Resumo

Nesta dissertação é efectuada uma abordagem à gestão centralizada de equipamentos de firewall em ambientes heterogéneos. Foi concebido e implementado um modelo de gestão centralizada e coerente de políticas de firewall, que deverão ser aplicadas uniformemente em diversos pontos da rede.

Para tal, foi realizada pesquisa e estudados modelos existentes de definiçãode politicas de firewall abstractas. Verificando que esses modelos eram bastante insatisfatórios e incompletos, foi desenvolvida uma nova solução.

A solução proposta é centralizada e assenta em 3 pilares: especificação de políticas de segurança, conversão de políticas de segurança e difusão, aplicação e verificação de políticas de segurança.

Esta solução permitirá a gestão dos equipamentos através de uma consola de gestão central. Possibilitará a criação/edição de políticas de segurança, com base numa linguagem de especificação de políticas de segurança independente, assim como a sua verificação. Para tal foi definido um XML Schema que servirá de base à criação/edição de políticas, em formato XML.

Depois de criadas as políticas independentes estas serão convertidas para políticas específicas de um determinado equipamento, utilizando, para tal, os módulos da aplicação de conversão de políticas de segurança – Security Policy Conversion Application (SPCA).

Por fim estas políticas serão difundidas para o ponto de rede onde cada uma deverá ser aplicada localmente. Isto realizar-se-á através de uma aplicação de difusão de políticas de segurança - Security Policy Diffusion Application (SPDA), que se baseará num descrição pormenorizada dos equipamentos de firewall existentes na rede a gerir.

Para demonstrar o conceito inerente à solução proposta foi desenvolvido um protótipo, que foi submetido a vários testes.

Palavras-chave: Firewalls distribuídas, gestão centralizada de firewalls, regras de firewall abstacta, linguagem de especificação de políticas de segurança.

Abstract

In this dissertion, we approach the firewall centralized managenement in heterogeneous environments theme. It was concebed and implemented a centralized and coherent managenement firewall's policies model, which should be applied uniformously in several points of a data network.

To do so, existent models to define independent firewall's policies were research and studied. Coming to the conclusion that these models were pretty unsatisfactory and uncompleted, a new solution was developed.

The solution we propose is centralizaded and it was developed in 3 directions: security policy specification and verification, security policy conversion and security policy diffusion and application.

This solution will allow equipment managenement through a centralized managenement console. It will allow security policy creation/edition, based on a abstract security policy specification language, as well as its verification.

To do so, it was defined a XML schema, that will be the basis of policy creation/edition, in XML format Once the independent policies are created, these will be converted to specific policies of determined equipments, using the security policy conversion application (SPCA).

Finally, these policies will be led to the point of the data network where they must be applied. This will be done with the security policy diffusion application (SPDA), which will be based on a detailed network equipment description.

To demonstrate the concept inherent to the solution we propose, it was developed a prototype, which was submmited to several tests.

Keywords: Distributed firewalls, firewall centralized managenement, abstract firewall policies, security policy specification language.