SECURE TRANSPORT FOR SYSTEM MONITORING

Patrik Halfar
Master Degree Programme (2), FIT BUT
E-mail: xhalfa01@stud.fit.vutbr.cz

Supervised by: Petr Matoušek
E-mail: matousp@fit.vutbr.cz

ABSTRACT

The goal of this paper is the analysis of usability of NetFlow in networks with dislocated data centers which are linked by unsecured connections. The analysis focuses on reliability and confidentiality of data transfer. The solution, which is discussed in this paper, is based on the open source applications 'nfdump' and 'secure shell'.

1 ÚVOD

Monitorování sítí se stává jejich nezbytnou součástí, ať už jde o sítě střední nebo velké. Při monitorování nejčastěji rozlišujeme zjišťovaní stavu a sledování provozu. Každý z těchto cílů se monitoruje odlišnými nástroji. Stav lze nejlépe zjišťovat pomocí *Simple Network Managment Protocol* (SNMP), kdežto pro sledování provozu slouží *NetFlow*. Sledováním provozu na síti a zabezpečením těchto dat se zabývá tento článek.

2 NETFLOW

NetFlow je služba, která vzešla z dílny společnosti Cisco jako sekundární produkt snahy o urychlení aktivních prvků (směrovačů a L3 přepínačů).

Pro urychlení činnosti si aktivní prvky začaly uchovávat informace o aktivních tocích. Tok je identifikován pomocí sedmice

{adresa_zdroje, adresa_cíle, port_zdroje, port_cíle, protokol_vyšší_vrstvy, typ_služby, vstupní_rozhraní}.

Již o této sedmici lze říci, že má vysokou informační hodnotu. Jejím doplněním o časové razítko a čítače pro pakety a celkový objem přenesených dat vznikne záznam NetFlow. Je vhodné připomenout, že NetFlow nesbírá obsah přenášených dat[1].

Nebudou-li uvažovány speciální NetFlow sondy, které uchovávají všechna data lokálně a zajišťují jejich zpracování a vizualizaci, pak standardní koncept se skládá ze dvou zařízení. Jedním z nich je **exportér**, který sleduje síťový provoz a generuje NetFlow záznamy a zasílá je na druhé zařízení (tzv. **kolektor**) ve kterém se data shromažďují a zpracovávají. Kolektorem je obvykle počítač vybavený specializovaným softwarem, který dokáže data zpracovávat. V případě exportéru je situace komplikovanější, neboť původně byl součástí aktivního prvku, dnes běžně samostatné zařízení (jednoúčelový hardware nebo počítač s vhodnou aplikací). Protože stále je exportér součástí aktivních prvků je žádoucí, aby generování dat bylo náročné na zdroje zařízení (procesor, paměť) a vzhledem k tomu, že jde o službu podpůrnou, nesmí přenos zabírat příliš přenosového pásma a omezovat primární služby sítě. Splnění těchto požadavků je dosaženo

použitím bezstavového přenosu pomocí protokolu UDP, kterým probíhá komunikace pouze směrem od exportéru ke kolektoru (kolektor nekomunikuje s exportérem)[1].

Metadata, která získává NetFlow o provozu sítě, lze označit za *citlivá*, neboť je možné z těchto dat získat informace o činnostech uživatelů (kdo s kým komunikuje, pomocí jaké služby a jak často). Tyto informace se využívají pro různé účely:

- detekce útoků,
- statistické vyhodnocování,
- účtování,
- sledování uživatelů (zaměstnanců).

Podle požadovaného cíle se mění i požadavky na utajení a spolehlivost doručení přenášených dat. Mají-li data sloužit pro statistické vyhodnocování, je ztráta malého procenta dat přípustná a zároveň není potřeba přesně identifikovat cíl nebo zdroj toku. Na druhou stranu slouží-li data pro účtování, pak ztráta dat není žádoucí stejně jako nemožnost identifikovat zdroj nebo cíl. Zavádění spolehlivosti a důvěrnosti přenosu vede ke zvyšování nároků na zdroje výpočetního výkonu.

V poslední době aktivitu kolem NetFlow převzala organizace IETF s projektem IPFIX[2]. Ten vychází ze stejných principů, ale na rozdíl od NetFlow je formát zcela otevřen. Výše uvedené problémy i další zajímavé vlastnosti jsou již součástí návrhu tohoto protokolu. Přechodem na IPFIX by se tedy daly vyřešit popsané problémy.

3 MOTIVACE

Se zavedením IPFIX do běžné praxe nelze v nejbližší době počítat, a otázkou zůstává, zda se tak vůbec stane. Proto je cílem nalézt řešení aplikovatelné na stávající stav, čímž je chápáno nasazení NetFlow v rozsáhlých sítích, které jsou založeny na dislokovaných uzlech propojených pomocí veřejné sítě, kde bude zajištěno

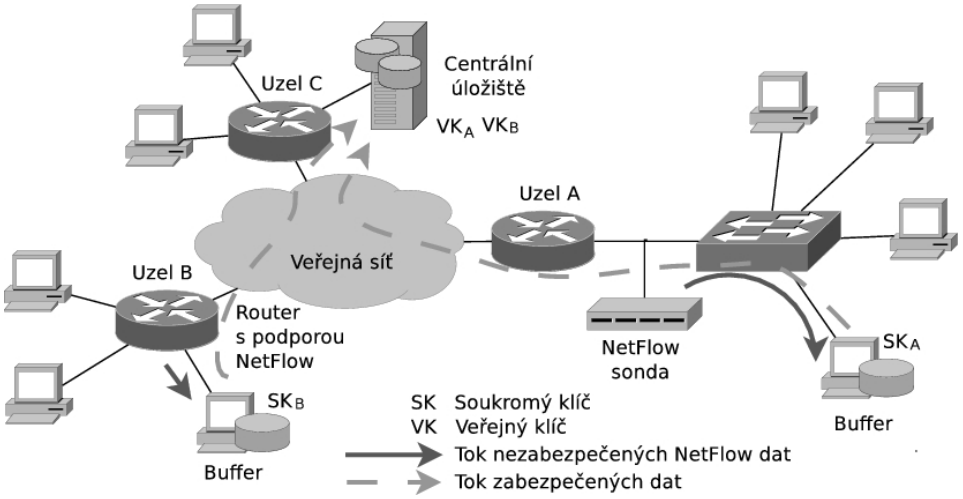
- spolehlivé doručení a
- utajený přenos.

V takovýchto případech je prioritním cílem, nasazení NetFlow, odhalení důvodu výpadku nebo případného útoku. Obě situace při využití NetFlow protokolu znamenají perzistentní ztrátu dat. Pro tyto účely nelze využít anonymizovaných dat a je tedy nezbytné jejich utajení při přenosu. V menších sítích (tedy takových, které se nacházejí v jedné lokalitě) se často problém důvěrnosti zajišťuje fyzickým oddělením, nebo pomocí VLAN, veřejné a privátní sítě. Problém nespolehlivosti přenosu pomoci UDP paketu je zanedbatelný, neboť výpadek lokální linky je mnohonásobně méně pravděpodobný než výpadek linky mezi datovými centry. Důvodem výpadku linky nemusí být ani její fyzické přerušení. Stačí, když dojde k přehlcení sítě a aktivní prvek začne zahazovat pakety. Jelikož NetFlow nezajišťuje zpětný kanál, je ztráta dat permanentní a neodhalitelná.

4 ŘEŠENÍ

Od řešení se očekává, že jeho použití nebude znamenat složitou konfiguraci a velké nároky na údržbu oproti stávající konfiguraci a údržbě NetFlow. Z tohoto důvodu není vhodné spoléhat na utajení dat pomocí VPN tunelu, neboť jeho správa roste s počtem propojených uzlů a navíc neochrání před ztrátou dat.

V případě malých sítích je vhodné umístit kolektor co nejblíže sondy a pomocí VLAN oddělit síť s důvěrnými daty od sítě veřejné. Aplikací tohoto konceptu na více lokalit znamená decentralizované uložení dat bez možnosti analýzy jako celku.



Obrázek 1: Topologie a rozložení tajemství

Uvažované řešení je založeno na nejrozšířenější open source aplikaci 'nfdump'[3]. Chování popisuje následující algoritmus:

1. Přijímej data z exportéru a ukládej je do souboru.
2. Po vypršení času *t* začni psát do nového souboru a původní
3. soubor se pokus spolehlivě a důvěrně doručit do kolektoru a pokud
   (a) byl úspěšně přenesen, pak jej smaž a pro každý soubor ve složce `neodeslané` opakuj krok 3.
   (b) došlo k chybě, přesuň soubor do složky `neodeslané` a skonči.

Tento algoritmus nepopisuje, jak data přenést spolehlivě a důvěrně, neboť takového přenosu lze dosáhnout různými způsoby. V tomto konkrétním případě je nasazen program *scp*, který pro přenos souboru využívá šifrovaného spojení přes *ssh*, které je zároveň spolehlivé. Tato aplikace používá pro vzájemné ověřování asymetrickou kryptografii a díky tomu existuje pouze jedno nesdílené tajemství na každý uzel. Rozložení klíčů je vidět na obrázku 1.

5 ZÁVĚR

Tato analýza aplikace byla provedena za účelem rozšíření NetFlow v síti VUT. V současné době je nasazena v testovacím režimu. Po ověření koncepce se předpokládá vytvoření *patche*, který umožní začlenění přímo do aplikace *nfcupd*, která je součásti balíku 'nfdump'[3].

PODĚKOVÁNÍ

Tato práce vznikla částečně za podpory grantu VUT FIT, FIT-S-10-2 a specifického výzkumu MSM0021630528.

REFERENCE

[1] Claise, B.: Cisco Systems NetFlow Services Export Version 9. RFC 3954. Říjen 2004.

[2] Quittek, J.; Zseby, T.; Claise, B.; aj.: Requirements for IP Flow Information Export (IPFIX). RFC 3917. Říjen 2004.

[3] Haag, P.; Jändling, T.: NFDUMP.
URL `http://nfdump.sourceforge.net/`.