

TECHNICKÁ UNIVERZITA KOŠICE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY
KATEDRA POČÍTAČOV A INFORMATIKY

Semestrálny projekt 2

**Analýza možnosti využitia nameraných údajov
v architektúre IPFIX**

Vypracoval:
Ondrej Malata
Šk. r.:2005/2006

1. IPFIX Architektúra

Dátová IP sieť primárne pozostáva z IP tokov prechádzajúcich cez sieťové prvky. Často je zaujímavé, ba dokonca potrebné mať prístup k informáciám o týchto tokoch. Časť IPFIX protokolu - zbierajúci proces - je schopný získať informácie o týchto tokoch, prechádzajúcich viacerými sieťovými prvkami v dátovej sieti. Export informácií o tokoch z internetového protokolu (IP Flow Information Export) je pripravovaný štandard pre detailné meranie a získavanie informácií o tokoch v počítačových sieťach. Pre ďalší popis je potrebné definovať základný pojem v špecifikácii IPFIX – tok (flow). Existuje mnoho definícií toku, pre účely bližšieho popisu bude použitá definícia.

1.1. Cieľ dokumentu

Tento dokument definuje architektúru pre IPFIX. Jeho hlavné ciele sú:

- Načrtnutie IPFIX kľúča architektonických súčiastok, pozostávajúcich z IPFIX zariadení a kolektorov komunikujúcich pomocou IPFIX protokolu.
- Definovanie IPFIX architektonických požiadaviek, napr. obnova, bezpečnosť atď.
- Načrtnúť charakteristiky pre IPFIX protokol.

1.2. Prehľad dokumentu IPFIX

IPFIX protokol poskytuje správcovské siete s prístupom k IP informáciám toku. Tento dokument určuje architektúru pre export odmeraných IP informácií toku z IPFIX exportovacieho procesu k IPFIX zhromažďovaciemu procesu, na požiadavky definované v IPFIX-REQS. Dokument IPFIX protokolu IPFIX-PROTO určuje ako IPFIX záznamy dát a šablóny sú uskutočnené cez congestion-aware transportný protokol z IPFIX exportovacieho procesu pre IPFIX zberný proces. IPFIX má oficiálny popis z IPFIX základných zložiek informácií (polia) , svoj názov, typ a ďalšie sémantické informácie, označované ako IPFIX-INFO. Nakoniec IPFIX-AS popisuje aký typ aplikácie môže používať IPFIX protokol a ako môžu používať informácie ktoré poskytnú. Poznámka: IPFIX systém nezabezpečí vzdialenú konfiguráciu z IPFIX zariadenia. Namiesto toho IPFIX zariadenia sú konfigurované sieťovými operátormi.

2. Terminológia

Popis zo základných IPFIX termínov takých ako tok IP prevádzky (IP Traffic Flow), exportovací proces, zhromažďovací proces, bod merania atď. sú významovo totožné s tými nájdenými v IPFIX dokumente IPFIX-REQS. Niektoré z termínov sú rozširované keď definujeme protokol. Doplňkový popis nutný pre architektúru má tiež byť definovaný. Pre rovnaké termíny definované v IPFIX-PROTO určené sú ekvivalentne v dokumentoch.

Pozorovací bod.

Pozorovací bod je miesto v sieti kde sú IP pakety sledované. Príkladom je napríklad sonda pripojená k zdieľanému médiu ako napr. LAN sieti založenej na Ethernete, port smerovača, alebo skupina rozhraní (fyzických, alebo logických) smerovača. Jeden pozorovací bod môže byť množina viacerých iných pozorovacích bodov.

Pozorovacia doména.

Pozorovacia doména je logický blok, ktorý navonok prezentuje jednu identitu pre skupinu pozorovacích bodov v IPFIX zariadení. Každá dvojica (pozorovací bod, merací proces) musí patriť do jednej pozorovacej domény. IPFIX zariadenie môže mať viacej pozorovacích domén, každá z nich s viacerými pozorovacími bodmi. Každá pozorovacia doména musí mať unikátne ID v kontexte IPFIX zariadenia. Jeden exportovací proces môže obsluhovať viacej pozorovacích domén. V tomto prípade exportovací proces používa toto unikátne ID na rozlíšenie exportovaných paketov medzi rôznymi pozorovacími doménami. Tento istý koncept je použitý aj v zberacom procese na identifikáciu paketov prichádzajúcich z rôznych pozorovacích domén v tom istom IPFIX zariadení.

IP Traffic Flow alebo Flow

Tok je definovaný ako množina IP paketov prechádzajúcich bodom siete za určitý časový interval. Všetky pakety patriace istému toku majú isté spoločné vlastnosti. Paket je definovaný ako patriaci k toku ak kompletne spĺňa všetky vlastnosti definované toku.

V kontexte IPFIX je tok definovaný nasledovne:

Tok je množina IP paketov alebo zapuzdrených IP paketov prechádzajúcich pozorovacím bodom v sieti počas určitého časového intervalu. Všetky pakety patriace určitému toku majú množinu spoločných vlastností. Každá vlastnosť je definovaná ako výsledok aplikácie funkcie na hodnoty:

1. Jeden alebo viac polí hlavičky aktuálneho paketu, napr. cieľová IP adresa, alebo pole v zapuzdrovacej hlavičke paketu, napr. koncové body IP-in-IP tunelu alebo polia transportnej hlavičky (číslo cieľového portu), alebo polia aplikačnej hlavičky.
2. Jedna alebo viac vlastností vlastného paketu, napr. dĺžka paketu.
3. Jedna alebo viac vlastností vyplývajúcich zo spracovania paketu, napr. (adresa ďalšieho skoku a pod.)

Paket je definovaný ako náležiaci toku, ak kompletne spĺňa všetky definované vlastnosti toku. Každá z položiek (1, 2, 3) je nazývaná kľúč toku. Táto definícia zahŕňa toky obsahujúce všetky pakety pozorované na sieti, až po toky obsahujúce jediný paket.

Kľúč toku (Flow key)

Každé z polí ktoré patrí:

1. Hlavičke paketu
2. Vlastnosti paketu ako takého
3. Vlastnosti vyplývajúcej zo spracovania paketu

Záznam o toku (Flow record)

Záznam o toku obsahuje informácie o špecifických tokoch, ktoré boli pozorované v pozorovacom bode. Záznam o toku obsahuje merané vlastnosti toku a charakteristické vlastnosti toku.

Merací proces (Metering proces)

Merací proces generuje záznamy o tokoch. Vstupom do procesu sú hlavičky paketov pozorované v pozorovacom bode a spracovanie paketu v pozorovacom bode. Merací proces pozostáva z množiny funkcií, ktorá obsahuje zachytávanie hlavičiek paketov, časové značkovanie, vzorkovanie, triedenie a správu záznamov o tokoch.

Exportovací proces (Exporting process)

Exportovací proces odosiela záznamy tokov na jeden alebo viac zhromažďovacích procesov. Záznamy tokov sú generované jedným alebo viacerými meracími procesmi.

Vývozca (Exporter)

Nástroj ktorý hostí jeden alebo viac vyvážajúcich procesov nazýva sa vývozca.

IPFIX zariadenie (IPFIX device)

IPFIX zariadenie obsahuje prinajmenšom jeden bod merania, merací proces a exportovací proces.

Zberací proces (Collecting process)

Zberací proces dostáva záznamy o tokoch z jedného alebo viacerých exportovacích procesov. Zberací proces môže obdržané záznamy ukladať, alebo ich ďalej spracovávať, ale tie sú mimo priestoru pre tento dokument.

Kolektor (Collector)

Zariadenie ktoré obsahuje jeden alebo viac zhromažďovacích procesov sa nazýva kolektor. Kolektor prijíma záznamy tokov (flow records) z jedného alebo viacerých exportérov. Môže upraviť alebo uložiť prijatý záznam toku (flow record). Kolektor je subsystem, ktorý je vo vzájomnej interakcii s jedným alebo viacerými IPFIX zariadeniami.

Šablóna (Template)

Šablóna je usporiadaná n-tica, používaná na kompletnú identifikáciu štruktúry a sémantiky určitej informácie, ktorá má byť sprostredkovaná z IPFIX zariadenia do zberača. Každá šablóna je identifikovateľná unikátne.

Riadiacia informácia, Dátový stream

Informácia ktorá potrebuje byť exportovaná z IPFIX zariadenia môže byť rozdelená do nasledovných kategórií:

Riadiaca informácia

Obsahuje definíciu typu toku, výberové kritériá pre pakety patriace tomuto toku a IPFIX správy. Kontrolný stream obsahuje všetky informácie potrebné na úplnú správu protokolu IPFIX.

Dátový stream (Data Stream)

Obsahujú dátové záznamy nesúce hodnoty polí pre rozličné pozorované toky na každom pozorovacom bode. Sekvencia takýchto záznamov môže byť popisovaná aj ako dátový stream.

IPFIX správa (IPFIX message)

IPFIX správa je odkaz odchádzajúci exportovacím procesom ktorý nesie IPFIX záznamy z exportovacieho procesu a ktorého cieľom je zbierka procesov. IPFIX správa je obalená na transportnej vrstve.

Základná zložka informácie (Information element)

Základná zložka informácie je protokol a kódovanie nezávislého opisu z vlastností, ktoré sa môžu objaviť v IPFIX zázname. IPFIX informačný model definuje základný súbor základnej zložky informácie pre IPFIX. Typ súvisiaci so základnou zložkou udáva obmedzenia, ktoré môže obsahovať a tiež určiť platné zakódovanie mechanizmu použitého v IPFIX.

3. Príklady tokov (Examples of flows)

Niektoré z príkladov sú uvedené nižšie:

Príklad1: Klúče tokov určujú rozdielne polia vďaka ktorým toky rozoznávame. Rozdielna informácia hodnôt polí vytvára jedinečné toky. Ak (prameň IP adresy, cieľ IP adresy, DSCP) sú klúče tokov, potom všetky z nich sú rozdielne toky:

1. {198.18.40.1, 198.18.23.5, 4}
2. {198.18.40.23, 198.18.23.67, 4}

3. {198.18.40.23, 198.18.23.67, 2}
4. {198.18.20.200, 198.18.23.67, 4}

Príklad 2: Maskovaná funkcia môže byť aplikovaná na všetky pakety, ktoré prejdú cez bod merania, za účelom spojiť niektoré hodnoty. Môže byť vytvorený definovaním súboru kľúčov toku ako (prameň IP adresy, cieľ IP adresy, DSCP) ako v príklade 1 návrhu a použitie činnosti, ktoré maskuje von najmenší 8 bitový prameň IP adresy a cieľ IP adresy (t.j. výsledok 24 adries). Štyri toky z príkladu 1 môžeme zhromaždiť do troch tokov splývaním tokov 1 a 2 jednodielneho toku.

1. {198.18.40.0/24, 198.18.23.0/24, 4}
2. {198.18.40.0/24, 198.18.23.0/24, 2}
3. {198.18.20.0/24, 198.18.23.0/24, 4}

Príklad 3: Filter definuje niektoré hodnoty kľúča toku, môže byť aplikovaný na všetkých paketoch, ktoré prejdú bodom merania za účelom vybrať iba spoľahlivý tok. Filter definuje výber hodnôt kľúčov toku z paketu. Všetky pakety ktoré vychádzajú od klienta siete 198.18.40.0/24 k inému odberateľovi 198.18.23.0/24 s DSCP potrebujú 4 aby definovali tok. Všetky ďalšie kombinácie nedefinujú tok a nie sú vzaté v úvahu. Tri toky z príkladu 2 zredukujeme do 1 toku filtráciou druhého a tretieho toku, odchádza len {198.18.40.0/24, 198.18.23.0/24, 4}.

Pod pojmom tok (flow) sa rozumie množina IP paketov prechádzajúcich pozorovacím bodom v sieti počas určitého časového intervalu. Všetky pakety patriace do daného toku majú spoločné vlastnosti. Každá vlastnosť je definovaná ako výsledok funkcie aplikovanej na niektorú z častí paketu. Takýmito časťami môžu byť:

- jedna alebo viac položiek hlavičky paketu (napr. cieľová IP adresa), hlavičky transportného protokolu (napr. cieľový port) alebo položky hlavičky aplikačného protokolu (napr. RTP (RFC1889, 1996))
- charakteristika samotného paketu (napr. počet MPLS návěstí)
- jeden alebo viac polí odvodených zo zaobchádzania s paketom (IP adresa nasledujúceho smerovača, výstupné sieťové rozhranie)

Paket patrí do toku, ak splňa všetky podmienky definované vlastnosťami.

Využitie informácií o tokoch je dôležité pri plánovaní siete, inžinieringu prevádzky, plánovaní rozšírení siete a výkonnostnom vylepšovaní jednotlivých komponentov siete. Takisto je tieto dáta možné použiť pri účtovaní podľa prenesených dát alebo podľa jednotlivých zákazníkov. Podľa týchto aplikačných oblastí boli vypracované požiadavky pre jednotlivé časti návrhu architektúry IPFIX.

4. Referenčný model IPFIX

Figúra nižšie ukazuje referenčný model IPFIX. Figúra obsahuje viacero možných scenárov, ktoré môžu byť v IPFIX systéme. Rôzne funkčné súčasti sú udávané vnútri hranatých zátvoriek []. Funkčná súčasť vnútri [*] nie je súčasťou IPFIX architektúry.

5. Funkčné a logické bloky IPFIX (Functional and logical blocks)

5.1. Merací proces (metering process)

Merací proces generuje záznamy tokov (flow records). Vstupom do meracieho procesu sú hlavičky paketov z bodu merania a hodnoty odvodené zo zaobchádzania s paketmi. Merací proces pozostáva z viacerých podprocesov, ako je spracovanie hlavičky, generovanie časových známok, vzorkovania, klasifikovania a spracovania záznamov tokov. Spracovanie záznamov tokov spočíva vo vytváraní nových záznamov, zmene existujúcich záznamov, počítania štatistík záznamov, odvodenia ďalších vlastností tokov, detekovania ukončenia platnosti záznamov tokov, odosielanie záznamov tokov do exportovacieho procesu a z odstraňovania záznamov tokov.

5.1.1. Zánik toku (Flow expiration)

Merací proces musí byť schopný detekovať expiráciu tokov. Tok sa pokladá za expirovaný, ak v danom časovom intervale nebol pozorovaný žiadny paket patriaci do daného toku. Merací proces môže podporovať mechanizmy expirácie pred vypršaním časového limitu pomocou sledovania príznakov TCP protokolu FIN (ukončenie spojenia), RST (zrušenie spojenia).

5.1.2. Export toku (Flow Export)

Exportovací proces je funkčný blok, ktorý zahŕňa jeden alebo viac inštancií IPFIX protokolu. Na jednej strane komunikuje s meracím procesom, alebo s procesom zaznamenávania tokov, aby získal záznamy tokov a na druhej strane spolupracuje so zberacím procesom v zberači.

5.2. Pozorovací bod (Observation point)

Bod merania je miesto v sieti, kde môžu byť pozorované IP pakety. Môže to byť linka, ku ktorej je pripojená sonda, zdieľané médium ako napr. LAN založené na Ethernete, jednoduchý port smerovača alebo množina rozhraní na smerovači.

5.3. Kritériá výberu paketov

Meracie procesy môžu definovať pravidlá tak, že len určité pakety v toku môžu byť vybrané na meranie v pozorovacom bode. Toto môže byť jednou z dvoch metód popísaných nižšie, alebo kombináciami týchto metód.

5.3.1. Vzorkovanie paketov (Sampling functions), Si

Pakety, ktoré spĺňajú vzorkovacie kritériá pre tento typ toku. Príklad: Vzorkuj každý 100tý paket, ktorý bol prijatý v pozorovacom bode a určí informácie o toku ku ktorému patrí. Vybranie všetkých paketov je špeciálny prípad vzorkovania, kde vzorkovací pomer je 1:1.

5.3.2. Funkcia na vlastnostiach určujúca typ toku, Fi

Pakety, ktoré spĺňajú funkciu na poliach definovaných hlavičkou paketu, alebo získaných spracovaním paketu, alebo vlastných polí paketu. Príklad: Mask/Match týchto polí definuje filter. Filter môže byť definovaný napr. ako Protokol == TCP, cieľový port medzi 80 a 120. Viaceré takéto filtre môžu byť použité za sebou na docielenie precíznejšej selekcie paketov.

5.4. Pozorovacia doména (observation domain)

Pozorovacia doména je logický blok, ktorý navonok prezentuje jednu identitu pre skupinu pozorovacích bodov v IPFIX zariadení. Každá dvojica (pozorovací bod, merací proces) musí patriť do jednej pozorovacej domény. IPFIX zariadenie môže mať viacej pozorovacích domén, každá z nich s viacerými pozorovacími bodmi. Každá pozorovacia doména musí mať unikátne ID v kontexte IPFIX zariadenia. Jeden exportovací proces môže obsluhovať viacej pozorovacích domén. V tomto prípade exportovací proces používa toto unikátne ID na rozlíšenie exportovaných paketov medzi rôznymi pozorovacími doménami. Tento istý koncept je použitý aj v zberacom procese na identifikáciu paketov prichádzajúcich z rôznych pozorovacích domén v tom istom IPFIX zariadení.

5.5. Exportovací proces (Exporting process)

Exportovací proces je funkčný blok, ktorý zahŕňa jeden alebo viac inštancií IPFIX protokolu. Na jednej strane komunikuje s meracím procesom, alebo s procesom zaznamenávania tokov, aby získal záznamy tokov a na druhej strane spolupracuje so zberacím procesom v zberači. Napríklad: Iba záznamy tokov ktoré vyberú kritéria vývozu:

1. Všetky záznamy tokov ktorých cieľom je zhoda adres {198.18.33.5}.
2. Každý iný záznam toku ktorého cieľ IP zhody adres {198.18.11.30}.

5.6. Zberací proces (Collecting process)

Zberací proces by mal prijímať záznamy dát bez spojenia so záznamom šablón. Ak záznamy šablón neboli prijaté v čase prijatia záznamov dát, zberací proces by mal uložiť záznamy dát na krátky časový interval a dekodovať ich potom ako budu prijaté záznamy šablón. Časový interval uloženia záznamov dát musí byť menší ako životnosť šablóny. Životnosť šablóny zberacieho procesu je obmedzená na pevne stanovené obnovenie

vypršaného časového intervalu (fixed refresh timeout). Zberací proces musí byť spojený so životnosťou každej prijatej šablóny prostredníctvom UDP.

Na vysokej úrovni, zberací proces:

1. Prijímanie a získavanie kontrolných informácií.
2. Dekódovanie a zásobovanie záznamov tokov pomocou riadiacej informácie.

6. Celkový pohľad z IPFIX protokolu

V IPFIX zariadení, funkcionality protokolu sídli na strane exportovacieho procesu. IPFIX protokol získava toky z procesu zaznamenávania tokov, alebo priamo od meracieho procesu a prenáša ich ku zberaču/zberačom. Na vyššej vrstve, IPFIX protokol vykonáva nasledovné: Funkcie:

1. Kódovanie vybraných kontrolných informácií do šablón.
2. Kódovanie tokov pozorovaných v pozorovacom bode do záznamov o tokoch.
3. Použitie transportnej vrstvy na posielanie exportovaných paketov zberaču.
4. Spracovanie exportných chýb a timeout-ov.
5. Spracovanie preťaženia IPFIX zariadenia.
6. Aplikácia selektívnych filtrov

IPFIX zariadenie je zariadenie obsahujúce aspoň jeden pozorovací bod, vymeriavací proces a exportovací proces. Obyčajne odpovedajúci pozorovací bod, vymeriavací proces a exportovací proces sú spoločne umiestnené na tomto zariadení, napr. na smerovači.

7.1. Prehľad informačného modelu

Kolektor prijíma definíciu šablóny od exportéra ešte pred prijatím záznamov tokov. Záznamy tokov môžu byť dekodované a lokálne uložené na zariadeniach. V prípade, že definície šablón neboli prijaté v čase prijatia záznamu toku, kolektor by mal udržať záznam toku pre neskoršie dekodovanie dotedy, kým nebude prijatá definícia šablóny.

Kolektor nesmie predpokladať, že FlowSet dát a pridružené ID šablón je exportované v tom istom vyexportovanom pakete. Kolektor nesmie predpokladať, že iba jedna šablóna FlowSetu je prítomná vo vyexportovanom pakete. V zriedkavom prípade, vyexportovaný paket môže obsahovať niekoľko šablón FlowSetov.

Šablóny existujú len určitý časový interval. Životnosť šablóny by mala byť odpočítaná (zistená) na kolektore na základe času, kde posledná šablóna FlowSetu bola prijatá z exportéra. Kolektor sa nesmie pokúšať dekodovať záznamy tokov s vypršanou platnosťou šablóny. Kolektor by mal udržiavať takýto zoznam: <exportér, exportné rozhranie, ID šablóny, definícia šablóny, posledné prijatie>. Ak je prijatá nová definícia šablóny (napr. v prípade reštartovania exportéra), existujúca definícia by mala byť okamžite nahradená.

7.2. Záznamy tokov (Flow records)

Záznam toku (Flow Record) pozostáva z informácií o špecifickom toku, ktorý bol pozorovaný v pozorovacom bode. Obsahuje merané vlastnosti toku (napr. celkový počet bitov všetkých paketov toku) a charakteristické vlastnosti toku (napr. zdrojová IP adresa).

7.3. Kontrolná informácia

Kódovanie kontrolných informácií sa riadi nasledujúcimi pravidlami:

- Kontrolná informácia by mala byť kódovaná tak, aby mohla zachytiť štruktúru a sémantiku korešpondujúceho toku pre každý tok exportovaný IPFIX zariadením.
- Konfiguračná kontrolná informácia by mala byť kódovaná tak, aby mohla zachytiť štruktúru a sémantiku korešpondujúcich konfiguračných dát. Konfiguračné data, ktoré sú zároveň aj kontrolnými informáciami by mali niesť ďalšie informácie o hraniciach, v ktorých je táto konfigurácia efektívna.

Kontrolné informácie sú používané zberacím procesom na:

- Dekódovanie a interpretáciu záznamov o tokoch.
- Rozlíšenie stavu exportujúceho procesu.

Ako taká, je kontrolná informácia z exportujúceho procesu kritická pre správnu funkcionálnosť IPFIX zberacieho procesu. Môžu byť použité nasledujúce prístupy na export kontrolných informácií.

1. Poslať všetky kontrolné informácie súvisiace so záznamami o toku ešte pred poslaním záznamov o toku. To zahŕňa všetky inkrementálne zmeny ktoré boli spôsobené na definícii záznamoch o toku.
2. Sprostredkovať, skoro na real-time báze, stav IPFIX zariadenia zberaciemu procesu. To zahŕňa všetky zmeny ako napr. konfiguračné zmeny, ktoré ovplyvňujú správanie toku, menia zdroje exportného procesu, menia rýchlosť exportu, atď., ktoré musí zberač poznať.
3. Keďže je dôležité aby mal zberací proces presnú znalosť o stave exportéra, export kontrolných informácií, by mal spoľahlivo dosiahnuť zberač. Jednou z možností ako to docieľiť, je posielat' kontrolné informácie spoľahlivým transportom.

7.4. Ohlasovanie povinností (Reporting responsibilities)

Občas IPFIX zariadenie nemusí byť schopné pozorovať všetky pakety siahajúce z jedného jeho bodu merania. Môže sa stať že merací proces nájde dočasné zdroje. Napríklad: Mohlo by to ísť mimo balíka zásobníkov pre IPFIX export, alebo by to mohlo zistiť chyby v jeho základnej transportnej vrstve. V takýchto situáciách, IPFIX zariadenie musí hlásiť stratu paketov ktoré sa vyskytujú v kolektoroch.

8. Detaily protokolu IPFIX

Keď IPFIX pracovná skupina bola autorizovaná tak existujú všeobecné postupy v oblasti exportu tokov. Napríklad Net Flow, Crane, LFAP, RTFM atď. Listina IPFIX požadovaná pracovnou skupinou berie do úvahy existujúce zvyklosti a vyberá jeden z najvhodnejších k IPFIX požiadavkám IPFIX-REQS. Dodatky alebo modifikácie by mali byť urobené k vybranému protokolu tak by sa hodili v IPFIX architektúre.

8.1. IPFIX Osnova protokolu

Funkcia IPFIX protokolu v zariadení IPFIX je na strane exportovacieho procesu. IPFIX protokol plní úlohu, ktorej cieľom je získať toky z procesu zaznamenávania tokov alebo ich získať priamo od meracieho procesu a prenáša ich ku zberaču.

IPFIX protokol spravuje:

- výber a posielanie kontrolných informácií a záznamov o tokoch
- kódovanie kontrolných informácií o tokoch
- expiráciu tokov
- správanie pri preťažení
- selektívny export záznamov o tokoch
- IPFIX protokol vykonáva nasledujúce funkcie:
- kódovanie vybraných kontrolných informácií do šablón
- kódovanie tokov pozorovaných v pozorovacom bode do záznamov o tokoch
- použitie transportnej vrstvy na posielanie exportovaných paketov zberaču
- spracovanie preťaženia IPFIX zariadenia
- aplikácia selektívnych filtrov

8.2. IPFIX protokol v zberacom procese

IPFIX protokol na kolektore je zodpovedný za:

1. Prijímať a dekódovať záznamy toku z IPFIX zariadení.
2. Schopnosť indikovať straty záznamov o toku exportovaciemu IPFIX zariadeniu a/alebo IPFIX používateľovi.
3. Voliteľne notifikovať stav a podmienky preťaženia IPFIX zariadeniu.

8.3. Podpora aplikácií

Aplikácie ktoré používajú informácie získané IPFIX môžu byť zistením podsystemu atď. Tieto aplikácie môžu byť neoddeliteľnou súčasťou zberacieho procesu alebo môžu byť umiestnené v zberacom procese. Cesta ktorou sa tieto aplikácie prepoja s IPFIX systémom je mimo tohto dokumentu.

9. Modely exportu

9.1. Model exportu so spoľahlivou kontrolou spojenia

Kontrolné informácie a dátový stream musia byť transportované po transporte s kontrolou preťaženia. Ak sieť, v ktorej sa IPFIX zariadenie a zberací proces nachádzajú, neposkytuje spoľahlivý transport, potom by aspoň jedna kontrolná informácia mala byť prenášaná cez spoľahlivý transport. Možu nastať aj bezpečnostné požiadavky medzi IPFIX zariadením a zberacím procesom. Z tohoto dôvodu môžu byť implementované nasledujúce riešenia:

- IP autentifikačná hlavička, môže byť použitá, ak prostredie vyžaduje silnejšiu integritu ale nepotrebuje utajenie.

- IP bezpečnostné zapuzdrenie paketu (IP Encapsulating Security Payload - EPS) môže byť použité na zabezpečenie utajenia a integrity.
- Ak je transportným protokolom TCP, voliteľne môže byť použitá TCP MD5 signatúra na obranu proti spoofovaným TCP segmentom.
- Ak je trenasportným protokolom TCP, voliteľne môže byť použitý TLS na zvýšenie integrity, autenticity a utajenia.

Dátový stream môže byť exportovaný po spoľahlivých, alebo nespoľahlivých transportných protokoloch. Ako bolo vysvetlené vyššie, transportné spojenie je predprípravou medzi IPFIX zariadením a zberačom. Keď sa spoja, zberač obdrží kontrolné informácie a použije tieto informácie na interpretáciu záznamov o toku. IPFIX zariadenie by malo nastaviť interval obnovovania na dostatočne nízku hodnotu, aby dokázalo včas zistiť poruchu zberača.

9.2. Model exportu so spoľahlivým kontrolným spojením

Porucha zberača je detekovaná v IPFIX zariadení prerušením kontrolného spojenia. Pri detekcii vypršania časového limitu spojenia, by malo IPFIX zariadenie prestať exportovať dáta zberaču a pokúsiť sa znovunadviazať spojenie. To platí pre prípad jedného zberača. Ak sú k dispozícii viaceré zberače pre jedno IPFIX zariadenie, potom si IPFIX zariadenie otvorí kontrolné spojenia na každý z týchto zberačov, ale dáta sú posielané iba na jeden z týchto zberačov, ktorý je označený ako primárny. Jeden alebo viac zberačov, môže byť označených ako sekundárny a môže im byť pridelená priorita. Porucha primárneho zberača je detekovaná na strane IPFIX zariadenia ako prerušenie kontrolného spojenia. Ak je toto spojenie prerušené, IPFIX zariadenie si otvorí spojenie so sekundárnym zberačom najvyššej priority. Tento zberač sa stáva primárnym. Maximálna strata exportovaných dát je množstvo dát, ktoré bolo vyexportované, kým bolo detekované prerušenie kontrolného spojenia na strane IPFIX zariadenia.

9.3. Redundancia zberačov

Pretože IPFIX protokol vyžaduje transport detekujúci preťaženie, redundancia pomocou multicastov nie je možná. Môžu byť však inicializované viaceré páry, kontrolná informácia, dátový stream, každý k inému zberaču z toho istého IPFIX zariadenia.

10. Zber IPFIX tokov pre špeciálne dáta

IPFIX zariadenie môže generovať, prijímať alebo meniť špeciálne typy dát ako napr.:

Tunelové dáta:

IPFIX zariadenie môže byť začiatkom, stredom, alebo koncom tunela. V takomto prípade IPFIX by mal spracovávať GRE, IPinIP, UTI dáta.

VPN dáta :

IPFIX zariadenie môže byť koncové zariadenie providera, ktoré prijíma dáta zo zákazníckej siete náležiacej do virtuálnej privátnej siete.

V takomto prípade by mali byť jasné pravidlá:

- Ako ak kedy klasifikovať pakety ako tok.
- Ak je na definovanie toku použité viacnásobné zapuzdrenie, ako preniesť rovnaké polia (napr. IP adresa) do rôznych vrstiev.
- Ako diferencovať toky založené na rôznych privátnych doménach.

11. Bezpečnosť

Informácie o IP tokoch môžu byť použité na rôzne účely, ako napríklad účtovníctvo, profilácia dát, analýza dát, detekcia vniknutí. Pre každú aplikáciu sa bezpečnostné požiadavky môžu meniť. Aby bolo možné uspokojiť bezpečnostné požiadavky rôznych IPFIX používateľov, architektúra IPFIX musí poskytovať rôzne stupne bezpečnosti.

11.1. Bezpečnosť dát

IPFIX dáta pozostávajú z kontrolných informácií a dátového streamu generovaného IPFIX zariadením. IPFIX dáta môžu existovať v IPFIX zariadení aj v zberači. Navyše, dáta sú aj transportované po spojení od IPFIX zariadenia ku zberaču, kedykoľvek je to potrebné. Kvôli bezpečnosti, tieto dáta by mali byť chránené pred nepriateľom.

Všade kde je potrebné zabezpečiť bezpečnosť. Je odporúčané zabezpečiť spodné vrstvy použitím IPsec, alebo TLS. Na ochranu dát na spojení su definované tri stupne ochrany:

11.1.1. Žiadna bezpečnosť

Bezpečnosť nemusí byť vyžadovaná, ak transport medzi IPFIX zariadením a zberačom je považovaný za bezpečný. Táto možnosť umožňuje protokolu bežať nanajvyš efektívne, bez zbytočnej extra záťaže.

11.1.2. Len autentizácia

Ochrana len autentizáciou poskytuje používateľovi IPFIX istotu dátovej integrity a autenticity. Dáta vymieňané medzi IPFIX zariadením a zberačom sú chránené autentizačným podpisom. Akákoľvek modifikácia IPFIX dát bude detekovaná príjemcom dát, čo vyústi do zahodenia prijatých dát. Napriek tomu, len autentizácia, nezaručuje utajenie dát. Používatelia IPFIX by sa mali tejto možnosti vyhnúť pokiaľ prenášajú citlivé alebo tajné dáta. Niektoré spôsoby ako dosiahnuť autentizáciu dát sú:

- TCP s MD5 voľbami
- IP autentizačná hlavička

11.1.3. Kryptovanie

Kryptovanie dát poskytuje najlepšiu bezpečnosť pre IPFIX dáta. Dáta sú kryptované odosielateľom a iba určený príjemca ich môže dekryptovať a získať tak prístup dátam. Táto voľba musí byť použitá, ak transport medzi IPFIX zariadením a zberačom nie je zabezpečený a IPFIX dáta potrebujú byť chránené. Niektoré spôsoby ako dosiahnuť tento stupeň bezpečnosti sú:

- Bezpečnostné zapuzdrenie paketu
- Transport Layer Security (TLS) Protokol

Kryptovanie dát zvyšuje veľkosť prenášaných dát. Môže limitovať rýchlosť, ktorou export odovzdáva dáta zberaču, kvôli veľkej spotrebe zdrojov pri kryptovaní.

11.2. Autentizácia koncového IPFIX bodu

Je dôležité zabezpečiť, aby IPFIX zariadenie komunikovalo so "správnym", nie maskovaným, zberačom. Tá istá logika platí aj pre pohľad zo strany zberača. IPFIX architektúra dovoľuje autentizačné možnosti tak, že sa môže vykonať jednosmerná alebo obojsmerná riadená autentizácia medzi zberačom a IPFIX zariadením. IPFIX architektúra by mala používať nejakú transportnú ochranu protokolov tak ako TLS alebo IPSEC spĺňajúce autentizačnú požiadavku.

12. Preťaženie IPFIX

V prípade preťaženia z nedostatku pamäte alebo nedostatku výpočtovej kapacity merací proces môže zmeniť svoje správanie, tak aby reagoval na nedostatok zdrojov. Možné reakcie zahŕňajú:

- znížiť počet meraných tokov. Toto môže byť dosiahnuté jednak zvýšením granularity meracieho procesu, alebo znížením počtu sledovaných tokov na podmnožinu z pôvodnej množiny sledovaných tokov
- začať vzorkovanie predtým ako sú pakety spracované meracím procesom, alebo, ak sa vzorkovanie už vykonáva, znížiť vzorkovaciu frekvenciu
- zastaviť meranie
- znížiť zaťaženie ostatnými procesmi

Správanie sa pri preťažení nie je obmedzené na vyššie popísané štyri spôsoby, ale v prípade vzniku preťaženia musí byť jednoznačne definované. Toky vytvorené jednou vzorkovacou metódou, alebo jednou vzorkovacou frekvenciou nesmú byť spojené s tokmi vytvorenými po zmene vzorkovacej metódy, alebo vzorkovacej frekvencie. Zhromažďovací proces musí byť schopný odlišiť toky vytvorené pred a po zmene vzorkovacej metódy, alebo frekvencie.

12.1. Prevencia Denial of service (DoS) útokov

Keďže jedno z potenciálnych využití IPFIX je pri detekcii vniknutí, je dôležité aby tento protokol podporoval nejaký druh DoS odolnosti.

12.1.1. Útok na sieť

Samotná sieť môže pod útokom vyústiť do množstva IPFIX správ. IPFIX by sa mal pokúsiť zachytiť maximálne možné množstvo informácií. Avšak, keď bude v krátkej dobe generované veľké množstvo IPFIX správ, protokol sa môže preťažiť.

12.1.2. Štandardný DoS útok na IPFIX systém

IPFIX systém môže čeliť štandardnému DoS útoku, ako každý systém na otvorenej sieti. Tieto typy útokov nie sú špecifické na IPFIX. Zabraňovanie a odpovedanie na takéto útoky nie je oblasťou tohto dokumentu.

12.1.3. Špecifické útoky na IPFIX

Je to špecifický útok na IPFIX časť IPFIX zariadenia alebo zberača.

- Útočník môže zahltiť zberač spoofovanými IPFIX export paketmi. Jednou z možností ako tomu zabrániť, je periodicky si vymeniť synchronizačné sekvenčné čísla záznamov o toku, medzi exportovacím procesom a zberačom.
- Útočník môže poskytnúť falošné správy IPFIX zariadeniu, poslaním spoofovaného kontrolného paketu.

Problémy spomínané vyššie, môžu byť vo veľkej miere riešené obojstranným kryptovaním kontrolných paketov.

13. IANA hľadisko

Ako opisujeme v tomto dokumente, architektúra IPFIX má dva druhy pridaných čísel. Ich pridávanie je ďalej opísané v dokumente.

13.1. Čísla použité v protokole

IPFIX správy, používajú dva polia predvolených hodnôt. Sú to číslo verzie IPFIX, ktoré poukazujú na verziu IPFIX protokolu, použitú na exportovanie IPFIX správy. Ako druhé je to číslo IPFIX šablóny, poukazujúce na typ každej informácie v IPFIX správe.

Zmeny čísla verzie IPFIX alebo šablóny požadujú konsenzus IETF, robia sa na základe RFC schváleného IESG.

13.2. Čísla použité v informačnom modeli

Polia IPFIX protokolu nesú informácie o meraní prevádzky. Sú modelované ako elementy IPFIX informačného modelu. Každý informačný element popisuje pole, ktoré sa môže objaviť v IPFIX správe.

Zmeny typu IPFIX poľa budú spravované IANA-ou, predmet expertného rozoberania, rozoberanie jednou zo skupín expertnou priradených IETF riaditeľom operácii

a manažmentu. Títo experti sa vyberú z vedenia pracovných skupín a editorov IPFIX a PSAMP pracovných skupín.

14. IPFIX Applicability

IPFIX protokol určuje ako môže byť IP informácia o toku poslaná z routera, snímača meraní alebo z iného zariadenia. Túto informáciu využijeme ako vstup k rôznym aplikáciám. IPFIX je základný dátový transportný protokol, jednoducho rozširiteľný pre potreby rôznych aplikácií. Tento dokument opisuje ktoré aplikácie používajú IPFIX protokol a ako ho môžu používať. Okrem toho opisuje vzťah IPFIX k ostatným systémom a architektúram.

15. Použitie IPFIX

IPFIX dáta umožňujú niekoľko dôležitých aplikácií. Táto časť opisuje ako sa dá využiť IPFIX protokol.

15.1. Účtovanie

V súčasnosti sa vyvíja niekoľko modelov spoplatňovania IP služieb. Okrem pripojenia typu flat rate, ktoré nepotrebuje špeciálny prístup k účtovaniu, účtovanie môže byť založené na čase prístupu k službe, ako aj na množstve prenesených údajov. Účtovanie podľa použitia je jednou z najvýznamnejších aplikácií, ktorá bola vyvinutá IPFIX protokolom. Poskytovatelia internetových služieb môžu využiť túto informáciu na prechod z jednotného účtovania k viac flexibilnému účtovaciemu mechanizmu založenému na dennom čase, využitia šírky pásma, využitia aplikácie, kvality služieb, atď. Aby sa využilo účtovanie podľa použitia v IPFIX, definíciu toku musíme vybrať podľa tarify modelu. IPFIX umožňuje veľmi rôznorodé definovanie toku, ktoré môže byť prispôbené potrebám iných tarifných modelov. Ľubovoľný model účtovania založený na toku môže byť vytvorený bez nejakých obmedzení vzhľadom na IPFIX protokol. Poplatok môže byť, napríklad, založený na tokoch medzi používateľmi, v tomto prípade účtovanie môže byť realizované definíciou toku určenou päticou ktorá pozostáva z pôvodnej adresy, adresy určenia, protokolu a čísiel portov. Iným príkladom je poplatok závislý na triede. V tomto prípade sa toky budú odlišovať len DSCP a zdrojovou IP adresou. Dôležitou súčasťou potrebnou na účtovanie je počet poslaných paketov a bitov na tok, ktoré sú obsiahnuté v IPFIX záznamoch o toku. Za účelom účtovania, je výhodou mať schopnosť využívať IPFIX záznamy tokov ako vstup účtovania v infraštruktúre AAA. AAA server potom umožňuje mapovanie medzi používateľom a informáciou o toku. Všimnite si, že požiadavky spoľahlivosti definované v (RFC3917) nie sú dostatočné, aby zabezpečili úroveň spoľahlivosti, ktorá je potrebná pre veľa systémov účtovania podľa použitia. Čiastočne sú požiadavky spoľahlivosti účtovacích systémov prediskutované v (RFC2975).

15.1.1. Príklad

Predpokladajme že niekto má SLA v sieti Diffserv a požiadavky účtovania založené na intenzite prevádzky.

Informácie potrebné na export v tomto prípade sú:

- IPv4 zdrojová IP adresa: sourceIPv4Address v (IPFIX-INFO) s dĺžkou 4 oktety
- IPv4 IP adresa určenia: destinationIPv4Address v (IPFIX-INFO) s dĺžkou 4 oktety
- Druh prevádzky: classOfServiceIPv4 v (IPFIX-INFO) s dĺžkou 1 oktet
- Počet oktetov toku: inOctetDeltaCount v (IPFIX-INFO) s dĺžkou 4 oktety

Šablóna potom vyzerá takto (v prípade že použijeme IETF-špecifikované informačné elementy):

```
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|   Set ID = 2       |   Length = 24 octets   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|   Template ID 256 |   Field Count = 4   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|0| sourceIPv4Address = 8 |   Field Length = 4   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|0| destinationIPv4Address = 12 |   Field Length = 4   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|0| classOfServiceIPv4 = 5   |   Field Length = 1   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|0| inOctetDeltaCount = 1   |   Field Length = 4   |
```

Informácia na odoslanie je zobrazená v nasledujúcej tabuľke:

Src. IP addr.	Dst. IP addr.	Type of service	Octets Number
198.18.1.12	198.18.2.254	101110	987410
198.18.1.27	198.18.2.23	101110	170205
198.18.1.56	198.18.2.65	101110	33113

Pole “druh prevádzky” obsahuje DiffServ Codepoint na prvých šiestich bitoch, zatiaľ čo posledné dva sú nevyužitú. V tomto príklade použijeme binárny kód 101110 odporúčaný pre EF PHB (RFC2598).

Záznam toku potom vyzerá takto:

```
0          1          2          3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|      Set ID = 256      |      Length = 32      |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|          198.18.1.12          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|          198.18.2.254          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| 101110 00 |          987410          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|          |          198.18.1.27          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|          |          198.18.2.23          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|          | 101110 00 |          170205          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|          |          198.18.1.56          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|          |          198.18.2.65          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|          | 101110 00 |          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|          33113          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

15.2 Bezpečnostná analýza a detekcia vniknutia s IPFIX

IPFIX poskytuje informácie o prevádzke v sieti. Z tohto dôvodu je veľmi vhodné na zohrávanie hlavnej úlohy pri detekcii sieťových ohrození ako napríklad vniknutí, rozširovania vírusov a wormov, port scanning a iné sieťové útoky. Systémy detekcií vniknutí (IDS) monitorujú a riadia bezpečnostné incidenty. Typický IDS systém tvorí viac komponentov, ako napríklad senzory, uzlové kolektory, uzly manažmentu. Senzory monitorujú sieť a prevádzku systému kvôli ohrozeniam a iným dejom spojeným s bezpečnosťou. Senzory reagujú a hlásia administrátorovi tieto deje tak ako nasledujú. Kolektory udalosti sú medzičlánkom zodpovedným za prenos dejov zo senzorov na konzolu a do databázy. Uzol manažmentu slúži na tieto účely:

- vizuálne monitorovanie dejov (s konzolou)
- zbieranie dáta zo senzorov (s jedným alebo viacerými kolektormi dejov)
- ukladá dáta zo senzorov (v databázy)

IPFIX môže hlásiť deje určené pre senzor buď pri zberacom procese alebo priamo exportným procesom. Ktorý prístup je najlepší záleží na scenári a na dejoch záujmu. Získavanie informácií priamo od exportovacieho procesu je výhodnejšie, pretože senzor

dostáva informáciu skôr. Nepotrebuje čakať na vyhodnotenie zbierania, alebo kým kolektor získa potrebné dáta. Získavanie dát z kolektora umožňuje porovnanie dát z rôznych exportovacích procesov (z rôznych routerov), aby sme získali lepší pohľad na deje v sieti.

IPFIX poskytuje užitočný vstup pre základne funkcie detekcie vniknutí ako napríklad detekcia neobyčajne vysokého zaťaženia, počet tokov, počet paketov určitého typu, TCP indikácie, aplikačné porty a objem toku. Tieto dáta môžu byť využité na analýzu bezpečnosti siete a identifikovanie útokov. Ďalšia analýza dát a funkcie post-processingu môžu byť potrebné na generovanie metriky záujmu pre špecifické typy útokov. Výsledná integrácia predošlých meraní pomáha stanoviť zmeny prevádzky a detekciu prevádzkových anomálií. Kombinácia s výsledkami z iných meracích bodov povoľuje vyhodnotenie rozšírenia útoku a môže pomôcť pri nájdení zdroja toku.

Pre niektoré scenáre, detekcia vniknutia môže potrebovať ďalší náhľad do obsahu paketov. Keďže IPFIX povoľuje flexibilné definovanie správ, merací proces a formát IPFIX správ môže byť rozšírený na podporu iných dát potrebných pre systémy detekcie vniknutia. Okrem toho je možné získať informáciu po paketoch pomocou IPFIX pre exportovanie PSAMP informácie.

Detekcia incidentov bezpečnosti v riadnom čase bude vyžadovať predbežné spracovanie dát v meracom zariadení a priamy export dát pre prípad možného incidentu. To znamená že IPFIX správy musia byť generované na základe hľadania incidentu javov a nie len na základe konca toku alebo určeného časového intervalu.

Navyše, bezpečnostné incidenty sa môžu stať hrozbou k procesom IPFIX (viď z bezpečnostného hľadiska v (IPFIX-PROTO)). Ak útok vytvára veľké množstvo tokov (napr. posielaním paketov so spoofovanými adresami alebo simulovanie ukončenia toku) exportovací a zhromažďovací proces sa môže preťažiť pri veľkom množstve záznamov dát, ktoré sú exportované. Flexibilné rozmiestnenie paketov alebo metódy snímania toku môžu zabrániť vyčerpaniu zdrojov. Detekcia vniknutia veľmi profituje z kombinácie IPFIX funkcií s AAA funkciami (viď kapitola 16.1.). Táto súčinnosť poskytuje ďalšie spôsoby na detekciu útočníkov, pokročilejšie stratégie obrany, a bezpečnú medzi doménovú spoluprácu.

K danej téme:

Súčasti IDS sa často výrazne odlišujú vnútornou štruktúrou, tento fakt často znemožňuje spoluprácu viacerých systémov pri zabezpečení siete. Dôsledkom sú snahy o štandardizáciu modelu IDS. Základom moderných systémov detekcie prienikov je model CIDF (Common Intrusion Detection Framework). Ten definuje jednotlivé komponenty systému a komunikačný protokol, ktorého súčasťou je jazyk, ktorým komponenty medzi sebou komunikujú. CIDF definuje tieto moduly:

Úlohou generátora udalostí je poskytovať informácie o vzniku danej udalosti ostatným častiam systému. Pod udalosťou si môžeme predstaviť napr. prihlásenie používateľa, spustenie programu, aktivitu sieťovej vrstvy a pod. Je dôležité si uvedomiť, že udalosť nemusí nevyhnutne indikovať útok, môže však poskytnúť indicie, ktoré po vyhodnotení môžu odhaliť nezvyklú aktivitu.

Analytický modul analyzuje udalosti poskytované generátorom udalostí. Veľká časť výskumu v oblasti detekcie prienikov je venovaná práve hľadaniu nových postupov pre rozbor udalostí. V súčasnosti sa používajú analytické techniky založené na štatistických anomáliách, modeloch resp. grafoch správania sa "bežného" používateľa a dokonca sú aj pokusy inšpirované biologickým imunitným systémom.

Ukladací mechanizmus generátor udalostí a analytický modul vyprodukovujú veľké množstvo údajov, ktoré je potrebné dočasne resp. trvalo uložiť. Ukladací mechanizmus systému detekcie prieniku definuje prostriedky, ktoré sa použijú pri ukladaní bezpečnostných informácií. Pritom nemusí ísť o uloženie celej informácie, často sa ukladá napríklad len varovanie, že daný typ udalosti nastal.

Modul protiopatrení umožňuje aby IDS reagoval aktívne v reálnom čase na predchádzajúce udalosti. Môže sa jednáť buď o lokálne akcie, ako zrušenie spojenia, odhlásenie používateľa, ukončenie procesu, alebo o akcie s dopadom na celú chránenú časť systému, napr. zmena pravidiel na firewall, zrušenie služby, zakázanie používateľa. Komponenty tohto modelu môžu byť realizované ako jeden monolitický celok, často sa však jedná o distribuované systémy v ktorých sú jednotlivé moduly prevádzkované na viacerých významných hosťovských počítačoch napr. na firewall, www serveri a mail serveri beží typický generátor udalostí prípadne aj analytický modul. Z nich sa informácie sieťovým ukladacím modulom predávajú jednému alebo viacerým systémom pre sieťový dohľad.

Znovuskladanie TCP spojenia umožňuje senzoru zachytávať viacero typov útokov:

Bezstavové útoky sú metódy, ktorými je možné zaplniť záznamy IDS falošnými poplachmi. Útočník môže použiť postupy, ktoré simulujú útok zaslaním paketu so signatúrou, ktorý nie je súčasťou spojenia. Takto skrýva vlastný útok preťažením analyzujúcej časti alebo zaplnením úložného priestoru.

Vloženie a preskočenie paketu sú metódy, ktorými môže útočník známe správanie sa cieľového operačného systému (pri spracovaní paketov) na to aby spôsobil buď nesprávne vloženie, keď IDS zaradí do spojenia paket, ktorý cieľový systém odmietne alebo preskočenie paketu IDS, keď zanedbá paket, ktorý cieľový systém spracuje. Keďže je senzor musí sledovať potenciálne správanie sa viacerých OS, jedná sa o relatívne časovo náročnú funkciu.

15.3. Plánovanie sietí

Údaje IPFIX, zozbierané počas dlhého časového intervalu, môžu byť použité na predvídanie rastu siete a plánovanie rozširovania siete prostredníctvom zvyšovania počtu aktívnych sieťových prvkov alebo sieťových rozhraní týchto prvkov. Údaje získané prostredníctvom IPFIX pomôžu optimalizovať strategické plánovanie siete (plánovanie upgradovania backbonu siete, plánovanie politiky smerovania), ako aj taktické rozhodnutia z oblasti sieťového inžinierstva (upgrade routera alebo zvýšenie kapacity prenosovej linky). Výsledkom je minimalizácia nákladov a maximalizácia priepustnosti a spoľahlivosti siete.

15.4. Dohody pre spojenie

IPFIX poskytuje všeobecný dátový formát na výpis výsledkov meraní. Preto je veľmi vhodný na zdieľanie informácií so susedným ISPs. Ak meracie prostriedky v rôznych oblastiach exportujú dáta v tom istom formáte a kolektory z rôznych oblastí rozumejú tomuto formátu, IPFIX dátový záznam by mohol byť priamo presunutý k susednému poskytovateľovi. Môže to skončiť samo pri IPFIX protokole alebo pri konvertovaní alebo zapuzdrovaní záznamov dát do zvyčajne používaného protokolu pre výmenu dát vo vnútri domény tak ako u DIAMETRA. Niektoré ISPs stále nemôžu zdieľať informácie kvôli tomu, že konkurenčný ISPs môže zneužiť sieťové informácie pre susedného používateľa na posilnenie svojej vlastnej pozície na trhu. Napriek tomu, technické potreby začali výmenu dát už skôr. Potreba poskytnutia medzi doménovej garancie je veľkým stimulom na zvýšenie medzi doménovej spolupráce. Navyše, potreba ochrany sietí proti aktuálnym a budúcim hrozbám, podporí nárast ochoty výmeny nameraných dát medzi poskytovateľmi.

15.5. Navrhovanie prevádzky

Zahŕňa metódy pre meranie, modelovanie, kontrolu a riadenie sietí. Cieľom tohto procesu je optimalizácia využitia zdrojov a výkonu, resp. priepustnosti sietí. Typické parametre, požadované pre tento druh činnosti, sú na využitie prenosových liniek, záťaž liniek medzi jednotlivými uzlami siete, počet, veľkosť a vstupné/výstupné uzly jednotlivých tokov, ako aj smerovacie informácie. Údaje získané prostredníctvom IPFIX poskytujú detailné informácie o prevádzke a môžu byť použité pri optimalizácii smerovacej politiky siete s využitím techník ako load balancing, alebo smerovanie určitého druhu prevádzky určitými trasami v sieti, ako aj prioritizácia prevádzky.

15.6. Analýza trendu

IPFIX dátové záznamy sú vhodné na analýzu prevádzky, pre analýzu trendu a ako základ obchodného modelu. Rôzne definície toku umožňujú iné druhy pohľadu na dáta. Skúmanie rôznych druhov štatistík prevádzky (ako počet tokov, prenášanie zvuku) postupom času poskytuje cenný vstup na využívanie existujúcich služieb alebo na plánovanie služieb do budúcnosti.

IPFIX záznamy dát môžu byť uložené na neskoršie použitie a metódy na podporu marketingu a programu služieb zákazníkom. Takým príkladom je rozhodnutie, ktoré aplikácie a služby využijú vnútorní a externí používatelia a potom sa treba zamerať na využitie služieb tak ako bolo publikované. Využíva sa to hlavne pri ISPs lebo IPFIX dáta im umožnia vytvoriť lepší balík služieb.

K danej téme:

Ide o proces charakterizovania IP tokov kľúčovými parametrami, takými ako je napríklad dĺžka trvania toku, objem prenesených údajov, čas vzniku toku. Je neodmysliteľnou súčasťou návrhu a dimenzovania sietí. Typické informácie potrebné pre profilovanie

prevádzky sú distribúcia služieb a protokolov v sieti, množstvo paketov určitého druhu (napr. podiel IPv6 paketov) a špecifické profily tokov. Nakoľko účel profilovania môže byť odlišný, merania vyžadujú vysoko flexibilnú meraciu infraštruktúru najmä s možnosťami konfigurácie meraní a klasifikácie prevádzky.

15.7. Platnosť SLA a Monitorovanie QoS

Vykonávanie QoS monitoringu je jedným, cieľom aplikácie IPFIX protokolu. QoS monitorovanie je pasívnym meraním kvality prenášania pre jednotlivé toky alebo celkovej prevádzky v sieti. Jedným z príkladov využitia je kontrola platnosti QoS, ktorá zaručuje dohody o úrovni služieb. Niektoré QoS metriky vyžadujú vzájomný vzťah dát s meracími bodmi. Kvôli tomu hodiny zabezpečujúce vývozné zariadenia musia byť synchronizované. Okrem toho niektoré merania môžu mať prospech z poprocesových funkcií (generovanie ID paketov a mapovanie) v exportéri alebo v kolektore. Táto časť popisuje ako meranie rôznych metrick sa môže vykonať v IPFIX. Väčšina metrick vyžaduje prinajmenšom pokračovanie v IPFIX informačnom modeli, pretože potrebná informácia ako spätočné oneskorenie IP paketu atď. nie je časťou bežného modelu. Akokoľvek podané, rozťažnosť a flexibilita IPFIX, chýbajúce hodnoty sa môžu ľahko určiť. Priame ohlasovanie IPPM metrick s IPFIX protokolom je opísané v kapitole 16.3.

K danej téme:

IPFIX sa v neposlednom rade dá využiť aj na monitorovanie parametrov QoS. Na druhej strane si treba uvedomiť, že požiadavky špecifikované štandardom IPFIX nepokrývajú monitorovanie všetkých parametrov QoS. Nakoľko informácie sú vyhodnocované na úrovni tokov a nie paketov, ktoré síce definujú charakter paketov patriacich do toku, nezahŕňajú však informácie o samotných paketoch. Typickým príkladom je meranie kolísania oneskorenia (jitter), kde sa vyžaduje pridelenie časových značiek (timestamps) pre jednotlivé pakety. Naproti tomu požiadavky IPFIX definujú časové značky len pre prvý a posledný paket patriaci do toku (z ktorých sa dá určiť kedy tok začal a ako dlho tok trval). Na druhej strane je možné za účelom takéhoto merania nakonfigurovať exportný proces tak, aby každý tok obsahoval práve jeden paket. Tým sa však stratí výhoda kategorizácie prevádzky do tokov a rapídne stúpne množstvo exportovaných údajov. Podobné riešenia by mali byť použité len za účelom vykonania špecifických meraní. Aj keď IPFIX nie je primárne určený na tieto účely, možnosť využitia aj v tejto oblasti dokazuje veľkú flexibilitu návrhu.

15.7.1. Meranie spätočného oneskorenia

Pasívne meranie spätočného oneskorenia môže byť uskutočnené použitím techniky porovnávania paketových párov opísaných v [Brow00]. Pre merania sú tvorené žiadosť/odpoveď paketové páry z protokolov ako napr. DNS, ICMP, SNMP alebo TCP (syn/syn-ack, data/ack)) na pasívne sledovanie RTT. Ako vždy pre pasívne merania, môže pracovať ak potrebná prevádzka je prítomná v sieti. Navyše, ak pozorovaný protokol podporuje retransmisiu (napr. TCP), RTT nie je sieťové RTT ale skôr RTT siete

a protokolovej obálky prijímateľa. V prípade ak paket odpovede je stratený alebo sa nedá pozorovať, RTT nemôže byť vytvorené.

Na použitie tejto meracej techniky, IPFIX merací proces potrebuje merať pakety oboch smerov. Klasifikácia vyššie uvedených protokolov musí byť vytvorená. To znamená, že časti transportnej hlavičky sa používajú na klasifikáciu. Keďže diferenciacia tokov založená na informáciách v transportnej hlavičke je jednou z požiadavok pre IPFIX, takáto klasifikácia môže byť uskutočnená bez dopĺňovania protokolu. Napriek tomu merací proces tiež potrebuje rozpoznať žiadosťové a odpoveďové pakety pre daný protokol a preto musí pozerieť hlbšie do paketov. Schopnosť vytvoriť túto analýzu nie je požiadavkou IPFIX-u, ale môže byť dosiahnutá rôznymi rozšíreniami klasifikačného procesu. Exportovacie zariadenie musí zadať časovú značku pre príchod paketov. Prepočet RTT môže byť uskutočnený priamo na exportéri alebo na kolektore. V druhom prípade, IPFIX potrebuje odoslať typy sledovaných paketov a časové značky na kolektor. Metrika RTT je definovaná v [RFC2681].

K danej téme:

Spiatočné oneskorenie (round trip time, RTT) je čas potrebný k odoslaniu paketu zo zdroja, jeho prijatiu v celi, okamžitému odoslaniu naspäť k zdroju a jeho prijatiu v zdroji. Spiatočné oneskorenie (round trip-time, RTT) patrí medzi časové charakteristiky, ktoré je možné merať aj jedným meracím bodom. Čas uzavretej slučky je čas, ktorý uplynie medzi vyslaním paketu s požiadavkou v jednom mieste a prijatím príslušného paketu s odpoveďou (napr. TCP-SYN/SYN- ACK). Tento spôsob sa ale nepoužíva na odhad jednosmerného oneskorenia, pretože nie je možné zabezpečiť rovnakú cestu pre požiadavku aj odpoveď. Cesty môžu mať rôzne charakteristiky a slučka môže byť asymetrická.

15.7.2. Meranie jednosmerneho oneskorenia

Pasívne meranie jednosmerného oneskorenia požaduje zbieranie údajov na dvoch meracích miestach. Je potrebné rozpoznať pakety v druhom meracom bode na porovnanie udalostí pri príchode paketu z oboch bodov. To môže byť uskutočnené zachytením hlavičky paketu a častí paketu, ktoré môžu byť použité na rozoznanie paketu v ďalšom meracom bode. Na zredukovanie množstva meraných dát môže byť z hlavičky, alebo celého paketu (prípadne určitej časti) vytvorené jedinečné ID paketu (napríklad použitím CRC alebo hashovacej funkcie). Možnosť využitia prenášanej informácie je mimo oblasti IPFIX, ale môže byť vytvorená rôznymi rozšíreniami. Napriek tomu v niektorých variantoch môže byť dostatočné vytvoriť ID paketu len z hlavičky. Ak ID paketov musia byť unikátne len počas určitého časového intervalu, alebo je povolený určitý počet kolízií paketov je toto riešenie dostatočné. Ďalším problémom je exportovanie ID paketov. IPFIX exportuje informácie počas toku. Exportovanie ID paketov je možné vďaka predstaveniu nového informačného člena.

Na poskytnutie efektívnejšieho exportovania, môžeme exportovať informáciu paketov s ID toku v dátových záznamoch. ID toku potom môže byť spájané s možnosťami toku v dátových záznamoch. Takto je potrebné prenášať informáciu toku len raz. Informácia

paketu je vo vzťahu s oveľa menším tokom ID-čiek, bez potreby na prenos celého toku informácií pre každý paket [BoMa05]. Metrika jednosmerného oneskorenia je definovaná v [RFC2679]. Exportovanie celých paketov a častí paketov je usmerňované PSAMP pracovnou skupinou [PSAMP]. PSAMP používa IPFIX ako exportovací protokol.

K danej téme:

Jednosmerné oneskorenie (one-way delay) je čas, ktorý uplynie od odoslania paketu zo zdroja až po jeho prijatie v cieľi. Skladá sa z dvoch častí:

- času potrebného na prenesenie paketu cez fyzické médium, čo je funkcia prenosovej rýchlosti linky a
- času, ktorý predstavuje oneskorenie spôsobené radením do front, spracovaním v sieťových zariadeniach a preťažením liniek.

Pasívne (neintruzívne) merania – pri meraní sa negeneruje žiadna dodatočná prevádzka, na tieto účely sa využíva výhradne existujúca prevádzka. Tento druh meraní predstavuje určité výhody oproti aktívnym. Odpadá problém emulácie prevádzky s určitými charakteristickými vlastnosťami reálnej, vzhľadom na neexistenciu umelej prevádzky nemôže dôjsť k ovplyvneniu výsledkov merania. Na druhej strane, medzi nevýhody tohto prístupu patrí fakt, že ide o neriaditeľné merania. Ďalšou nevýhodou je nutnosť prenášania riadiacich dát inou cestou, aby ani tieto neovplyvňovali skutočný tok dát. Pri meraní časových charakteristík je navyše potrebné zabezpečiť synchronizáciu času jednotlivých meracích bodov.

15.7.3. Meranie jednosmernej straty

Pre účely merania parametrov kvality služieb sú vhodnejšie pasívne merania, pretože negenerujú dodatočnú prevádzku, ale využívajú existujúcu reálnu prevádzku. Využitie reálnej prevádzky na účely merania prináša niekoľko výhod. Prvky siete sú zaťažované len reálnou prevádzkou. Neexistuje možnosť ovplyvnenia výsledkov merania samotným meraním. Výsledky pasívnych meraní sú dobre interpretovateľné a využiteľné v praxi. Nemožno tiež identifikovať testovaciu prevádzku poskytovateľom a následne ju uprednostňovať za účelom dosiahnutia lepších výsledkov. Charakter pasívnych meraní prináša určité nevýhody ako napríklad nemá možnosť riadiť testovaciu prevádzku. Aby sa vylúčilo ovplyvnenie výsledkov priebehom merania nie je možné prenášať ani riadiace dáta. Táto skutočnosť výrazne komplikuje meranie časových charakteristík, napr. jednosmerného oneskorenia. Riešením je zabezpečiť synchronizáciu hodín v jednotlivých meracích bodoch mimo meranú sieť. Ďalším významným problémom je potreba identifikovať pakety v meracích bodoch.

15.7.4. Meranie kolísania oneskorenia (IPDV)

IP zmena oneskorenia je definovaná ako rozdiel hodnoty jednosmerného oneskorenia pri vybratých paketoch (RFC3393). Z tohto dôvodu táto metrika môže byť vypočítaná pri pasívnom meraní jednosmerného oneskorenia pre ďalšie pakety a potom vypočítame

rozdiel. Ako vstup algoritmu pre výpočet kolísania oneskorenia sa používa výstup z programu pre výpočet oneskorenia.

Po spustení sa začne vykonávať cyklus čítania riadku zo súboru. Po prečítaní riadku obsahujúceho časovú známku, identifikátor toku (FID) a oneskorenia (D), sa kontroluje existencia prvku podľa X s indexom FID (X [FID]). Ak existuje, tak sa vypočíta kolísanie oneskorenia ako rozdiel X [FID] ID a vypíše sa na výstup spolu s TS a FID. Potom sa uchová hodnota D do prvku X [FID]. Cyklus pokračuje kontrolou konca súboru a čítaním ďalšieho riadku. Ak neexistuje X [FID], tak sa do X [FID] uchová hodnota D a pokračuje sa v cykle.

15.7.5. Prenos metriky IPPM

IPFIX protokol môžeme použiť na prenos vstupov, nielen na výpočet metriky IPPM, ale aj na prenos samotnej metriky. Potrebujeme mať dostatočné informácie na to aby sme ju mohli zdefinovať.

15.7.6. Ďalšie využitie

IPFIX je všeobecný a vplyvný protokol. Poskytuje exportný mechanizmus, ktorý by mohol byť užitočný aj v iných aplikáciách. Okrem posielania základných informácií o toku sa môžu používať na posielanie zhromaždených údajov. Na to potrebujeme nové šablóny a základné zložky informácie. Kvôli činnosti v režime push je to aj na posielanie sieťou iniciovaných udalostí ako alarmy alebo iné hlásenia. Môže sa to využívať aj na výmenu informácií medzi uzlami siete k samostatne zlepšujúcej sa činnosti siete. Predsa len IPFIX bol vytvorený s ohľadom na preukázané požiadavky v (RFC3917). Preto vybavenie IPFIX má byť pomaly kontrolované proti požiadavkám nových aplikácií pred použitím na iné účely ako boli adresované v (RFC3917).

16. Prepojenie IPFIX na ostatné systémy a protokoly

16.1. IPFIX a AAA

AAA je definované ako protokol a architektúra autentizácie, autorizácie a účtovania na využívanie služieb (RFC2903). Protokol DIAMETER sa používa na AAA komunikáciu, na ktorú je potrebná služba sieťového prístupu. Architektúra AAA (RFC2903) poskytuje systém na rozšírenie AAA s podoprou ďalších služieb. DIAMETER zabezpečuje výmenu správ medzi AAA entitami, napr. medzi AAA klientmi a prístupovými zariadeniami a AAA servermi a medzi AAA servermi. Využíva sa aj na prenos účtovných záznamov. Účtovanie podľa typu použitia vyžaduje meranie dát siete. IPFIX používa protokol na export dát zo smerovačov, meranie snímačov a iných zariadení. Účtovanie môže byť realizované aj bez infraštruktúry AAA ako už bolo spomenuté v podkapitole 2.1. Účtovanie môžeme využiť priamo na pripojenie IPFIX zberacieho procesu, ktorý získava záznamy dát IPFIX a informácie o prenose zvuku. Ak je AAA infraštruktúra na mieste,

spolupráca medzi IPFIX a AAA má veľkú hodnotu. Záznamy dát IPFIX môžu byť vstupom pre AAA účtovanie a sú základom tvorby DIAMETER účtovných záznamov. Diameter je ďalším vývojovým stupňom protokolu RADIUS (Remote Authentication Dial In User Service). RADIUS sa stal rozšíreným prostriedkom na zabezpečenie autentifikácie v prostrediach voľného prístupu (dialup, wireless). Diameter je zovšeobecnený a rozšíriteľný protokol za účelom podpory autentifikácie, autorizácie a účtovania (AAA) v rôznych aplikáciách. Komunikácia prebieha v režime peer-to-peer. Riadenie sa vykonáva pomocou štrnástich príkazov, organizovaných ako sedem párových príkazov požiadavka/odpoveď. Zahrnutá je aj podpora potvrdzovania a oznamovania chýb. Preferovaným nosným protokolom je SCTP, ale je možné využiť aj TCP. Autentifikácia a kryptovanie zabezpečuje IPsec alebo TLS. Tento protokol bol navrhnutý s ohľadom na potrebu zvýšenia bezpečnosti (end-to-end security). Dáta sú prenášané vo forme párov atribút/hodnota. Každý pár pozostáva z osem bitovej hlavičky a priestoru pre dáta rôznych typov. Okrem veľkého množstva preddefinovaných typov, možno definovať ďalšie nové typy na reprezentáciu informácií o toku.

16.1.1. Spojenie AAA klienta

Jednou z možností spojenia IPFIX a AAA je nechať bežať AAA klienta na kolektore IPFIX. Tento klient môže generovať správy a posielat' ich AAA serveru. Zobrazenie informácií o toku cez používateľské ID môže byť ukončené v AAA servery použitím dát z procesu autentizácie. Správy môžu byť posielané účtovnej aplikácií alebo iným AAA serverom.

16.1.2. Spojenie cez ASM

Ďalšou možnosťou na priame spojenie IPFIX kolektora s AAA serverom je spojenie cez ASM. ASM bol navrhnutý na výskum pre IRTF AAA architektúru (AAARCH) v (RFC2903). Využíva sa ako rozhranie medzi AAA serverom a servisným prístrojom. V tomto prípade je IPFIX kolektor časťou ASM. ASM slúži aj ako rozhranie medzi IPFIX protokolom a vstupným rozhraním AAA servera. ASM prekladá prijaté IPFIX dáta do vhodného formátu pre AAA server. AAA server tak môže pridať informácie o používateľovi ID a generuje DIAMETER účtovný záznam. Tento účtovný záznam môže byť poslaný účtovnej aplikácii alebo iným AAA serverom.

16.2. IPFIX a RTFM

RTFM (Real-time Traffic Flow Measurement) pracovná skupina definuje architektúru na meranie toku (RFC2722). Táto časť porovnáva RTFM systém so systémom IPFIX.

16.2.1. Architektúra

RTFM sa skladá z merača, čítacieho zariadenia a riadiaceho programu, ktorý komunikuje cez SNMP. Riadiaci program nastavuje merač a čítacie zariadenie zbiera dáta z merača.

IPFIX architektúra (IPFIX-ARCH) popisuje merací, zberací a exportovací proces. Architektúra RTFM je veľmi podobná IPFIX architektúre. Jeden mohol vidieť merací proces ako časť merača a zberací proces ako časť čítacieho zariadenia. IPFIX hovorí o procesoch namiesto zariadení a tak objasňuje, že väčšina z týchto procesov sa viaže na to isté zariadenie. Napriek tomu, IPFIX práve neopisuje proces riadenia, pretože vzdialená konfigurácia je v tom čase mimo dosahu pracovnej skupiny.

16.2.2. Definícia toku

RTFM a IPFIX v oboch sa využíva tá istá definícia toku; tok je súbor paketov ktorý zdieľa spoločný súbor z hodnoty koncového bodu adresy. Tok je preto celkovo označovaný ako súbor hodnôt, spolu s vypršaním časového limitu. Tok je považovaný za konečný, keď žiadny z paketov nevykazuje činnosť. RTFM toky, hoci sú obojsmerné napr. RTFM meria zhodné pakety z B do A a A do B ako samostatné časti toku a udržiava 2 súbory toku a počítadla bitov, jedného z každej oblasti. IPFIX toky sú jednosmerné. Používatelia ktorý potrebujú obojsmerné toky musia mať zhodné obidva smery v post-processingu.

K danej téme:

Tok je definovaný ako množina IP paketov prechádzajúcich bodom siete za určitý časový interval. Všetky pakety patriace istému toku majú isté spoločné vlastnosti. Paket je definovaný ako patriaci k toku ak kompletne spĺňa všetky vlastnosti definované toku.

V kontexte IPFIX je tok definovaný nasledovne:

Tok je množina IP paketov, alebo zapuzdrených IP paketov prechádzajúcich pozorovacím bodom v sieti počas určitého časového intervalu. Všetky pakety patriace určitému toku majú množinu spoločných vlastností. Každá vlastnosť je definovaná ako výsledok aplikácie funkcie na hodnoty:

1. Jeden alebo viac polí hlavičky aktuálneho toku, napr. cieľová IP adresa, alebo pole v zapuzdrovacej hlavičke toku, napr. koncové body IP-in-IP tunelu alebo polia transportnej hlavičky (číslo cieľového toku), alebo polia aplikačnej hlavičky.
2. Jedna alebo viac vlastností vlastného toku, napr. dĺžka toku.
3. Jedna alebo viac vlastností vyplývajúcich zo spracovania toku, napr. (adresa ďalšieho toku a pod.)

Paket je definovaný ako náležiaci toku, ak kompletne spĺňa všetky definované vlastnosti toku. Každá z položiek (1, 2, 3) je nazývaná kľúč toku. Táto definícia zahŕňa toky obsahujúce všetky pakety pozorované na sieti, až po toky obsahujúce jediný paket.

16.2.3. Nastavenie a ovládanie

V RTFM, odstránenie nastavení (použitím SNMP MIB) je jediný spôsob ako nastaviť merač. IPFIX merací proces môže byť nastavený na mieste systémovým administrátorom. Skupina IPFIX práve neposiela odstránenie nastavení IPFIX. IPFIX merací proces posiela občas ich konfiguráciu, napr. usporiadanie dát bez ich šablón. Zberací proces IPFIX používa informácie zo šablóny, na vysvetlenie ako sa v IPFIX prijíma tok dát.

16.2.4. Súbor dát

Jedným z hlavných rozdielov medzi IPFIX a RTFM je že RTFM využíva typ pull zatiaľ čo IPFIX využíva typ push pre súbor dát. IPFIX exportovací proces je nastavený na prenos záznamov dát k stanovenému IPFIX zberaciemu procesu. Záznamy dát sú smerované k zberaciemu procesu. Podmienkou kedy poslať záznamy dát môže byť nastavenie v meracom alebo exportovacom procese. Na rozdiel od toho RTFM čítacie zariadenie načítava dáta z merača použitím SNMP. Bezpečnosť SNMP na merači určuje či čítacie zariadenie je schopné načítavať z neho dáta.

16.2.5. Podklady modelu dát

RTFM popisuje všetky jeho hodnoty v RTFM merači MIB (RFC2720). Základná zložka informácie IPFIX je popísaná v (IPFIX-INFO). RTFM používa 64 bitové počítadlá na uloženie paketov toku. Počítadlá sa nikdy nenulujú len v prípade že bol prekročený rozsah počítadla. Toky môžu byť načítavané kedykoľvek. Rozdiel medzi snímaním počítadiel dáva výslednú aktivitu v čase medzi snímaním. IPFIX povoľuje absolútne (totalcounter) a relatívne počítadlá (deltacounter). Totalcounter nie je nulovaný a blíži sa k 0 ak je hodnota veľmi veľká, presne ako počítadiel používaných v RTFM. Deltacounter je nulovaný, keď priradený záznam o toku je exportovaný.

16.2.6. Aplikačný / Transportný protokol

RTFM ma štandardné normy merania MIB (RFC2720), ktoré sa používajú na konfiguráciu meracieho prístroja a ukladanie výsledkov merania. MIB poskytuje druh čítania príznakových súborov so samostaným objektovým identifikátorom, ktorý výrazne znižuje prevádzkové náklady SNMP na zber tokov dát. SNMP, samozrejme používa UDP ako transportný protokol. Odvtedy čo RTFM požaduje spoľahlivý systém na transport tokov dát, RTFM merač, snímač musí byť prerušený a opätovne posíla nezodpovedané SNMP požiadavky. Vedľa jeho neobratnosti, môže obmedziť maximálnu prenosovú rýchlosť z merača k snímaču meraní.

IPFIX je navrhnutý na prerobenie množstva iných transportných protokolov. SCTP a SCTP-PR sú povinné. UDP a TCP sú voliteľné. Okrem toho, IPFIX protokol kóduje dáta efektívnejšie ako SNMP, preto IPFIX bude mať menší transport dát ako RTFM.

16.2.7. Súhrn RTFM

IPFIX poskytuje jednoduchý a výkonný protokol na exportovanie tokov dát v meracom procese. IPFIX poskytuje obojsmerné toky a výlučne len adresy dynamickej konfigurácie s veľmi flexibilnou definíciou toku. Môže byť vhodnejší v situáciách vo výskume, ktoré potrebujú tieto rysy. Hlavným rozdielom medzi oboma systémami je že RTFM pracuje v pull režime a IPFIX používa push režim na zber dát.

K danej téme:

Odporúčanie pre meranie dátových tokov v reálnom čase (Real Time Flow Measurement, RTFM) poskytuje všeobecný rámec pre opis a meranie toku prevádzky v sieti v reálnom čase. Architektúra princípov merania dátových tokov je znázornená na obrázku. Jednotlivé komponenty používajú ako komunikačný protokol jednoduchý protokol pre správu siete (Simple Network Management Protocol, SNMP). Samotná architektúra pozostáva z niekoľkých komponentov. Základom sú merače, odchyťávajú a počítajú prevádzku. Čítacie procesy na základe pravidiel čítajú hodnoty a preposielajú do analyzujúcej aplikácie. Pravidlá pre výber hodnôt sú uložené v manažéri pravidiel, kde je možné definovať nové pravidlá pre meranie dátových tokov.

16.3. IPFIX a IPPM

IPFIX protokol môže byť využívaný na ochranu IPPM sieťovej metriky alebo informácie ktorú môže využiť na výpočet týchto metrik (viď. v kapitole 15.7.).

K danej téme:

IPPM predstavuje všeobecný rámec pre definíciu a vývoj nových metrik pre meranie výkonnosti internetového protokolu (IP). Definuje kritériá pre vývoj nových metrik a terminológiu pre ich opis. Vývojom IPPM sa zaoberá pracovná skupina organizácie IETF (Internet Engineering Task Force) s názvom IPPM-WG (Internet Protocol Performance Metric Working Group). Pod pojmom metrika sa rozumie veličina vzťahujúca sa k výkonnosti a spoľahlivosti internetu. Hlavným cieľom definovania metrik výkonnosti internetového protokolu je poskytnúť používateľom a poskytovateľom služieb dostatočne výstižnú a pritom všeobecnú charakteristiku výkonnosti a spoľahlivosti komponentov Internetu (sietí, podsietí, smerovačov, atď.). Pre dosiahnutie tohoto cieľa je potrebné metriky definovať.

16.4. IPFIX a PSAMP

PSAMP skupina definuje metódu výberu paketov a ohlasovanie informácie paketu. Taktiež opisuje konfiguráciu výberových metód paketov. Hlavným rozdielom medzi IPFIX a PSAMP je že doba predošlých adries exportuje záznamy o toku, novšie adresy exportujú záznamy paketov. PSAMP skupina je rozhodnutá používať IPFIX ako jeho transportný protokol pre paketové informácie. Pracovná skupina opisuje súbor požiadaviek v (PSAMP-FM), ktorý má priamy vplyv na transportný protokol. V (PSAMP-PROTOCOL), požiadavky sú analyzované s ohľadom na IPFIX. Záverom je že IPFIX je hlavný exportný protokol vhodný pre PSAMP export. Ak je potrebný, informačný model môže byť ľahšie rozšírený. PSAMP definuje PSAMP MIB na konfigurovanie procesu výberu paketov. Môžeme uvažovať o rozšírení tohto MIB na umožnenie konfigurácie v IPFIX procesoch.

K danej téme:

Architektúra vzorkovania PSAMP (packet sampling) sa skladá z viacerých navzájom prepojených procesov. Ku každému z týchto procesov môžeme priradiť jednoznačné vstupy a výstupy. Každý proces si načítava konfiguráciu z vopred pripraveného konfiguračného súboru.

Tok paketov je odchyťovaný v pozorovacom bode. Proces selekcie skúma každý paket či má byť vybraný. Oznamovací proces zostavuje správu o každom pakete s využitím obsahu paketu a iných informácií týkajúcich sa paketu ako napr. časová známka, výstupné rozhranie. Exportovací proces posielá správy kolektoru spolu s informáciou potrebnou na ich interpretáciu. Kompozícia procesu selekcie a oznamovacieho procesu je známa ako merací proces. Merací proces architektúry IPFIX obsahuje zachytávanie hlavičiek paketov ako prvý krok. Táto funkcia môže byť poskytnutá implementáciou PSAMP architektúry dvoma odlišnými spôsobmi. Merací proces IPFIX-u môže slúžiť ako proces kolektora v architektúre PSAMP. Potom informácia o pakete vzorkovaného pomocou PSAMP komponentu môže byť poslaná z PSAMP exportovacieho procesu do IPFIX meracieho procesu použitím PSAMP protokolu. Alternatívne, bez použitia štandardizovaného protokolu alebo API, proces selekcie a proces vzorkovania architektúry PSAMP môžu poskytovať priamo informáciu o pakete meraciemu procesu IPFIX. V oboch prípadoch, PSAMP komponent bude prevádzať zachytávanie hlavičky paketu, priradenie časovej známky a vzorkovací proces pre IPFIX merací proces.

16.5. IPFIX a RMON

RMON (RFC3577) je všeobecne používaný monitorovací systém ktorý zahŕňa prepravu dát od RMON agentov v sieťových zariadeniach a využíva SNMP. RMON MIB sa delí na časti, každá časť zabezpečuje inú monitorovaciu činnosť. RMON nepokrýva meranie toku úplne. To znamená, že jeden potrebuje rozšíriť RMON pridaním MIB modulu na udržanie tokov. Ďalej je potrebné vymyslieť schému na export väčšej časti tokov dát. V skratke, IPFIX je na zabezpečenie efektívnejšieho exportu toku; RMON nie je.

16.6. IPFIX a IDMEF

IDMEF je štandardný dátový formát vyvinutý vnútri IDWG pracovnej skupiny na výmenu dátových výstrah medzi automatizovaným IDS. IDMEF poskytuje štandardné zobrazenie poplášnej informácie, ktorú ohlásí analyzér detekcie vniknutia, keď je objavený podozrivý jav. Tieto poplachy môžu byť jednoducho alebo komplexne závislé na schopnostiach analyzérov, komerčných obchodných cieľoch, a prostredia detekcie vniknutia. IDMEF správy sú implementované v XML a založené na základe schémy a module rozšírenia na určenie porúch ktoré sú komplexnejšie. Druhy poplachov, ktoré boli poslané boli určené analyzérom, musia byť formátované nasledujúcimi IDMEF pravidlami. Väčšinou, poplachy sú poslané, keď analyzéry lokalizujú jav, ktorý má byť konfigurovaný na hľadanie. IPFIX protokol sa môže používať na určenie vstupu pre systémy intrúzie vniknutia, ale tiež komplementárny k IDMEF pri poskytovaní

podrobných informácií vniknutia dopravy, podozrivých javov alebo neobvyklej dopravy, ktorá sa líši od bežného správania siete.

K danej téme:

Intrusion Detection System (skrátene IDS) je technika odhaľovania neoprávnenej, nesprávnej alebo nezvyklej aktivity počítačového systému alebo siete. Systémy detekcie prienikov, môžu byť implementované ako senzory, ktoré neustále sledujú celú komunikáciu v počítačovej sieti a porovnávajú údaje prenášané v jednotlivých spojeniach s databázou známych sieťových útokov. V tomto prípade hovoríme o tzv. network based IDS. Ďalšiu skupinu tvoria systémy, ktoré detekujú útoky priamo na sledovanom hostiteľovi (host based IDS). IDS často nedetekujú iba známe útoky, ale snažia sa zachytiť aj takzvané "pre-attack probes", čo sú typické akcie útočníka pred zahájením vlastného útoku. Na základe získaných informácií, môžu systémy detekcie vniknutia poskytovať informácie administrátorovi, v reálnom čase prekonfigurovať systém a tak zamedziť potenciálnemu prieniku, prípadne sledovať a kontrolovať ďalšie akcie útočníka a aktívne obmedzovať ich deštruktívne dôsledky. Kombináciou uvedených prístupov je takzvané hybridné IDS.

17. Nedostatky (limitations)

Cieľom tejto kapitoly je odporúčanie ktoré nebolo použité v dokumente IPFIX. Lebo protokol je dostačujúci na prenos záznamov o toku vo viacerých aplikáciách, ale stále má svoje nedostatky.

17.1. Použitie iného protokolu prenosu ako SCTP

SCTP je preferovaným protokolom pre IPFIX, napr. vyhovujúca implementácia musí pracovať pomocou SCTP. Hoci IPFIX môže pracovať pomocou TCP alebo UDP, používatelia majú dôvody na využívanie protokolov iných ako SCTP.

17.2. Push a pull režim

IPFIX pracuje v režime push. To znamená, že záznam dát je automaticky posielený bez čakania na požiadavku. Zodpovedný za prenos dát je exportný proces. Kritériá prenosu sú dôležitou súčasťou exportného procesu. Vo všeobecnosti existujú dva spôsoby exportu údajov: push a pull. Pri prvom spôsobe exportný proces po odštartovaní autonómne posiela záznamy tokov podľa nastavených kritérií bez potreby nejakého impulzu zvonku. Toto je základný spôsob, ktorý definuje štandard IPFIX. Naproti tomu pri pull spôsobe sú záznamy exportované na vyžiadanie – exportný proces teda čaká na externý pokyn zvyčajne od zberacieho procesu, na základe ktorého dôjde k exportu nazhromaždených záznamov. Pri push spôsobe exportný proces musí byť schopný exportovať záznamy v pravidelných nastaviteľných intervaloch. Merací proces môže počas komunikácie posielat upozornenia zberaciemu procesu, v prípade, že nastane nejaká špecifická

udalosť (napr. vytvorenie nového toku, čo zodpovedá príchodu prvého paketu daného toku, alebo expirácia toku po vypršaní časového limitu).

17.3. ID šablóny

Každá šablóna dostáva pri vytvorení jedinečný identifikátor. Jedinečnosť je vyžadovaná iba v rámci jednej meracej oblasti. Identifikátor šablóny pre dáta môže nadobúdať hodnoty od 256 do 65535. Šablóna je usporiadaná n-tica, používaná na kompletnú identifikáciu štruktúry a sémantiky určitej informácie, ktorá má byť sprostredkovaná z IPFIX zariadenia do zberača. Každá šablóna je identifikovateľná unikátne.

17.4. IPFIX a IPv6

Máme 2 otázky nad ktorými môžeme uvažovať:

- Vytváranie a ohlasovanie dátových záznamov v prevádzke IPv6
- Exportovanie dátových záznamov cez IPv6

Vytváranie a ohlasovanie dátových záznamov v prevádzke IPv6 je možné ak existuje vhodná základná zložka informácie (IPFIX-PROTO). Exportovanie dátových záznamov cez IPv6 nie je výlučne adresované v (IPFIX-PROTO). Aj tak, potom IPFIX beží cez SCTP, SCTP-PR, UDP alebo TCP, je zanedbateľné, že IPFIX beží cez IPv6 sieť, za predpokladu že na prevádzku sa použil transportný protokol IPFIX, ktorý beží na sieti IPv6.

18. Bezpečnostné hľadisko

Tento dokument opisuje využívanie IPFIX z rôznych pohľadov. Bezpečnostné požiadavky pre cieľové aplikácie IPFIX a bezpečnostné hľadisko sú adresované v (RFC3917) a v (IPFIX-PROTO). Tieto požiadavky považujeme za smernicu IPFIX protokolu. Rozšírenia IPFIX navrhnuté v tomto dokumente nespôsobujú bezpečnostné riziká. Kapitola 16 v tomto dokumente opisuje ako sa môže využívať IPFIX v kombinácii s inými systémami. Nové bezpečnostné riziká môžu vzniknúť keď 2 samostatné bezpečné systémy sa skombinujú. Kombináciou AAA s IPFIX, aplikačný špecifický modul (ASM), alebo IPFIX kolektor môžu fungovať ako tranzitný bod pre správy. Musí byť zaistené, že v tomto bode aplikovaný bezpečnostný mechanizmus pokračuje.