VALIDATION OF NETWORK PARAMETERS BASED ON NETWORK MONITORING

Radim Martínek

Master Degree Programme (2), FIT BUT

E-mail: xmarti42@stud.fit.vutbr.cz

Supervised by: Martin Žádník

E-mail: izadnik@fit.vutbr.cz

Abstract: This article introduces a new approach for verification of required computer network setup. Used technology is based on validation of selected network parameters with the help of monitoring of real network traffic. The article proposes design and implementation of a tool, which validates user-selected network parameters with the help of network flow analysis through the use of NetFlow technology. This process generally verifies whether the network comply with its specification.

Keywords: Validation, NetFlow, NFDUMP

1. ÚVOD

Současné moderní počítačové sítě jsou charakteristické svou komplexností a různorodou škálou poskytovaných služeb. Pro představu jsou to služby jako internet telefonie (VoIP), internetové bankovnictví, virtuální privátní sítě (VPN), sdílení souborů a tiskáren, připojení vzdáleného diskového prostoru (iSCSI), systémy centrálního zálohování. Dané síťové služby jsou různou mírou náročné na zabezpečení zasílaných dat, garanci přenosového pásma, případně stabilní odezvy. Díky tomu se návrh, realizace a následná správa sítě stává místem, kde lze snadno udělat kritickou chybu. Navíc i bez zanesení chyb administrátorem, může síť jevit známky nežádoucího chování, které je způsobeno používáním různých uzavřených protokolů, četných chyb v softwaru i hardwaru a výrazné složitosti možného provozu v síti. Práce popsaná v tomto článku si klade jako hlavní cíl právě takovéto chybné chování sítě odhalit a tím ověřit, zda síť v praxi opravdu splňuje požadavky, se kterými byla navrhována. Za tímto účelem je použita metoda validace sítových parametrů založená na sledování skutečného provozu. V reálném provozu se tedy zkoumá, zda se síť chová dle předem specifikovaných požadavků. Článek je rozdělen do pěti kapitol. Po úvodní části následuje v druhé kapitole vysvětlení základního principu validace. Třetí kapitola popisuje nástroj implementující tyto techniky. Ve čtvrté kapitole je představena ukázková síť s vybranými parametry k validaci a nakonec pátá kapitola v závěru zhodnocuje dosavadní výsledky.

2. VALIDACE SÍTĚ

Validace je proces hodnocení produktu během nebo na konci vývoje pro zaručení shody s jeho požadavky [1]. Prokazuje vhodnost produktu pro jeho provozní poslání (zamýšlené použití). Validace nás ujišťuje, že vyrábíme správný produkt. Pro doplnění naproti tomu verifikace nás ujišťuje, zda vyrábíme daný produkt správně [2].

V kontextu počítačových sítí za pomocí monitorování reálného provozu nám validace ověřuje, že všechny stanovené podmínky kladené na danou síť, byly splněny. Přičemž síť splňující všechny tyto podmínky je ve shodě se svou specifikací, tedy vhodná pro své provozní poslání. Popisovaná technika validace je založena na sběru sítových toků, jejich následné analýze a rozhodnutí, zda daný tok splňuje zadané požadavky či nikoliv. K tomu je třeba mít v síti vhodně rozmístěné monito-

rovací sondy, znát síťovou topologii, počáteční konfiguraci a nakonec mít dobře definované požadavky na parametry sítě určené k validaci.

Pro definování sběru a práci se sítovými toky je v tomto případě použito NetFlow [3], což je Cisco technologie, která za pomocí rozdělení provozu na síťové toky umožňuje sledování charakteristických informací posílaných dat v síti. Nezkoumá konkrétní obsah zasílaných informací, ale pouze informace vyskytující se v hlavičce datových paketů. K tomu potřebuje dva typy zařízení nazývající se exportér a kolektor. Exportér sleduje procházející pakety a na jejich základě vytváří a aktualizuje informace o aktuálních sítových tocích. Ke každému toku se obvykle zaznamenávají statistické údaje, jako počet přenesených bajtů, čas trvání toku nebo TCP příznaky. Kolektor časem dostává informace od exportérů, ukládá je a případně analyzuje.

3. NÁVRH A IMPLEMENTACE

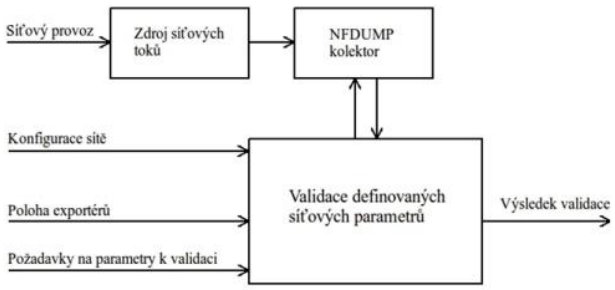
Hlavními cíli práce jsou výběr vhodných parametrů sítě určených k validaci a následně navrhnout a implementovat nástroj, který bude pomocí monitorování reálného provozu zvolené parametry validovat.

3.1. VÝBĚR VHODNÝCH PARAMETRŮ K VALIDACI

Zvolené parametry k validaci je možné rozdělit do tří hlavních skupin na omezující parametry (filtrovací pravidla, limity příchozího a odchozího provozu, maximální celkové zatížení sítě), parametry popisující dosažitelnost uzlů v síti a časové parametry (zpoždění paketů, odezva). Zároveň je třeba při použití NetFlow toků počítat při vybírání vhodných parametrů s jistými omezeními. Záznamy síťových toků neobsahují informace o času, kdy pakety procházejí jednotlivými místy sítě. Z tohoto důvodu je třeba při validaci časových parametrů počítat s rozšířením NetFlow technologie o přesnou časovou synchronizaci exportérů s přesnou lokalizací a použití dalších síťových sond specificky nastavených pro sbírání dodatečných informací (například zaznamenání času zpracování a TCP příznaků prvního paketu každého síťového toku).

3.2. NÁVRH A IMPLEMENTACE NÁSTROJE

Nástroj je implementován v programovacím jazyku Java, má grafické uživatelské rozhraní a jeho blokové schéma je znázorněno na Obr. 1. Vstupními daty jsou požadavky na síťové parametry, konfigurační údaje sítě, informace o poloze exportérů a síťové toky. Požadavky na síťové parametry představují konkrétní vlastnosti sítě, které jsou určeny k validaci. Konfigurační údaje obsahují v jednom souboru nastavení všech aktivních prvků v síti. Informace o poloze exportérů obsahují IP adresy jednotlivých exportérů a jejich polohu v rámci topologie sítě. Síťové toky jsou ukládány na disk do binárního souboru a



Obrázek 1: Nástroj pro validaci I/O.

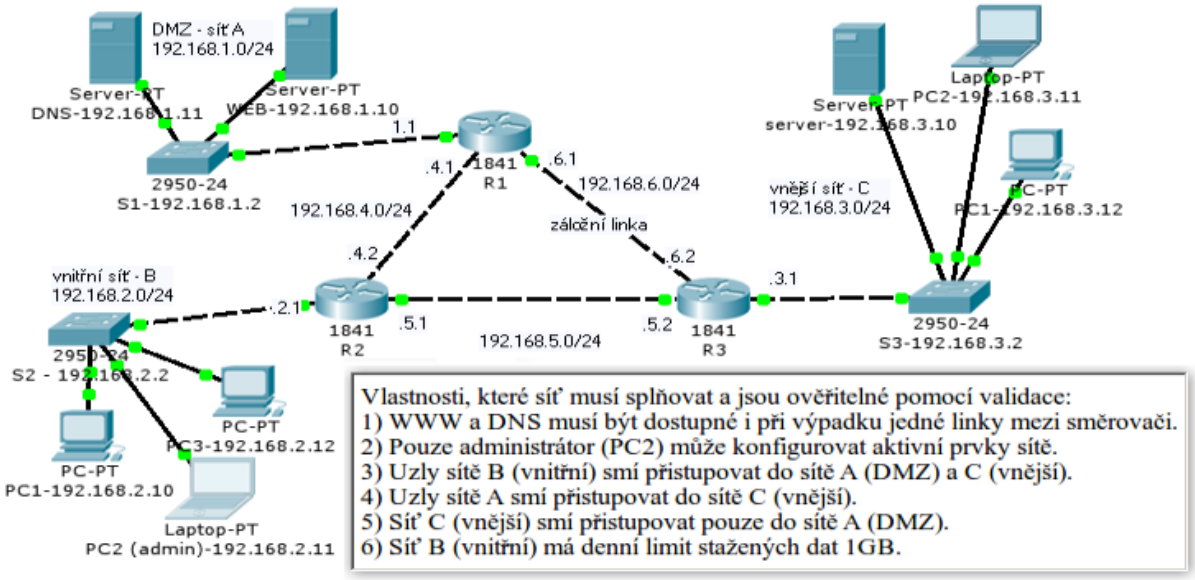
následně jsou dle potřeby validace pomocí služeb nástroje NFDUMP [4] zpracovány. Jejich výstup je dále použit k rozhodnutí o výsledku validace. Výstupem nástroje je zpráva podrobně informující uživatele o splnění, či nesplnění zadaných požadavků na parametry sítě. (Zmíněný nástroj NFDUMP označuje množinu nástrojů pro sběr, zpracování a analýzu NetFlow dat. Umožňují agregaci toků, filtrování i tvorbu statistik. Pracují v příkazové řádce s optimalizací pro rychlé zpracování.)

Aplikace podporuje tyto hlavní uživatelské činnosti: Načíst požadavky na parametry k validaci, polohu exportérů, konfiguraci sítě. Nastavit kolektor (v případě online validace), polohu exportérů, umístění vstupních sítových toků (v případě offline validace), požadavky na parametry k validaci (v případě, že nebyly načteny ze vstupu). Exportovat požadavky na parametry k validaci, výsledky

validace. Zahájit validační proces. Ukončit validační proces. Zobrazit výsledky validace. Po spuštění procesu validace jsou pomocí služeb nástroje NFDUMP prozkoumány dostupné síťové toky a probíhá analýza, zda tyto toky splňují zadané požadavky. Pro každý zadaný požadavek se vytvoří charakteristická konfigurace, která je pro každý vhodný síťový tok zkoumána. Podle toho, zda tuto charakteristiku tok obsahuje nebo ne, je možné určit, zda je tok v souladu se zadaným požadavkem. Proces se opakuje, dokud nejsou zkontrolovány všechny dostupné toky nebo nedojde k ukončení procesu uživatelem. Poté následuje podrobné zobrazení zprávy o výsledcích validace.

4. PŘÍKLAD POUŽITÍ

Na Obr. 2 je zobrazena topologie sítě skládající se z chráněné vnitřní sítě s PC stanicemi, demilitarizované zóny obsahující WWW, DNS servery a z vnější sítě představující WAN. Součástí obrázku je seznam požadavků, které musí být dodrženy, aby síť splnila svou specifikaci. Všechny tyto požadavky jsou ověřitelné popisovaným nástrojem a tedy pokud administrátor nešikovným způsobem pozmění konfiguraci sítě, bude vzápětí informován o případném nežádoucím chování sítě.



Obrázek 2: Příklad typických požadavků na síťové parametry v kontextu topologie sítě.

5. ZÁVĚR

Článek představuje základní pohled na tématiku, kterou se zabývá diplomová práce: „Validace parametrů sítě založená na sledování síťového provozu“. Důležitým přínosem práce je použití nového přístupu v oblasti správy počítačových sítí. Do budoucna lze předpokládat rozšíření této techniky o větší míru automatizace a o zvýšení množství typů podporovaných síťových parametrů.

REFERENCE

[1] Boehm, B, W.: Verifying and Validating Software Requirements and Design Specifications, Software, IEEE. Leden 1984. Sv. 1,1, stránky 75-88.

[2] Boehm, B, W.: Guidelines for Verifying and Validating Software Requirements and Design Specifications. Euro IFIP 79. 1979, stránky 711-719.

[3] RFC 3954 - Cisco Systems NetFlow Services Export Version 9. Internet FAQ Archives. [Online] [Citace: 5. 10 2010.] http://www.faqs.org/rfcs/rfc3954.html.

[4] NFDUMP. SOURCEFORGE.NET. [Online] [Citace: 29. 12 2010.] http://nfdump.-sourceforge.net/.