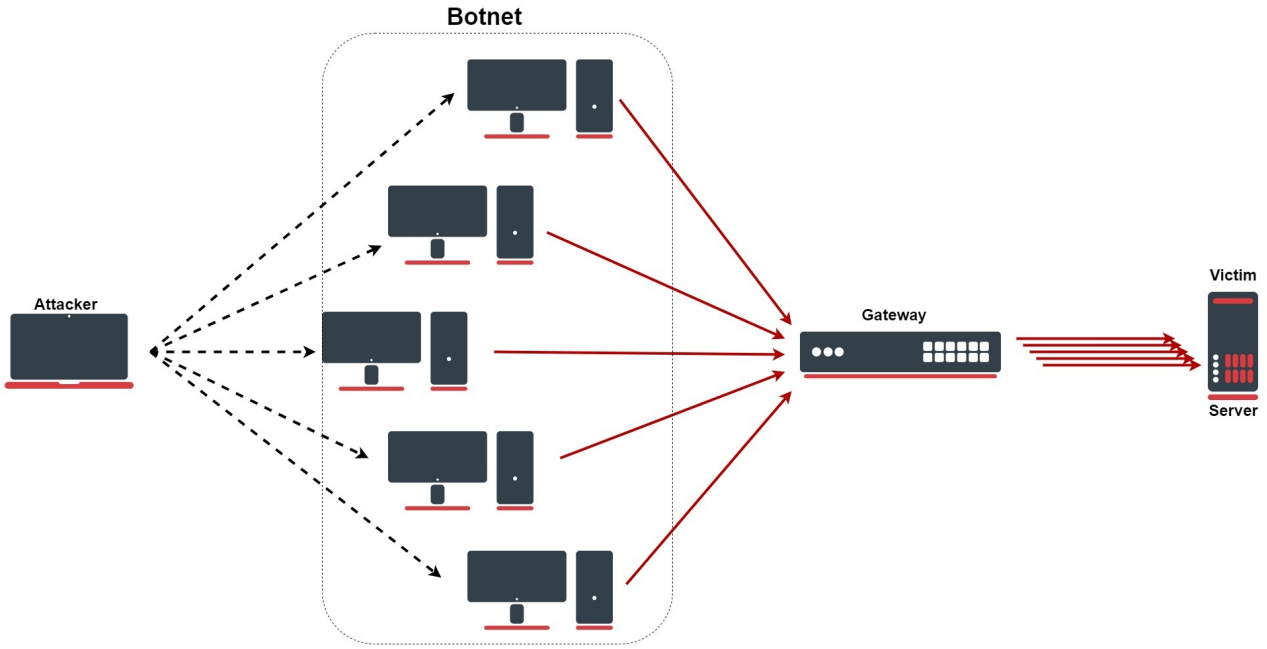
SYN/DoS/DDoS Protection

help.mikrotik.com/docs/pages/viewpage.action

Úvod

Denial-of-service (DoS) nebo distribuovaný denial-of-service (DDoS) útok je škodlivý pokus narušit normální provoz cílového serveru, služby nebo sítě zahlcením cíle nebo jeho okolní infrastruktury záplavou internetu. provoz. Existuje několik typů DDoS útoků, například HTTP flood, SYN flood, DNS amplification atd.



Ochrana proti DDoS

Konfigurační linky

Tato pravidla jsou pouze vylepšením firewallu, nezapomeňte své zařízení řádně zabezpečit: Vytvoření prvního firewallu !

```
/ip firewall address-list
add list =ddos-attackers
add list =ddos-targets
/ip firewall filter
add action =return chain =detect-ddos dst-limit =32,32,src-and-dst-addresses/10s
add action =add-dst-to-address-list address-list =ddos-targets address-list-timeout =10m chain =detect-ddos
add action =add-src-to-address-list address-list =ddos-attackers address-list-timeout =10m chain =detect-ddos
/ip firewall raw
add action =drop chain =prerouting dst-address-list =ddos-targets src-address-list =ddos-attackers
```

Konfigurace vysvětlena

Nejprve odešleme každé nové připojení do specifického firewallového řetězce, kde budeme detekovat DDoS:

```
/ip/firewall/filter/ add chain =forward connection-state =new action =jump jump-target =detect-ddos
```

Do nově vytvořeného řetězce přidáme následující pravidlo s parametrem „dst-limit“. Tento parametr je zapsán v následujícím formátu : **dst-limit= count[/time],burst,mode[/expire]** . Porovnáme 32 paketů se shlukem 32 paketů na základě toku cílové a zdrojové adresy, který se obnovuje každých 10 sekund. Pravidlo bude fungovat, dokud nebude překročena daná rychlost.

```
/ip/firewall/filter/ add chain =detect-ddos dst-limit =32,32,src-and-dst-addresses/10s action =return
```

Dosud by měl veškerý legitimní provoz procházet "akcí=návrat", ale v případě DoS/DDoS bude "dst-limit" buffer naplněn a pravidlo "nechytne" žádný nový provoz. Zde jsou další pravidla, která se budou zabývat útokem. Začněme vytvořením seznamu útočníků a obětí, který vypustíme:

```
ip /firewall/address-list/ add list =ddos-attackers
```

```
ip /firewall/address-list/ add list =ddos-targets
```

```
ip /firewall/raw/ add chain =prerouting action =drop src-address-list =ddos-attackers dst-address-list =ddos-targets
```

Pomocí sekce filtru brány firewall přidáme útočníky do seznamu „DDoS-útočníci“ a oběti do seznamu „ddos-targets“:

```
/ip/firewall/filter/
```

```
add action =add-dst-to-address-list address-list =ddos-targets address-list-timeout =10m chain =detect-ddos
```

```
add action =add-src-to-address-list address-list =ddos-attackers address-list-timeout =10m chain =detect-ddos
```

SYN útok

SYN Flood

Záplava SYN je forma útoku DoS, ve kterém útočník posílá sled požadavků SYN do systému cíle ve snaze spotřebovat dostatek serverových zdrojů, aby systém přestal reagovat na legitimní provoz. Naštěstí v RouterOS máme pro takový útok specifickou funkci:

```
/ip/settings/ set tcp-syncookies =yes
```

Tato funkce funguje s odesíláním zpět ACK paketů, které obsahují malý kryptografický hash, který odpovídající klient odešle zpět jako součást svého paketu SYN-ACK. Pokud jádro nevidí tento "cookie" v paketu odpovědi, bude předpokládat, že připojení je falešné a zahodí jej.

Povodeň SYN-ACK

Záplava SYN-ACK je metoda útoku, která zahrnuje odesílání falešného paketu SYN-ACK cílovému serveru vysokou rychlostí. Server vyžaduje značné zdroje ke zpracování takových paketů mimo pořadí (není v souladu s normálním třícestným handshake mechanismem SYN, SYN-ACK, ACK TCP), může být tak zaneprázdněn zpracováváním útočného provozu, že nezvládne legitimní provoz, a proto útočníci dosáhnou podmínky DoS/DDoS. V RouterOS můžeme nakonfigurovat podobná pravidla z výše uvedeného příkladu, ale konkrétněji pro SYN-ACK flood:

```
/ip/firewall/filter add action =return chain =detect-ddos dst-limit =32,32,src-and-dst-addresses/10s protocol =tcp tcp-flags =syn,ack
```

Žádné štítky