

الخلاصة

في هيكلية هذا الجدار الناري المقرر لحماية الشبكات، هذا الجدار يشكل اول خط دفاعي ضد الهجوم وفي كثير من الاحيان يعتبر الخط الوحيد لصد الهجوم في الشبكة. مثل هذه الهيكلية تكون مناسبة للشبكات ذات الحجم الصغير (الشبكات المحلية) لكن هذه الهيكلية تفشل مع الشبكات الكبيرة. عدة مشاكل تواجه هذه الهيكلية مثل : تضيق حزمة التردد في الشبكة، مستوى واطيء مشكوك بثقته، التهديدات الداخلية في الشبكة. كل هذه المشاكل تقود للحاجة الى هيكلية الجدران النارية المنتشرة حيث ان الحماية ممكن ان تزود بمستويات مختلفة بالشبكة (أضافة طبقات دفاعية جديدة). هذا الهدف يتم الوصول اليه عن طريق تقسيم الشبكة الكبيرة الى أجزاء أصغر يسمى كل جزء (شبكة فرعية) و يتم حماية كل جزء بجدار ناري خاص به. هذا يقود الى عدة فوائد و هي : تحسين الأداء الجدار الناري، التقليل من اختناق حزمة التردد، عمق في الدفاع من خلال مستويات مختلفة بالشبكة ينتج عنه شبكة أكثر سرية.

تقدم هذه الأطروحة أول خطوة باتجاه هذه الهيكلية لتتقدم للشبكات الكبيرة كحل أمثل لكثير من هذه المشاكل التي تخص حماية الشبكة.

تم تنفيذ البرنامج باستخدام لغة الفيجوال بيسك كلغة برمجية و (packet filtering) كطريقة تقنية. إما هيكلية ربط الشبكة كانت باستخدام ال(dual-homed host). في هذه الأطروحة تم تنفيذ هيكلية الجدران النارية المنتشرة بتوزيع ثلاثة جدران نارية (وهي الجدار الناري الحدودي والجدران الفرعيات) بثلاثة مواقع في الشبكة وبذلك تم اضافة مستويات حماية إضافية و تقليل عدد الضوابط القانونية في الجدار الناري الحدودي. بتلك الوسيلة سيقبل الواجب على الجدار الناري الحدودي.

إن باستخدام هذه الهيكلية تم الحصول على مستوى حماية عالي الثقة، مستوى أداء عالي الجودة، التقليل من اختناق حزمة التردد و بالتالي كل ذلك يؤدي إلى شبكة آمنة ذات مستوى حماية عالي.

Abstract

With single-firewall architecture, firewalls often form the first, and most times the only, line of defense against attack. Such architecture is practical for a small network, but it fails in large and enterprise networks. Some of problems faced by single-firewall architecture are insider threats, bandwidth bottleneck, and low-trust level. This brings in the need for the distributed firewall architecture, wherein security can be provided at different levels in the network (add extra layers of defense). This aim is achieved by dividing the complete network into smaller parts namely subnets and securing each of which with its own firewall. That leads to increase the performance of the firewall. This thesis presents the first step towards such architecture - distributed firewall architecture for large network as the solution for some problems about issues related to network security.

The proposed software was developed using Microsoft Visual Basic 6.0 programming language. The implementation of the proposed system uses the packet filtering mechanism as a technical method to filter the IP packets and the Dual-Homed host as an architecture in which firewall components are managed to provide effective protection against unauthorized users. In this thesis the distributed firewall model implemented by distribute the localized firewalls in three positions in the protected network to add extra levels for protection and to reduce the number of rules in the border firewall, thereby the load on the Border Firewall is also reduce.

Hence architecture provides higher trust level, high performance and mitigates the Bandwidth bottleneck, defense in depth, all that resulting in secure network.