GRAPHICAL USER INTERFACE FOR FIREWALL CONFIGURATION

Zdeněk BURDA, Master Degree Programme (5)
Dept. of Computer Systems, FIT, BUT
E-mail: xburda01@stud.fit.vutbr.cz

Supervised by: Dr. Daniel Cvrček

ABSTRACT

We are going to describe basic ideas and architectural overview of system for secure management of firewall's configuration. Profound requirement for the system is universality, which guarantees reusability for different firewalls with different configuration files. Using XML exchange file format and JAVA programming language provides the system's universality.

1 ÚVOD

Organizace jsou stále silněji pod tlakem na zabezpečení integrit, důvěrnosti a dostupnosti dat uchovávaných v jejich informačních systémech. Využití informačních technologií bohužel přináší s mnohými výhodami i stále silnější bezpečnostní rizika a hrozby. Zabezpečení a ochrana informačních systémů se tak stává jednou z primárních úloh.

Důležitou součástí bezpečnosti je bezpečnost síťových připojení a řízení toku dat jak uvnitř organizace, tak mezi organizací a veřejnými sítěmi. Jedním ze základních prostředků používaných pro řízení komunikace je firewall. Volba konkrétního firewallu a jeho správná instalace jsou sice základními předpoklady pro splnění bezpečnostní politiky, ale nejsou nejdůležitější. Většina dostupných firewallů je schopna zajistit bezpečnost vnitřní sítě, ale chyba v konfiguraci může mí za následek vážné narušení bezpečnosti bez ohledu na firewall.

Konfigurace firewallů je bohužel stále složitější – přesně v souladu s tím, jak se zvyšují možnosti firewallů a jak roste složitost vnitřních sítí. Proto určitě není ztrátou času zabývat se způsobem konfigurace jednotlivých firewallů, pokusit se jejich nastavení v rámci možností sjednotit a zpříjemnit tak uživateli často ne zcela jednoduchou úlohu.

2 FIREWALL A JEHO UŽIVATELSKÁ ROZHRANÍ

Každý firewall obsahuje výkonnou a konfigurační část. Kvalita zpracování obou těchto částí firewallu má zásadní vliv na jeho správnou funkci. Komfortní administrátorské rozhraní (se špatnou výkonnou částí) a výborně pracující výkonná část (bez jednoduché konfigurace a kontroly síťové komunikace) snižují funkčnost firewallu a představují pro chráněnou síť

potencionální bezpečností rizika spojená s úspěšnými útoky na vnitřní síť.

2.1 „IDEÁLNÍ“ ZPŮSOB KONFIGURACE

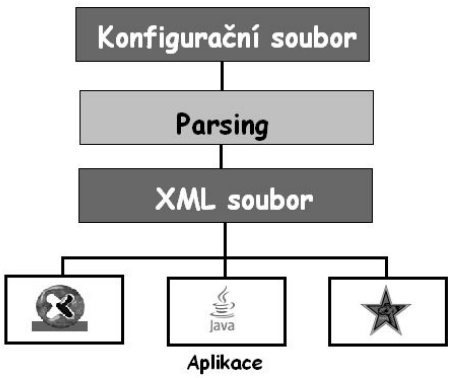
Konfigurace založená na několika (málo) textových konfiguračních souborech s “rozumnou”, člověku srozumitelnou syntaxí a jejich editace spolehlivým textovým editorem, je z mnoha hledisek nejelegantnějším řešením. Jeho nespornou výhodou je spolehlivost, srozumitelnost, archivace, snadná modifikace bez speciálních nástrojů a jednoduchost realizace vzdálené správy bez velkých nároků na přenosovou kapacitu.

Konfigurace pomocí textových souborů má pochopitelně i své nevýhody – s rostoucí složitostí konfigurace nemusí být snadné poznat neoprávněné změny, případně chyby při konfiguraci. Přirozeným řešením je grafická reprezentace konfiguračních souborů a přehledné znázornění implementace bezpečnostní politiky.

2.2 NÁVRH SYSTÉMU

Použití jednoho typu firewallu v organizaci je spíše výjimkou. Tudíž chceme, aby co největší část systému byla obecně použitelná bez ohledu na typ firewallu. Chceme-li sjednotit konfiguraci více firewallů musíme použít jednotnou vnitřní datovou reprezentaci schopnou popsat libovolnou gramatiku konfiguračního souboru. Jedním z řešení je použití textového formátu XML, který je nezávislý na jakékoliv platformě natož pak hardwaru. Formát XML je standardizovaný a celosvětově užívaný pro výměnu informací mezi různými programy a platformami. Rovněž tak by měl mít dostatečné množství prostředků pro popis libovolné gramatiky firewallu.

Funkci systému si pak můžeme představit tak, že pro jednotlivé firewally budeme definovat převod z jejich vlastního konfiguračního souboru do standardního XML formátu s definovanou sémantikou. Tento formát pak použijeme jako vstup libovolné aplikace (webový prohlížeč[1] či tzv. XML parser), nebo daný soubor zpracujeme v námi definované speciální aplikaci.



Obr. 1: *Způsob zpracování konfiguračního souboru a jeho použití v aplikacích*

Po prostudování několika konfigurační souborů[2] jsme zjistili, že konfigurace firewallu zahrnuje dvě podstatné části:

1 při použití kaskádových stylů (CSS) lze dosáhnout prakticky libovolného a velmi kvalitního zobrazení

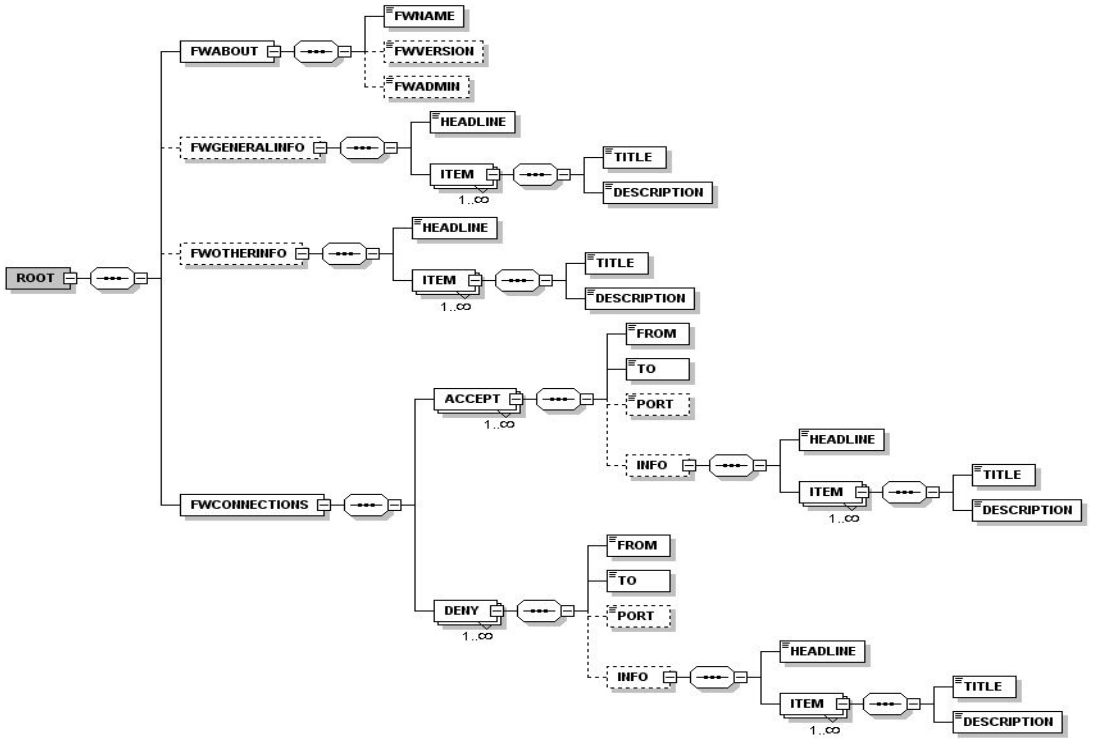
2 Firewally: Kernun, Gauntlet, GiP, ipfw, fiaif a sf

- Konfiguraci pravidel pro směrování dat a
- Speciálních nastavení firewallu a jeho příznaků

Na základě této analýzy jsme gramatiku XML souboru, rozdělili do čtyř sekcí:[3]

- Informace specifikující daný firewall – orientační informace (název, verze)
- Informace o konkrétním nastavení hlavních vlastností firewallu – jako např. adresa vnitřní sítě, identifikace síťového hardwaru
- Informace o konkrétním nastavení jiných vlastností firewallu – jako např. omezení datových přenosů jednotlivých proxy, počet čekajících proxy procesů apod.
- Informace o nastavení pravidel pro řízení komunikace – vlastní bezpečnostní pravidla pro výkonnou část

Kompletní gramatiku XML souboru popsanou pomocí schématu, můžeme zobrazit takto:



Obr. 2: *Popis gramatiky XML souboru pomocí XML schématu*

LITERATURA

[1] Hanáček, P., Staudek, J.: Bezpečnost informačních systémů. Praha, Úřad pro státní informační systémy 2000, ISBN 80-238-5400-3

[2] Macháček, M., Pojsl, J.: Firewally - Úvod do problematiky. Brno, Trusted Network Solutions 2002, 9.února 2004. Dokument dostupný na URL http://www.tns.cz/clanky/fw_uvod_MM.rtf

3 nic nám nebrání v přidávání nových sekcí a rozšiřování tak systému