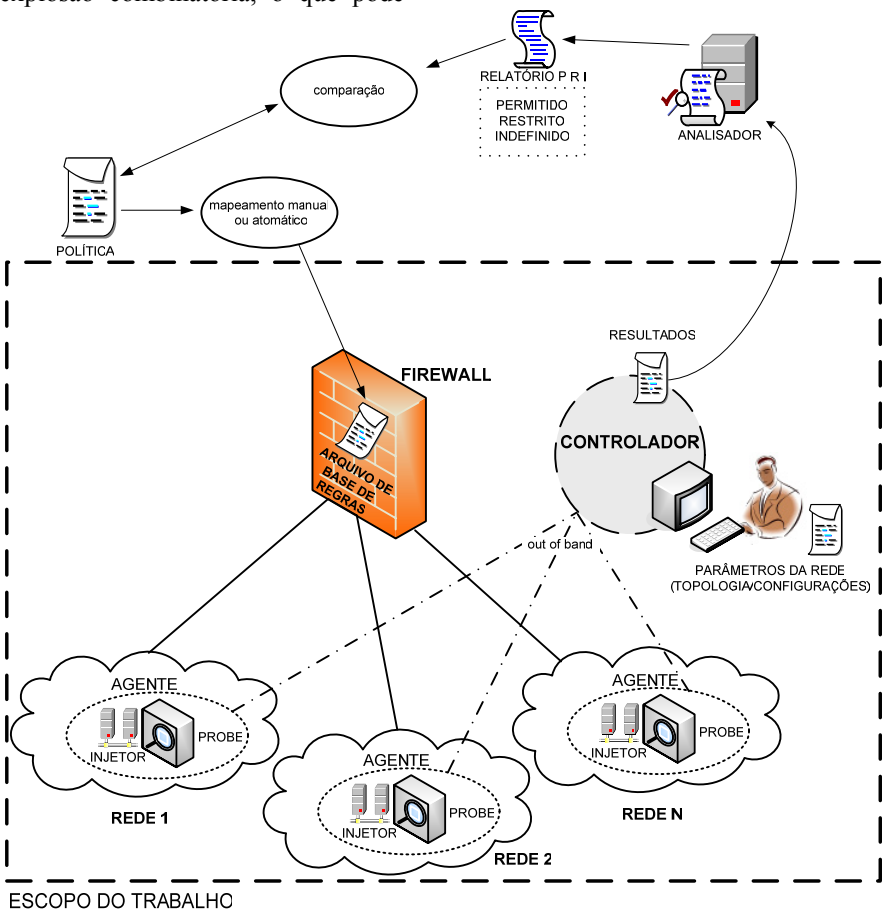

Fig. 1 – Arquitetura geral do sistema WHATWALL.

núcleo do sistema, interagindo com o usuário e os diversos agentes existentes. Deve existir um agente associado à cada interface de rede do firewall. A comunicação entre agente e controlador deve ser *out of band*, ou seja, utilizando um meio de comunicação alternativo.

7.1 Controlador

O Controlador é responsável por selecionar quais testes serão realizados a cada momento e interagir com os agentes seja para disparar uma análise, seja para coletar os resultados.

O Controlador é também responsável pela interface com o usuário para entrada de informações a respeito da topologia da rede e, também, de algumas "dicas" a respeito das configurações do firewall. Estas "dicas" tem por objetivo identificar faixas de IPs e portas que possuam tratamento específico de forma que seja possível reduzir o número de pacotes necessários em algumas análises.

Ao final do processo cabe ao controlador consolidar os resultados e apresentá-los ao usuário.

7.2 Agente

O agente é responsável pela condução das análises, seja injetando pacotes, seja observando o resultado nas interfaces do firewall.

O agente é composto por diversos módulos. Estes módulos podem ser classificados em injetores ou probes.

7.2.1 Módulos Injetores

Os módulos injetores são responsáveis pela geração de pacotes direcionados ao firewall. Existem diversos módulos injetores, cada um responsável pela realização de um determinado tipo de análise. A atuação de qualquer um dos módulos injetores é direcionada pelo módulo controlador.

7.2.2 Módulos Probes

Os módulos probes são responsáveis pela captura e registro (log) dos pacotes observados, para análise futura. Todos os pacotes observados são repassados, posteriormente, ao módulo controlador.

7.3Prova de Conceito

Como prova de conceito foram escolhidas duas análises para implementação. Uma para determinação dos datagramas UDP filtrados e outra para análise dos mecanismos de proteção contra SYN flood implementados.

7.3.1Módulo Probe Genérico

O módulo probe genérico é responsável pela observação dos pacotes em um determinado enlace de comunicação e seu registro (log) para futuro encaminhamento ao controlador.

Além disso, o módulo probe genérico é responsável por responder às requisições "ARP request" associadas a endereços IPs inexistentes na subrede na qual está inserido. Para isto, no momento em que é ativado inicia um processo de descoberta de equipamentos baseado no envio de requisições "ARP request". Exemplos de módulos injetores são:

- Espião ICMP: filtragem de datagramas ICMP;
- Espião UDP: filtragem de datagramas UDP;
- Espião TCP: filtragem de segmentos TCP;
- SYN Flood: resistência contra ataques *SYN Flood*;
- Source routing: filtragem de datagramas IP *source routing*;
- Fragmentação: controle e resistência a ataques de fragmentação;
- ICMP direct broadcast: filtragem de datagramas ICMP direcionados para endereços broadcast;

Destes, alguns módulos injetores foram selecionados para implementação na prova de conceito e estão detalhados a seguir.

7.3.2 Módulo Injetor Espião UDP

O módulo injetor Espião UDP é responsável pela injeção de datagramas UDP para determinação daqueles que são filtrados pelo firewall.

7.3.3 Módulo Injetor SYN Flood

A principal função do Injetor SYN Flood é realizar análises de resistência do firewall a ataques de inundação de segmentos TCP SYN. São realizadas duas análises:

(a) *SYN Flood protection*: Utilizada para verificar se o firewall implementa alguma técnica de proteção contra SYN Flood (SYN Cookies ou SYN protection);

(b) *SYN Flood resistence*: Utilizada para verificar se a implementação desta proteção não causa degradação de funcionalidades do próprio firewall em uma situação de ataque.

A análise *SYN Flood protection* são enviados 3 segmentos TCP com o flag SYN ativo para uma porta TCP aberta de um equipamento localizado após o firewall.

A análise *SYN Flood resistence* procura verificar se o firewall é susceptível a exaustão de recursos quando da implementação de algum mecanismo contra ataque a SYN Flood. O método utilizado é:

Repetir:
/* inundação*/
Repetir N vezes
Enviar segmento TCP com flag SYN ativo na taxa máxima possível

/* análise do impacto em conexões legítimas */
Repetir 3 vezes
Estabelecimento de conexão TCP legítima

8. IMPLEMENTAÇÃO E TESTES

Como prova de conceito foram implementados os seguintes módulos: probe genérico, injetorUDP e injetor SYN Flood. Para geração dos datagramas IP pelos injetores foi utilizando a biblioteca socket BSD que "formata" os pacotes e os envia através da interface sockets raw. O probe genérico captura os datagramas IP. Para isto, utiliza a biblioteca pcap (Tcpdump, 2005). Ambos também geram um arquivo de registro dos pacotes transmitidos e recebidos.

Os equipamentos utilizados no ambiente de teste foram, conforme representado na Figura 2:

- 3 servidores Xeon Dual processor (2.4GHz, hyperthread off, 1GBde memória, 1 HD 30GB SCSI, Kernel Linux 2.6.x) contendo interfaces de rede Gigabit Ethernet;
- 1 Switches Gigabit Ethernet.

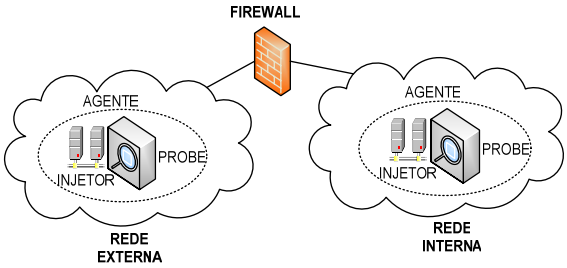

Fig.2 – Ambiente de Testes.

9. CALIBRAÇÃO

Alguns testes, antes de serem realizados, necessitam de uma fase de calibração. O objetivo da calibração é possibilitar que o teste seja efetuado na taxa máxima aceitável sem que sejam perdidos pacotes devido à exaustão de recursos.

Particularmente os módulos Espião ICMP, Espião UDP e Espião TCP necessitam de uma fase de calibração antes da execução dos testes.

Foram realizados testes com envio de pacotes sem intervalo de transmissão entre os pacotes, variando o número de pacotes nos testes de 10.000 a 300.000 pacotes e as portas UDP de origem e destino de 1025 a 65535. Com esta variação no número de pacotes pretende-se verificar a influência da memória disponível do sistema ou de algum outro fator na sua capacidade de transmissão de pacotes. Todos os testes foram repetidos 5 vezes, o que resultou em um total de 30 testes realizados. Os pacotes UDP gerados para os testes não continham dados, sendo compostos apenas pelo cabeçalho IP e UDP, tendo um tamanho de apenas 28 bytes.

Foi observado que não ocorreu perda de pacotes, não sendo necessário impor intervalo de tempo entre o envio dos pacotes.

Neste teste foi obtida uma taxa média de transmissão (média aritmética) de 21.517 pacotes/s com desvio padrão da taxa de transmissão é de 199,72 pacotes/s, o que corresponde à 0,78% da taxa média de transmissão. A Tabela 1 apresenta os resultados dos testes de calibração.

Tabela 1: Resultados dos testes de calibração

Pacotes transmitidos	Duração (s)	Taxa de transmissão (pacotes/s)
10.000	0,462412	21.625
50.000	2,330732	21.452
100.000	4,665658	21.433
150.000	6,862468	21.858
200.000	9,320084	21.439
300.000	14,098549	21.278

10. RESULTADOS

Foram realizados alguns testes com análise de filtragem UDP (Espião UDP). Em uma das análises a topologia consistia de um firewall interligando uma rede protegida à Internet. A faixa da rede protegida consistia em uma Classe C. No conjunto de regras do firewall não continha referência a endereços IPs ou portas externas específicas. Assim, na análise das restrições de comunicação da Internet para a rede protegida o Injetor UDP gerou pacotes variando o endereço IP destino (de 192.168.25.0 a 192.168.25.244) e a porta UDP destino (de 1 a 65535). O endereço de origem e a porta UDP de origem foi mantida fixa. Isto representa 2^{25} pacotes (2^8 end. IP destino, 2^{16} portas UDP, 1 retransmissão). A duração do teste foi de 1.400 s em uma taxa média de 23.967 pacotes/s.

A análise dos registros gerados correspondeu às regras definidas no firewall.

O principal problema na análise ativa está relacionado aos testes do tipo espião. Nesta classe de análise é necessária a utilização de técnicas que minimizem a explosão combinatória decorrente.

11. CONCLUSÃO

Foi apresentada uma arquitetura para análise ativa de firewalls de rede e alguns módulos desta arquitetura foram implementados para verificação da viabilidade de uso desta técnica. A técnica apresentou-se viável desde que sejam adotadas técnicas para minimização do espaço de análise.

Existem diversos desafios para um uso efetivo da análise ativa principalmente o problema da explosão combinatória na análise de filtragem de datagramas IP.

A principal vantagem desta técnica é a possibilidade de sua utilização para qualquer tipo de firewall de rede sem que seja necessário implementar módulos adaptadores para firewalls

específicos. As técnicas baseadas em análise de estado de configuração necessitam de adaptadores para cada modelo específico.

12. TRABALHOS FUTUROS

Existem diversas atividades que estão sendo conduzidas como a implementação de outros módulos injetores (para outros tipos de análises) e módulos de consolidação dos resultados das análises. Porém, o principal trabalho consiste no estudo e implementação de técnicas para minimização da explosão combinatória.

Conforme pode ser observado na Figura 1, alguns módulos externos ao sistema auxiliariam em outras tarefas, como por exemplo, o módulo de comparação, que recebe os resultados do sistema WHATWALL e os compara com a política de segurança definida pela corporação.

REFERÊNCIAS BIBLIOGRÁFICAS

ADI, K. et al. Evaluation of current research in firewall analysis. Disponível em: <http://lotos.site.uottawa.ca/ftp/pub/Lotos/TechRep/Department of National Defense.2003>. Acesso em: 3 ago 2003.

AL-SHAER, E.S.; HAMED, H.H. Modeling and management of firewall policies. eTransactions on Network and Service Management, v. 1, n. 1, Apr. 2004b. Disponível em: <http://www.comsoc.org/livepubs/etn/public/2004/apr/index.html>. Acesso em: 2 set 2004.

AL-TAWIL, K.; AL-KALTHAM, I.A. Evaluation and testing of internet firewalls. International Journal of Network Management, New York, v. 9, n. 3, p. 135-149, May/June 1999.

BARTAL, Y. et al. Firmato: a novel firewall management toolkit. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, Oakland, 1999. Proceedings. Los Alamitos: IEEE Computer Society, 1999. p. 17-31.

CHECK POINT Software Technologies Ltd. Check Point firewall-1: guide. 2001. Disponível em: <http://www.checkpoint.com/support/technical/documents/docs-5.0/firewall_ng_sp0.pdf>. Acesso em: 02 jan 2004.

CHESWICK, W.R.; BELOVIN, S.M.; RUBIN, A.D. Firewalls e segurança na Internet: repelindo o hacker ardiloso. 2.ed. Porto Alegre: Bookman, 2005. 400 p.

CISCO SYSTEMS. IOS firewall. [2002]. Disponível em: <http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_white_paper0900aecd8029d0a6.shtml>. Acesso em: 10 out 2004.

ERONEN, P.; ZITTING, J. An expert system for analyzing firewall rules. In: NORDIC WORKSHOP ON SECURE IT SYSTEMS, 6., Copenhagen, 2001. Proceedings: NordSec 2001. Helsinki: Nixu, 2001. p. 100–107. (Technical University of Denmark. Technical Report, IMM-TR-2001-14). Disponível em: <http:\\citeseer.ist.psu.edu/eronen01expert.html>. Acesso em: 3 Jan. 2003.

GUTMAN, J.D. Filtering postures: local enforcement for global policies. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, Oakland, 1997. Proceedings. Los Alamitos: IEEE Computer Society, 1997. p. 120-129.

LUCENT TECHNOLOGIES. Managed firewall. 1998. Disponível em: <http://www.lucent.com/press/0398/980316.nsb.html>. Acesso em 03 jan 2003.

MAYER, A.; WOOL, A.; ZISKIND, E. Fang: a firewall analysis engine In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, Berkeley, CA, 2000. Proceedings: S&P 2000. Los Alamitos: IEEE Computer Society, 2000. p. 177-187.

PERMPOONTANALARP, Y.; RUJIMETHABHAS, C. A unified methodology for verification and synthesis of firewall configurations. In: INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATIONS SECURITY, 3., Xian, China, 2001. Proceedings: ICICS 2001. Berlin: Springer, 2001. p. 328-339. (Lecture Notes in Computer Science, 2229).

STREBE, M.; PERKINS, C. Firewalls 24 seven. São Paulo: Makron Books, 2002. 411 p.

SUN MICROSYSTEMS. SunScreen3.1 Lite. [2002]. Disponível em: <http://www.sun.com/software/securenet/lite/>. Acesso em: 4 jan. 2004.

URIBE, T.E.; CHEUNG S. Automatic analysis of firewall and network intrusion detection system configurations. In: ACM WORKSHOP ON FORMAL METHODS IN SECURITY ENGINEERING, Washington, 2004. Proceedings: FMSE'04. New York: ACM, 2004. p. 66-74.

VERMA, P.; Prakash, A. FACE: a firewall analysis and configuration engine. In: 2005 SYMPOSIUM ON APPLICATIONS AND THE INTERNET, Trento, 2005. Proceedings: SAINT

2005. Los Alamitos: IEEE Computer Society, 2005. p. 74-81.

WOLL, A. Architecting the Lumeta firewall analyzer. In: USENIX SECURITY SYMPOSIUM, 10., Washington, DC, 2001. Proceedings. Berkeley: USENIX, 2001. Disponível em: <www.usenix.org/events/sec01/full_papers/wool/wool.pdf>. Acesso em: 14 set. 2004.

WOLL, A. A quantitative study of firewall configuration errors. Computer, New York, v. 37, n. 6, p. 62-67, June 2004a.