Souhrná výzkumná zpráva

Projekt: **DDoS ochrana v sítí člena sdružení CESNET**

Řešitelé: Ing. Matěj Grégr, Ph.D. FIT VUT Brno, Ing. Tomáš Podermański, CVIS VUT Brno

1. Postup při řešení, způsob řešení

Řešení projektu bylo rozděleno do několika částí. V první fázi řešení projektu byla provedena Modernizace testovacího prostředí. Před zahájením projektu bylo k dispozici testovací prostředí, pro ověření funkcionality nových síťových zařízení, experimentálních protokolů nebo nových vlastností protokolu BGP. V rámci projektu byla provedena modernizace testovacího prostředí tak, aby ho bylo možno využít pro generování testovacích útoků DDoS. Cílem bylo také navýšit dostupnou portovou a rychlostní kapacitu. Vzhledem ke stále vysokým cenám rozhraní 100 Gb/s byla pro testovací prostředí zatím uvažována kapacita v násobcích 40Gb/s. Testovací prostředí bylo rozšířeno jednak o přepínače HP 5940, s kapacitou portů 48x10G a 4x40G. Lze tak do budoucna dosáhnout i testování 100 Gb/s zařízení, které bude možné připojit prostřednictvím deseti portů o rychlosti 10 Gb/s.

Testovací prostředí může sloužit a být k dispozici celé komunitě. Vzhledem k tomu, že v současné době je k dispozici velká kapacita a výpočetní síla, je třeba zohlednit bezpečnostní riziko provozu takového testovacího prostředí a zamezit tak případné nevhodné použití. Díky těmto faktům je testovací prostředí izolováno od běžné provozní sítě. Přístup ostatních členů, bezpečnostní komunity a spolupracujících stran, lze řešit individuálně na základě dohody s řešitelem.

Dalším krokem v rámci řešení projektu bylo zdokonalení nástroje pro generování testovacích DDoS útoků. Současné existující nástroje, které byly využívány před zahájením projektu, přestávaly být vyhovující - ať už z kapacitních důvodů (nebyly schopny dosáhnout vyšší rychlosti a velkého počtu paketů/s na dostupném hardware) nebo díky složitosti instalace, případně nepodporované kombinaci hardware - software (zejména nástroje využívající DPDK). V rámci projektu byla vytvořena sada skriptů, které využívají akcelerační knihovnu PF_RING společně s upraveným ovladačem síťové karty, který umožňuje ZC (Zero Copy) přístup. Společně se sadou skritpů byl vytvořen generátor pcap souborů, který je schopen vytvořit pcap podle specifikovaných pravidel (např. množství rozdílných IP adres, portů 4. vrstvy, aj.). Díky tomu bylo možné začít generovat útoky několika desítek GB/s přehráním zvoleného vygenerovaného datového provozu. Flexibilita generátoru pak zajistila, že je možné rychle a jednoduše změnit charakter provozu při DDoS útoku - např. přejít s velkých paketů DNS provozu na krátké pakety NTP, aj.

Na předchozí kroky navazovala instalace a testování dostupných detekčních nástrojů. V rámci projektu jsme se zaměřili primárně na volně dostupné detekční nástroje (fastnetmon), nástroje vyvíjené sdružením CESNET - DDoS Protector, případně nástroje, které jsou často používány v sítích operátorů - DDoS Defender od společnosti Flowmon. U těchto nástrojů byla provedena analýza funkčnosti a možností, které poskytují pro mitigaci útoků.

Finálním krokem byla pilotní integrace vybraných nástrojů do infrastruktury VUT. V této části došlo k testování jednotlivých přístupů mitigace DDoS útoků (RTBH, Flowspec), vybrání a otestování detekčních nástrojů (fastnetmon, DDoS Defender, DDoS Protector) a začlenění těchto detekčních nástrojů do infrastruktury VUT. V rámci nasazení byla ověřena BGP funkcionalita a kompatibilita detekčních nástrojů se zařízeními různých výrobců - primárně NetX, HP, Cisco, které jsou používány v síti VUT. V současné době tak lze pro vybrané síťové prefixy, které jsou monitorovány detekčními nástroji, nastavit akci, která zašle Flowspec pravidlo pro mitigaci daného útoku. Dané pravidlo se potom aplikuje přímo do hardware síťové karty a dojde k zablokování DDoS provozu dříve, než pakety vstoupí do operačního systému. Oproti filtraci standardním firewallem tak lze efektivně blokovat útoky o velké kapacitě. Kromě podpory BGP Flowspec bylo pro zadávání blokovaných adres a síťových prefixů testováno i využití NetX REST API.

2. Dosažené cíle

V projektu se podařilo dosáhnout cílů, které byly určeny při návrhu projektu.

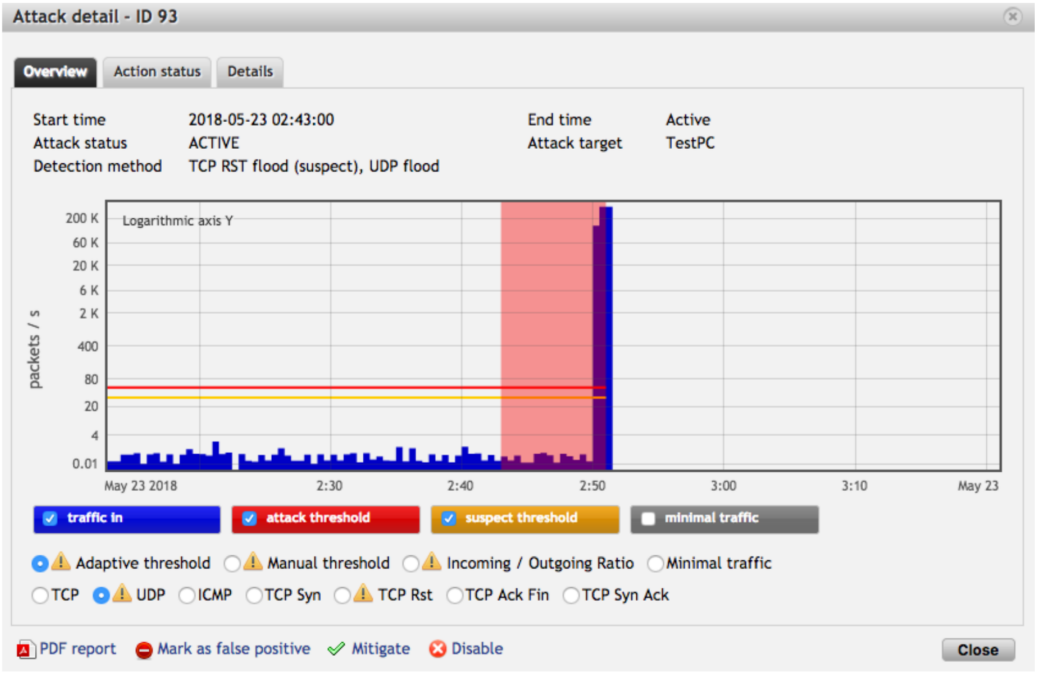
- Byla zvýšena kapacita a počet 10G a 40G portů v testovacím prostředí. Zároveň proběhla příprava pro nasazení portů o rychlostech 100G.
- Došlo k vylepšení nástrojů pro generování testovacích DDoS útoků pro rychlosti vyšší jak 10 Gb/s. V testovacím prostředí, tak lze vygenerovat datový tok v řádek několika desítech Gb/s. Testovací prostředí je také otevřeno celé bezpečnostní komunitě zapojené v rámci CSIRT týmů.
- V rámci testovací fáze byly podrobně analyzovány nástroje pro detekci DDoS útoků a pilotně napojeny v rámci sítě VUT. Při řešení projektu bylo úzce spolupracováno s oddělením 707 a testován nástroj DDoS Protector v komerčních sítích a v topologiích odpovídajících IXP. Výsledky tohoto testování byly prezentovány na pracovní skupině NIX.CZ v rámci bezpečnostního projektu FENIX.
- Při napojení byla rozšířena opensource implementace směrovacího démona bird2 aby byla umožněna bezproblémová komunikace mezi detekčním nástrojem a směrovačem provozovaných na VUT. Zároveň bylo testováno, že se daná Flowspec pravidla správně integrovala do hardware síťové karty směrovače.

3. Zdůvodnění případných změn v projektu

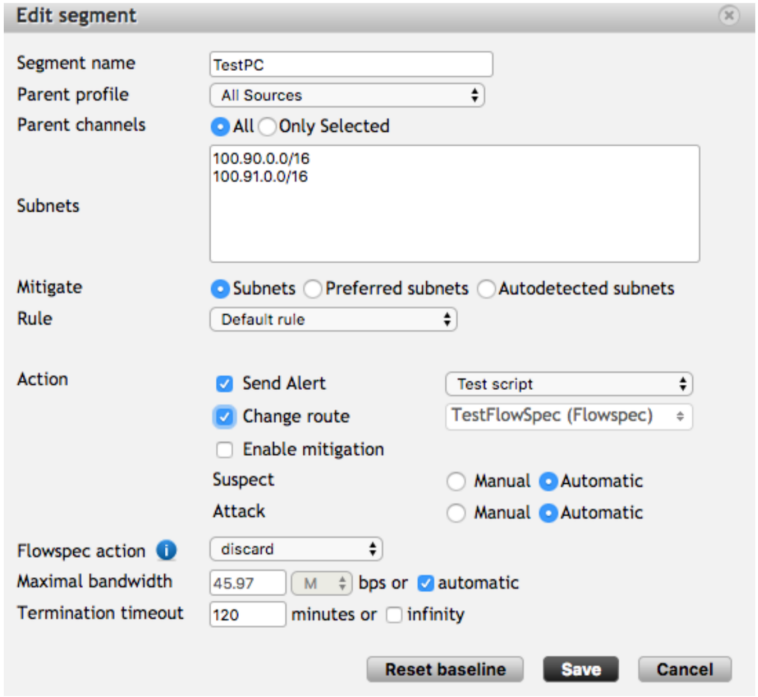
Hlavním cílem projektu bylo otestování jednotlivých nástrojů pro detekci DDoS útoků a pilotní nasazení těchto nástrojů v síti člena sdružení. Těchto cílů se podařilo dosáhnout. Nedošlo tedy ke změnám v projektu.

4. Konkrétní výstupy, další využitelnost

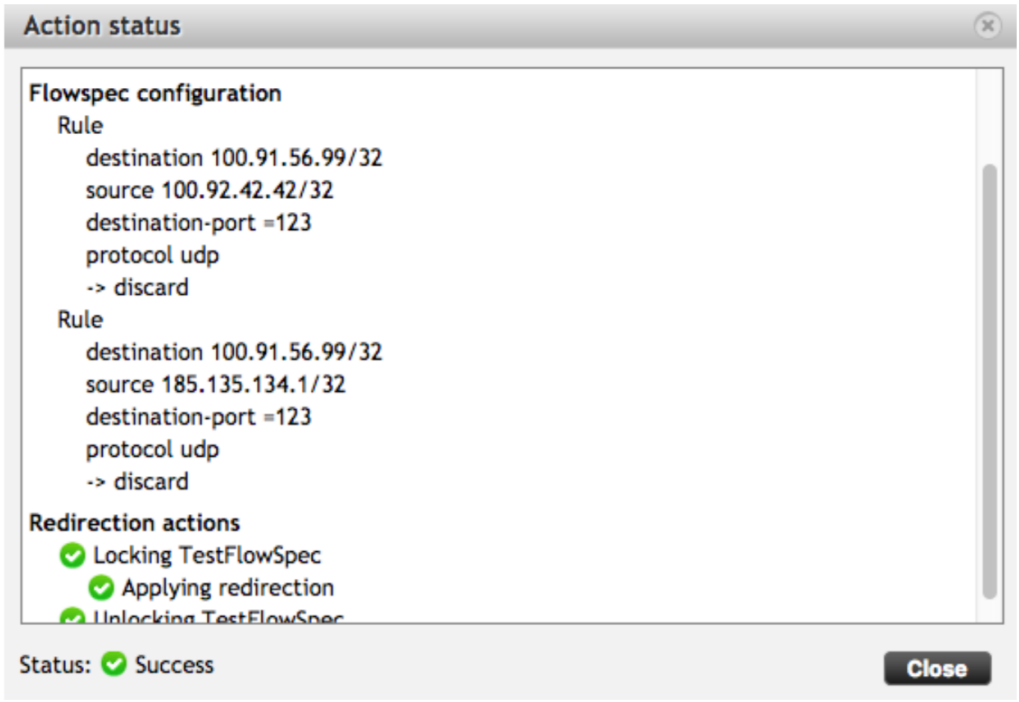
Následující obrázky zobrazují průběh testování jednotlivých detekčních nástrojů a ukázují integraci ve směrovačích NetX, které jsou využívány v rámci sítě VUT pro centrální routing, shaping a BGP.



Obrázek 1: Ukázka detekce v rámci nástroje DDoS Defender od firmy Flowmon



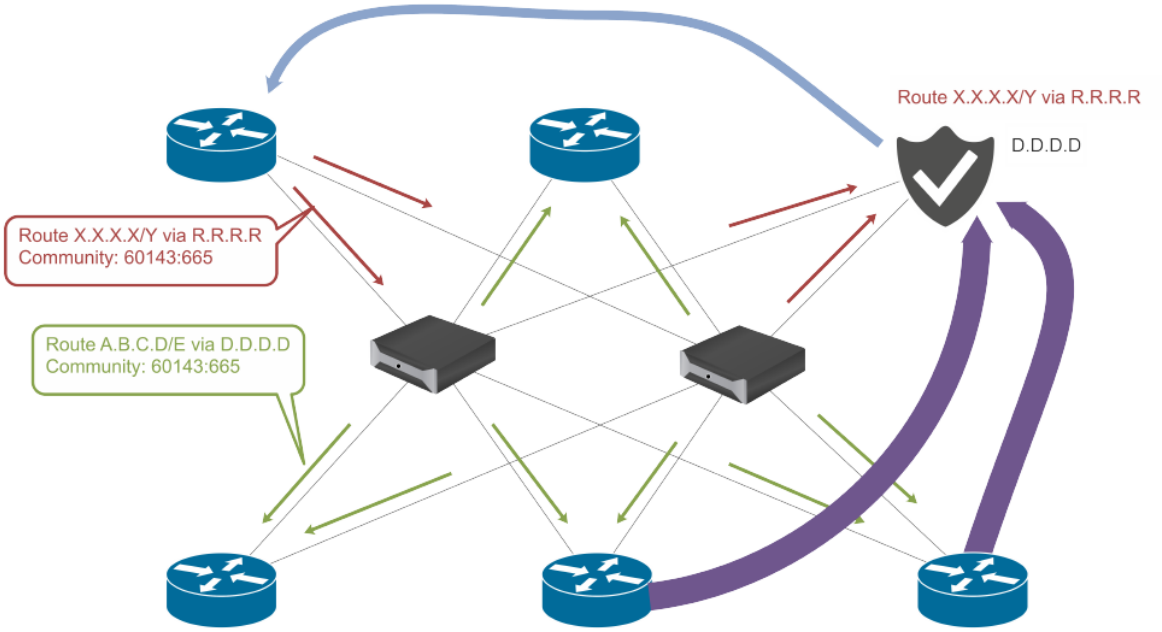
Obrázek 2: Ukázka nastavení monitorovaných prefixů a exportu informací pomocí BGP Flowspec



Výpis odpovídajících Flowspec pravidel:

```
# birdc show route table flowtab4
BIRD 2.0.2 ready.
flow4 { dst 100.91.56.96/32; src 185.135.134.1/32; proto 17; dport 123; }
[IBGP_DDOS_DEFENDER 12:12:39.037 from 147.229.3.139] * (100) [i]
flow4 { dst 100.91.56.96/32; src 100.92.42.42/32; proto 17; dport 123; }
[IBGP_DDOS_DEFENDER 12:12:39.030 from 147.229.3.139] * (100) [i]
```

Obrázek 3: Ukázka mitigačního pravidla zaslaného detekčním nástrojem DDoS Defender a odpovídající výpis Flowspec pravidel ve směrovacím démonovi bird



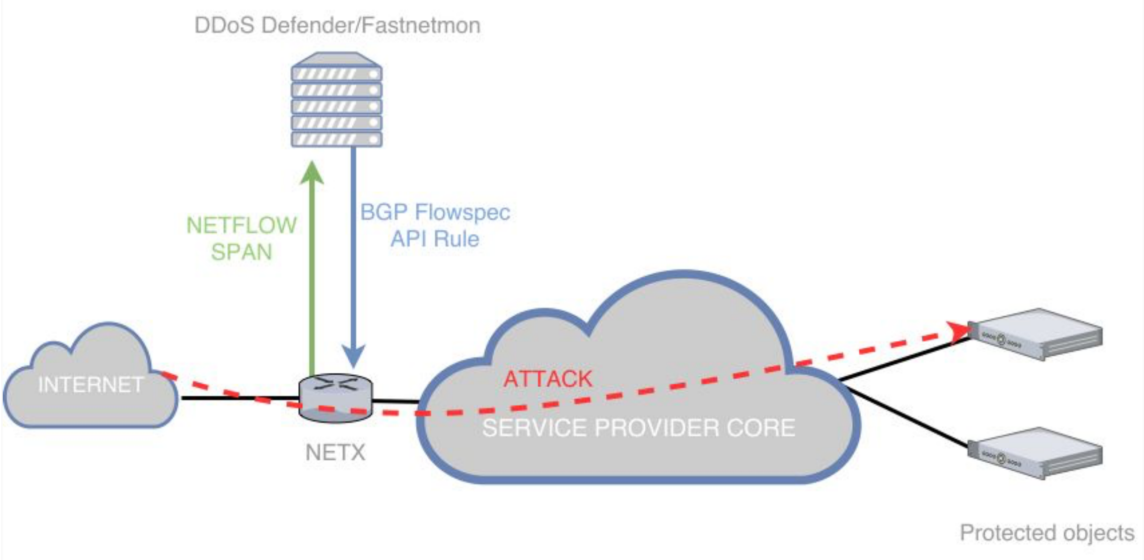
Obrázek 4: Ukázka principu přesměrování útoku na zařízení DDoS Protector v topologii IXP. Pro směrovací záznam šířený ze směrovače je na route serverech přepsán NEXT_HOP, který provoz pošle do zařízení DDoS Protector. Ten provoz profiltruje a vrátí zpět na hraniční směrovač.

```
Output filter na RS:
if ((60143,665) ~ bgp_community ) then {
      bgp_next_hop = 185.1.25.65; }
```

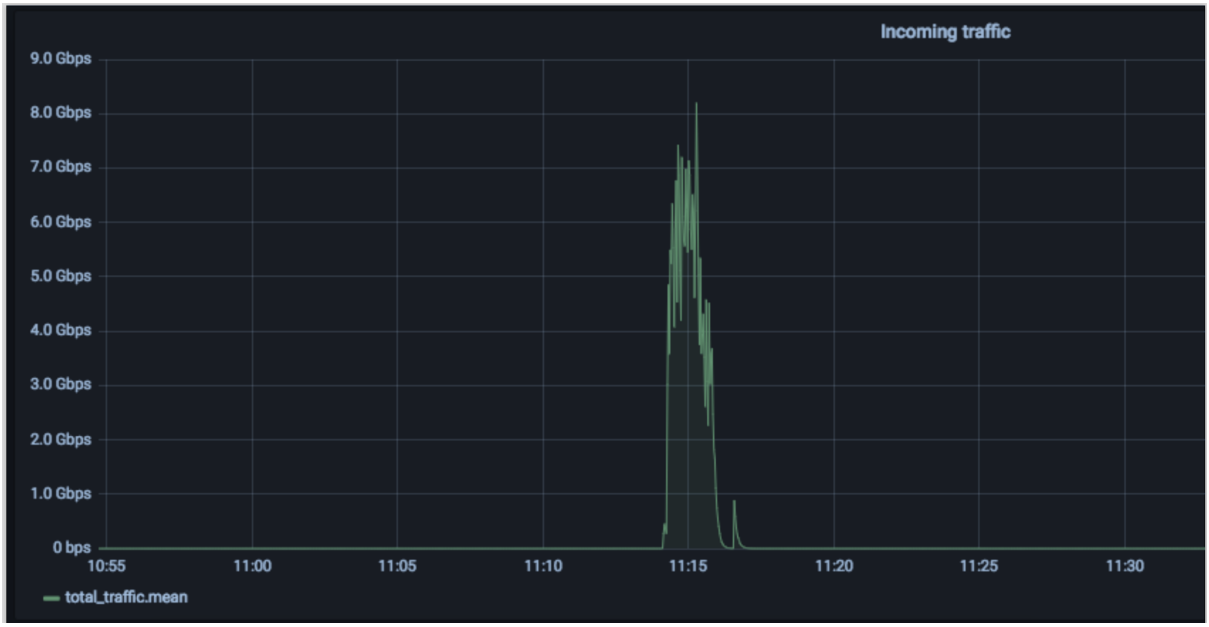
Export filtr u chráněného člena:

```
export filter {
if ( net ~ [ 185.135.134.0/24 ] ) then {
      bgp_community.add((60143,665));
      accept; }
};
```

Obrázek 5: Doplnění k Obrázku 4. Ukázka nastavení démonů bird v rámci IXP. Prefix, který chce člen v IXP ochránit exportuje a přidá definovanou komunitu (v příkladě 665). Route-server pro prefix s touto komunitou přepíše atribut NEXT_HOP v BGP a pošle na DDoS Protector či jiné zařízení.



Obrázek 6: Schéma pilotního zapojení v rámci sítě VUT. Páteřní směrovač NetX odbočuje provoz do detekčního nástroje - DDoS Protector/Defender/Fastnetmon. Nástroj při detekování DDoS útoku zašle pomocí BGP Flowspec pravidlo eliminující tento útok. Testován byl i mechanismu, kdy detekční nástroj volá přímo NetX REST API.



Obrázek 7: Ukázka eliminace DDoS útoku v nástroji Grafana. Díky automatickému zaslání Flowspec pravidla detekčním nástrojem došlo k eliminaci DDoS útoku v řádu několika minut.

Využitelnost:

Prezentované výstupy jsou využívané v rámci sítě VUT a získané zkušenosti jde aplikovat i na další členy sdružení CESNET. Podrobná zpětná vazba při spolupráci s oddělením 707

vedla k zlepšení funkcionality nástroje DDoS Protector. Vysokokapacitní testovací prostředí mohou také využít další členové sdružení CESNET pro vlastní testování nebo pro penetrační testy vlastní sítě. K využití jak testovacího prostředí, tak nástroje DDoS Protector dalšími členy sdružení CESNET, došlo již v průběhu řešení projektu, kdy z testovacího prostředí byly vedeny různé typy simulovaných útoků na koncové sítě TUL Liberec. Současně probíhalo ověřování DDoS mitigačního nástroj DDoS Protector vyvíjeného v rámci oddělení 707. Zkušenosti získané při řešení projektu a testování jednotlivých nástrojů jsou dále předávány ostatním správcům a studentům ve formě prezentací na odborných seminářích a v síťových předmětech. V rámci projektu současně započala příprava odborných článků zabývající se touto problematikou v podobě seriálu pro server root.cz. Tyto články podrobně rozebírají problematiku DDoS útoků a nástrojů pro jejich mitigaci.

5. Přínosy projektu, vlastní hodnocení

Přínos projektu: DDoS útoky jsou častými bezpečnostními incidenty a velkokapacitní sítě členů sdružení CESNET jsou častým cílem. Síť VUT byla cílem několika útoků se silou přesahující 10G. Projekt tedy vyřešil reálné problémy, se kterými se správce sítě člena sdružení v dnešní době setká. Díky výsledku projektu lze využít opensource nástroje a nástroje vyvíjené sdružením CESNET pro detekci těchto útoků a pomocí v projektu navrženého systému automaticky eliminovat daný útok před vstupem do sítě člena sdružení. Přínosem je tedy automatická ochrana člena sdružení CESNET, která je ověřená v produkčním nasazení. Získané zkušenosti jde aplikovat i u dalších členů řešení, kteří mají zájem o automatickou DDoS ochranu. Testovací prostředí již bylo využito TUL Liberec pro penetrační testování jejich sítě.

Vlastní hodnocení: Projekt zpracoval a vyřešil všechny body z návrhu projektu. Byla podrobně otestována řada nástrojů a získané zkušenosti byly přímo využity v produkční síti VUT. Řešitelský tým by tímto chtěl také zvláště poděkovat oddělení 707 (Oddělení nástrojů pro administraci a bezpečnost) za skvělou spolupráci a podporu při řešení projektu, bez které by realizace projektu, vzhledem k jeho finančnímu krácení o 50% oproti původnímu záměru, byla v plném rozsahu obtížně zvládnutelná.

6. Tisková zpráva

FIT a CVIS VUT v Brně, ve spolupráci s organizací CESNET, vytvořili systém pro automatickou mitigaci distribuovaných DoS útoků. Systém dokáže na základě informací z detekčních systémů aplikovat filtr provozu do síťové karty a eliminovat tak útok přímo v hardware. Systém je pilotně nasazen pro vybrané síťové prefixy VUT.