Uma Metodologia para Verificação de Filtros de Pacotes

André Luís Fávero, Raul Fernando Weber

Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brasil
{alfavero,weber}@inf.ufrgs.br

Abstract. *This paper describes a methodology for coherence verification in packet filters. For this purpose, each pair of filtering rules are compared, looking for errors, partial or total redundancy, or for situations that should be further analyzed (warnings). The proposed methodology can be used not only in a single filter but also in hierarchically distributed filters. Stateless and stateful filters are also considered into the verification process.*

Resumo. *Este artigo descreve uma proposta de metodologia para verificação de incoerências em regras de filtros de pacotes. Para tanto, as regras são comparados duas a duas, procurando-se por erros, redundâncias totais ou parciais ou por situações que devem ser analisadas (avisos). A metodologia pode ser utilizada tanto em um único filtro como em filtros hierarquicamente distribuídos. O aspecto do filtro operar com ou sem informação de estado também é considerado.*

1. Introdução e Objetivos

A necessidade de garantir a segurança das informações e da rede como um todo, tem impulsionado o uso de mecanismos que vão ao encontro destes requisitos. Os mecanismos de firewall, definidos como qualquer dispositivo, software, arranjo ou equipamento que limitam o acesso à rede [Cheswick, Bellovin, Rubin, 2005], são considerados atualmente fundamentais e estão presentes na maioria das redes de computadores, efetuando a função de regular o tráfego entre redes distintas.

Tipicamente, filtros de pacotes são formados por um conjunto de regras que descrevem uma determinada condição a ser a avaliada e na ocorrência desta, uma ação, também descrita para cada regra, deve ser efetuada. Na grande maioria dos filtros, a verificação ocorre conforme o ordenamento das regras e caso a condição seja satisfeita as demais regras subseqüentes são ignoradas. Não sendo satisfeita a condição de uma regra, passa-se para avaliação da próxima regra, até o fim da lista de regras. Se nenhuma regra tiver suas condições satisfeitas, aplica-se sobre o pacote a política de segurança default [Northcutt, 2002].

Apesar de ser uma tecnologia bem estabelecida e realmente usada em grande escala, os filtros não realizam nenhuma verificação na semântica das regras que o administrador define. Com isso as regras podem ser descritas de forma errônea, o que acaba alterando a política realmente implementada pelo filtro. A complexidade de fatores que deve-se ter conhecimento para a construção das tabela de regras, juntamente com complexidade na topologia da estrutura que se pretende controlar, manutenções rotineiras para adicionar ou limitar novos serviços e ainda complexidades causadas por um grande número de regras do filtro são os itens que tornam a tarefa de administração de filtros extremamente difícil e passível de erros, podendo acarretar problemas como

perda de disponibilidade de algum serviço, ou, pior, a falsa sensação de segurança causadas pela existência de um filtro que esta comprometido por um conjunto incoerente de regras.

Objetivando avaliar a coerência das regras algumas metodologias tem sido propostas. O uso de projetos diversitários, por exemplo, onde diferentes equipes definem o que consideram o conjunto ideal de regras para a política definida e, após a conclusão, os projetos são comparados em busca de discrepâncias[Liu, Gouda, 2004]. Outros trabalhos são mais específicos na automatização do método para a checagem. O Modelo de Wang propõe uma abordagem que identifica correlações entre regras. A existência destas são abordadas como conflitos. Não indicam a existência de um erro propriamente dito [Wang, Hao, Lee, 2003], mas apontam regras a serem melhor avaliadas. Interessante também é o modelo de Al-shaer, que define uma classificação de anomalias mediante uma tabela de relações entre as regras. Considera que para o bom funcionamento do filtro, estas anomalias deverão ser detectadas e informadas ao administrador. Cabe a este a análise e possível resolução [Al-shaer, Hamed, 2003].

Os modelos de Al-shaer e Wang efetuam as verificações, mediante a comparação de pares de regras nas quais são limitados os campos possíveis para a formação da condição (*protocol type, source IP address, source port, destination IP address and destination port*). Independente de comparação dos modelos, cabe salientar que a limitação de uso dos campos anteriormente citados torna os modelos inadequados para filtros do tipo *statefull*, [Northcutt, 2002] que consideram estados de conexão.

O objetivo deste trabalho é verificar a coerência das regras de filtragem mediante uma metodologia de análise destas. A etapa de análise deverá ser implementada de forma automática através de uma ferramenta de verificação que, com base na metodologia, deve apontar regras errôneas.

2. Modelo de Falhas

O modelo de falhas tratado pela metodologia corresponde a identificação de regras consideradas erradas (erros), que na prática nunca serão ativadas, e regras de alguma forma relacionadas e que potencialmente podem levar a situações errôneas (avisos), a decisão neste caso cabe ao administrador.

A metodologia pretende apontar situações anômalas através da comparação de pares de regras. Sempre que existir intersecção nas condições de duas regras, poderá existir uma incoerência. Para definir o tipo de incoerência algumas relações entre regras precisam ser estabelecidas. Considerando a comparação de duas regras, podem ocorrer as seguintes situações:

- Iguais: todos os campos correspondentes das duas regras possuem valores iguais;
- Superconjunto: As regras não são iguais e todos os campos de uma das regras são iguais ou superconjuntos do campo correspondente da outra regra;
- Subconjunto: As regras não são iguais e todos os campos de uma das regras são iguais ou são subconjuntos do campo correspondente da outra regra;
- Correlação: As regras são correlacionadas quando não forem iguais, superconjunto ou subconjunto e todos os campos da primeira regra são iguais, subconjunto ou superconjunto aos campos correspondentes da segunda regra.
- Relação Parcial: As regras são parcialmente relacionadas quando existir pelo menos

um campo na primeira regra que seja igual, subconjunto ou superconjunto ao campo correspondente da segunda regra e se existir pelo menos um campo na segunda regra que não seja igual, subconjunto ou superconjunto ao campo correspondente da primeira regra;

- Sem relação: Nenhum dos valores dos campos correspondentes entre as duas regras tem relação;

Uma intersecção é definida pela existência de uma igualdade, um superconjunto, um subconjunto, ou uma correlação entre duas regras. Regras com relação parcial ou sem relação não definem uma intersecção e portanto não precisam ser comparadas.

3. Caracterização da Falha

A partir da existência de uma intersecção entre duas regras, pode-se então caracterizar uma falha em potencial. Alguns aspectos são importantes e necessários para a checagem e classificação da intersecção. Estes aspectos são: grau de intersecção, identidade ou não da ação e ordenação parcial das regras. Através da relação destes aspectos, pode-se apontar a seguinte classificação:

- Erro: a existência da falha compromete o correto funcionamento do filtro; é necessária uma correção.
- Aviso: situação pode ou não ser errônea; a decisão final neste caso cabe ao administrador.
- Normal: as regras estão corretas uma em relação à outra.
- Normal com redundância parcial: A situação é normal, porém as regras contém uma redundância para algumas condições. Orienta-se que as regras sejam reescritas para eliminar a redundância e facilitar a compreensão.
- Redundância desnecessária: Uma das regras nunca será ativada, orienta-se a excluir a que for subconjunto da outra.

Para redes que possuam mais de um filtro em sua topologia, além das incoerências locais de cada filtro, novas falhas podem existir entre as regras destes filtros, desde que os mesmos façam parte do caminho para um determinado fluxo de pacotes. Primeiramente cada filtro deve ser avaliado para resolução de incoerências locais e então ser comparado às regras do segundo filtro. A caracterização de falhas neste ambiente é realizada da mesma forma que é executada para as regras de um único filtro, entretanto o aspecto de ordenação parcial é substituído pela ordenação do sentido do tráfego, sendo que em operação normal a checagem de um pacote é primeiro efetuada na tabela de regras do primeiro filtro no sentido do tráfego. A classificação de falhas também é a mesma, entretanto o diagnóstico para cada item deve mudar, uma vez que, por exemplo, uma redundância desnecessária em um filtro local passa a ser necessária (e normal) em filtros distribuídos.

Para qualquer regra que permita um determinado tipo de tráfego a uma aplicação, deverá existir outra regra permitindo o tráfego de retorno necessário. É interessante então verificar no conjunto de regras se para as situações que existam regras com ação de aceite, as regras de retorno estão implementadas. Para filtros do tipo stateless, onde não existe tabela de estados para as conexões, para cada regra deverá existir uma regra inversa, ou seja, com os campos de origem e destino trocados. Para filtros do tipo stateful, que possuem capacidade de manter o estado das conexões, não

deverá existir uma regra desta natureza, entretanto, deve existir uma regra permitindo o retorno de conexões que estejam estabelecidas. As regras que não possuírem uma correspondente para retorno deverão ser apontadas pela ferramenta de checagem. A checagem para este tipo de falha deve ocorrer somente após a verificação de incoerências.

4. Exemplos de Uso da Metodologia e Considerações

Através da metodologia proposta, cada par de regras são avaliadas na busca de uma intersecção. Quando for caracterizada uma intersecção, avalia-se: o grau da mesma, identidade ou não da ação e ordenação parcial das regras. Comparando-se a regra 1 e 2, pode-se classificar uma igualdade entre as duas. Para relações de igualdade a ordenação e o grau da intersecção não é relevante, entretanto, quando não houver identidade na ação pode-se caracterizar um erro entre estas duas regras.

Tabela 1. Conjunto de Regras

regra	protocolo	ip origem	porta origem	ip destino	porta destino	ação
1	tcp	10.0.0.0/8	*	192.168.1.1	53	deny
2	tcp	10.0.0.0/8	*	192.168.1.1	53	accept
3	*	*	*	192.168.1.2	80	accept
4	udp	10.0.1.0/24	*	192.168.1.0/24	53	accept
5	*	10.0.1.0/24	*	192.168.1.2	80	deny

Para as regras 3 e 5, tem-se uma intersecção cuja o grau é do tipo superconjunto, aonde a regra 3 é um superconjunto da regra 5. Para subconjuntos aonde não existe identidade da ação e a regra que está contida vem após, caracteriza-se um aviso. A regra 5 nunca será ativada, pois todos os pacotes que seriam verificados por esta regra, já tem condição aceita pela regra 3.

Através do uso desta metodologia torna-se possível a verificação de conjuntos de regras de filtros de pacotes indicando possíveis incoerências que poderiam estar comprometendo o nível de segurança fornecido pelo mecanismo.

Referências

Al-shaer, Ehab, Hamed, Hazem. Discovery of Policy Anomalies in Distributed Firewalls. IEEE INFOCOMM'04, Mar. 2004.

Al-shaer, Ehab, Hamed, Hazem. Firewall Policy Advisor for Anomaly Detection and Rule Editing. IEEE/IFIP Integrated Management IM'2003, Mar. 2003.

Cheswick, William R., Bellovin, Steven M., Rubin, Aviel D. Firewalls e Segurança na Internet: repelindo o hacker ardiloso. 2.ed. Porto Alegre: Bookman, 2005.

Northcutt, Stephen, et al. Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems. 1.ed Sams, Jun. 2002.

Liu, Alex X., Gouda, Mohamed G., The University of Texas at Austin. Diverse Firewall Design, 2004 International Conference on Dependable Systems and Networks (DSN'04), Florence, Italy, Jun. 2004.

Wang, Dong, Hao, Ruibing, Lee, David. Fault detection in Rule-based Software systems. Information & Software Technology, v. 45, n. 13, Out. 2003.