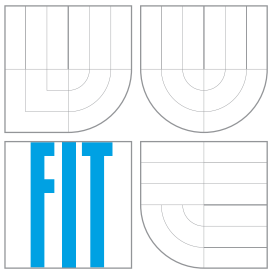
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

ANALÝZA SÍŤOVÉHO PROVOZU POMOCÍ ZAŘÍZENÍ NIFIC

NETWORK TRAFFIC ANALYSIS USING NIFIC DEVICE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — JURAJ MELO
AUTHOR

VEDOUCÍ PRÁCE — Ing. JAN KOŘENEK,
SUPERVISOR

BRNO 2010

Abstrakt

Tato bakalářská práce popisuje příklady použití zařízení NIFIC na potlačení bezpečnostních rizik v počítačových sítích. NIFIC je bezstavový paketový filtr s hardvérovou akcelerací vhodný na nasazení do vysokorychlostních sítí. Práce obsahuje příklady, ve kterých je prezentováno použití tohoto zařízení, které ve spolupráci s dalšími bezpečnostními systémy dokáže zvýšit bezpečnost sítě, na které je nasazeno. Některé příklady jsou rozšířeny o popis jeho dalších užitečných vlastností, které zlepšují efektivitu správy a monitorování počítačových sítí.

Abstract

This bachelor's thesis describes examples of using NIFIC device in order to suppress security risks in computer networks. NIFIC is a stateless packet filter with hardware acceleration, suitable for deploying on high-speed networks. This thesis contains examples, presenting usage of this device which can improve network security, in cooperation with other security systems. Some examples are extended with description of another useful features, which provide higher effectivity of network managing and monitoring.

Klíčová slova

NIFIC, firewall, filtrování paketů, analýza síťového provozu

Keywords

NIFIC, firewall, packet filtering, traffic analysing

Citace

Juraj Melo: Analýza síťového provozu pomocí zařízení NIFIC, bakalářská práce, Brno, FIT VUT v Brně, 2010

Analýza síťového provozu pomocí zařízení NIFIC

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Jana Kořenka. Další informace mi poskytli lidé z projektu Liberouter. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Juraj Melo
13. mája 2010

Poděkování

Týmto chcem poďakovať vedúcemu práce Ing. Jánovi Kořenkovi za jeho pomoc a rady pri písaní tejto práce. Taktiež ďakujem ľuďom z projektu Liberouter za poskytnuté informácie.

Obsah

Kapitola 1

Úvod

V dnešnom svete má výpočtová technika a hlavne celosvetová počítačová sieť internet, svoje nezastupiteľné miesto. V minulosti bol internet nástrojom iba malej skupiny odborníkov, no za niekoľko rokov zaznamenal masívny nárast používateľov. Dnes je už intenzívne využívaný v každej oblasti nášlo života. Neustále rastie počet pripojených počítačov, objem a hlavne hodnota prenášaných dát.

Internet, a spolu s ním aj privátne siete firiem a organizácií sa tak stávajú terčom útočníkov, ktorí vedia získané informácie speňažiť, alebo tieto siete dočasne vyradiť z prevádzky v prospech konkurencie. O aktuálnosti, týchto hrozieb svedčí aj objem financií vynakladaný spoločnosťami na ochranu svojich lokálnych sietí.

Po internete už dávno nekolujú iba bezcenné informácie, práve naopak. Je využívaný na uskutočňovanie finančných transakcií, prenášanie dôverných dát a o kybernetickom priestore sa začína uvažovať aj ako o novodobom bojisku. Preto sa do popredia sa dostávajú pojmy ako: kyberterorizmus, či kybernetická vojna. Tieto skutočnosti nútia štáty zaoberať sa vojenskými stratégiami na obranu a ovládnutie kybernetického priestoru, a na budovanie „kybernetických síl“. Úspešný útok na kybernetický priestor nepriateľa môže mať za následok značné taktické a hospodárske škody, či dokonca aj straty na životoch. [12]

Problém bezpečnosti počítačových sietí sa však týka aj obyčajných používateľov. Na nich taktiež číha množstvo škodlivého softvéru, ktorý si veľakrát oni sami nič netušiac stiahnu do počítača. Takto sú ohrozené ich financie, súkromné údaje a v neposlednom rade môžu poskytnúť útočníkovi miesto, odkiaľ bude napádať ďalšie ciele.

Snaha o prevenciu útokov vedených na poli internetu, ich detekciu a boj proti nim, je určite opodstatnená. Existuje mnoho nástrojov a postupov, ako svoju sieť ubrániť. Základným a najznámejším nástrojom obrany je firewall. Okrem neho však existujú aj sofistikovanejšie a komplexnejšie systémy ochrany. Jedná sa napríklad o systémy IDS (*Intrusion Detection Systems*), ktoré dokážu útoky a bezpečnostné incidenty detekovať, a IPS (*Intrusion Prevention Systems*) ktoré navyše vedia na vzniknutú situáciu účinne reagovať.

V rámci projektu Liberouter je vyvíjané zariadenie NIFIC, ktoré sa dá použiť na ochranu siete pred viacerými bezpečnostnými hrozbami. Toto zariadenie slúži na filtrovanie sieťových tokov na vysokorýchlostných linkách. Jedná sa o paketový filter s hardvérovou akceleráciou, ktorý pracuje na platforme COMBOv2 a môže byť zapojený na linku s rýchlosťou až 10 Gb/s. NIFIC filtruje pakety podľa zadaných filtrovacích pravidiel, pričom umožňuje zmenu týchto pravidiel počas činnosti, bez straty jediného paketu.

Táto práca je zameraná na vytvorenie a popísanie prípadov použitia zariadenia NIFIC. Jedná sa o prípady, kedy môžme jeho zapojením do siete, zvýšiť úroveň jej zabezpečenia. NIFIC môže priamo plniť funkciu bezpečnostného systému zapojeného v sieti, alebo môže

zefektívniť už existujúci bezpečnostný systém a pridať mu užitočné vlastnosti.

Práca má nasledujúce členenie. V kapitole 2 sa čitateľ oboznámi so základným popisom počítačových sietí, útočníkmi a bezpečnostnými hrozbami, ktorými sú vystavené počítače pripojené do internetu. Kapitola 3 popisuje zariadenie NIFIC, jeho vlastnosti, softvérovú a hardvérovú architektúru a spôsob jeho používania. Nasleduje kapitola 4, v ktorej sú rozpísané jednotlivé prípady použitia zariadenia NIFIC, a v kapitole 5 je uvedený popis použitia vybraného prípadu v reálnej sieti. Záverečné zhrnutie práce je v kapitole 6.

Kapitola 2

Teoretický rozbor

Táto kapitola obsahuje potrebný teoretický základ pre realizovanie prípadov použitia zariadenia NIFIC, uvedených v kapitole 4. Najskôr je predstavený základný model, podľa ktorého pracujú počítačové siete. Potom nasleduje popis bezpečnostných hrozieb, ktoré ohrozujú pripojené počítače. Na koniec sú uvedené nástroje, ktoré zabraňujú sieťovým útokom a ktoré boli použité aj pri tvorbe prípadov použitia.

2.1 Počítačová sieť

Internet, ako ho poznáme dnes je založený na modeli TCP/IP. Popis tohto modelu je čerpaný z [17]. Obsahuje základné protokoly, ktorými medzi sebou komunikujú počítače pripojené do siete. Skladá sa zo štyroch vrstiev, ktoré popisujú komunikáciu na jednotlivých úrovniach pripojenia. Sú nasledovné:

- linková vrstva – popisuje prenos paketov medzi dvomi zariadeniami pripojenými na jednu linku
- sieťová vrstva – rieši problém smerovania paketov pri ich posielaní z jednej siete do druhej. Využíva protokol IP (Internet Protocol), pre adresovanie jednotlivých počítačov v sieti a protokol ICMP (Internet Control Message Protocol) pre posielanie chybových správ.
- transportná vrstva – zabezpečuje prenos správ z jedného koncového miesta na druhé, nezávisle na použitom type prenosovej linky. Zavádza adresovanie aplikácií pomocou čísla portu. Existujú dva protokoly, ktoré popisujú posielanie správ na tejto vrstve. Jedná sa o protokol TCP (Transmission Control Protocol), ktorý poskytuje spoľahlivý prenos dát, a protokol UDP (User Datagram Protocol). Tento protokol na rozdiel od protokolu TCP negarantuje prijímanie dát v rovnakom poradí, v akom boli odoslané, nekontroluje integritu a doručenie posielaných paketov, neposkytuje kontrolu zahltenia a preto je označovaný ako nespoľahlivý.
- aplikačná vrstva – obsahuje protokoly, ktorými posielajú dáta jednotlivé aplikácie (FTP, HTTP, Telnet, SMTP, ...) Tieto aplikácie majú pridelené štandardné čísla portov na ktorých očakávajú pripojenie klientov. Komunikácia prebieha na princípe klient - server.

Pri návrhu tohto modelu a protokolov, nebola vo veľkej miere zohľadňovaná sieťová bezpečnosť. To vyústilo do stavu, kedy je potrebné používanie ďalších špeciálnych protokolov, ktoré zabezpečujú komunikáciu internetom pred útokmi, odpočutím a zneužitím.

Obrázok 2.1: Porovnanie vrstiev modelu OSI a TCP/IP

Okrem modelu TCP/IP exituje aj model OSI (Open Systems Interconnection), ktorý sa používa ako referenčný model. Obsahuje až sedem vrstiev, no jednotlivé protokoly sa podľa neho striktne neriadia. Porovnanie TCP/IP modelu a OSI modelu je na obrázku 2.1 .

2.2 Bezpečnostné riziká

Nasledujúca časť práce popisuje bezpečnostné riziká, ktoré sú aktuálne pri pripojení do počítačovej siete. Je zameraná na popis útočníkov, ich motiváciu a na techniky útokov, ktoré používajú.

2.2.1 Útočníci

Útočníci sú ľudia, ktorí sa snažia získať neoprávnený prístup do počítačovej siete a tým pre seba získať materiálne, alebo iné výhody, prípadne spôsobiť škodu v napadnutej sieti. Často sú označovaný ako crackeri, a nesprávne aj ako hackeri.

Útočníkov môžeme rozdeliť do niekoľkých skupín. Podľa [13] sú to: odborníci na zabezpečenie, script - kiddies, hackeri bez práce, ideologický hackeri, hackeri - zločinci, priemyslový špióni a frustrovaný zamestnanci.

Odborníci na zabezpečenie – sú odborníci v oblasti počítačovej bezpečnosti, ktorí majú potrebné zručnosti k útoku na počítačovú sieť. Napriek tomu využívajú tieto schopnosti z ekonomických, alebo etických dôvodov na odhaľovanie nových bezpečnostných hrozieb, prípadne vývoju účinnejších metód obrany. Často sa jedná o bývalých crackerov, ktorých si organizácie zamestnali na testovanie bezpečnosti svojich systémov.

Script - kiddies – neskúsení ľudia, ktorí útočia za účelom bezplatného získania softvéru, alebo hudby a zvýšenia ich prestíže. Útočia hlavne nástrojmi, ktoré vytvoril niekto iný a podieľajú sa asi na 90 %-tách hackerskej činnosti na Internete.

Dospelí hackeri bez práce – ich motiváciou je zdolávanie náročných technických problémov a sú zruční v útokoch na sieť. V minulosti patrili medzi script - kiddies. Zaoberajú sa softvérovým, alebo mediálnym pirátstvom, tvorbou počítačových vírusov a nástrojov, ktoré script - kiddies používajú k útokom.

Ideologický hackeri – útočia aby podporili nejaký politický cieľ. Zvyčajne vedú útoky na webové stránky a systémy svojich odporcov, ktorých dôsledkom je napríklad odoprenie služby. Snažia sa vyhľadávať pozornosť médií a zvyčajne majú tichú podporu zo strany svojej vlády. V poslednom čase je táto skupina útočníkov na vzostupe a časom svoje útoky môže rozvinúť do informačnej vojny. Podľa [12] sú do celkovej bojovej stratégie štátov čoraz viac začleňované aj kybernetické sily, ktoré sú využívané ako doplnok k vojenským operáciám.

Zločinci a priemyselný špióni – obe skupiny majú rovnaký motív. Snažia sa svojou činnosťou získať peniaze bez ohľadu na škody, ktoré napáchajú. Rozdiel medzi nimi je ten, že jedni útočia priamo na inštitúcie, z ktorých ukradnú peniaze, a druhí sú za útoky platení. Ich zamestnávateľom býva konkurenčná firma, ktorá sa usiluje získať výhodu na trhu.

Frustrovaní zamestnanci – útočníci, ktorí sa nabúrajú do firemnej siete za účelom poškodiť firmu, v ktorej sú zamestnaní. Zvyčajne ich k tomu vedie pomsta. Táto skupina útočníkov má veľkú výhodu, lebo poznajú firemnú sieť a ich útoky sa pred uskutočnením odhaľujú len ťažko. Na druhej strane ich je ľahké vystopovať a použiť proti nim zákon.

Do počítačovej siete sa dá preniknúť niekoľkými spôsobmi. Prvý z nich je vniknutie cez Internet. Jedná sa o najdostupnejšie, a najľahšie zneužiteľné preniknutie do siete. Ochranu pred ním poskytuje firewall. Aj firewall však dokáže skúsený útočník obísť, napríklad nedostatočne zabezpečenou VPN (Virtual Private Network) sieťou. Časté útoky boli v minulosti vedené aj vytáčaným pripojením, na server RAS — server spájajúci viac typov komunikačných kanálov.

Ďalším spôsobom, ako sa dostať do siete je priame pripojenie sa k nej. Tento spôsob je využiteľný hlavne ak sa jedná o bezdrôtovú sieť, alebo ak sieť obsahuje WAP (Wireless Access Point) — prípojný bod pre bezdrôtový prístup. Toto pripojenie využíva protokoly rodiny 802.11x. Keďže dáta sa prenášajú bezdrôtovo, je toto spojenie ľahko odpočúvateľné. Preto sa odporúča používať šifrovanie technológiami WPA (Wi-Fi Protected Access) a WPA2. V minulosti sa používalo aj šifrovanie WEP (Wired Equivalent Privacy), no v dnešnej dobe je veľmi ľahko rozlúštiteľné.

Všetky technické zabezpečenia sú neúčinné proti poslednému spôsobu útoku, ktorým je fyzické vniknutie. Útočník sa pri ňom fyzicky dostane ku klientskému počítaču pripojenému k sieti, alebo k serverom a pripraví si tak základy pre budúce vniknutie.

2.2.2 Typy útokov

Technika útokov na počítačové siete sa neustále zdokonaľuje. V tejto časti je uvedený typický priebeh a techniky útoku, ako ich popisuje [13] .

Útok na počítačovú sieť sa dá rozdeliť do niekoľkých fáz. Prvá z nich je výber cieľu, kedy si útočník identifikuje konkrétny počítač, ktorý napadne. Nasleduje fáza získavania informácií o vybranom počítači. Tieto informácie môžu byť voľne dostupné, alebo získané použitím neútočných metód. Na základe zhromaždených informácií si útočník naplánuje metódu a spôsob útoku, ktorý použije. Poslednou fázou je samotný útok na vybraný cieľ.

Typy a techniky útokov sú nasledovné:

Odpočúvanie – najjednoduchšia metóda, ktorou útočník získava informácie o sieti. Sem patrí zachytávanie sieťovej komunikácie a jej následná analýza. Sieťová komunikácia môže prezradiť umiestnenie brán a smerovačov v skenovanej sieti a IP adresy počítačov nachádzajúcich sa v sieti. Ďalšie užitočné informácie sú objem prichádzajúcej a odchádzajúcej komunikácie, či zvláštne druhy komunikácie počítačov. Príkladom je identifikovanie DNS (Domain Name System) servera, na základe DNS požiadavkov posielaných na jeden server v sieti. Účinnou obranou proti takémuto skenovaniu je použitie aplikačných proxy a prekladu sieťových adries vo firewalli.

Ďalšou metódou získavania informácií o konkrétnom počítači je skenovanie IP adries a portov. Posielaním paketov ICMP Echo je možné zistiť IP adresy počítačov v sieti. Podľa stavu jednotlivých portov sa dá zistiť typ nainštalovaného operačného systému a služby, ktoré server poskytuje. Na základe týchto informácií je útočník schopný vybrať vhodné nástroje a techniky na ďalší útok. Jednou z možností obrany proti skenovaniu portov je nasadenie honeypotu do siete, ktorý bude slúžiť ako návnada. Podrobnejší popis tohto zariadenia je uvedený v sekcií 2.3.3 .

Pomocou služby DNS sa dá zistiť štruktúra siete, pretože DNS záznamy obsahujú IP adresu každého počítača v sieti. Útočník si môže vytvoriť program, ktorý sa javí ako peer DNS server požadujúci informácie. Správne nastavenie firewallu v tomto prípade nie je jednoduché z toho dôvodu, že lokálny DNS server potrebuje komunikovať aj s DNS servermi mimo lokálnej siete. Jednou z možností je zablokovať prístup k lokálnemu DNS serveru pre všetky počítače mimo lokálnej siete, s výnimkou nadradeného DNS servera.

Poslednou technikou odpočúvania je zachytenie hesla. Útočníkovi stačí zachytávať sieťovú komunikáciu, v ktorej môže nájsť posielané heslo a dokonca aj v nešifrovanej podobe. V prípade, že je algoritmus šifrovania slabý, je možné heslo dešifrovať a následne použiť.

Odoprenie služby – útok, ktorý je známy aj ako DoS (Denial of Service). Existuje niekoľko spôsobov, ako útokom dosiahnuť odoprenie služby. Jedným z nich je „ping of death“, kedy útočník pošle špeciálne upravený ICMP paket, ktorý spôsobí pád systému. V dnešnej dobe už systémy kontrolujú korektnosť formátu ICMP paketov, takže sú proti tomuto útoku odolné. Pád starších operačných systémov spôsobí aj útok teardrop, ktorý využíva slabiny v spätnom zoskupovaní fragmentov IP paketov.

Nasledovné útoky fungujú na princípe spotrebovania výpočetných prostriedkov servera, čím ho vyradia z prevádzky. Jedná sa o záplavu SYN paketov „SYN flood“ a ICMP paketov. SYN paket je prvý paket posielaný pri nadviazaní spojenia protokolom TCP. Počítač, ktorý obdrží tento paket alokuje časť svojich systémových prostriedkov na nové spojenie. Ak server zaplavíme veľkým počtom takýchto paketov, napadnutý server nebude schopný spracovávať nové požiadavky na pripojenie od legitímnych používateľov. V prípade, že SYN paketu nastavíme rovnakú zdrojovú aj cieľovú adresu, bude posielať pakety potvrdzujúce vytvorenie spojenia sám sebe.

Táto varianta sa nazýva „land“ útok. Na rovnakom princípe funguje záplava ICMP paketov typu „Echo Request“. Napadnutý počítač bude spotrebovávať svoju kapacitu hlavne na generovanie odpovedí pre príchodzie pakety.

Účinným útokom spôsobujúcim DoS, je útok „smurf“. Pri ňom útočník pošle veľké množstvo správ ICMP Echo Request na broadcast adresu siete, čo spôsobí preposlanie tejto správy všetkým počítačom v sieti. Počítače, ktoré obdržia túto správu, naviac vygenerujú odpoveď ICMP Echo Reply, a tým značne zvýšia objem komunikácie v sieti. Vylepšením útoku je určenie cieľového počítača, a nastavenie jeho adresy ako zdroj správ ICMP Echo Request. Na tento počítač sa následne odošlú všetky odpovede ICMP Echo Reply. Ďalšou variantou je útok „fraggle“, ktorý funguje na rovnakom princípe, ale namiesto protokolu ICMP využíva protokol UDP a správy typu echo.

Ďalším útokom je zanesenie vyrovnávacej pamäte DNS. Útočník pošle na DNS požiadavku falošnú odpoveď, ktorá môže obsahovať neplatné, alebo podvrhnuté IP adresy. Neplatnými adresami v odpovedi vyradí v sieti službu DNS, a podvrhnutými adresami môže presmerovať komunikáciu na server, ktorý je pod jeho kontrolou. Presmerovanie komunikácie je možné aj získaním kontroly nad smerovačom, zapojeným v sieti. Smerovače smerujú sieťovú komunikáciu na základe údajov v ich smerovacích tabuľkách. Vhodnou úpravou týchto tabuliek je možné presmerovať komunikáciu podľa potreby, prípadne nastaviť odoprenie služby pre počítače v sieti. Presmerovanie sa dá dosiahnuť aj posielaním paketov ICMP Redirect, ktorý informuje počítač o tom, že zasiela pakety na nesprávny smerovač.

Zneužívanie protokolov – útok, ktorý je založený na napadnutí chyby vo verejnej službe za účelom získania neoprávneného prístupu. Najbežnejšia forma je spôsobenie pretečenia vyrovnávacej pamäte, kedy útočník zaplní vyrovnávaciu pamäť pripravenými dátami, ktoré spôsobia spustenie škodlivého programu. Inštrukcie tohto kódu sú umiestnené na adrese, ktorá je ako návratová adresa podvrhnutá na správnu pozíciu v zásobníku.

Krádež totožnosti – prevzatie totožnosti dôveryhodného počítača v sieti, a jej využitie na získanie prístupu k ďalším počítačom. Pri tomto type útokov sa využíva priame smerovanie. Priamym smerovaním sa nastaví presná cesta paketu v sieti. Slúži hlavne na diagnostiku siete a riešenie problémov pri smerovaní. Pri vhodnom nastavení cesty, môžu dáta pochádzajúce od útočníka vyzerať ako dáta ktoré prichádzajú z iného, dôveryhodného zdroja. Príkladom je prevzatie totožnosti dôveryhodného DNS servera a posielanie upravených aktualizácií DNS záznamov.

Na útok sa dá využiť aj zachytené šifrované oprávnenie prihlásenia na server. Toto oprávnenie môže útočník znovu použiť aj neskôr, a získať tak prístup na daný server.

Prostredník – útočník, ktorý je v pozícií prostredníka medzi serverom v zabezpečenej sieti a klientom vo verejnej sieti, pričom si už vopred zaistil smerovanie komunikácie medzi týmito počítačmi na jeho server. Keď sa klient prihlási na server, útočník toto prihlásenie prevezme a prihlási sa na server pod menom klienta. Toto útočníkovi umožní sledovať a pozmeňovať všetku komunikáciu medzi klientom a serverom.

Nakoniec je potrebné spomenúť aj trójske kone a červy. Jedná sa o softvér, ktorý sa tajne nainštaluje do systému útočníkom, a často aj nič netušiacim používateľom. Tieto

programy poskytujú mechanizmus, ktorým môže útočník počítač vzdialene riadiť. Červy sú trójske kone, ktoré sa po sieti šíria automaticky.

2.3 Ochrana

V tejto časti sú popísané nástroje na prevenciu popísaných bezpečnostných hrozieb, ktoré budú použité v jednotlivých prípadoch použitia v kapitole 4.

2.3.1 Firewall

Firewall je zariadenie, umiestnené medzi chránenou a nechránenou časťou siete. Na základe množiny filtrovacích pravidiel definuje akú sieťovú komunikáciu bude blokovať a akú povolí. Existuje niekoľko typov firewallov, od jednoduchých paketových filtrov, cez stavové firewally[1], až po aplikačné proxy. Definícia firewallov a ich popis je čerpaný z [11].

Filtrovanie paketov patrí medzi kľúčové funkcie firewallov. Pri filtrovaní sa porovnávajú príchodzie pakety s databázou filtrovacích pravidiel a prepúšťajú sa iba tie pakety, ktoré vyhovujú pravidlám. Najčastejšie sa pakety filtrujú na základe položiek v ich hlavičke. [13]

Ochrana siete filtrovaním paketov sa dá prekonať niekoľkými spôsobmi. Jedným z nich je „spoofing“ — falšovanie paketov. Ide o zámernú zmenu zdrojovej adresy v hlavičke posielaného paketu, ktorý sa následne bez problémov dostane cez firewall. Ďalším je fragmentovanie paketov. Zo začiatku sa povoľoval prechod všetkých fragmentov, no keď túto vlastnosť začali využívať útočníci, zaviedla sa kontrola prvého fragmentu. V prípade, že bol tento fragment zablokovaný, pôvodnú správu nebolo možné opätovne zostaviť. Postupom času sa metódy inšpekcie fragmentov stále zdokonalovali. Nakoniec zostáva tunelovanie komunikácie, napríklad tunelovanie cez port 80 (HTTP komunikácia). V tomto prípade sa škodlivá komunikácia zabalí do paketov, ktoré firewall na základe informácií z hlavičky vyhodnotí ako HTTP komunikáciu.

Stavové firewally pracujú na rovnakom princípe ako paketové filtre. Na rozdiel od nich však obsahujú tabuľku stavov, ktorá uchováva informácie o stave spojení prepúšťaných firewallom. Do tejto tabuľky sa po analýze paketu zahajujúceho spojenie vloží nová položka o tomto spojení, a ostatné pakety daného spojenia už nie sú analyzované do takej hĺbky, ako prvý paket. Problém nastáva pri stavovom filtrovaní paketov protokolu UDP a ICMP. Tieto protokoly sú, na rozdiel od protokolu TCP, nespojované a preto žiadny stav nemajú. Nespojované protokoly sa filtrujú pseudo - stavovým spôsobom, pri ktorom sa sledujú určité znaky daného spojenia.

Posledným typom sú proxy firewally, ktoré majú často podobu proxy serverov. Proxy server zaisťuje komunikáciu určeným protokolom medzi počítačom v privátnej sieti a počítačom vo verejnej sieti. Na proxy servery väčšinou beží viac programových proxy a každé z nich spravuje komunikáciu jedným protokolom. Princíp činnosti je nasledovný. Klient nadviaže spojenie s proxy serverom a proxy server sa následne spojí s cieľovým serverom. Medzi klientom a cieľovým serverom nie je priame spojenie a všetka komunikácia medzi nimi prechádza cez proxy server. Ich nevýhodou je, že sú v porovnaní s ostatnými typmi firewallov najpomalšie.

Aplikačné proxy dokonca umožňujú aj filtrovanie obsahu prenášanej komunikácie. Touto technikou je možné blokovať nevhodný, alebo nebezpečný obsah webových stránok, a obmedziť šírenie spamu a trójskych koní. [13]

[1] Príkladom firewallu, ktorý implementuje stavové aj bezstavové filtrovanie paketov je *iptables*. Informácie o ňom sú dostupné na adrese http://www.netfilter.org/.

2.3.2 IDS

Intrusion Detection System, ako ho popisuje [11] , je systém ktorý detekuje nežiadúce a potenciálne nebezpečné aktivity v sieti a upozorňuje na ne. V sieti môže byť umiestnené jedno zariadenie, ktoré komunikáciu zachytáva a hneď aj analyzuje. Taktiež je možné rozmiestniť v sieti viacero IDS senzorov, ktoré budú monitorovať komunikáciu v dôležitých bodoch siete. Tieto senzory posielajú dáta na centrálny server, kde sa porovnávajú a vyhodnocujú.

Analýza komunikácie je založená na vyhľadávaní signatúr v analyzovanej komunikácii. Jednotlivé signatúry popisujú rôzne známe sieťové útoky a priebežne sa aktualizujú. Ak sa v komunikácií takáto signatúra objaví, IDS vygeneruje výstrahu, alebo udalosť, prípadne tento nález zaznamená. Útočníci sa proti IDS systémom bránia tak, že svoje útoky pozmenia, aby sa vyhli odhaleniu. Toto pozmeňovanie sa označuje ako IDS evasion.

Časť z takto vygenerovaných výstrah môžu tvoriť falošné výstrahy — false positives. Jedná sa o neškodnú komunikáciu, ktorá je vyhodnotená IDS systémom ako útok. V prípade, že systém útok neodhalí, jedná sa o false negatives — falošné negatívne zhodnotenie. Výskyt oboch typov udalostí sa dá redukovať vhodným výberom systému IDS a použitím vhodných signatúr.

Vyššie popísaný IDS systém patrí do skupiny Network-based IDS. Okrem nej existuje aj skupina Host-based IDS. Tieto systémy detekcie narušenia monitorujú sieťové aktivitu daného serveru, jeho súborový systém a operácie používateľov. Výhodou tohto typu IDS systémov je možnosť monitorovania aktivity konkrétneho používateľa a tiež sledovania komunikácie, ktorá sa po sieti prenáša v šifrovanej podobe.

Kontrola integrity súborového systému slúži na detekciu neoprávnených zmien v systéme. Využíva sa porovnávanie aktuálneho stavu súborového systému so „snímkom“. Tento snímok predstavuje dôveryhodný referenčný stav súborového systému v minulosti. Pri zistení významných odchýlok je generovaná výstraha. Integrita jednotlivých súborov sa kontroluje pomocou kontrolného súčtu, ktorý sa porovnáva s pôvodným kontrolným súčtom súboru.

Novinkou sú aj gateway IDS systémy, ktoré kombinujú funkčnosť firewallu a IDS systému v jednom zariadení. Ich výhodou je schopnosť aktívne reagovať na bezpečnostné incidenty, pričom niektoré z nich môžu byť zastavené skôr, ako sa dostanú cez firewall. Fakt, že je viac služieb spojených v jednom zariadení má aj svoje nevýhody, a to z hľadiska bezpečnosti, výkonnosti a poruchovosti. V dnešnej dobe však tieto hybridné zariadenia nie sú natoľko vyspelé, aby sa ich používanie výrazne presadilo na úkor tradičných IDS systémov.

Okrem systémov IDS existujú aj systémy IPS (Intrusion Prevention System). Tieto systémy okrem detekcie bezpečnostných narušení dokážu na nájdené incidenty aj aktívne reagovať.

Program *snort*[2] je príkladom systému, ktorý kombinuje funkčnosť IDS a IPS systému.

2.3.3 Honeypot

V bakalárskej práci [8] je honeypot popísaný ako program simulujúci bežiace sieťové služby. Jedná sa o návnadu, ktorá sleduje sieťovú komunikáciu a zaznamenáva informácie o útočníkových aktivitách na danom servery. Keďže tento server, ani jeho služby nie sú využívané používateľmi, každé spojenie s ním je považované za podozrivé.

[2]Program *snort* je voľne dostupný na adrese http://www.snort.org/ .

Honeypoty poskytujú záznamy, z ktorých je možné analyzovať postup útoku a zvyky útočníkov. Na základe zhromaždených informácií sa zdokonaľujú a vyvíjajú nové metódy na ochranu počítačových sietí. V sieti môže byť ako návnada umiestnený program simulujúci službu, celý server simulujúci poskytovanie sieťových služieb, alebo celé siete takýchto serverov, ktoré sa nazývajú honeynets. [13]

Príkladom je Honeynet Project[3], ktorý prevádzkuje sieť honeypotov a zaoberá sa vývojom bezpečnostných zariadení na základe analýzy zachytených dát.

Aj samotný honeypot sa však môže stať cieľom útoku a preto je vhodné priebežné sledovanie tohto systému a bezpečné zaobchádzanie s jeho zaznamenanými systémovými informáciami. Ideálne je uchovávať tieto informácie mimo honeypotu, pretože po jeho prezradení bývajú prvým cieľom útočníka.

2.3.4 NetFlow

Popis protokolu NetFlow v tejto sekcií, je čerpaný z bakalárskej práce [9]. Tento sieťový protokol je vyvinutý firmou Cisco Systems, Inc. a slúži na zber záznamov o IP tokoch na sieti. Podľa technického prehľadu [5] tvorí tok sekvencia paketov, ktorá je definovaná rovnakými hodnotami nasledovných položiek:

- zdrojová IP adresa
- cieľová IP adresa
- typ IP protokolu
- zdrojový port
- cieľový port
- vstupné rozhranie NetFlow sondy
- Class of Service

V monitorovanej sieti môžu byť zapojené viaceré NetFlow sondy, ktoré vytvárajú NetFlow záznamy a exportujú ich na jeden NetFlow kolektor. Exportovanie záznamov prebieha protokolom UDP, alebo SCTP (Stream Control Transmission Protocol). Pri analýze sondy nezasahujú do analyzovanej komunikácie a sú tak neviditeľné z pohľadu potenciálneho útočníka.

Analýza sieťovej komunikácie prebieha podľa [2] nasledovne. Sonda vytvorí NetFlow záznam pre každý aktívny tok, ktorý je umiestnený do cache pamäte. Podľa zachytávanej komunikácie sa aktualizujú príslušné NetFlow záznamy. Tieto záznamy sú periodicky exportované na NetFlow kolektor a to pri nasledovných udalostiach: uplynutie inactive timeoutu — ak je tok istú dobu neaktívny, uplynutie active timeoutu — ak je tok danú dobu aktívny, zaplnenie cache pamäte a ukončenie TCP spojenia.

NetFlow záznamy obsahujú okrem spomenutej pätice údajov aj ďalšie informácie o sieťovej komunikácií, ako sú: sekvenčné číslo, SNMP index vstupného a výstupného rozhrania, časovú značku začiatku a konca toku, počet bajtov a paketov v toku a TCP príznaky. Dve najpoužívanejšie verzie protokolu NetFlow sú: NetFlow v5 a NetFlow v9. Na základe verzie NetFlow v9 vznikol nový štandard IPFIX (Internet Protocol Flow Information eXport), ktorý začína byť mohutne podporovaný výrobcami sieťových zariadení. [16]

[3] Ďalšie informácie o tomto projekte sú dostupné na adrese http://www.honeynet.org/ .

Podľa zhromaždených NetFlow záznamov sa dajú zistiť užitočné informácie o sledovanej sieti, ako sú: majoritný zdroj sieťovej komunikácie, typ prenášanej komunikácie, či dokonca neoprávnený prístup do siete. NetFlow záznamy tiež používajú aj poskytovatelia internetového pripojenia na účtovanie poskytovaných sieťových služieb. [9]

Kapitola 3

Popis zariadenia NIFIC

Paketový filter NIFIC (Network Interface Card with Packet Filtering and Forwarding) je zariadenie určené na filtrovanie sieťových tokov pri plnej rýchlosti pripojenej linky. V súčasnosti dokáže pracovať na linkách s rýchlosťou až 10 Gb/s. Tento paketový filter je hardvérovo akcelerovaný a pracuje na platforme kariet rodiny COMBOv2. Popis zariadenia, uvedený v tejto kapitole je čerpaný z príručky [15].

Klasifikácia a filtrovanie paketov prebieha na základe sady pravidiel, ktoré popisujú akým spôsobom bude sieťová komunikácia filtrovaná, či presmerovaná. Aktuálna verzia podporuje filtráciu až podľa 2048 pravidiel súčasne a umožňuje meniť sadu filtrovacích pravidiel bez straty jediného paketu. Pakety je možné filtrovať podľa ich nasledovných položiek:

- zdrojová a cieľová IPv4 adresa
- zdrojový a cieľový port
- zdrojová a cieľová MAC adresa
- IPv4 protokol
- TCP príznaky
- číslo vstupného rozhrania

Taktiež je podporované aj replikovanie paketov, preposlaním na viac rozhraní súčasne a orezávanie paketov, ktoré sú poslané na softvérové rozhranie, na požadovanú veľkosť. Podrobnejšie informácie o formáte pravidiel a princípe klasifikácie paketov sú uvedené v podkapitole 3.1.

Existujú dva režimy práce tohto zariadenia. V prvom režime pracuje NIFIC ako samostatný paketový filter, ktorý je konfigurovaný lokálne z hosťovského počítača, v ktorom je zapojená COMBO karta. Popis lokálnej konfigurácie je uvedený v sekcií 3.2.1. Ďalšou možnosťou je jeho konfigurácia z monitorovacieho centra, kedy je umožnené aj exportovanie vyfiltrovaných paketov na vzdialené počítače. Princíp vzdialenej konfigurácie je popísaný v sekcií 3.2.2.

NIFIC môže pracovať na dvoch typoch COMBO kariet. Je to karta COMBO-10G2, ktorá poskytuje dva ethernetové porty s priepustnosťou až 10 Gb/s a karta COMBO-1G4, ktorá poskytuje štyri porty s priepustnosťou 1 Gb/s. Firmvér pre kartu COMBO-1G4 však v súčasnosti umožňuje používať iba dva zo štyroch portov. Okrem ethernetových portov sa

tu nachádza jedno softvérové rozhranie (PCI - E), pripojené na hosťovský počítač, ktoré je ešte rozdelené na 14 virtuálnych rozhraní (rozhrania číslo 2 – 15). Priepustnosť z hardvéru do softvéru hosťovského počítača je okolo 5 Gb/s.

Toto zariadenie je možné použiť napríklad ako bezstavový firewall s hardvérovou akceleráciou, dvojportovú sieťovú kartu, či ako analyzátor jednotlivých typov sieťovej komunikácie. Jednotlivé prípady použitia sú popísané v kapitole 4.

3.1 Princíp klasifikácie paketov

Pakety prichádzajúce na vstupné rozhranie sú klasifikované na základe zadanej sady filtrovacích pravidiel. Tieto pravidlá sú pri ich vložení predspracované konfiguračným softvérom, ktorý vygeneruje binárne dáta, podľa ktorých dokáže hardvér rýchlo priradiť ku klasifikovaným paketom výsledné pravidlo.

Sada filtračných pravidiel je zoznam pravidiel, ktoré definujú hodnoty položiek v hlavičke paketov a akciu, ktorá sa vykoná, ak paket nadobúda určené hodnoty položiek v jeho hlavičke. Tieto pravidlá sú zapísané v jazyku, ktorý je podobný jazyku OpenBSD Packet Filter. Tento jazyk nie je case sensitive, čo znamená že nie je rozdiel medzi malými a veľkými písmenami. Usporiadanie pravidiel v rámci sady určuje ich prioritu, pričom platí že pravidlo uvedené na začiatku sady má najväčšiu prioritu. NIFIC porovnáva údaje z paketu s pravidlami od začiatku sady pravidiel až do konca. Posledné pravidlo je implicitné, a vyhovuje mu každý prijatý paket. Sada pravidiel je v prípade lokálnej konfigurácie umiestnená v textovom súbore, pričom platí že jeden riadok zodpovedá jednému pravidlu. V prípade vzdialenej konfigurácie je sada pravidiel definovaná v XML súbore a jednotlivé pravidlá sú uzavreté v príslušných tagoch.

Pravidlo sa skladá z čísla pravidla (priorita pravidla), definície hodnôt v hlavičke paketu a z akcie, ktorá sa má s vyhovujúcimi paketmi urobiť. Pravidlo definuje požadované číslo vstupného rozhrania, na ktorom bol paket prijatý, číslo protokolu, zdrojovú IPv4 adresu, zdrojovú MAC adresu a zdrojový port, ďalej cieľovú IPv4 adresu, cieľovú MAC adresu a cieľový port a nakoniec TCP príznaky. Okrem toho môžme každému paketu priradiť flow id — číslo, ktorým sa dá definovať sieťový tok, popísaný viacerými pravidlami. V pravidle sa namiesto jednej hodnoty IPv4 adresy, MAC adresy, protokolu a čísla portu dajú definovať zoznamy, alebo rozsahy hodnôt týchto položiek.

Ďalej je v pravidle definovaná akcia, ktorá určí či bude paket preposlaný na jedno, prípadne viac rozhraní, alebo bude paket zahodený (blokovaný). Pri poslaní paketu na softvérové rozhranie je možné nastaviť aj orezanie paketu na zadanú veľkosť.

Pravidlá sa po ich zadaní najskôr softvérovo predspracujú a výsledky sa nahrajú do hardvéru. Klasifikácia paketov sa potom riadi nasledovným algoritmom:

1. Po prijatí paketu na vstupnom rozhraní, sa extrahujú informácie z jeho hlavičky.

2. Jednotlivé položky z hlavičky sa paralelne spracujú algoritmom LPM (Longest Prefix Match). Pre spracovanie jednotlivých položiek sa používajú rôzne metódy, ako treebitmap algoritmus, alebo CAM pamäť na čipe.

3. Výsledné slovo z LPM vstúpi do perfektnej rozptyľovacej funkcie, ktorá zámernými kolíziami eliminuje vznik pseudopravidiel tak, že sa zobrazia na rovnaké číslo. Rozptyľovacia funkcia využíva dáta, ktoré boli predspracované softvérom a nahrané do externej pamäte QDR - II. Výstupom tejto funkcie je výsledné číslo pravidla.

4. Nakoniec je nutné skontrolovať, či paket naozaj odpovedá pravidlu, ktorého číslo sme dostali v predchádzajúcom kroku. Je to potrebné z toho dôvodu, že rozptyľovacia funkcia vracia číslo pravidla aj v prípade, keď paket žiadnemu pravidlu nevyhovuje.

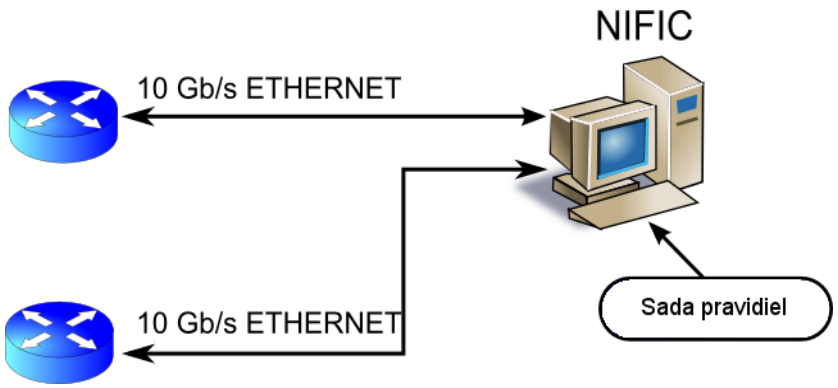
Takto je určené pravidlo, ktorému daný paket vyhovuje. Následne sa s paketom vykoná akcia, ktorá je v rámci pravidla definovaná. [6]

3.2 Softvér

Softvérové nástroje umožňujú používať NIFIC v dvoch režimoch činnosti. V prvom režime je konfigurovaný lokálne, z toho istého počítača, na ktorom je umiestnený a v druhom režime je konfigurovaný zo vzdialeného počítača.

3.2.1 Lokálna konfigurácia

Pri lokálnej konfigurácií sa sada filtrovacích pravidiel nahráva z lokálneho stroja, na ktorom je NIFIC zapojený. V tomto prípade je možné filtrovanie komunikácie v rámci pripojených ethernetových liniek, a jej prípadné posielanie do softvéru lokálneho počítača, pomocou štandardných sieťových rozhraní. Princíp lokálnej konfigurácie je na obrázku 3.1 .



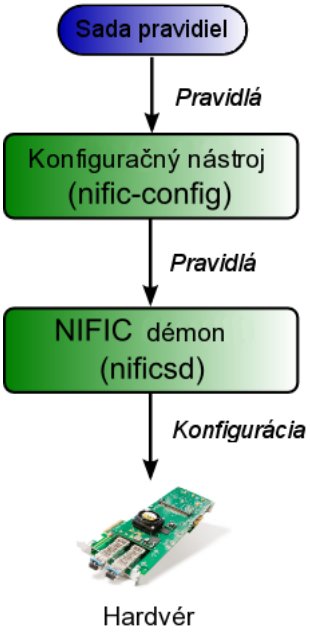
Obrázok 3.1: NIFIC ako lokálne konfigurovaný filter

Hlavným softvérovým nástrojom je démon *nificsd*. Tento konfiguračný démon zabezpečuje inicializáciu a bootovanie COMBO karty, nahrávanie pravidiel a generovanie konfigurácie pre firmvér. S ostatnými softvérovými nástrojmi komunikuje pomocou systému D-BUS.

Princíp nahrávania novej sady filtrovacích pravidiel je popísaný na obrázku 3.2 a jeho postup je nasledovný:

- filtrovacie pravidlá sa zapíšu do textového súboru
- súbor s pravidlami je spracovaný softvérovým nástrojom *nific-config*
- *nific-config* pošle požiadavky softvérovému démonovi *nificsd*, ktorý nahrá novú sadu pravidiel do hardvéru

Počas činnosti zariadenia je možné preposielať pakety z jej virtuálnych rozhraní na novovytvorené štandardné sieťové rozhrania. Tieto štandardné sieťové rozhrania môžu byť využité na príjem aj odosielanie paketov ďalšími aplikáciami. Vytváranie týchto rozhraní,



Obrázok 3.2: Lokálna konfigurácia zariadenia NIFIC

ich IP adresy, názvy a zodpovedajúce virtuálne rozhrania, sa definujú v konfiguračnom súbore `nific.conf`. Na základe týchto nastavení spustí konfiguračný démon nástroj *nific2tap*. Jedna inštancia tohto nástroja zabezpečí vytvorenie jedného štandardného sieťového rozhrania a jeho namapovanie na virtuálne rozhranie zariadenia NIFIC.

Pakety, ktoré nespadajú do protokolu IPv4 sa smerujú podľa nastavení v konfiguračnom súbore `nific.conf`. Pomocou bitmapy rozhraní sa pre každé vstupné rozhranie určia výstupné rozhrania, na ktoré budú tieto pakety preposlané. Taktiež sa dá nastaviť ich prípadné orezanie na zadanú dĺžku. Ďalej sú v tomto súbore uložené predvolené cesty k súborom firmvéru, ktoré sa nahrajú do jednotlivých typov COMBO karty a XML súbory popisujúce design a iné nastavenia, ktoré sú podrobne popísané v [15].

Pakety, ktoré sú po klasifikácií odoslané na softvérové rozhrania, môžu byť ďalej poslané do hostiteľského počítača na ďalšie spracovanie niekoľkými spôsobmi. Prvý z nich, pomocou nástroja *nific2tap* bol popísaný vyššie. Jeho výhodou je, že pakety môžu byť posielané aj opačným smerom — zo softvéru do siete. Nevýhodou je však obmedzená priepustnosť na 1 Gb/s.

Ďalším spôsobom je použitie knižnice *libpcap*, ktorá sa bežne využívaná na zachytávanie paketov v linuxových systémoch. V tom prípade je možné využiť plnú priepustnosť do softvéru, ktorá je 5 Gb/s. Nevýhodou tohto prístupu je, že pakety nemôžu byť posielané smerom zo softvéru do siete.

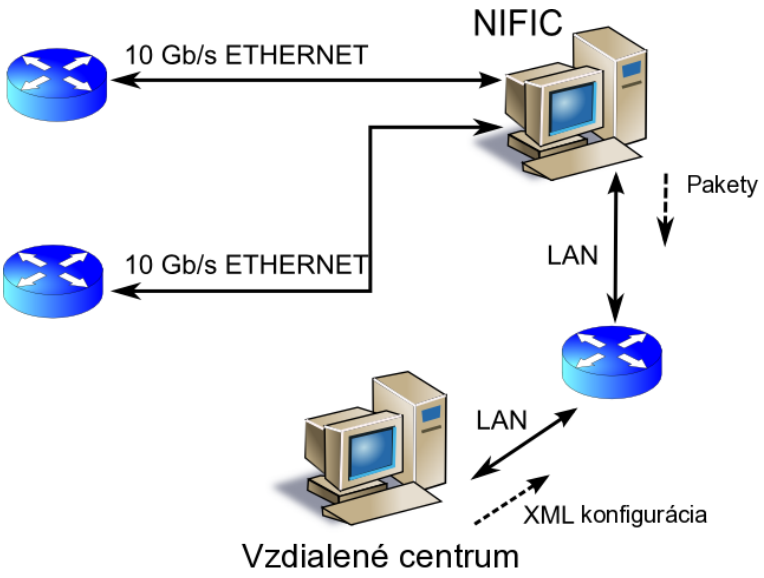
Poslednou možnosťou sú softvérové nástroje, používajúce knižnicu *libsze2*[1] Tento spôsob je vhodný hlavne pre jednoduché testovacie účely.

3.2.2 Vzdialená konfigurácia

V tomto režime činnosti sa NIFIC konfiguruje zo vzdialeného monitorovacieho centra, z ktorého posiela XML súbory obsahujúce novú konfiguráciu. Pakety môžu byť po klasifikácií

[1]Knižnica *libsze2* je vyvíjaná v rámci projektu Liberouter.

odoslané tak ako pri lokálnej konfigurácií na dva ethernetové porty, alebo virtuálne porty, prípadne môžu byť exportované na vzdialené počítače. Tento spôsob konfigurácie je znázornený na obrázku 3.3 .



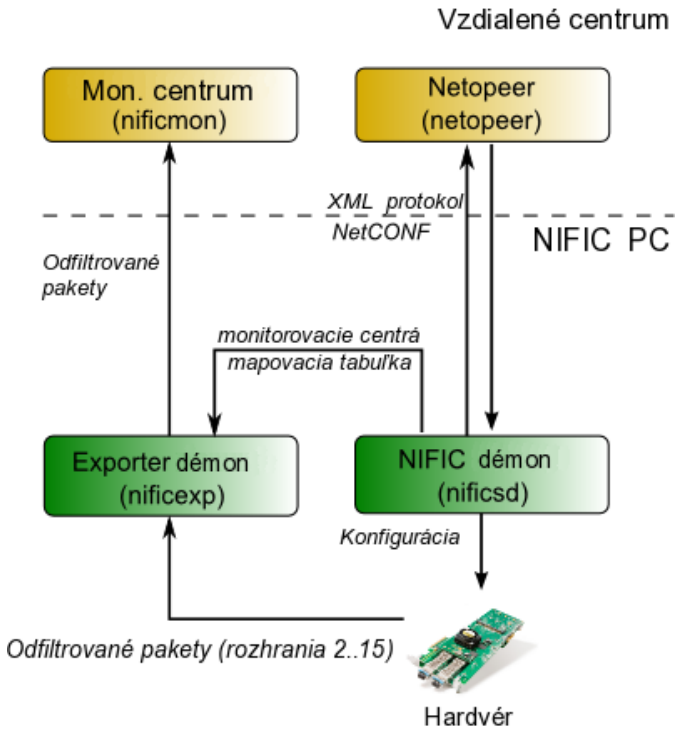
Obrázok 3.3: NIFIC ako vzdialene konfigurovaný filter

Posielanie konfiguračných XML súborov, obsahujúcich sadu filtrovacích pravidiel a nastavenie exportovania paketov, zaisťuje dvojica programov: *netopeer* (označovaný aj ako netopeer manager) a *netopeer-agent*. Tieto programy pracujú na princípe klient - server. Program *netopeer* poskytuje konzolové rozhranie na monitorovacom centre, pre vzdialenú konfiguráciu. Pomocou neho sa používateľ pripojí na *netopeer-agent*, ktorý beží na počítači, ku ktorému je pripojený NIFIC. Manažér posiela príkazy a konfiguračné XML súbory agentovi protokolom NETCONF. Program *netopeer-agent* tieto príkazy spracuje a pošle ich konfiguračnému démonovi *nificsd*, ktorý podľa nich nakonfiguruje hardvér. [15]

NIFIC používa tri konfiguračné súbory, ktoré sa nazývajú: startup datastore, running datastore a candidate datastore. Startup datastore obsahuje filtračné pravidlá a nastavenie exportu paketov, ktoré sa načíta pri štarte. Umiestnenie tohto súbora je špecifikované v konfiguračnom súbore `nific.conf` . Running datastore obsahuje aktuálne nastavenie, podľa ktorého NIFIC filtruje a exportuje pakety. Pri zmene obsahu tohto úložiska sa zmeny prenesú pomocou démona *nificsd* aj do hardvéru. Candidate datastore je určené na pripravenie sady filtračných pravidiel pomocou postupného pridávania a odoberania jednotlivých pravidiel. Toto úložisko sa po skončení úprav skopíruje do running datastore a pravidlá v ňom sa začnú používať.

Spolupráca softvérových nástrojov používaných v režime vzdialenej konfigurácie je znázornená na obrázku 3.4 .

Pri režime vzdialenej konfigurácie je možné aj exportovanie odfiltrovaných paketov, z virtuálnych rozhraní na vzdialené počítače. Export týchto paketov zabezpečujú nástroje *nificexp* a *nificmon*, na ktorých vývoji som sa podieľal aj ja. Exportér *nificexp*, ktorý je v prípade potreby automaticky spustený démonom *nificsd* spracuje XML súbor obsahujúci parametre exportu paketov a podľa nich odosiela pakety na vzdialené počítače. Na týchto počítačoch beží *nificmon*, ktorý slúži na zachytávanie exportovaných paketov a ich prípadné preposlanie na štandardné sieťové rozhranie, kde sú k dispozícii ďalším aplikáciam.



Obrázok 3.4: Softvérová architektúra zariadenia NIFIC pri vzdialenej konfigurácií

Parametre exportovania sa posielajú spolu s filtrovacími pravidlami v XML súbore a dajú sa nastaviť pre každé virtuálne rozhranie samostatne. Sú nasledovné:

- číslo virtuálneho rozhrania, z ktorého budú pakety exportované
- adresa vzdialeného počítača, na ktorý sa budú pakety exportovať
- číslo portu vzdialeného počítača
- protokol použitý pri prenose paketov (TCP/UDP)
- mód prenosu

Mód prenosu paketov určuje, či sa bude odfiltrovaným paketom pred exportom pripájať hlavička s informáciami o čísle pravidla, na základe ktorého boli preposlané na toto rozhranie, softvérová časová značka a číslo toku (flow id) — ak bolo definované v sade filtrovacích pravidiel.

3.3 Firmvér

Firmvér pre zariadenie NIFIC pracuje na platforme NetCOPE, ktorá je vyvíjaná v rámci projektu Liberouter. Táto platforma umožňuje rýchlu implementáciu hardvérovo akcelerovaných aplikácií a poskytuje jednotné rozhranie pre prácu s hardvérom. [14]

Hardvérové spracovanie paketu je nasledovné. Pakety sa v hardvéri prenášajú protokolom FrameLink. Po zachytení paketu na vstupnom rozhraní prebieha analýza hlavičiek paketov, tromi jednotkami HFE. Výsledkom tejto analýzy sú jednotlivé položky z hlavičiek paketov.

Po analýze sa paket uloží do paketového bufferu a položky z hlavičiek sa začnú klasifikovať klasifikačným algoritmom, popísaným v podkapitole 3.1 . Klasifikáciou sa určí číslo pravidla, podľa ktorého bude paket filtrovaný. Nakoniec klasifikácie sa podľa akcie v príslušnom pravidle vytvorí bitmapa výstupných rozhraní, na ktoré bude paket preposlaný.

Jednotka Header Insert pripojí výsledok klasifikácie (číslo pravidla a bitmapu rozhraní) k paketu, čakajúcemu v paketovom buffery. Takto klasifikované pakety vstupujú do crossbaru, ktorý podľa bitmapy prepošle paket na jedno, alebo viac rozhraní, prípadne ho zahodí. Paket je nakoniec poslaný na výstupné rozhranie. V prípade výstupu na softvérové rozhranie, je možné paket orezať v jednotke trimming unit. [6]

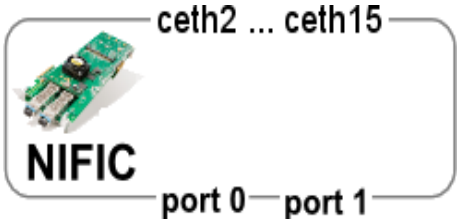
Kapitola 4

Prípady použitia

Táto kapitola sa zaoberá popisom jednotlivých prípadov použitia zariadenia NIFIC, ktoré riešia rôzne bezpečnostné problémy so sieťou, alebo vylepšujú činnosť a flexibilitu sieťových zariadení. Konfiguračné súbory a súbory s pravidlami pre jednotlivé prípady použitia, sa nachádzajú v prílohe. Pri tvorbe prípadov použitia v podkapitolách 4.1, 4.5, 4.6 a 4.7, som vychádzal z možností použitia tohto zariadenia, uvedených v [15].

4.1 Dvojportová sieťová karta

Zariadenie NIFIC môžeme využiť ako NIC (Network Interface Card) — štandardnú sieťovú kartu. Keďže COMBO karta, na ktorej je nahraný firmvér, obsahuje dva ethernetové porty, môžeme vytvoriť dvojportovú sieťovú kartu s priepustnosťou až 10 Gb/s.



Obrázok 4.1: NIFIC ako sieťová karta

Obrázok 4.1 znázorňuje NIFIC, ktorý má k dispozícii dva ethernetové porty a 14 softvérových rozhraní. Jednou z možností ako ho konkrétne zapojiť, je prepojenie dvoch lokálnych sietí. Jedna bude zapojená na port 0. Pakety z nej sa budú preposielať na štandardné sieťové rozhranie `ceth2` a opačným smerom. Druhá sieť sa zapojí na port 1. Pakety z tejto siete sa budú preposielať na softvérové rozhranie `ceth3` a naopak. Softvérovým rozhraniam môžme priradiť aj IP adresy, ktoré budú zodpovedať IP adresám pripojených lokálnych sietí. Takto zapojený NIFIC bude fungovať ako dvojportová sieťová karta.

Pravidlá zabezpečujúce prepojenie portov a softvérových rozhraní sú nasledovné:

```
10 pass 2 on 0
20 pass 0 on 2
30 pass 3 on 1
40 pass 1 on 3
```

Identickým spôsobom sa budú smerovať aj pakety, ktoré nespadajú do IPv4 komunikácie.

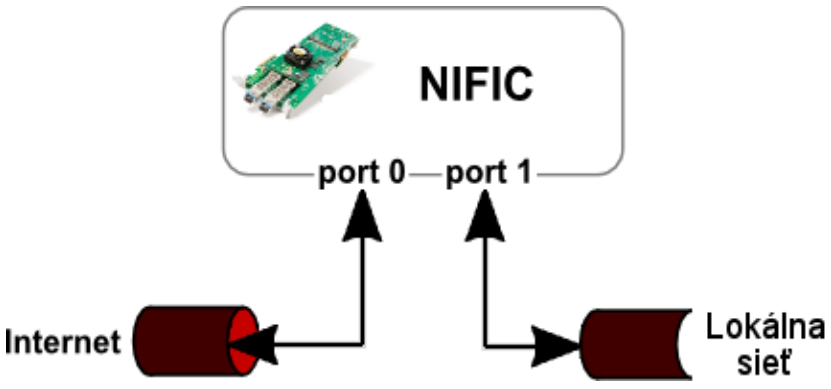
Na rozdiel od klasickej sieťovej karty, môže NIFIC zároveň chrániť pripojené siete, ako jednoduchý firewall, ktorého použitie je popísané v podkapitole 4.2. Taktiež sa dá istý typ komunikácie odfiltrovať a preposlať na vlastné softvérové rozhranie, kde môže byť ďalej spracovaný špeciálnym softvérom. Príkladom je použitie uvedené v podkapitole 4.8.

4.2 Firewall

Firewall patrí medzi základné prvky ochrany počítačových sietí. Dokáže filtrovať komunikáciu podľa typu a tým umožňuje blokovanie potenciálne nebezpečných typov komunikácie. Existuje viac druhov týchto zariadení, no v tomto prípade použitia sa budeme venovať najjednoduchšiemu typu firewallu – paketovému filtru. Paketový filter je založený na porovnávaní informácií z hlavičky paketov, s databázou pravidiel. Filter prepustí iba tie pakety, ktoré vyhovujú sade filtračných pravidiel [13]. Podrobný popis firewallu a jeho činnosti je uvedený v sekcií 2.3.1.

Zariadenie NIFIC umožňuje filtrovanie paketov na základe dát v ich hlavičkách a preto sa dá použiť ako paketový filter. Okrem tejto základnej funkčnosti poskytuje aj niekoľko výhod. Filtrovanie paketov je hardvérovo akcelerované a preto je možné nasadiť ho do vysokorýchlostných sietí, ako bezstavový firewall. Okrem toho poskytuje aj možnosť zmeny sady pravidiel počas behu, čím získava na flexibilite.

Firewall sa do siete umiestňuje medzi jej chránenú a nechránenú časť. Často teda býva zapojený ako prvé zariadenie hneď za bránou do internetu, čím chráni celú lokálnu sieť. Veľmi výhodným býva vytvorenie demilitarizovanej zóny, kedy sa firewallom rozdelí sieť na dve hlavné časti s rôznym stupňom zabezpečenia. NIFIC má v súčasnosti dve ethernetové rozhrania, a preto nie je vhodný na na vytvorenie demilitarizovanej zóny. Tento nedostatok sa však dá odstrániť prepínačom (zariadením switch), prípadne ďalším zariadením NIFIC. Ďalšou možnosťou je vytvorenie demilitarizovanej zóny pomocou softvérového rozhrania. V tom prípade bude demilitarizovaná zóna zahŕňať iba server, na ktorom je pripojený NIFIC a všetky služby, ktoré v nej majú byť umiestnené musia byť na jednom serveri. Riešením by bola aj úprava firmvéru pre COMBO kartu typu 1G4 tak, aby sa dali použiť aspoň 3 ethernetové porty. Nevýhodou však bude menšia priepustnosť dát (1 Gb/s), ako pri použití designu s dvomi portami (10 Gb/s).



Obrázok 4.2: NIFIC zapojený ako firewall

Zapojenie tohto prípadu použitia do siete je na obrázku 4.2. Vstup do lokálnej siete je prepojený na port 1 a port 0 smeruje do internetu.

Pravidlá, podľa ktorých sa bude filtrovať sieťová komunikácia sa zvyčajne tvoria dvomi spôsobmi:

- všetky pakety sa budú implicitne blokovať, a povolí sa iba komunikácia, ktorá je potrebná
- všetky pakety sa budú implicitne prepúšťať cez firewall a blokovať sa bude iba komunikácia, ktorú označíme za podozrivú, lebo nesie znaky útoku, prípadne je o nej známe, že sa na útok často využíva

Prvý spôsob je bezpečnejší, lebo máme explicitne zadané, ktoré typy komunikácie sú povolené. Ak aj povoľujeme komunikáciu, ktorá so sebou nesie bezpečnostné riziká, vieme o nej, a počas prevádzky s touto hrozbou počítame. Ak však použijeme druhý prístup, môžme zabudnúť blokovať typ komunikácie, o ktorej je všeobecne známe, že sa používa na útok, alebo je inak nebezpečná.

Jediným problémom je vytvoriť pravidlá, podľa ktorých bude NIFIC filtrovať komunikáciu. Tieto filtrovacie pravidlá sa zapisujú v jazyku, ktorý je podobný jazyku OpenBSD Packet Filter [15]. Teoreticky je možné transformovať ľubovolné pravidlo pre bezstavový paketový filter do tvaru, ktorý akceptuje NIFIC.

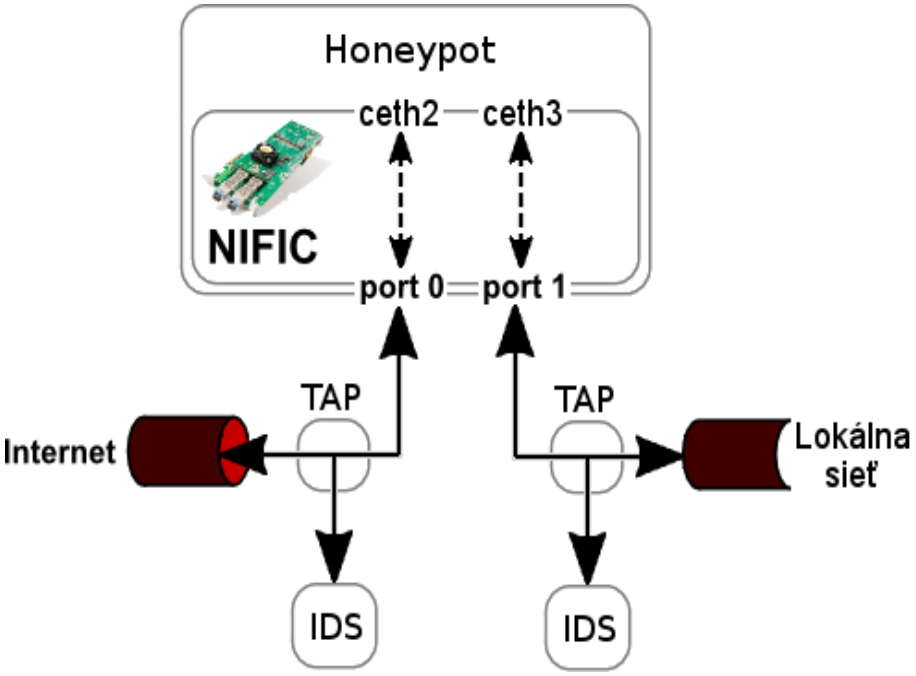
4.3 Flexibilný honeypot

Lokálnu sieť chráni najčastejšie firewall, ktorý sám o sebe nie je postačujúca obrana lokálnej siete, a preto je potrebné používať aj ďalšie nástroje na jej ochranu. Jednou z možností je umiestniť do siete systém IDS a honeypot. Honeypot sa zvyčajne umiestňuje do siete rovnako ako hociktorý iný server, aby nebolo na prvý pohľad útočníkovi jasné, že ide o návnadu. Taktiež je potrebné, aby sa útočník zameral na honeypot, a neohrozoval tak ostatné počítače v sieti. NIFIC môžeme využiť na podvrhnutie honeypotu útočníkovi tak, že komunikáciu ktorú označí IDS systém ako škodlivú, budeme preposielať priamo na honeypot. Význam honeypotu, a jeho popis je uvedený v sekcií 2.3.3.

Podrobný popis IDS systému, ktorý analyzuje komunikáciu v sieti a hľadá rôzne znaky indikujúce útok alebo zneužitie, je uvedený v sekcií 2.3.2. Ak máme k dispozícií jeden IDS senzor, existujú dve možné umiestnenia tohto senzora v okolí firewallu. Buď ho umiestnime do vonkajšej siete — pred firewall, odkiaľ bude informovať o všetkých útokoch na sieť, aj o tých ktoré neprejdú cez firewall, ale bude im zároveň aj vystavený bez akejkoľvek ochrany. Druhou možnosťou je umiestniť senzor do vnútornej siete — za firewall, kde bude detekovať útoky, ktoré firewall nezastavil. Najlepším riešením je však použiť dva IDS senzory, umiestnené na oboch stranách firewallu. [11]

V tomto prípade budú systém IDS tvoriť dve sondy, umiestnené na oboch stranách zariadenia NIFIC a centrálny IDS server. Ďalej budeme používať softvérový honeypot, pracujúci nad softvérovými rozhraniami `ceth2` a `ceth3`.

Výhodou tohto spôsobu zapojenia honeypotu je jeho flexibilita. Pri normálnej prevádzke sa na softvérové rozhrania honeypotu neposiela žiadna komunikácia a všetku komunikáciu kontroluje IDS. V prípade, že IDS vyhodnotí komunikáciu od nejakého serveru ako útok, nastavíme NIFIC tak aby sa táto komunikácia preposielala na honeypot, kde sa bude podrobne analyzovať. Na honeypot teda budeme preposielať iba určitý typ komunikácie a podľa vývoja situácie môžme preposielaný typ komunikácie operatívne meniť. Zapojenie do siete je na obrázku 4.3. Port 0 bude smerovať do internetu a na port 1 bude pripojená lokálna sieť. Na oba porty ešte umiestnime IDS senzory, ktoré zapojíme pomocou zariadení TAP.



Obrázok 4.3: Schéma zapojenia zariadenia NIFIC, honeypotu a IDS

Firewall, chrániaci túto sieť môže byť pripojený medzi TAP a port 0, alebo jeho funkciu môže vykonávať priamo NIFIC. Podľa toho bude vyzerať aj jeho konfigurácia. Pri použití externého firewallu bude nakonfigurovaný tak, aby spájal internet s lokálnou sieťou. To znamená že všetky pakety (vrátane paketov nespadajúcich do IPv4 komunikácie) sa budú preposielať z portu 0 na port 1 a naopak. V druhom prípade bude nakonfigurovaný ako firewall.

Pri potrebe presmerovať určitú komunikáciu na honeypot pridáme pravidlá, ktoré vyfiltrujú požadovaný typ komunikácie a prepošlú ju na rozhranie `ceth2`, alebo `ceth3`. Rozhranie `ceth2` použijeme v prípade, že podozrivá komunikácia prichádza z portu 0 — z miesta mimo našej siete. Druhé rozhranie `ceth3` použijeme ak komunikácia prichádza z lokálnej siete. Nakoniec je potrebné zabezpečiť aj správne preposielanie prípadných odpovedí z honeypotu tým, že budeme smerovať pakety zo softvérových rozhraní na port 0, alebo 1.

Takto môžu vyzerať pravidlá v prípade, že chceme aby server v našej sieti s IP adresou `10.0.0.12` komunikoval s honeypotom.

```
10 pass 3 on 1 from 10.0.0.12
20 pass 1 on 3
```

V prípade, že má NIFIC funkciu firewallu, musia za týmito pravidlami nasledovať ostatné pravidlá, ktoré zabezpečujú ochranu siete. Ak je použitý externý firewall, musia byť ešte doplnené pravidlá pre transparentné preposielanie paketov medzi portami 0 a 1.

4.4 Flexibilný NetFlow

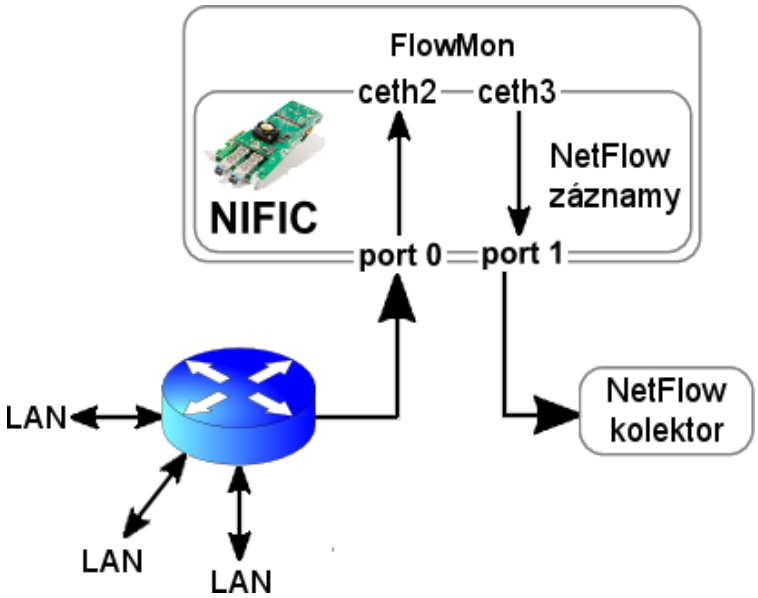
Na základe NetFlow štatistík sa dá získať množstvo užitočných informácií o monitorovanej sieti. Napríklad majoritné zdroje sieťovej komunikácie, jej dĺžku a typ, čo sa dá využiť

na účtovanie za poskytnuté pripojenie na internet a tvorbu štatistík poskytujúcich prehlad o komunikácií prebiehajúcej na sieti. Zber týchto štatistík je dôležitý pre zvýšenie bezpečnosti a výkonu siete. Na ich základe sa optimalizuje používanie sieťových zdrojov, detekujú sa DoS útoky, sieťou sa šíriace červy a iné anomálie. [5]

Tieto záznamy sú tvorené NetFlow sondami, ktoré analyzujú komunikáciu v sieti a posielajú svoje výsledky na centrálny NetFlow kolektor, ktorý ich ďalej spracováva. Problematika zberu NetFlow štatistík je popísaná v sekcií 2.3.4 .

Na sietiach tečie veľké množstvo dát, ktoré nás pri monitorovaní nezaujímajú. Ak máme napríklad NetFlow sondu umiestnenú na chrbtovej sieti a potrebujeme tvoriť záznamy o jednom špecifickom type komunikácie, musíme spracovávať všetky dáta na sieti. Tieto dáta tak vytvárajú ďalšie NetFlow toky, ku ktorým sa na sonde vytvárajú zbytočné NetFlow záznamy a tie zaberajú výpočetné a záznamové prostriedky NetFlow sondy. [18]

NIFIC môžme použiť na zredukovanie komunikácie, ktorú chceme analyzovať NetFlow sondou. Ako zariadenie monitorujúce sieťovú komunikáciu, a ako exportér NetFlow záznamov môžme použiť softvérovú sondu *FlowMon* [3] . Ďalej musí byť v sieti umiestnený NetFlow kolektor, ktorý zberá záznamy z *FlowMon* sondy a následne ich ďalej spracováva a analyzuje.



Obrázok 4.4: NIFIC redukujúci objem komunikácie pre NetFlow sondu

Zapojenie zariadenia NIFIC do siete je na obrázku 4.4 . Budeme pracovať iba s kópiou reálnej sieťovej komunikácie a preto port 0 zapojíme na zrkadlový port smerovača. Na porte 1 bude pripojený NetFlow kolektor. Softvérový *FlowMon* bude bežať na rovnakom serveri ako NIFIC, a bude pripojený na jeho softvérové rozhranie. NetFlow záznamy bude *FlowMon* exportovať na softvérové rozhranie a odtiaľ budú preposlané na port 1. Z komunikácie, ktorá príde na port 0 si do *FlowMon* sondy prepošleme iba komunikáciu z požadovaného rozsahu IP adries. Pravidlá sú jednoduché:

```
10 pass 2 on 0 from pozadovane_adresy to any
20 pass 2 on 0 from any to pozadovane_adresy
30 pass 1 on 3
40 pass 3 on 1
```

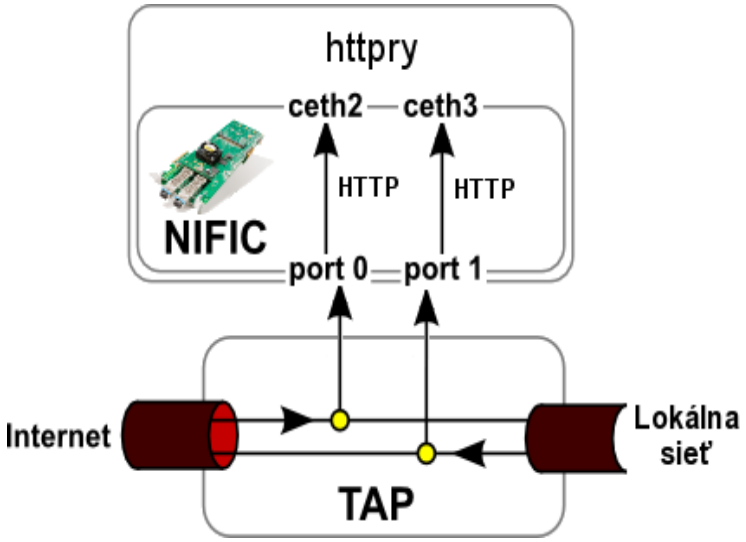
Typ komunikácie, ktorá sa bude posielať do sondy na monitorovanie sa dá samozrejme meniť a na jej špecifikovanie je možné použiť všetku silu jazyka pre popis pravidiel použitých v zariadení NIFIC.

4.5 Analyzátor prístupu na webové stránky

Dnes má už takmer každá väčšia firma svoju podnikovú sieť a s ňou aj zamestnancov, ktorý ju radi zneužívajú. Využívajú ju počas pracovného času na osobné účely, a dokonca navštevujú stránky s nevhodným, či nelegálnym obsahom. Na potlačenie týchto javov je vhodné zistiť, ktorí zamestnanci pristupujú na spomínané stránky a tým zneužívajú sieť.

Zariadenie NIFIC môžme použiť pri tvorbe záznamov o prístupoch jednotlivých používateľov na určené webové stránky, z lokálnej siete. Ďalej využijeme nástroj *httpry*[1]. Jedná sa o paket sniffer, ktorý je určený na výpis a logovanie HTTP komunikácie. Ďalšou jeho užitočnou vlastnosťou je, že okrem IP adresy serveru zobrazí aj URL adresu, na ktorú používateľ pristupoval. [7]

NIFIC bude zapojený podľa obrázku 4.5. Do siete ho pripojíme pomocou zariadenia TAP. Monitorovacie porty TAP prepojíme s jeho fyzickým portami. Pri tomto zapojení bude pracovať iba s kópiou komunikácie medzi lokálnou sieťou a zbytkom sveta.



Obrázok 4.5: Schéma zapojenia analyzátoru prístupu na web

Na získanie požadovaných dát nakonfigurujeme NIFIC tak, aby všetky pakety ktoré obsahujú HTTP komunikáciu (TCP pakety s cieľovým portom 80) preposielal na softvérové rozhrania, kde ich bude ďalej spracovávať. Jedno rozhranie bude zachytávať z pohľadu lokálnej siete prichádzajúcu HTTP komunikáciu a druhé rozhranie zasa odchádzajúcu HTTP komunikáciu. Keďže nás zaujímajú iba informácie uložené v hlavičkách paketov, môžme nastaviť orezávanie paketov preposielaných do softvéru na veľkosť 300 B. Znížime tak veľkosť zbytočných dát posielaných na softvérové rozhrania.

Pravidlá, ktoré zabezpečia odfiltrovanie požadovanej komunikácie do softvéru sú nasledovné:

[1]Nástroj *httpry* je voľne stiahnuteľný na adrese `http://dumpsterventures.com/jason/httpry/`.

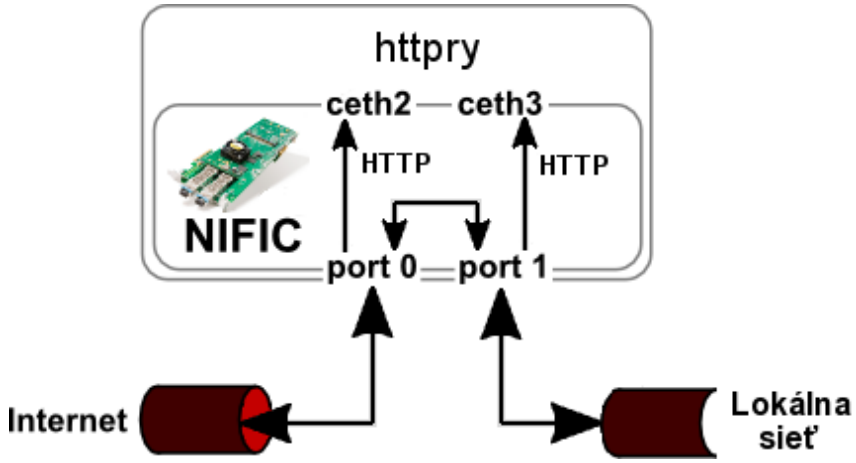
```
10 pass 2 crop 300 on 0 proto tcp from any to any port 80
20 pass 3 crop 300 on 1 proto tcp from any to any port 80
```

Nakoniec je vhodné nastaviť NIFIC tak, vytvoril štandardné sieťové rozhrania (na obrázku 4.5 nazvané `ceth2` a `ceth3`), na ktoré bude posielať dáta z jeho softvérových rozhraní. Na tieto štandardné rozhrania zapojíme nástroj *httpry* a necháme ho zapisovať výslednú HTTP komunikáciu do logovacích súborov pre ďalšiu analýzu.

4.5.1 Manažér prístupu na webové stránky

Predchádzajúci príklad sa dá vhodne rozšíriť aj o kontrolu prístupu používateľov na webové stránky. Riadenie prístupu je možné realizovať vytvorením blacklistu stránok, ku ktorým bude z lokálnej siete zakázaný prístup. To je užitočné v prípade stránok, o ktorých je známe, že sú zdrojom bezpečnostných rizík, a ktorými by mohli zamestnanci — počítačový laici, ohroziť firemnú sieť. K predošlému prípadu použitia doplníme prvky firewallu, ktoré budú filtrovať prístup na webové stránky.

V tom prípade, však musí byť NIFIC zapojený do siete priamo, a to spôsobom zobrazeným na obrázku 4.6 , bez použitia zariadenia TAP. Takto bude pracovať s reálnou sieťovou komunikáciou, do ktorej môže aj aktívne zasahovať. Na jeho fyzický port 1 pripojíme lokálnu sieť a na port 0 vonkajšiu sieť — internet.



Obrázok 4.6: Schéma zapojenia manažéra prístupu na webové stránky

Prvým krokom pri konfigurácií je umožniť komunikáciu medzi lokálnou sieťou a internetom. Tá sa zabezpečí preposielaním všetkých paketov z portu 0 na port 1 a naopak. To platí aj pre pakety, ktoré nespadajú do komunikácie protokolom IPv4, tzv. „non IPv4“ pakety. Následne by NIFIC tak, ako v predchádzajúcom prípade, preposielal HTTP komunikáciu na štandardné sieťové rozhranie, kde by bola analyzovaná nástrojom *httpry*.

Blacklist stránok vytvoríme nasledujúcimi pravidlami:

```
10 block on 0 proto TCP from public-server port 80 to any
20 block on 1 proto TCP from any to public-server port 80
```

kde `public-server` nahradíme IP adresou servera, na ktorom je umiestnená škodlivá web stránka. Dodatočné pridávanie, či odoberanie stránok z blacklistu je samozrejme možné aj počas prevádzky.

Za predpokladu, že je NIFIC zapojený za prípadným NAT zariadením, cez ktoré sa pripája firemná sieť do internetu, môžme zakázať prístup k danej stránke len vybraným počítačom v lokálnej sieti. V tom prípade by sme nahradili kľúčové slovo `any` IP adresou servera v lokálnej sieti, ktorý by mal prístup na danú stránku zakázaný.

Filtrovacie pravidlá budú nasledovné:

```
10 block on 0 proto TCP from public-server port 80 to any
20 block on 1 proto TCP from any to public-server port 80
30 pass 1 2 on 0 proto TCP from any to any port 80
40 pass 0 3 on 1 proto TCP from any to any port 80
50 pass 1 on 0
60 pass 0 on 1
```

Najvyššiu prioritu majú pravidlá reprezentujúce blacklist. Nasledujú pravidlá pre zber informácií o HTTP komunikácií. Odfiltrované pakety protokolu HTTP sa budú posielať jednak na softvérové rozhranie na analýzu a jednak ďalej do siete, alebo zo siete. Nakoniec sú uvedené pravidlá pre transparentný prenos ostatnej komunikácie.

4.6 VoIP analyzátor

Voice over Internet Protocol je skupina technológií, ktoré umožňujú prenos ľudského hlasu počítačovou sieťou. Analýzou tejto komunikácie sa dá získať prehľad o uskutočnených VoIP hovoroch a ich parametroch, prípadne sa dá zistiť ich kvalita. V prípade že sa takáto analýza uskutočňuje na chrbtovej sieti, je vhodné oddeliť tento typ komunikácie od ostatnej, napríklad zariadením NIFIC.

Pre analýzu VoIP komunikácie budeme zachytávať pakety SIP (Session Initiation Protocol) protokolu, ktoré budú analyzované programom *wireshark* [2]. Tento program veľmi dobre poslúži pri zachytávaní sieťovej komunikácie z lokálneho, alebo vzdialeného rozhrania a jej následnej analýze. Protokol SIP zaisťuje telefónnu signalizáciu a stará sa o iniciovanie, riadenie a rušenie VoIP hovoru, pričom vlastné dáta hovoru sú prenášané nezávisle. [1]

Analýzou tejto komunikácie teda nezískame informácie o obsahu hovorov, iba informácie o ich dĺžke, IP adresy komunikujúcich serverov počet prenesených paketov a stav VoIP hovorov.

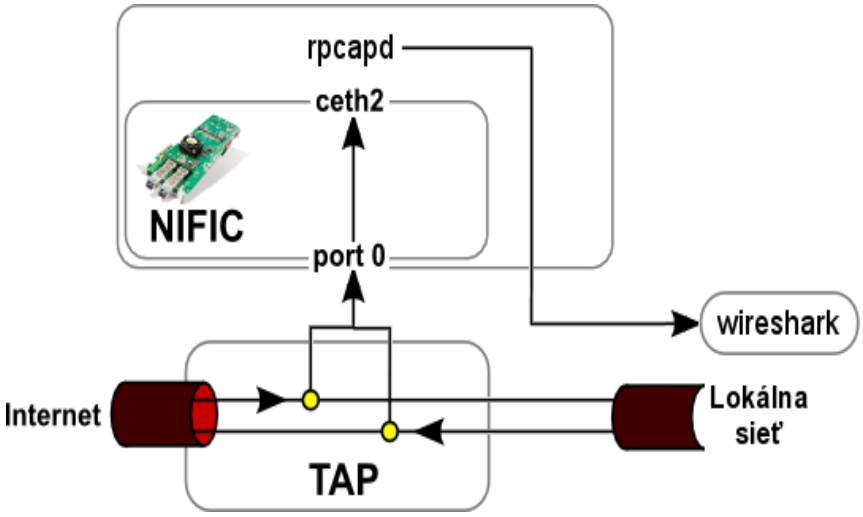
V tomto prípade použitia popíšem dve možnosti, ako môžme posielať zachytenú VoIP komunikáciu na vzdialený server, kde bude prebiehať jej analýza. Jednou z nich je použiť knižnicu *winpcap*, konkrétne démona *rpcapd* [3], ktorý vytvorí vzdialené sieťové rozhranie. Na toto rozhranie sa môže zo vzdialeného servera pripojiť analyzátor, ktorý z neho číta dáta a tie analyzuje. V tejto situácií môžme využiť skutočnosť, že *wireshark* je multiplatformový nástroj a týmto spôsobom sa VoIP komunikácia nemusí spracovávať iba na servery s operačným systémom GNU/Linux. [10]

Pri použití knižnice *winpcap* je zapojenie zariadenia NIFIC znázornené na obrázku 4.7. Filtrovať budeme komunikáciu protokolom SIP (TCP a UDP port 5060), ktorá bude preposielaná na softvérové rozhrania. SIP komunikácia bude smerovaná na rozhranie `ceth2`. Pravidlo pre filtráciu paketov je nasledovné:

```
10 pass 2 on 0 proto {udp, tcp} from any to any port 5060
```

[2] Program *wireshark* je voľne stiahnuteľný na adrese http://www.wireshark.org/download.html.

[3] Zdrojové kódy knižnice *winpcap* (vrátane démona *rpcapd*) sú voľne dostupné na adrese http://www.mirrorservice.org/sites/ftp.wiretapped.net/pub/security/packet-capture/winpcap/devel.htm.



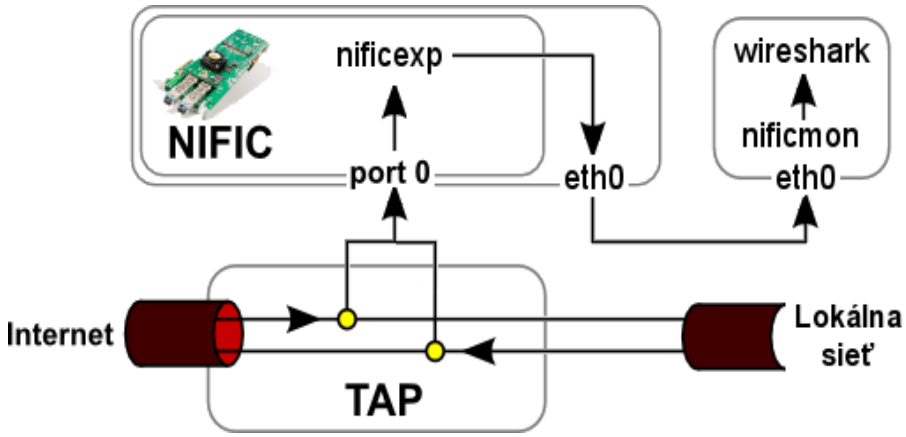
Obrázok 4.7: Vzdialená analýza VoIP hovorov s použitím knižnice *winpcap*

Po príprave vzdialeného rozhrania na export paketov nastavíme *wireshark* tak, aby zachytával pakety z tohto rozhrania. Jeho adresa je:

`rpcap://`*`IP_adresa_serveru_s_NIFICom`*`:2002/ceth2`

Démon *rpcapd* beží implicitne na porte s číslom `2002`, takže v prípade iného nastavenia je potrebné toto číslo zmeniť. Nakoniec si necháme zobraziť štatistiku zachytených VoIP hovorov.

Ďalšou možnosťou, ako vzdialene analyzovať VoIP komunikáciu je využitie nástrojov *nificexp* a *nificmon*. Tieto nástroje fungujú na princípe klient - server. Nificmon beží na serveri, kde bude prebiehať analýza a čaká na pakety, ktoré mu pošle *nificexp*. Tieto pakety následne posiela na štandardné sieťové rozhranie, kde sú k dispozícii ostatným aplikáciam. Exportér beží ako démon na hostiteľskom počítači, na ktorom je zapojený NIFIC, a podľa nastavenia exportuje pakety zo softvérových rozhraní na vzdialené servre, na ktorých beží *nificmon*. Podrobný popis nastavenia exportu paketov pomocou týchto nástrojov je popísaný v sekcií 3.2.2 .



Obrázok 4.8: Vzdialená analýza VoIP hovorov, s použitím nástroja *nificexp*

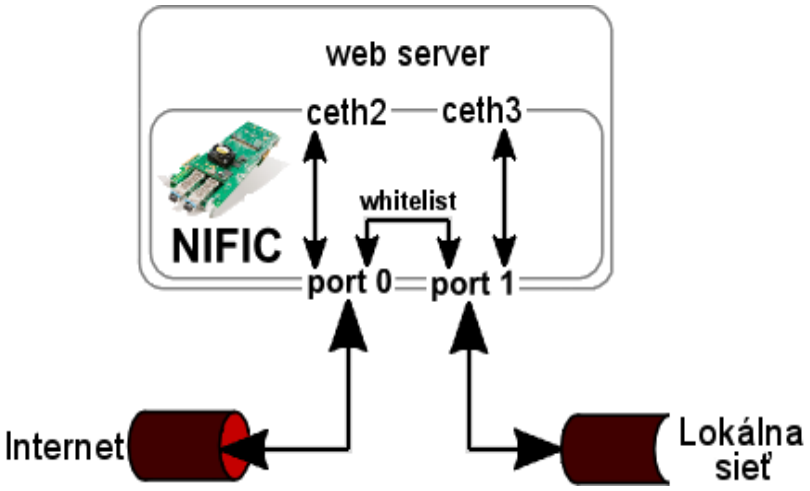
Zapojenie je uvedené na obrázku 4.8 a konfigurácia je rovnaká ako v predošlom prípade. Analýza paketov bude realizovaná programom *wireshark*, ktorý bude prijímať pakety z lokálneho sieťového rozhrania.

4.7 Manažér verejnej siete

Zariadením NIFIC je možné uľahčiť prevádzkovanie verejnej siete. Ako príklad môže slúžiť hotelová sieť, ktorá poskytuje ubytovaným hosťom pripojenie na internet. V tomto prípade potrebujeme zaistiť, aby sa jej prostredníctvom nepripájali na internet neregistrovaný používatelia. Každý používateľ s novou IP adresou, sa preto musí najskôr prihlásiť do siete, aby sa k jeho IP adrese priradilo meno, číslo izby a iné informácie potrebné na vystavenie účtu za používanie siete.

Vo verejnej sieti teda máme dva druhy počítačov. Prihlásené, ktorým je umožnený voľný prístup do internetu a neznáme počítače, ktorých pokusy o pripojenie sú blokované.

Popísané filtrovanie prístupu na internet bude zabezpečovať NIFIC. Jeho zapojenie v sieti je znázornené na obrázku 4.9. Port 0 bude zapojený do brány, ktorou sa sieť pripája do internetu a port 1 bude zapojený do lokálnej siete. Ďalej budeme mať vytvorené dve štandardné softvérové rozhrania. Na jedno z nich sa bude smerovať komunikácia z internetu, ktorá nesmeruje na počítače prihlásené v sieti. Na druhé softvérové rozhranie pôjde komunikácia z počítačov, ktoré nie sú v našej sieti prihlásené.



Obrázok 4.9: Schéma zapojenia manažéra siete

NIFIC bude nakonfigurovaný tak, aby implicitne smeroval všetku komunikáciu z lokálnej siete na softvérové rozhranie `ceth3`, a komunikáciu z internetu na rozhranie `ceth2`. V počítači, na ktorom prebieha filtrovanie paketov, bude naviac spustený HTTP server, napríklad *apache*[4]. Na tento server je možné umiestniť verejné webové stránky daného hotela.

Pripojenie nového počítača do siete bude prebiehať nasledovne. Najskôr bude tomuto počítaču DHCP serverom pridelená nová IP adresa. Podľa nastavenia zariadenia NIFIC sa pokus o prístup na web presmeruje na rozhranie `ceth3` a používateľ sa tak dostane na stránky, ktoré umožňujú prihlásenie do hotelovej siete. Následne sa IP adresa počítača vloží

[4] *The Apache HTTP Server* je voľne stiahnuteľný na adrese `http://httpd.apache.org/download.cgi`.

do whitelistu a sada filtrovacích pravidiel sa doplní o pravidlá, ktoré umožnia transparentné preposielanie komunikácie s danej IP adresy smerom do internetu a naopak. Budú mať nasledovný tvar (`IP` bude nahradené adresou servera):

```
10 pass 0 on 1 from IP to any
20 pass 1 on 0 from any to IP
```

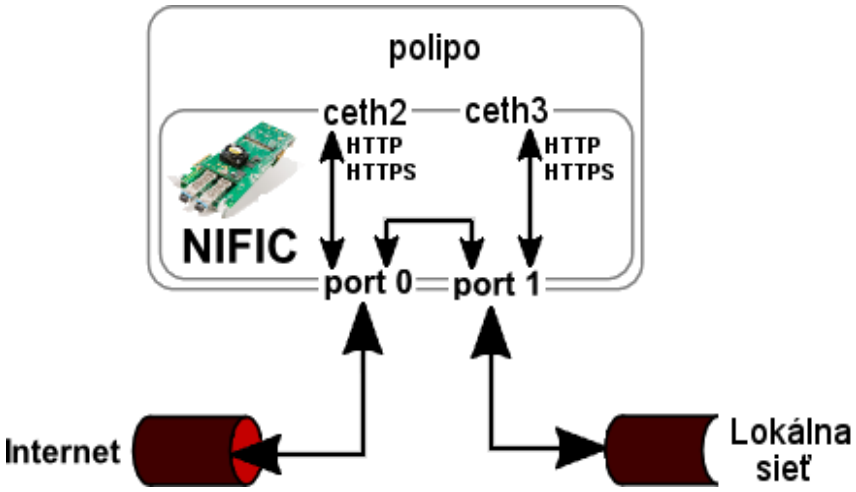
Pri odpojení používateľa zo siete sa tieto pravidlá odstránia, aby neumožnili prístup používateľovi, ktorý bude mať v budúcnosti rovnakú IP adresu ako práve odhlásený.

Problémom tohto prípadu použitia je práve pridávanie a odoberanie používateľov z whitelistu. Keďže tieto akcie sa budú vykonávať často, je vhodné automatizovať ich. V súčastnosti však neexistuje žiadny softvér, ktorý by zabezpečil požadovanú činnosť.

4.8 HTTP proxy server

Prezeranie webových stránok je možné zefektívniť použitím HTTP proxy serveru. Takto dokážeme eliminovať nevyžiadanú reklamu v podobe vyskakujúcich okien, zrýchliť načítavanie jednotlivých stránok a v neposlednom rade zmenšiť obsah informácií o našom systéme, ktoré sú posielané v hlavičkách protokolu HTTP. Na zapojenie HTTP proxy použijeme NIFIC, a jednoduchú aplikáciu *polipo*[5].

Program *polipo* implementuje caching HTTP proxy. Poskytuje web cache, čo znamená že odpovede na HTTP požiadavky si ukladá do cache pamäte a pri príchode rovnakej požiadavky, načíta odpoveď z cache pamäte, čím sa vybavovanie HTTP požiadavok stáva efektívnejším. Taktiež sa tým zmenšuje objem komunikácie a samozrejme aj latencia načítavania často navštevovaných web stránok. Ďalej umožňuje cenzúrovanie hlavičiek HTTP požiadavkov a odpovedí, čím zabezpečuje súkromie pri prístupe na web stránky. Nakoniec dokáže odstrániť reklamy z načítávaných stránok a umožňuje vytvorenie blacklistu stránok, ktoré budú blokované. [4]



Obrázok 4.10: NIFIC ako HTTP proxy

NIFIC zapojíme do siete podľa obrázku 4.10. Na port 0 bude zapojená brána z firemnej siete do internetu, a na port 1 bude pripojená firemná sieť. Softvérové rozhrania

[5]Program *polipo* je voľne stiahnuteľný na adrese http://www.pps.jussieu.fr/~jch/software/polipo/.

budú pridelené nasledovne: `ceth2` bude reprezentovať internet a rozhranie `ceth3` lokálnu sieť. Počítač na ktorom bude prebiehať filtrovanie paketov je vhodné umiestniť hneď za zariadenie predstavujúce bránu do internetu.

Pravidlá podľa ktorých sa bude filtrovať sieťová komunikácia sú nasledovné. Najskôr budeme všetku komunikáciu z portu 0 preposielať na port 1 a naopak. To isté sa bude diať aj s „non IPv4“ paketmi. Takto zaistíme prepojenie lokálnej siete s internetom.

HTTP komunikáciu bude spracovávať *polipo* a preto si ju presmerujeme cez softvérové rozhrania. Nastavíme teda pravidlá tak, aby HTTP a aj prípadná HTTPS komunikácia bola posielaná z portu 0 na rozhranie `ceth2` a naopak. Taktiež aj zo strany lokálnej siete nastavíme posielanie HTTP a HTTPS paketov z portu 1 na rozhranie `ceth3` a naopak.

Aplikáciu *polypo* nakonfigurujeme tak, aby bežala nad rozhraním `ceth2` a aby čakala na HTTP požiadavky na rozhraní `ceth3`. Okrem toho budeme na rovnaké softvérové rozhrania preposielať aj prípadnú komunikáciu protokolom HTTPS (TCP port 443), kedže program *polipo* dokáže spracovať aj tú. Výsledné pravidlá budú nasledovné:

```
10 pass 2 on 0 proto tcp from any to any port {80,443}
20 pass 0 on 2
30 pass 3 on 1 proto tcp from any to any port {80,443}
40 pass 1 on 3
50 pass 1 on 0
60 pass 0 on 1
```

Obdobným spôsobom je možné filtrovať rôzne typy komunikácie, pričom každý z nich môže byť spracovávaný na vlastnom softvérovom rozhraní.

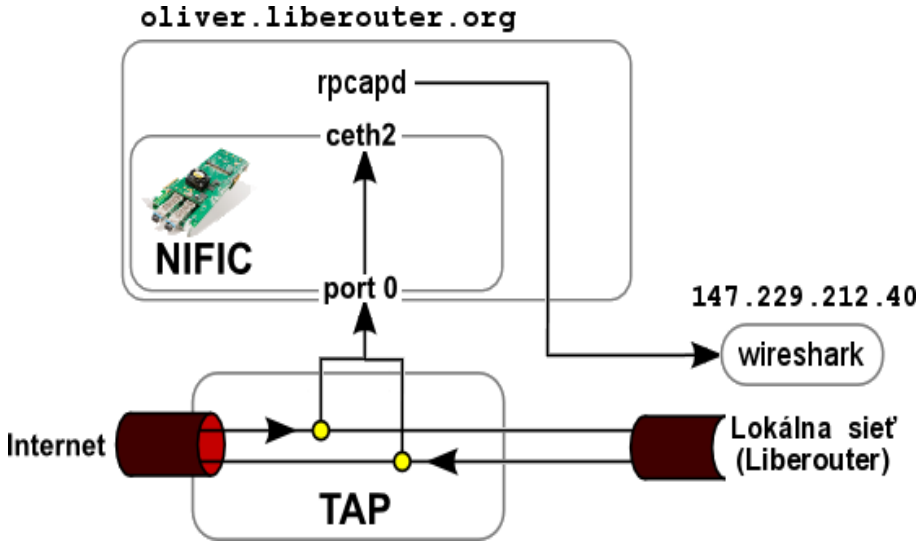
Kapitola 5

Nasadenie v praxi

Funkčnosť prípadu použitia, popísaného v podkapitole 4.6, som vyskúšal aj na reálnej počítačovej sieti. Tento prípad použitia popisuje filtrovanie sieťovej komunikácie protokolom SIP a jej následnú analýzu programom *wireshark* na vzdialenom počítači.

Zariadenie NIFIC bolo umiestnené na serveri `oliver.liberouter.org`, na ktorom bola zapojená karta COMBO-LX155T a karta rozhrania COMBO-10G2. Na stroji bol nainštalovaný operačný systém CentOS s jadrom verzie 2.6.18-164.6.1.el5.slab_fix. Na port 0 bolo pripojené zariadenie TAP, ktoré kopírovalo sieťovú komunikáciu. Vzdialený virtuálny počítač, na ktorom prebiehala analýza odfiltrovanej komunikácie, bol pripojený na IP adrese `147.229.212.40`.

Softvér potrebný na prevádzku zariadenia NIFIC, v podobe RPM balíkov som získal a nainštaloval z repozitáru projektu Liberouter[1]. Tieto balíky obsahovali aj démona *rpcapd*, ktorý je súčasťou knižnice *winpcap*. Do vzdialeného počítača som si nainštaloval program *wireshark*, ktorý bude použitý na analýzu a tvorbu štatistík o získanej SIP komunikácií. Schéma zapojenia serveru `oliver.liberouter.org` a vzdialeného počítača je na obrázku 5.1.



Obrázok 5.1: Reálne zapojenie analyzátora VoIP komunikácie

[1]Repozitár RPM balíkov je umiestnený na privátnych stránkach projektu.

Sada filtrovacích pravidiel obsahovala iba dve nasledujúce pravidlá, ktoré odfiltrovali SIP komunikáciu z fyzického rozhrania, na virtuálne rozhranie číslo 2:

```
10 pass 2 on 0 proto {udp, tcp} from any to any port 5060
100 block
```

Konfiguračným súborom `nific.conf` som nastavil blokovanie prípadných paketov, ktoré nepatria do protokolu IPv4, a vytvorenie štandardného softvérového rozhrania `ceth2`, ktoré bolo namapované na virtuálne rozhranie číslo 2. Ďalej som na danom stroji spustil démona *rpcapd* s nasledujúcimi parametrami, ktoré povoľujú pripojenie vzdialeného počítača na vytvorené rozhranie:

```
$ rpcapd -4 -n -l 147.229.212.40
```

Na vzdialenom počítači som nastavil *wireshark* tak, aby sa pripojil na vzdialené rozhranie na serveri `oliver.liberouter.org`, ktoré bolo definované:

```
rpcap://147.251.21.44:2002/ceth2
```

Filtrovanie SIP komunikácie prebiehalo nasledovne. SIP pakety boli najskôr skopírované zariadením TAP na fyzické rozhranie zariadenia NIFIC. Ten ich odfiltroval a preposlal na rozhranie `ceth2` a odtiaľ boli pomocou démona *rpcapd* prenášané na vzdialený počítač aplikáciou *wireshark*.

Touto aplikáciou som zachytil 7654 paketov protokolu SIP. Z nich som vytvoril tabuľku 5.1 , ktorá obsahuje počty zachytených paketov, rozdelených podľa typu. V tabuľke 5.2 som uviedol počty paketov, rozdelených podľa požadovaných metód.

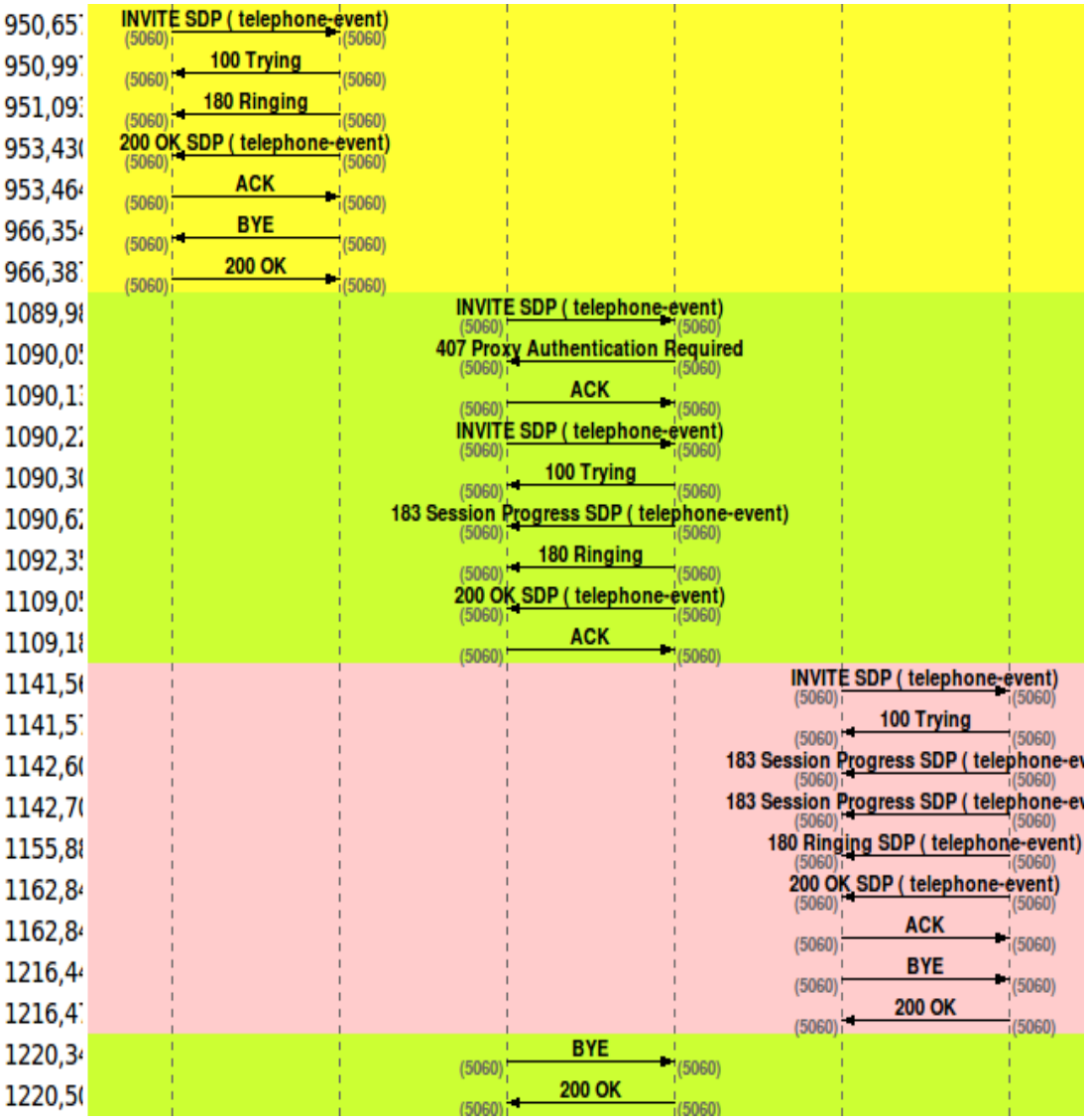
Typ zachytených SIP paketov	**Počet zachytených paketov**
SIP 100 Trying	710
SIP 180 Ringing	9
SIP 183 Session progress	14
SIP 200 OK	1539
SIP 401 Unauthorized	474
SIP 404 Not Found	131
SIP 405 Method Not Allowed	133
SIP 407 Proxy Authentication Required	33
SIP 487 Request Terminated	2
SIP 500 Server Internal Error	9
SIP 501 Not Implemented	22

Tabuľka 5.1: Štatistika zachytených SIP paketov

V rámci zachytených paketov bolo detekovaných 21 VoIP hovorov, pričom priebeh všetkých hovorov sa dal zobraziť v grafe. Pre nedostatok miesta uvádzam na obrázku 5.2 iba časť grafu, v ktorom sú znázornené prenosy jednotlivých SIP paketov v čase, medzi komunikujúcimi servermi. V grafe sú zachytené 3 VoIP hovory, ktoré sú rozlíšené rôznou farbou.

Názov požadovanej metódy	Počet zachytených paketov
PUBLISH	35
MESSAGE	1
INVITE	27
BYE	157
ACK	25
CANCEL	2
SUBSCRIBE	135
OPTIONS	1335
NOTIFY	951
REGISTER	1910

Tabuľka 5.2: Štatistika požadovaných metód v SIP paketoch



Obrázok 5.2: Ukážka grafu zachytených VoIP hovorov

Kapitola 6

Záver

Táto bakalárska práca je zameraná na použitie zariadenia NIFIC v počítačovej sieti, ako nástroja na zvýšenie jej bezpečnosti. Jedná sa o prípady kedy toto zariadenie priamo ochraňuje sieť pred útokmi, alebo slúži na monitorovanie sieťovej komunikácie a tým prispieva k odhaleniu potenciálnych bezpečnostných rizík.

Prvým krokom bolo naštudovanie problematiky bezpečností počítačových sietí. V rámci tohto štúdia som sa oboznámil s profilom kybernetických útočníkov, bezpečnostnými hrozbami, a najčastejšími typmi útokov. Ďalej som si zaobstaral informácie o nástrojoch, ktorými sa dá spomenutým hrozbám predchádzať. Zameral som sa hlavne na nástroje, ktoré som použil pri popise prípadov použitia. Boli to firewally, systémy detekcie sieťového narušenia, honeypoty a NetFlow záznamy.

Po získaní znalostí o bezpečnosti počítačových sietí som sa zameral na zariadenie NIFIC. Naštudoval som si softvérovú a hardvérovú architektúru a tieto poznatky som uplatnil pri popise nových možností tohto zariadenia pre analýzu sieťovej komunikácie. Pri tvorbe prípadov použitia som vychádzal aj z možností tohto zariadenia, ktoré sú popísané v príručke. V každom prípade použitia je popísaný prínos jeho nasadenia v danej sieti, jeho zapojenie a spolupráca s inými nástrojmi, a nakoniec konfigurácia. Taktiež som pripravil konfiguračné súbory a súbory s filtrovacími pravidlami pre jednotlivé prípady použitia. Vo vhodných prípadoch použitia som demonštroval možnosť vzdialenej správy a vzdialeného sledovania sieťovej komunikácie.

Nakoniec som vyskúšal zapojenie vybraného prípadu použitia v reálnej sieti. Vybral som analýzu VoIP komunikácie, na ktorú som použil server so zariadením NIFIC, ktorý je umiestnený v sieti projektu Liberouter. Do bakalárskej práce som uviedol popis a výsledky tejto analýzy.

Ďalšie pokračovanie tejto práce by mohlo spočívať v návrhu nových vlastností zariadenia NIFIC, na základe analýzy jednotlivých prípadov použitia.

Literatúra

[1] Bazala, D.: *Telekomunikace a VoIP technologie*. Praha: BEN - technická literatura, první vydání, 2006, ISBN 80-7300-201-9, 222 s.

[2] Caligare s.r.o.: What is Netflow? [online], poslední modifikace: 10. května 2006. [cit. 2010-04-14].
URL http://netflow.caligare.com/

[3] Cesnet z.s.p.o.: FlowMon Probe. [online], [cit. 2010-03-01].
URL http://www.liberouter.org/flowmon/index.php

[4] Chroboczek, J.: The Polipo Manual. [online], [cit. 2010-03-09].
URL http://www.pps.jussieu.fr/~jch/software/polipo/polipo.html

[5] Cisco Systems, Inc.: Introduction to Cisco IOS NetFlow – A Technical Overview. [online], poslední modifikace: říjen 2007. [cit. 2010-03-29].
URL http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html

[6] Dedek, T.; Kořenek, J.; Krejčí, R.; aj.: *Optická síť národního výzkumu a její nové aplikace 2009*, kapitola Programovatelný hardware. Praha: Cesnet z.s.p.o., 2009, ISBN 978-80-904173-6-6, s. 49–81.

[7] Dumpster Ventures: httpry. [online], poslední modifikace: 2. července 2009. [cit. 2010-03-01].
URL http://dumpsterventures.com/jason/httpry/

[8] Hank, A.: *Detekcia narušenia počítačovej siete*. Bakalářská práce, FIT VUT v Brně, Brno, 2007.

[9] Kubička, V.: *Detection of Network Attacks Based on NetFlow Data*. Bakalářská práce, FIT VUT v Brně, Brno, 2009.

[10] Lamping, U.; Sharpe, R.; Warnicke, E.: Wireshark User's Guide. [online], [cit. 2010-03-16].
URL http://www.wireshark.org/docs/wsug_html_chunked/index.html

[11] Northcutt, S.; Zeltser, L.; Winters, S.; aj.: *Inside Network Perimeter Security: the definitive guide to firewalls, VPNs, routers, and intrusion detection systems*. Indianapolis: New Rider's Publishing, 2003, ISBN 0-7357-1232-8, 678 s.

[12] Shimeall, T.; Williams, P.; Dunlevy, C.: Obrana pred kybernetickou vojnou. *Euro-atlantic Quarterly*, 04 2008, ISSN 1336-8764.

[13] Strebe, M.; Perkins, C.: *Firewally a proxy-servery: Praktický průvodce*. Brno: Computer Press, první vydání, 2003, ISBN 80-7226-983-6, 450 s.

[14] The Liberouter Project Team: NetCOPE Platform Handbook. [online], poslední modifikace: 8. březen 2010. [cit. 2010-04-09].
URL http://www.liberouter.org/netcope/handbook.html

[15] The Liberouter Project Team: NIFIC Handbook. [online], poslední modifikace: 24. březen 2010. [cit. 2010-03-29].
URL http://www.liberouter.org/nific/handbook.html

[16] Wikipedia: NetFlow. [online], poslední modifikace: 26. března 2009. [cit. 2010-04-14].
URL http://cs.wikipedia.org/wiki/Netflow

[17] Wikipedia: TCP/IP model. [online], poslední modifikace: 31. března 2010. [cit. 2010-04-15].
URL http://en.wikipedia.org/wiki/TCP/IP_model

[18] Žádník, M.; Špringl, P.; Čeleda, P.: Flexible FlowMon. In *Networking Studies II: Selected Technical Reports*, editace L. Lhotka; P. Satrapa, Praha: Cesnet z.s.p.o., první vydání, 2008, ISBN 978-80-254-2151-2, s. 61–83.

Dodatok A

Konfiguračné súbory

Konfiguračné súbory, a súbory s filtrovacími pravidlami pre jednotlivé prípady použitia zariadenia NIFIC sú umiestnené na priloženom CD nosiči.