NetX - DDoS

Filtrační jednotka pro eliminaci DDoS útoků s využitím komoditního hardware

Instalační příručka

Matěj Grégr

Dokument k projektu TARZAN
Fakulta informačních technologií, Vysoké učení technické v Brně

Filtrační jednotka pro eliminaci DDoS útoků s využitím komoditního hardware – Dokumentace

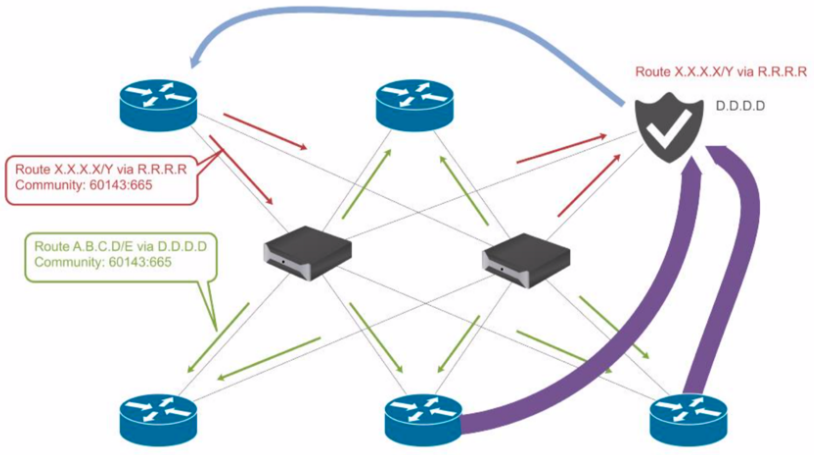
Matěj Grégr

Vysoké učení technické v Brně, email: mgregr@fit.vutbr.cz

Abstrakt V rámci projektu Tarzan byla pro účely detekce a mitigace DDoS útoků vyvinuta sada nástrojů a technik, které byly implementačně ověřeny v počítačové síti VUT a v rámci propojovacího centra BR-IX. Pro detekci DDoS útoků bylo využito řešení firmy Flowmon, které umožňuje detekovat útok a zaslat popis útoku pomocí protokolu BGP Flowspec na zařízení, které provede samotnou filtraci. V rámci propojovacího centra BR-IX jsou tyto informace předávány pomocí route serverů, kde pro směrovací záznam šířený z postiženého směrovače je na route serverech přepsán NEXT_HOP, který provoz přepošle do zařízení, které provede filtraci a vyčištění provoz vrátí zpět na hraniční směrovač.

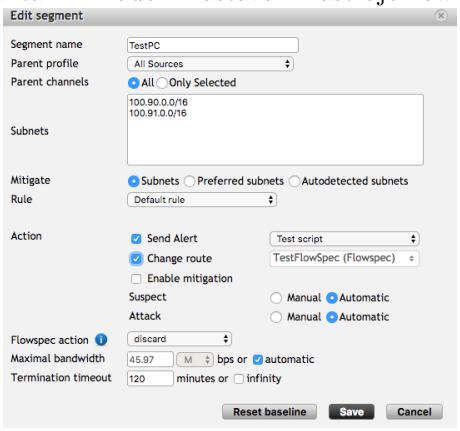
1 Schéma zapojení

Pro mitigaci DDoS útoku je třeba mít nainstalován v síti daný funkční vzorek. Jedná se o 1U HW řešení, které je třeba mít nainstalován v datacentru a propojené do sítě. Topologie každé sítě je odlišná, proto je v rámci této dokumentace uvažováno a zapojení v propojovacím uzlu (peering-center) - viz následující obrázek.

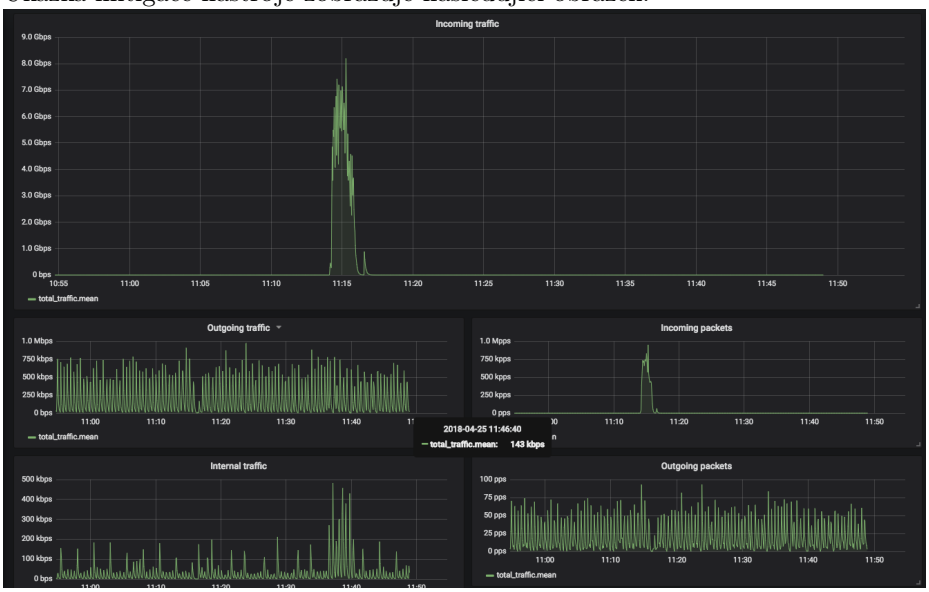


Pro správnou funkcionalitu filtrační jednotky je nutné mít k dispozici systém, který DDoS útoky detekuje. V rámci projektu byly testovány systémy společnosti Flowmon Networks a opensource řešení fastnetmon. Řešení firmy Flowmon

umožnuje mitigaci útoku pomocí protokolu BGP s rošířením Flowspec, řešení fastnetmon využívá REST API platformy NetX, na které běží mitigační funkcionalita. Příkladem nastavení nástroje flowmon ukazuje následující obrázek:



Ukázka mitigace nástroje zobrazuje následující obrázek.



Filtraci lze také zadat přímo na dané platformě podle zdokumentovaných příkazů - viz následující způsob použití, kdy dojde k filtraci provozu zdrojové IP adresy 1.1.1.1 na port 80.

```
  _   _      _    __  __
 | \ | | ___| |_  \ \/ /
 |  \| |/ _ \ __|  \  /
 | |\  |  __/ |_   /  \
 |_| \_|\___|\__| /_/\_\

 Docs:    https://docs.netx.as
 Support: support@netx.as


rt-netx-a# interface tge11
rt-netx-a(if-tge11)# hw-filter action drop ?
 <cr>
 dmask                - destination wildcard mask
 dport                - destination port number
 dst                  - destination IP address
 id                   - filter id
 proto                - protocol name/number
 smask                - source wildcard mask
 sport                - source port number
 src                  - source IP address

rt-netx-a(if-tge11)# hw-filter action test src 1.1.1.1 sport 80
```

2 Závěr

Dokumentace popisuje proces nasazení a zapojení filtrační jednotky pro mitigaci DDoS útoků, která byla vyvinuta v rámci projektu TARZAN [1].

Tato instalační příručka navazuje na další publikace:

- diplomovou práci, která podrobně popisuje daný systém [2];
- zdrojové kódy [3];

Odkazy

[1] *Integrovana platforma pro zpracovani digitalnich dat z bezpecnostnich incidentu*. https://www.fit.vut.cz/research/project/1063/. navstiveno: 2019-09-10.

[2] Peter Nagy. „Automatická mitigace DDoS útoku“. czech. Diplomová práce. Brno, CZ: Vysoké učení technické v Brně, Fakulta informačních technologií, 2018. URL: https://www.fit.vut.cz/study/thesis/20619/.

[3] *Zdrojové kódy aplikace*. https://www.dropbox.com/sh/cp5esofp0q7xlik/AACLGX0lLkWTlM3yt44j58BSa?dl=0. navstiveno: 2020-02-10.