Mikrotik – Ochrana před DDoS útoky (Mikrotik – DDoS protection)

martinuvzivot.cz/mikrotik-ochrana-pred-ddos-utoky-mikrotik-ddos-protection

administrator January 22, 2023

Last Updated on 22/01/2023 by administrator

Mikrotik – Ochrana před DDoS útoky (Mikrotik – DDoS protection)

Motivace:

Článek popisuje, jak vytvořit na RouterBOARDu od společnosti Mikrotik firewall pravidla proti DDoS útokům (DDoS protection) a ochránit tak před těmito útoky vše, co je "schované" za RouterBOARDem, ale i běžící služby na RouterBOARDu.

Na úvod:

Obecně DoS či DDoS útok, zahlcuje CPU, RAM a internetovou linku. Už jen pokud útok, vedený na server jde přes Mikrotik, zahlcuje to nejen server ale i samotný Mikrotik. To zatěžuje Mikrotik CPU, kde afektovaný je třeba firewall (filter, NAT, mangle), logování, fronty, .., a také RAM, neboť se alokují nové connections ve stateful flow tabulce. Tímto vznikají větší latence až může dojít k timeoutu paketů a Mikrotik se může stát nedostupný.

Obecně neexistuje dokonalé řešení ochrany před DDoS útoky, nicméně dá se minimalizovat dopad útoku a to pomocí:

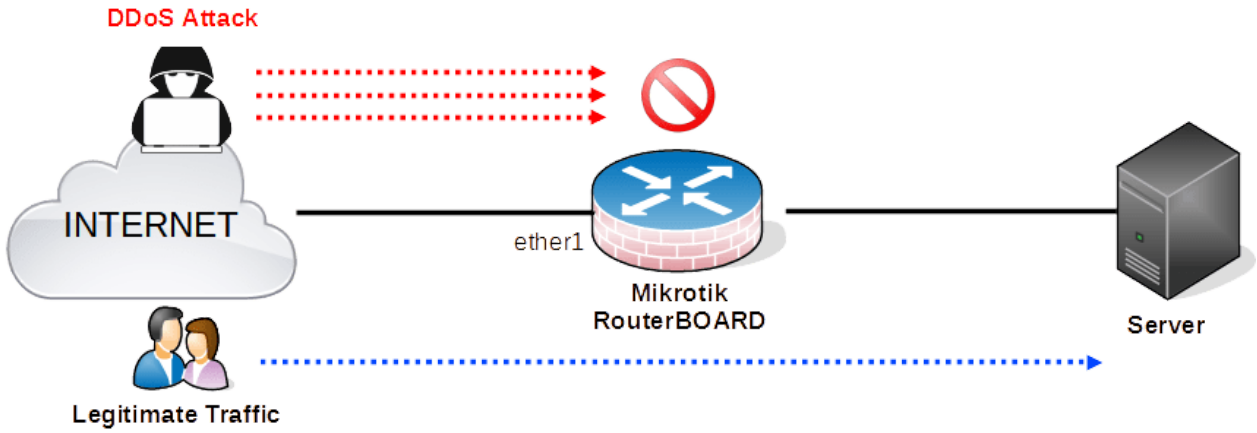
- výkonnějšího routeru
- rychlejším uplinkem
- menším počtem firewall pravidel, front či dalších akcí pro manipulaci s pakety

Vždy je nejlepší zablokovat útok co nejblíže ke zdroji, aby nevytěžoval síťová zařízení “po cestě”.

OS:

Postup byl prováděn na verzi RouterOS 6.x. konkrétně RouterOS 6.49.6

1. Implementace IDS/IPS chránící síťová zařízení nacházející se za RouterBOARDem



Firewall pravidla níže poskytují DDoS ochranu pro všechny protokoly (TCP, UDP, ICMP, ..).

Jednotlivé části firewall pravidel jsou označeny čísly pomocí komentáře (#1, #2, ..). Každá tato jednotlivá číselná část firewall pravidla je popsána níže.

```
/ip firewall filter

#1
add action=jump chain=forward connection-state=new jump-
target=detect-ddos in-interface ether1
#2
add action=return chain=detect-ddos dst-limit=30,10,src-and-
dst-addresses/10s
#3
add action=add-dst-to-address-list address-list=ddos-dst
address-list-timeout=10d chain=detect-ddos
#4
add action=add-src-to-address-list address-list=ddos-src
address-list-timeout=10d chain=detect-ddos
#5
add action=drop chain=forward connection-state=new dst-address-
list=ddos-dst src-address-list=ddos-src
```

Popis firewall pravidel výše:

1# pravidlo – každé nové spojení (což definované TCP SYN) [*connection-state=new*], přicházející ze vstupního rozhraní ether1 [*in-interface=ether1]*, se předá na target “detect-ddos” [*jump-target=detect-ddos*]

2# pravidlo – na vstup přichází chain (řetězec) “detect-ddos” [*chain=detect-ddos*], (který definuje z 1# pravidla všechna nově vytvořená spojení) a toto pravidlo nastavuje per zdrojovou a cílovou IP adresu limit 30 paketů za sekundu (pps) s burstem 10 paketů [*dst-limit=20,5,*] a díky řetězce action “return” [*action=return*] se předá informace zpátky do chain (řetězce) “detect-ddos”

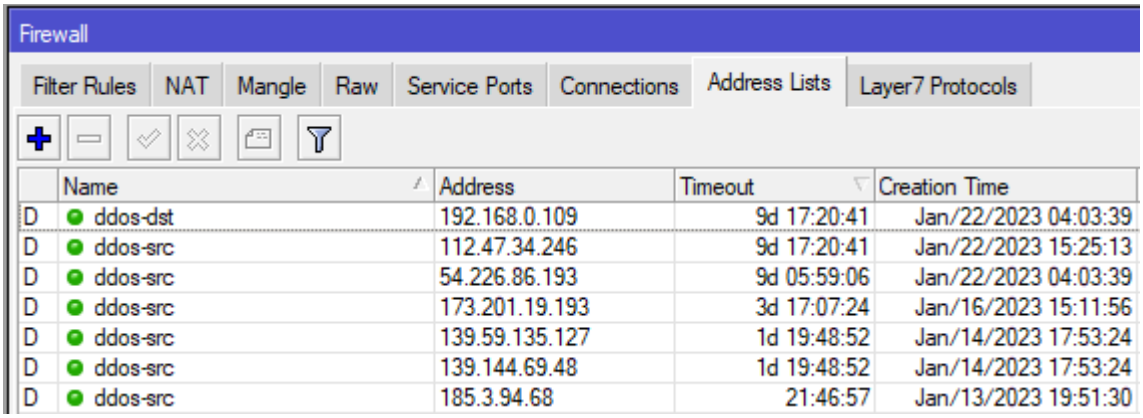
3# pravidlo – na vstup přichází již upravený chain (řetězec) “detect-ddos” [*chain=detect-ddos*], kde byl nastaven limit paketů a burst 2# pravidlem. Při překročení se cílová IP adresa [*action=add-dst-to-address-list*] dostává do Address Listu se jménem “ddos-dst” na 10 dní [*address-list=ddos-dst address-list-timeout=10d*].

4# pravidlem (podobně jako 3#) na vstup přichází již upravený chain (řetězec) “detect-ddos“[*chain=detect-ddos*], kde byl nastaven limit paketů 2# pravidlem. Při překročení se zdrojová IP adresa [*action=add-src-to-address-list*] dostává do Address Listu se jménem “ddos-src” na 10 dní [*address-list=ddos-dst address-list-timeout=10d*].

5# pravidlo zahazuje všechny pakety [*action=drop*] nového vytvořeného spojení [*connection-state=new*], které prošly Address Listem “ddos-dst” a “ddos-src” [*dst-address-list=ddos-dst src-address-list=ddos-src*].

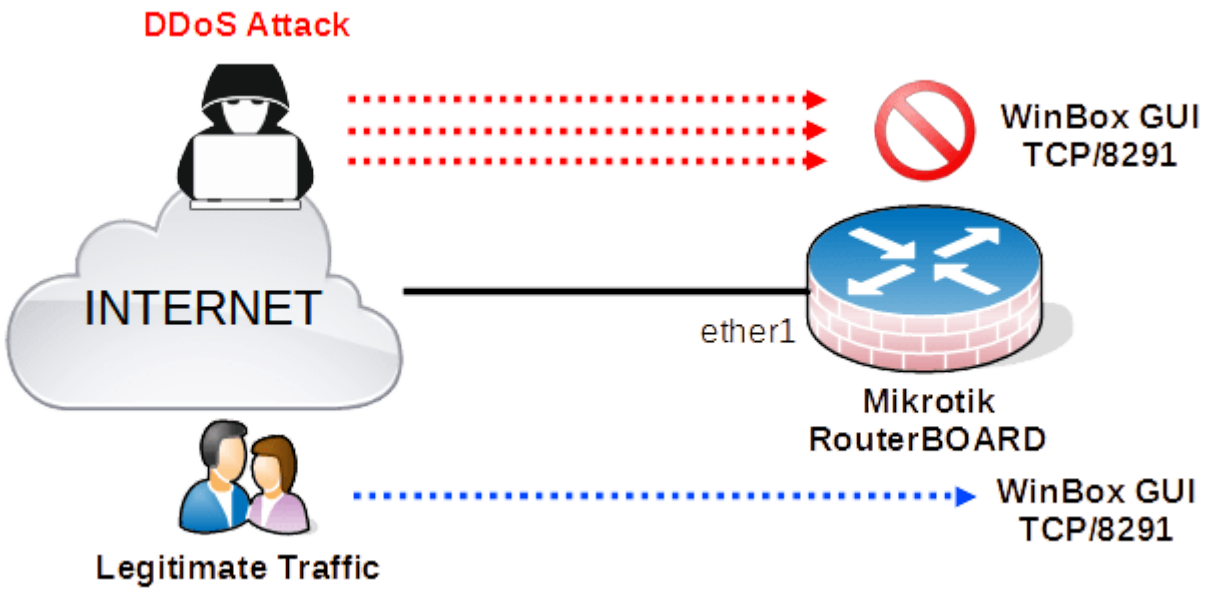
Poznámka: Jak moc citlivě se bude pravidlo chovat při DDoS útoku je nutné individuálně otestovat a korektně zvolit **dst-limit**.

Ukázka blokace zdrojových IP adres (ddos-src):



	Name	Address	Timeout	Creation Time
D	ddos-dst	192.168.0.109	9d 17:20:41	Jan/22/2023 04:03:39
D	ddos-src	112.47.34.246	9d 17:20:41	Jan/22/2023 15:25:13
D	ddos-src	54.226.86.193	9d 05:59:06	Jan/22/2023 04:03:39
D	ddos-src	173.201.19.193	3d 17:07:24	Jan/16/2023 15:11:56
D	ddos-src	139.59.135.127	1d 19:48:52	Jan/14/2023 17:53:24
D	ddos-src	139.144.69.48	1d 19:48:52	Jan/14/2023 17:53:24
D	ddos-src	185.3.94.68	21:46:57	Jan/13/2023 19:51:30

2. Implementace IDS/IPS chránící služby na RouterBOARDu



Příkladem může být ochrana pro WinBox GUI, PPTP server či L2TP server, které běží přímo na zařízení Mikrotik. Níže je uveden příklad pro ochranu **WinBox GUI**.

Pár let tuto IDS/IPS ochranu používám na svém RouterBoardu.

Princip funkce:

Uživatel má 3 pokusy pro zadání správných přihlašovacích údajů. Po 4 nesprávném pokusu dojde v rámci 1 minuty k zablokovaní jeho IP adresy na WinBox GUI portu TCP/8291 a to na 10 dnů.

Každé nesprávné zadaní přihlašovacích údajů vytváří na Mikrotik novou konexi TCP SYN a na tom jsou založena firewall pravidla níže. Čili 4 zprávy TCP SYN obdržené na portu TCP/8291 v rámci 1 minuty blokují IP adresu na 10 dnů.

Opět jednotlivé části firewall pravidel jsou označeny čísly pomocí komentáře (#1, #2, ..). Každá tato jednotlivá číselná část firewall pravidla je popsána níže.

```
/ip firewall filter

1#
add chain=input action=drop protocol=tcp src-address-
list=winbox_blacklist in-interface=ether1 dst-port=8291
2#
add chain=input action=add-src-to-address-list connection-
state=new protocol=tcp src-address-list=winbox_blacklist_stage3
address-list=winbox_blacklist address-list-timeout=1w3d in-
interface=ether1 dst-port=8291
3#
add chain=input action=add-src-to-address-list connection-
state=new protocol=tcp src-address-list=winbox_blacklist_stage2
address-list=winbox_blacklist_stage3 address-list-timeout=1m
in-interface=ether1 dst-port=8291
4#
add chain=input action=add-src-to-address-list connection-
state=new protocol=tcp src-address-list=winbox_blacklist_stage1
address-list=winbox_blacklist_stage2 address-list-timeout=1m
in-interface=ether1 dst-port=8291
5#
add chain=input action=add-src-to-address-list connection-
state=new protocol=tcp address-list=winbox_blacklist_stage1
address-list-timeout=1m in-interface=ether1 dst-port=8291
6#
add chain=input action=accept protocol=tcp in-interface=ether1
dst-port=8291
```

Popis firewall pravidel výše:

Pro vysvětlení jednotlivých pravidel je nutné je popsat od posledního 6 pravidla až k 1 pravidlu:

6# pravidlo – povoluje věškerou komunikaci [*action=accept*] přicházející z rozhraní ether1 [*in-interface=ether1*] na cílovém portu TCP/8291 [*protocol=tcp dst-port=8291*]

5# pravidlo – pro každé nové spojení (což definované TCP SYN) [*connection-state=new*], na portu TCP/8291 ze vstupního rozhraní ether1 [*protocol=tcp in-interface=ether1]*, se dostává zdrojová IP

adresa do Address Listu se jménem winbox_blacklist_stage1 na 1 minutu [*action=add-src-to-address-list address-list=winbox_blacklist_stage1 address-list-timeout=1m*]

4# pravidlo – Pokud zdrojová IP adresa, která byla přidána v Address Listu winbox_blacklist_stage1 [*src-address-list=winbox_blacklist_stage1*] naváže druhé nové spojení (což definované novým TCP SYN) [*connection-state=new*] přidá se tato zdrojová IP adresa do dalšího Address Listu winbox_blacklist_stage2 na 1 minutu [*action=add-src-to-address-list address-list=winbox_blacklist_stage2 address-list-timeout=1m*]

3# pravidlo – Pokud zdrojová IP adresa, která byla přidána v Address Listu winbox_blacklist_stage2 [*src-address-list=winbox_blacklist_stage2*] naváže třetí nové spojení (což definované opět novým TCP SYN) [*connection-state=new*] přidá se tato zdrojová IP adresa do dalšího Address Listu winbox_blacklist_stage3 na 1 minutu [*action=add-src-to-address-list address-list=winbox_blacklist_stage3 address-list-timeout=1m*]

2# pravidlo – Pokud zdrojová IP adresa, která byla přidána v Address Listu winbox_blacklist_stage3 [*src-address-list=winbox_blacklist_stage3*] naváže čtvrté nové spojení (což definované opět novým TCP SYN) [*connection-state=new*] přidá se tato zdrojová IP adresa do finálního Address Listu winbox_blacklist a to na 10 dní [*action=add-src-to-address-list address-list=winbox_blacklist address-list-timeout*=1w3d]

1# pravidlo – Všechny zdrojové IP adresy co byly přidány do Address Listu winbox_blacklist [*src-address-list=winbox_blacklist*] jsou zahozeny [*action=drop*].

3. Implementace ochrany před TCP SYN útoky

Využívá se zapnutí volby **TCP SynCookies**. Výhoda je ze SYN-cookies jsou kompatibilní se všemi specifikacemi TCP

Zjednodušený princip funkce:

Pro navázání TCP komunikace se používá 3-way handshake. Klient nejdříve vyšle SYN paket. Mikrotik příjme tento SYN a odpoví zprávou SYN-ACK. Nicméně pokud je zapnutá funkce **TCP SynCookies** Mikrotik vloží navíc do zprávy **SYN-ACK kryptograficky hash**. Jak odpověď na SYN-ACK Mikrotik příjme zprávu ACK od klienta. Pokud Mikrotik v této **ACK zprávě nevidí kryptograficky hash, připojení je falešné a zahodí ho**. Pokud je stejný hash přítomný v ACK, **až teprve potom Mikrotik alokuje TCP buffer** a komunikace klasicky proběhne. Tím pádem nedojde k přetečení TCP bufferu při TCP SYN útoku Viz. více popisuje tento obrázek zde

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

Zdroj:

[1] http://srijit.com/how-to-protect-your-mikrotik-router-from-ddos-attacks/

Dobrovolný dar

Ahoj čtenáři, rád bych tě poprosil aby ses zamyslel, co je vše potřeba ke vzniku článku.
Jakožto amatérský softwarový kutil musím:

1) Nejdříve vše nastudovat v cizích jazycích.
2) Vše následně prakticky vyzkoušet.
3) Svoje poznatky a zkušenosti napsat do článku který si právě přečetl v jazyku kterému rozumíš.
4) Dát článku hlavu a patu a publikovat.

Každý článek zabere několik hodin práce, za kterou mi nikdo neplatí.
Prosím zvaž, kolik času jsem ti právě ušetřil.
Pokud ti to stojí aspoň za cenu jedné kávy, tak mi ji kup.
Předem moc děkuji.

Příspěvek tak můžeš provést zasláním libovolné částky na mé číslo účtu **1558701011/3030** Nebo můžeš dar poslat kliknutím na tento odkaz **Podpořit tento WEB** , který tě přesměruje na mou platební bránu Revolut.

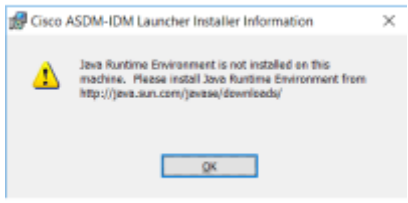
Dar je také možné poslat ve formě Bitcoinu na BTC peněženku **bc1qqdf5fp42a7srwwhh2rut8zr9x4jm5c8fqc9qw6**

Veškeré peněžní prostředky budu také používat na zlepšení kvality své webové tvorby a na psaní nových technických návodů. **Za každý dar předem děkuji.**

Další články

PuTTY, type 3 SSH2_MSG_UNIMPLEMENTED – chyba

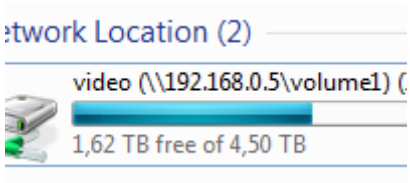
ASDM – Java Runtime Environment is not installed on this machine



Mounting (namapování) disku ve Windowsu k NFS serveru

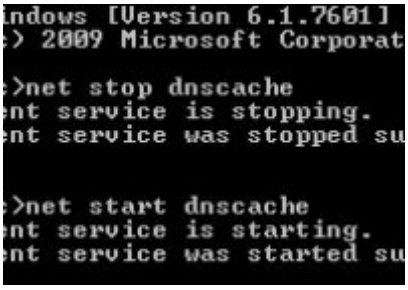
Zasílání logů z NAS Synology na Syslog server

DNS cache, aneb co dělat když ipconfig /flushdns nefunguje (WIN 7)



Vypnutí IPv6 adresy / IPv6 protokolu v Linuxu


How to send
logs to
Syslog server
Synology


indows [Version 6.1.7601]
) 2009 Microsoft Corporat
>net stop dnscache
nt service is stopping.
nt service was stopped su
>net start dnscache
nt service is starting.
nt service was started su


IPv6