Testujte síťové prostředí pořádně, jinak vám vyjdou nesmysly (CSNOG 2024)

V úterý 23. ledna proběhl první den setkání CSNOG, které je zaměřeno na provozovatele internetových sítí. Mluvilo se především o budování anycastových sítí, současných bezpečnostních hrozbách a měření výkonu.

Thomas Weible, Gerhard Stein: Současnost a budoucnost koherentních optických transceiverů

Když zvyšujete frekvenci světla a s tím i šířku pásma, je stále těžší signál detekovat. Dochází například k chromatické disperzi a kabely musejí být čím dál kratší. Světlo má ale další vlastnosti, máme tedy více možností detekce. Kromě amplitudy je tu také fáze a polarizace. Můžeme používat různou polarizaci světla a koherentní transcievery jsou schopny přenášet signál v prostorovém uspořádání. Ve skutečnosti se tu kombinuje amplituda a fáze a dochází k rozložení signálu například do šestnácti kvadrantů v modulaci 16QAM, kdy fázová komponenta značí reálnou složku a amplituda pak imaginární složku.

Bylo představeno konkrétní řešení v peeringovém centru DE-CIX, kde byly použity transceivery Flexoptix nasazené v přepínači značky Nokia. Výhodou koherentních transceiverů je, že mají laditelnou frekvenci laseru. Mají také standardní diagnostické rozhraní, které dovoluje zjišťovat vstupní napětí, kvalitu signálu či teplotu. Teplota je zásadní, neměli byste transeivery přehřívat a musíte monitorovat. Každý transceiver potřebuje až 20 wattů a když jich v prvku je třeba 32, vzniká velký zdroj tepla jen na samotných modulech.

Pro odhalení a kompenzaci chyb v přenosu se posílají takzvané pilotní signály, které jsou vždy v rozích diagramu. Používáme QPSK pro ověření a opravu signálu, takže dokážeme kompenzovat různé posuny vznikající při přenosu.

Při praktickém nasazení je potřeba hlídat kompatibilitu, tedy jaké transceivery podporuje operační systém v daném prvku. Musíte opravdu dobře hlídat specifikace, abyste si byli jisti, že všechno bude společně fungovat. Dnes už se běžně používají 400G transceivery, svět postupně míří k 800G a později pak k 1,6T.

Robert Šefr: Co DNS4EU přinese uživatelům i poskytovatelům internetu?

DNS4EU se zaměřuje na dostupnost překladu dotazů do DNS, ale také na blokaci odpovědí znamenajících hrozbu pro uživatele. Nejste schopni tím zastavit všechny útoky, ale zhruba 94 % jich na úrovni DNS zastavit umíme. V případě phishingové kampaně je

možné na resolveru zablokovat přístup k závadnému webu kradoucímu uživatelská data.

DNS4EU byl iniciován Evropskou komisí a cílem je nabídnout překladače v Evropě a zároveň nabídnout bezpečnost. Je to v souladu se strategií evropské soběstačnosti, abychom měli v případě problémů možnost využívat místní resolvery. Zároveň se v Evropě řeší jiné bezpečnostní problémy než v Americe nebo Asii, proto je dobré ochranu cílit na naše evropské problémy.

Na projektu se podílí konsorcium organizací jako CZ.NIC, ČVUT a další. Jedním z výstupů projektu bude i překladač DNS dostupný pro veřejnost, ale další součástí je i dostupnost překladu pro telekomunikační operátory a státní organizace. Vždy bude na uživateli, který druh překladu bude používat. Jestli chce čistý překlad nebo chce i blokaci některých služeb. Nikdo nikomu nic nenutí. Důležitou součástí projektu je anonymizace, kdy se nesbírají data o uživatelích.

Schopnost překládat DNS a blokovat problematický provoz je pro stát zajímavá, protože může nabídnout vlastním organizacím přístup k ochranným prostředkům. Je velmi snadné pak zapojit i úplně malé organizace, třeba malý městský úřad, který nemá prostředky na komplexní bezpečnostní ochranu. V DNS resolveru se mohou scházet různé informace a snižovat významně riziko třeba phishingových útoků v různých sítích.

Centrální součástí DNS4EU je Knot Resolver, který je vyvíjen v CZ.NIC. Ten zatím nepodporuje ochranu proti DDoS útokům, ale je v plánu ji doplnit. Resolver pak může chránit zbytek internetu proti různým zesilujícím útokům, ale také omezit provoz

k autoritativním serverům. Měl by ale chránit i sebe sama, kdy bude fungovat i pod velmi velkou zátěží a dokáže obsloužit ty nejdůležitější dotazy.

Už dnes běží infrastruktura, která se stará o synchronizaci resolverů, monitoring, hlášení, upozornění na problémy a distribuci dat o hrozbách. Rozšiřujeme podporu backendu pro Knot Resolver 6.x a chceme zlepšit výkon, abychom unesli velké množství provozu.

S provozem souvisí také právnické a etické otázky, například v případě zacházení s daty. Veřejná část bude plně anonymizovaná data, jakmile se něco ukládá, už na úrovni resolverů se vše anonymizuje. Pokud bude resolver používat telekomunikační společnost, je tato společnost správcem údajů a rozhoduje o tom, jak bude s údaji zpracovávat. V případě použití vládou je situace opačná, tam jsou potřeba data, aby bylo možné odhalit například phishingové útoky. Tam se sbírají všechna data. Tento režim ale není určen pro koncové uživatele.

Přístup ke zdrojovým datům lze poskytnout na základě shody celého konsorcia a po splnění přísných podmínek. Něco takového budeme podporovat jen v případě, že to bude mít přínos pro státy Evropské unie, ať už bezpečnostní nebo infrastrukturní. V rámci unie se také sdílejí informace o jednotlivých útocích, aby bylo možné reagovat co nejrychleji na nové útoky. Hlavní platformou pro výměnu dat je platforma MISP, na kterou je zvyklá většina bezpečnostních týmů.

Filip Hron: Útoky na privátní sítě v roce 2023 z pohledu sítě Turris Sentinel

Turris Sentinel je soubor komponent sbírajících data o útocích. Jedna část data sbírá a klientská část pak aplikuje ochranu. Ochrana pak probíhá v reálném čase pomocí dynamického firewallu. Zdrojem dat jsou takzvané minipoty, na které se útočníci pokoušejí přistupovat pomocí protokolů FTP, SMTP, telnet a HTTP. Data jsou kategorizována a zobrazována na webu Sentinel View, kde je k dispozici náhled dynamického firewallu, ale také kontrola hesel proti heslům používaným útočníky.

Mezi nejpoužívanější hesla útočníků patří číselné řady od jedničky, upravené varianty slova Password a sekvence kláves jako QWERTY. Útočníci se liší také metodikou zkoušení hesel, někteří například zkoušejí jedno heslo denně, další den zkoušejí jiné. Nejvíce unikátních útočníků je z Číny, následuje Indie, Spojené státy a Brazílie. Nechceme na nikoho ukazovat prstem, tohle jsou země, ze kterých pocházejí útočící IP adresy.

Dmitry Belyavskiy: Postkvantový přechod: problémy pro populární protokoly

Odborná veřejnost se shoduje na tom, že kvantové počítače prolomí tradiční kryptografii. Znamená to, že dříve zaznamenaná šifrovaná komunikace může být dešifrována, takže celý svět pracuje na řešení postkvantových algoritmů. Algoritmy navrhuje například americký NIST, pracovní skupiny v rámci IETF pracují na standardizaci protokolů a existují také specializované skupiny v rámci OASIS.

Předpokládá se, že klasická kryptografie bude prolomena, ale nová schémata nejsou ještě prověřená a nikdo si vlastně není ničím příliš jistý. Nejčastěji se dnes používají takzvaná hybridní řešení, která kombinují tradiční přístupy s novými úpravami, které by měly být odolné.

Nové algoritmy přinášejí samozřejmě řadu očekávaných problémů s kompatibilitou. Například různé middleboxy nerozeznávají nové algoritmy a proto je jako neznámé blokují. Zvyšuje se také velikost šifrovacích klíčů a mají nižší výkon, takže musíte být připraveni na potřebné změny.

Dalším problémem je zhoršení problému zesílení (amplifikace), protože větší klíče vytvářejí několikanásobně větší odpovědi, které mohou být v některých sítích blokovány. Bude potřeba také prozkoumat algoritmy řešící zahlcení linky (congestion) v TCP, kdy historicky roste MSS na hodnotu okolo 10, ale kvůli navýšení round-tripů by bylo zajímavé prozkoumat vyšší hodnoty. CDN dnes nabízejí vyšší MSS, stejně tak QUIC má vlastní implementaci, kterou bude třeba znovu prověřit.

Další problémy se objeví v jednotlivých protokolech, například v případě DNSSEC se nám delší podpisy nevejdou do jednoho paketu. Navrhuje se rozdělit data na aplikační úrovni, ale potřebujeme kolem toho udělat další výzkum. Současné linuxové distribuce už nabízejí některé postkvantové algoritmy, zmíněna byla konkrétně Fedora 39.

Jan Žorž: Cesta k anycastu

Unicast znamená jeden na jednoho, anycast znamená jeden na nejbližšího. Jak postavit vlastní anycastovou síť? Plán byl postavit prototyp, měřit, udělat úpravy, postavit produkční verzi a je hotovo. Nestavěli jsme anycast, protože bychom ho potřebovali. Prostě jsme to chtěli a byli jsme zvědaví.

Byly použity různé resolvery: BIND, KnotDNS, NSD a PowerDNS. Pro BGP routing byl nasazen BIRD a pro rozkládání zátěže balancer dnsdist. Pro překlad konfigurace pro různé servery jsme si napsali vlastní skript v Pythonu. Na jednotlivých nodech je jednoduchý skript v bashi, který se ptá místního resolveru a při problému shodí BIRD. Když nefunguje resolving, neměl by být uzel vidět v BGP. Použito je jedno ASN, ze kterého se oznamují tři IPv4 prefixy /24 a tři IPv6 prefixy /48.

Na začátku celé řešení nefungovalo tak, jak se předpokládalo. Ale nevěděli jsme proč, kdy a odkud to nefunguje správně. Využita byla síť RIPE Atlas, která umožňuje pomocí tisíce sond oslovovat cíle a měřit výsledky. Každé auto potřebuje tachometr, takže podrobně monitorujeme a sledujeme každý uzel a jeho výkon.

Anycast ale znamená nové problémy, například získat certifikát od Let's Encrypt je problém. Není možné zajistit, aby komunikace od autority končila v uzlu, který ji vyvolal. Musíme tedy proxovat konfiguraci ze všech uzlů na ten jeden, kde běží Certbot.

Pomocí anycastu je možné provozovat další služby, nejen DNS. Zmíněna byla možnost například takto distribuovaně provozovat SMTP server, replikovanou databázi nebo replikované úložiště elektronické pošty. Stále s tím experimentujeme v laboratoři, když máme čas.

Tomáš Hála: Novinky na DNS anycastu pro národní doménu .CZ

DNS anycast sdružení CZ.NIC je dnes ve 20 lokalitách ve 13 zemích. Pokrýváme všechny kontinenty kromě Antarktidy. Slouží primárně pro provoz národní domény, ale k dispozici je i hosting pro jiné TLD nebo nově i domény druhého řádu v .CZ.

Anycast byl stavěn s ohledem na dostupnost a robustnost, aby odolal různým síťovým problémům. Musí být odolný vůči útokům a různým chybám, které mohou nastat. Celá služba běží v současnosti na 75 serverech.

V předchozím roce došlo k posílení hardware ve Frankfurtu, který je velmi významnou lokalitou. Naopak v Milánu jsme optimalizovali směrem dolů. Postaven byl také druhý velký DNS stack a místo 30 serverů s 10GE bylo použito jen 10 serverů s konektivitou 25GE. Začali jsme používat XDP, což nám umožňuje lépe využít hardware a s menším počet serverů dosáhnout vyšší propustnosti.

XDP umožňuje obsloužit mnohonásobně více dotazů, ale dělá problémy při snaze o softwarovou diverzitu. Problém je, že kromě našeho KnotDNS žádný jiný server tento režim nepodporuje.

Správci provádějí neustále výkonnostní testování celého stacku, aby si byli jisti, že vše funguje podle očekávání. Sledujeme také, ze kterých zemí máme kolik provozu a jaká máme zpoždění. Cílem je dostat se na odezvu pod 75 ms, zejména v nejexponovanějších lokalitách. Máme třikrát více dotazů z Ameriky než z Česka, což je pochopitelné kvůli největším resolverům. Ty provozují firmy Google, Cloudflare a Microsoft.

V plánu je přidat novou lokalitu ve Spojených státech, přidat další evropskou lokalitu a nový velký DNS stack v neveřejné lokalitě. Brzy bychom se také chtěli připojit do NIX.CZ pomocí 400GE, ale znamená to také posílit velký stack, aby byl schopen odbavit takový provoz.

Alexander Zubkov: Simulace sítě pro testování

Qrator Labs provozuje službu na ochranu proti DDoS útokům, celá síť je postavena na Linuxu, včetně samotných uzlů, ale třeba i síťových prvků. Všechno máme automatizované a formálně popsané pomocí automatizačních nástrojů. To umožňuje provádět komplexní testování novinek před nasazením.

Je možné testovat samozřejmě na jednom zařízení, ale není tím možné ověřit, jak uzly komunikují mezi sebou nebo jak například propagují prefixy. Mohli bychom vytvořit skutečnou síť, ale to příliš neškáluje a je s tím hodně práce. Je také možné vytvořit virtuální simulaci celé sítě, kde je možné vytvořit řadu uzlů a dívat se, co se tam děje. Čím ale tuhle simulaci dělat a jak ji nastavit?

Jako řešení bylo nakonec zvoleno Conteinerlab, které využívá Docker a má připravené obrazy s různými operačními systémy. Konfigurace je v YAML a umožňuje jednoduše spustit a spravovat velkou virtuální infrastrukturu. Nástroj spustí sadu kontejnerů a mezi nimi vytvoří požadovaná síťová rozhraní. Pro generování konfigurace virtualizovaných uzlů je pak možné použít stejné šablony, jaké se nasazují na produkci.

Přístup IaaC (Infrastructure as a Code) je dobrá věc a umožňuje spoustu věcí zjednodušit a automatizovaně testovat. Vyžaduje to ale nějaké programátorské schopnosti a je to hodně práce, ale je to užitečné. Je vhodné také přidávat testy průběžně, jak se přidávají nové funkce. Když pak budete chtít testovat, nebudete muset všechny testy napsat najednou.

Marian Rychtecký: Monitoring a statistiky v NIX.CZ

Technici v NIX.CZ postupně dospěli k tomu, že nechtějí konfigurovat síťové prvky pomocí příkazové řádky. Chceme mít možnost pracovat s příkazovou řádkou po SSH, ale nechceme to používat pro automatickou konfiguraci. Proto bylo rozhodnuto používat REST API nazvané DME API, které je velmi rychlé a dovoluje reagovat na příkazy v řádu milisekund.

Bylo ovšem potřeba vytvořit poměrně komplexní překladovou vrstvu, která umožňuje tradiční příkazy převést do formátu JSON. Nexus má vlastní překladač, ale bohužel ne na všechny. Dokumentace existuje, ale není v ideálním stavu. Museli jsme na spoustu věcí přijít sami, ale troufám si říct, že 98 procent máme zvládnutých.

Pro komunikaci se síťovými prvky byla vyvinuta knihovna v Pythonu, která komunikuje s DME API a načítá údaje z Netboxu. Poté se vše zkombinuje a informace se uloží do InfluxDB. Tam si je čteme a používáme je k zobrazení údajů ve svých systémech. Toto vše probíhá každých 30 sekund. Bylo by možné informace číst i každou sekundu, ale zatím v tom nevidíme žádný benefit.

Dohromady se takto čtou informace z 37 zařízení a 2339 síťových rozhraní, což vytváří 63080 metrik každých 30 sekund. Všechny informace čteme 700 milisekund a dalších 250 milisekund je ukládáme. Zatím jde jen o počítadla, ale v plánu je rozšířit data o další informace.

Už teď databáze naroste každý měsíc o 4 GB, ale nedává smysl data takto udržovat donekonečna. Využíváme vlastností moderních databází, které umožňují data agregovat. Vytváří se tak denní, týdenní, měsíční a roční statistiky. Tím se sníží velikost každé sady na desítky megabajtů.

Výhodou takto podrobného sběru dat jsou detailnější data o tocích na jednotlivých rozhraních. Dříve jsme sledovali jen průměrný tok, ale mě jako síťaře při návrhu sítě zajímá, kolik dat tam skutečně proteče. Je totiž potřeba přenést všechna data, nejen průměr. V těchto třicetisekundových datech vidíme, že na portech přenášíme výrazně více dat než je průměr.

Zbyněk Kocur: iPerf3 aneb Měřit pouze maximální propustnost je nesmysl

iPerf je k dispozici ve dvou verzích, které se vyvíjejí paralelně vedle sebe: iPerf2 a iPerf3. Pokrytí operačních systémů je velmi široké, ale není stejnoměrné. Ne v každém systému funguje všechno a ne všechno funguje tak, jak by si uživatel představoval. Měření běží v režimu klient-server, kdy klient posílá provoz na server a zobrazuje naměřená data.

Hlavním rozdílem mezi druhou a třetí verzí je rozdílný formát výstupu. Zatímco jednička data vypisuje v CSV, trojka používá JSON. Starší verze také musí mít na obou stranách nastavené stejné parametry, trojka už si přenese informace o měření po síti. U dvojky

bylo možné získat data jen z klientské strany, trojka umožňuje stáhnout log i ze serveru a získat tím více dat.

iPerf3 je konstruován jako měřák, který je schopen vytížit nejmodernější přenosové technologie. Pokud jej vhodně nastavíte, můžete jej použít od jednotek megabitů až po stovky gigabitů. Je ale nutné nakonfigurovat nejen nástroj samotný, ale také operační systém pod ním.

Výsledná přenosová rychlost je závislá na propustnosti linky, době zpoždění a chybovosti. U linek s velkým zpožděním, například 600 ms u stacionárních družic, je potřeba mít nastavené TCP okno na desítky megabajtů, abychom dokázali dosáhnout rozumně velkých toků v řádu desítek megabitů. Stačí přidat chybovost jen 0,25 % a datový tok se na lince s takovým zpožděním propadne na zlomek rychlosti.

Spousta měřáků má dnes zabudované měření podle RFC 6349, které popisuje, jak by se mělo při měření TCP postupovat. Žádný konkrétní návod tam ale není. Dokument je navíc z roku 2011 a řada doporučení dnes kvůli novým algoritmům zahlcení už neplatí. Naznačuje například, že TCP má smysl měřit do ztrátovosti 5 %, ale viděli jste, že už malá ztrátovost ovlivňuje provoz. Svět protokolů se ale vyvíjí tak rychle, že se nikdo nemá k aktualizaci metodik.

Petr Špaček: Smysluplné měření kapacity DNS serverů

Problém jednoduchého měření je, že měříme v neznámém prostředí, konkrétně nastavený server, který nám vrací nějaké odpovědi. Co když ale server ve všech případech odpověděl chybou a nedával smysluplné odpovědi? Už se nám to stalo.

Pokud měříme DNS, musíme rozlišovat mezi autoritativním serverem a resolverem. Jsou to úplně jiné kusy software, které jen mluví stejným jazykem. Představte si, že jedno je kráva a druhé je kůň. Jsou to dva úplně různé živočišné druhy, které mají velmi málo společného. Oba žerou trávu, takže vstup je stejný. Ale tím podobnost končí.

Pokud například měříme resolver, musíme počítat s tím, že se jeho stav mění v čase. Keš má totiž omezenou platnost, takže jak běží čas, mění se její obsah. To je noční můra. Při měření tedy musíme počítat také s časováním posílání jednotlivých dotazů.

Problémem jsou také data, která budeme k testu používat. Dotazy totiž mají různou cenu a například dobu zpracování. Je tedy nutné mít vzorek reálného provozu a ne jen posílat stejné dotazy dokola. U resolverů navíc musíme mít reálná data včetně reálného časování. Pokud jde například o webový provoz, musíme počítat s tím, že i prohlížeče mají svou keš.

Samostatnou kapitolou jsou pak DDoS útoky, které si obvykle vybírají nejdražší dotazy a může dojít k nějakému problému uvnitř serveru a výkon se propadne. Další problém je správa serveru, která probíhá během provozu. Zahrňte takovou akci taky, protože v laboratoři to může vypadat dobře, ale jakmile v produkci správce přidá zónu, může se server zpomalit.

Existuje celá řada nástrojů pro měření: dnsperf, kxdpgun, resperf, shotgun a další. Pozor ale na to, že ne všechny se hodí ke všem testům. Někdy je také v dokumentaci píše něco, co ve skutečnosti moc nefunguje.

Výhodou nástroje dnsperf je, že je snadno použitelný, ale není příliš výkonný. Nehodí se proto k měření útoků, ale dává průběžné výsledky a je dobrý v měření latence. Naopak kxdpgun je extrémně výkonný a hodí se k měření útoků. Osvědčilo se mi kombinovat obě věci, běžný provoz simulovat pomocí dnsperf a zároveň valit útok s kxdpgun.

Důležité je ověřit si vlastní měření, například vyhodit skutečný server a nahradit ho nějakým odpovídačem jako dumdumd, což je jednoduchý opakovač paketů. Je to velmi jednoduché, nepřidává to žádné zpoždění zpracováním. Je tím možné objevit problémy v rovnoměrném zatížení procesoru nebo nevhodném měřicím nástroji.

Výkonnostní testy nedávají smysl bez otestování samotného testovacího prostředí. Nejspíš vám bez toho vyjdou nesmysly.

Kryštof Šádek: Výkonnostní testy 400G DNS stacku

DNS stack je skupina nezávislých serverů, které mají stejnou komunikaci. Nekomunikují spolu, ale jsou zapojeny v jednom síťovém prostředí. Odpovídají stejným způsobem a rozložení zátěže mezi nimi je zajištěno pomocí BGP multipath.

CZ.NIC postavil nový DNS stack s konektivitou 400 GE, v praxi do něj ale proudí běžný provoz o velikosti 14 Mbit/s. Museli jsme tedy vytvořit testovací provoz, abychom ověřili přesnost výpočtu teoretické kapacity.

Interní kapacita sítě ani produkčních serverů neumožňovala vytvořit dostatečný provoz. Měli jsme ale připravený hardware pro stavbu dalšího stacku, takže jsme se rozhodli jej použít. Nakonec ale nebyly testovány všechny servery, ale zapojeny byly jen tři. Provoz generovalo deset serverů.

Při testování byl simulován skutečný provoz, který zahrnuje dotazy do zóny .CZ, podíl NXDOMAIN vůči NERROR asi 8 % a podíl IPv4 vůči IPv6 o velikosti 66 %. K testování byl použit nástroj xkdpgun.

Bez DNSSEC dokáže stack odbavit 240 milionů dotazů za sekundu. Pokud se ptáme naopak jen na záznamy pro DNSSEC, klesne výkon na 127 milionů dotazů. Při reálných 20 % dotazů na DNSSEC se dostaneme přibližně na 210 milionů dotazů každou sekundu. Spoustu jsme toho neotestovali a je určitě velký prostor pro další testování.

Oto Šťáva: Novinky v Knot Resolver 6.x

Knot Resolver je open-source DNS resolver, je modulární, má rychlé tenké jádro a umožňuje přidávat moduly psané v C a Lua. Resolver je jednovláknový a využívá služeb operačního systému ke škálování na více jader. Tento přístup ale znesnadňuje agregaci statistik a metrik. Správa procesů je postavena na systemd, který ale není dostupný ve všech prostředích.

Modularita sice umožňuje oddělit pokročilou funkcionalitu, která není zbytečnou zátěží v běžném provozu. Před použitím ale je nutné moduly explicitně načíst v Lua.

Konfigurace napsaná v jazyce Lua je sice velmi mocná, ale pro potřeby většiny uživatelů je těžko uchopitelná. Některé chyby se také mohou objevit až po nějaké době, kdy už resolver běží.

Verze 6 se snaží tyto problémy řešit a už je dostupná k veřejnému testování. Pro správu procesů vznikl nový správce Manager napsaný v Pythonu, který zároveň sbírá statistiky a metriky. Přibyla také nová deklarativní konfigurace napsaná v YAML, která má rigidnější pravidla a je komplexně validovaná. Je možné předem zjistit, jestli je konfigurace správná nebo ne. Nový formát konfigurace je také lépe uchopitelný pro většinu uživatelů. Lua ovšem nikam nemizí, ale používá se pro interní účely.

Nový Manager sjednocuje správu procesů ve všech prostředích a umí automatickou rekonfiguraci procesů. Knot Resolver neumí nic jako reload, ale umí vyměnit jednotlivé instance postupně bez výpadku. Manager umí také HTTP API pro změnu konfigurace či vyčítání statistik a metrik.

Vývojáři nyní získávají zpětnou vazbu z testování, ostrou verzi by chtěli vydat ještě v prvním čtvrtletí letošního roku. Nový Knot Resolver by měl být také nasazen na veřejných resolverech ODVR provozovaných organizací CZ.NIC. Podrobnosti si lze přečíst v článku Novinky v Knot Resolveru 6.x: správce procesů a přehlednější konfigurace.

Lukáš Šišmiš: Zabezpečení sítí pomocí systému Suricata (7)

Suricata je velmi výkonný open-source nástroj pro monitoring sítí. Je možné do ní vložit pravidla, podle kterých jsou pak generována varování. I bez těchto pravidel jsou ale vytvářeny informace o jednotlivých událostech v provozu.

Je možné připravit pasivní monitoring, kdy odkloníme provoz na switchi a vytvoříme tak detekční systém IDS. Můžeme ale vytvořit i aktivní monitoring, čímž vznikne IPS, který blokuje nechtěný provoz. Standardní komunikační formáty YAML a JSON umožňují také snadnou integraci se systémy SIEM jako Elastic nebo Splunk.

Suricata umožňuje také extrahovat data z různých protokolů. Pokud někdo například stahuje soubor, umí ho extrahovat, vytvořit z něj haš a tu porovnat s databází nějakých škodlivých souborů.

Během uplynulých dvou let vznikla Suricata 7.0, která postupuje v přechodu z jazyka C na Rust. To je dobrý směr, kterým chceme nadále pokračovat. Přibyla podpora XDP, podmíněné logování PCAP, možnost inspekce hlaviček HTTP/HTTP2, parser Bittorrentu a stoupl výkon.

(Autorem fotografií je Petr Krčmář.)