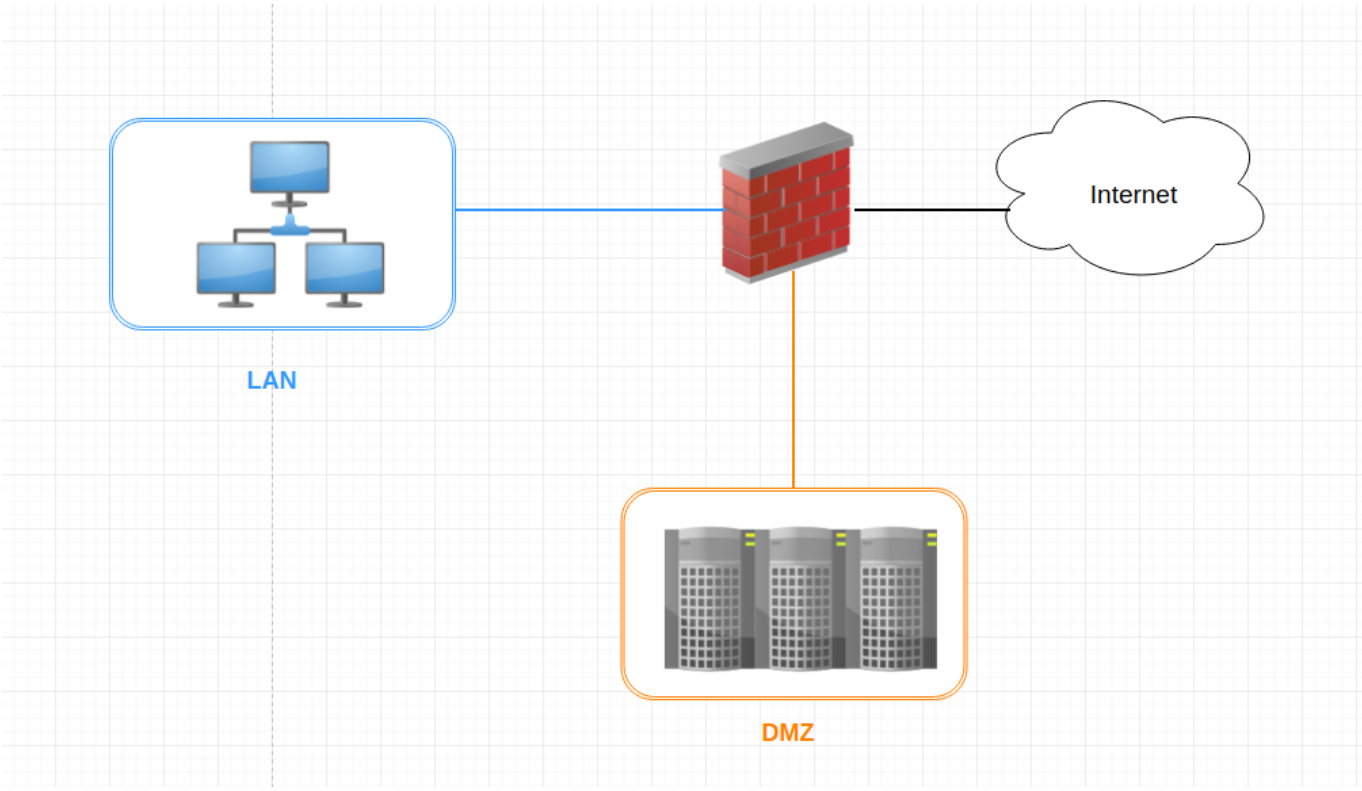
Configuration d'un DMZ

Un DMZ est un réseau ou sous-réseau distinct et isolé du réseau local et d'Internet par un parefeu.

> Les pare-feu sont utilisés comme moyen de prévenir ou de minimiser les risques de sécuritéinhérents à la connexion à d'autres réseaux.
> Un pare-feu correctement configuré joue un rôle clé dans le déploiement efficace et sécurisé del'infrastructure réseau.
> En cas de compromission d'un des services dans le dmz le pirate n'aura accès qu'aux machines de la dmz et non au réseau local

Donc pour mes configuration, je dois utiliser un seul firewall avec 3 interfaces réseau: LAN, DMZ et WAN

> - Le trafic initié dans le LAN avec la destination DMZ ou WAN doit être autorisé, ainsi que la réponse DMZ ou WAN au LAN
> - Le trafic initié dans la DMZ avec la destination LAN doit être refusé. Ne doit être autorisé que s'il existe une règle autorisant cette connexion initiée sur DMZ.



Inconvénient: cette architecture tombera si cette unique firewall est compromis.

Conseils: Pour une architecture plus sécurisée, on peut utiliser 2 firewalls pour créer une DMZ.

> 1- Cette architecture laisse passer uniquement le trafic vers la DMZ
> 2- N'autorise que les trafic entre la DMZ et le réseau interne.

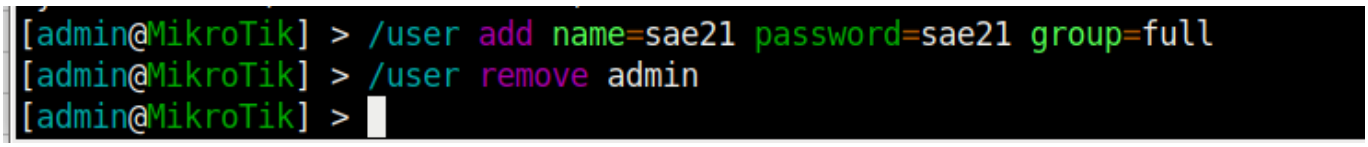
- Le pirate doit pouvoir compromettre deux machines pour accéder au lan interne.

Configuration

Accès au nom d'utilisateur

Modifiez l'administrateur du nom d'utilisateur par défaut en un nom personnalisé ou différent qui aide à protéger l'accès au routeur, si quelqu'un accède directement au routeur.

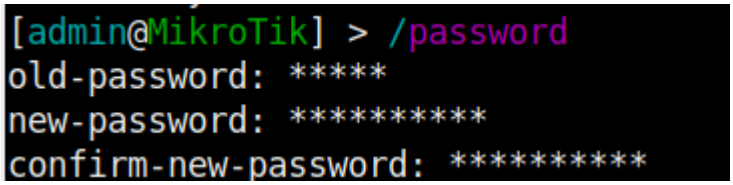
```
/ user add name = myname password = mypassword group = full
/ user remove admin
```



> L'option pour définir un mot de passe est:

```
/password
```

Il est préférable d'utiliser un mot de passe au routeur afin de le protéger contre les accès non autorisés.



> ***Activez le Safe Mode***:

- Il n'y a aucun moyen d'annuler la dernière modification lorsque la connexion au routeur est déjà coupée.Le mode sans échec peut être utilisé pour minimiser ce risque. Donc toutes vos modifications sont effectuées normalement. Il permet de frapper CTRL+Z si vous avez vraiment raté quelque chose
- Sur la ligne de commande, on l'active comme suit:

```
[admin@MikroTik] route IP>
[CTRL]+[X]
[Mode sans échec pris]
[admin@MikroTik] route ip<SAFE>
```

> *Le mode sans échec est entré en simplifié sur [CTRL] + [X].
> *Pour enregistrer les modifications et quitterle mode sans échec, appuyez à nouveau sur [CTRL] + [X].
> *Pour quitter sans enregistrer les modifications médiocres, appuyez sur [CTRL] + [D]

Autoriser les connexions établies et associées

> - Pour réduire la charge sur le processeur central du routeur

```
/ip firewall filter add action=accept chain=inputconnection-
state=established,related comment="Rule #0 \"Trusted\": allowestablished, related
connections.
```

Supprimer les packages non valides

```
/ip firewall filter add chain=input action=drop connection-
state=invalidcomment="Chain: Input. Rule #1 \"Drop Invalid Packet\": drop packets
connectionstate: invalid."
```

Autoriser ICMPRègle «ICMP»

> - Autorise le trafic ICMP vers le périphérique.

```
/ip firewall filter add chain=input protocol=icmp action=accept
comment="Chain:Input. Rule #3 \"ICMP\": accept icmp packets."Autoriser le port
Winbox/ip firewall filter add chain=input protocol=tcp dst-port=30122
action=accept comment="Chain: Input. Rule #10\"Winbox\": accept Winbox port
connections."
```

Supprimer les connexions non autorisées

> - Règle «Drop all» – nous supprimerons toutes les connexions qui n'étaient pas autorisées auparavant et qui ne sont pas incluses dans la liste des interfaces (internes) de confiance (Interfacesinternes).

```
/ip firewall filter add action=drop chain=input in-interface-
list=!InternalInterfacescomment="Chain: Input. Rule #15 \"Drop All\": drop_all
packets that do not meet the earlyconditions, except from trusted interfaces."
```

Placez la règle à la dernière position dans les règles de Firewall ***FilterRules***.

> Le script ci-dessous n'autorisera que des adresses IP spécifiques à accéder aux écrans deconnexion de configuration du routeur

```
/ip firewall address-listadd address=123.123.14.254 disabled=no list=supportadd
address=123.123.14.1 disabled=no list=Routers

/ip firewall filteradd action=drop chain=input\protocol=tcp dst-
port=21,22,23,80,8291 dst-address-list=Routerssrc-address-list=!support
comment="Block Client Router Access"disabled=yes

/tool mac-serverset [ find default=yes ] disabled=yesadd disabled=yes
```

```
interface=bridge
/tool mac-server mac-winboxset [ find default=yes ] disabled=yesadd disabled=yes
interface=bridge
/tool mac-server pingset enabled=no
```

```
[admin@MikroTik] > ip firewall address-list
[admin@MikroTik] /ip firewall address-list> add address=123.123.14.254 disabled=no list=support
[admin@MikroTik] /ip firewall address-list> add address=123.123.14.1 disabled=no list=Routers
[admin@MikroTik] /ip firewall address-list>
```

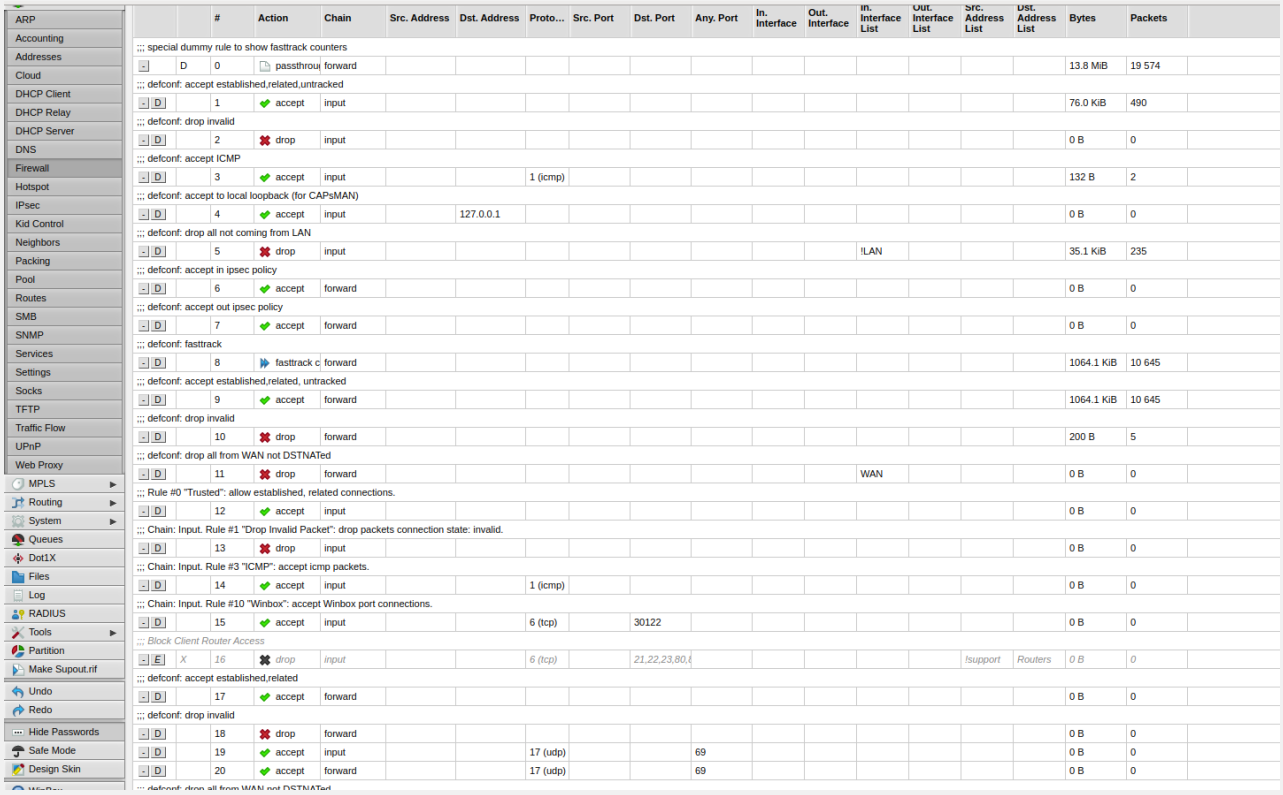
> ***Voici le script des règles essentielles du pare-feu qui vous aideront à protéger votre routeur***

```
/ip firewall address-list
add address=0.0.0.0/8 comment="Self-Identification [RFC 3330]" list=Bogons
add address=10.0.0.0/8 comment="Private[RFC 1918] - CLASS A # Check if you nee\
 d this subnet before enable it" list=Bogons
add address=127.0.0.0/8 comment="Loopback [RFC 3330]" list=Bogons
add address=169.254.0.0/16 comment="Link Local [RFC 3330]" list=Bogons
add address=172.16.0.0/12 comment="Private[RFC 1918] - CLASS B # Check if you \
 need this subnet before enable it" list=Bogons
add address=192.0.2.0/24 comment="Reserved - IANA - TestNet1" list=Bogons
add address=192.88.99.0/24 comment="6to4 Relay Anycast [RFC 3068]" list=\
 Bogons
add address=198.18.0.0/15 comment="NIDB Testing" list=Bogons
add address=198.51.100.0/24 comment="Reserved - IANA - TestNet2" list=Bogons
add address=203.0.113.0/24 comment="Reserved - IANA - TestNet3" list=Bogons
add address=224.0.0.0/4 comment=\
 "MC, Class D, IANA # Check if you need this subnet before enable it" \
 list=Bogons
/ip firewall filter
add action=accept chain=forward comment="defconf: accept established,related" \
    connection-state=established,related
add action=drop chain=forward comment="defconf: drop invalid" \
    connection-state=invalid
add action=accept chain=input port=69 protocol=udp
add action=accept chain=forward port=69 protocol=udp
add action=drop chain=forward comment=\
    "defconf:  drop all from WAN not DSTNATed" connection-nat-state=!dstnat \
    connection-state=new in-interface=ether1
add action=drop chain=forward comment="Drop to bogon list" dst-address-list=\
 Bogons
add action=accept chain=input protocol=icmp
add action=accept chain=input connection-state=established
add action=accept chain=input connection-state=related
add action=drop chain=input in-interface=ether1
```

Si vous obtenez une erreur lors du chargement du script, remplacez le nom de l'interface dans le script par le nom attribué à l'interface WAN de votre routeur.

```
[admin@MikroTik] /ip firewall address-list<SAFE> /
[admin@MikroTik] <SAFE> /ip firewall address-list
[admin@MikroTik] /ip firewall address-list<SAFE> add address=123.123.14.254 disabled=no list=support
[admin@MikroTik] /ip firewall address-list<SAFE> add address=123.123.14.1 disabled=no list=Routers
[admin@MikroTik] /ip firewall address-list<SAFE> /
[admin@MikroTik] <SAFE> /ip firewall filter
[admin@MikroTik] /ip firewall filter<SAFE> add action=drop chain=input\
\... protocol=tcp dst-port=21,22,23,80,8291 dst-address-list=Routers  src-address-list=!support comment="Block Client Router Access" disabled=yes
[admin@MikroTik] /ip firewall filter<SAFE> /
[admin@MikroTik] <SAFE> /ip firewall address-list
[admin@MikroTik] /ip firewall address-list<SAFE> add address=0.0.0.0/8 comment="Self-Identification [RFC 3330]" list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=10.0.0.0/8 comment="Private[RFC 1918] - CLASS A # Check if you nee\
"\...  d this subnet before enable it" list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=127.0.0.0/8 comment="Loopback [RFC 3330]" list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=169.254.0.0/16 comment="Link Local [RFC 3330]" list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=172.16.0.0/12 comment="Private[RFC 1918] - CLASS B # Check if you \
"\...  need this subnet before enable it" list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=192.0.2.0/24 comment="Reserved - IANA - TestNet1" list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=192.88.99.0/24 comment="6to4 Relay Anycast [RFC 3068]" list=\
\...  Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=198.18.0.0/15 comment="NIDB Testing" list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=198.51.100.0/24 comment="Reserved - IANA - TestNet2" list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=203.0.113.0/24 comment="Reserved - IANA - TestNet3" list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> add address=224.0.0.0/4 comment=\
\...  "MC, Class D, IANA # Check if you need this subnet before enable it" \
\...  list=Bogons
[admin@MikroTik] /ip firewall address-list<SAFE> /ip firewall filter
[admin@MikroTik] /ip firewall filter<SAFE> add action=accept chain=forward comment="defconf: accept established,related" \
\...     connection-state=established,related
[admin@MikroTik] /ip firewall filter<SAFE> add action=drop chain=forward comment="defconf: drop invalid" \
\...     connection-state=invalid
[admin@MikroTik] /ip firewall filter<SAFE> add action=accept chain=input port=69 protocol=udp
[admin@MikroTik] /ip firewall filter<SAFE> add action=accept chain=forward port=69 protocol=udp
[admin@MikroTik] /ip firewall filter<SAFE> add action=drop chain=forward comment=\
\...     "defconf:  drop all from WAN not DSTNATed" connection-nat-state=!dstnat \
\...     connection-state=new in-interface=ether1
[admin@MikroTik] /ip firewall filter<SAFE> add action=drop chain=forward comment="Drop to bogon list" dst-address-list=\
\...  Bogons
[admin@MikroTik] /ip firewall filter<SAFE> add action=accept chain=input protocol=icmp
[admin@MikroTik] /ip firewall filter<SAFE> add action=accept chain=input connection-state=established
[admin@MikroTik] /ip firewall filter<SAFE> add action=accept chain=input connection-state=related
[admin@MikroTik] /ip firewall filter<SAFE> add action=drop chain=input in-interface=ether1
[admin@MikroTik] /ip firewall filter<SAFE>
[admin@MikroTik] /ip firewall filter<SAFE>
```

Dans le web config on verra :



	#	Action	Chain	Src. Address	Dst. Address	Proto…	Src. Port	Dst. Port	Any. Port	In. Interface	Out. Interface	In. Interface List	Out. Interface List	Src. Address List	Dst. Address List	Bytes	Packets
;;; special dummy rule to show fasttrack counters																	
D	0	passthrou	forward													13.8 MiB	19 574
;;; defconf: accept established,related,untracked																	
D	1	accept	input													76.0 KiB	490
;;; defconf: drop invalid																	
D	2	drop	input													0 B	0
;;; defconf: accept ICMP																	
D	3	accept	input			1 (icmp)										132 B	2
;;; defconf: accept to local loopback (for CAPsMAN)																	
D	4	accept	input		127.0.0.1											0 B	0
;;; defconf: drop all not coming from LAN																	
D	5	drop	input									!LAN				35.1 KiB	235
;;; defconf: accept in ipsec policy																	
D	6	accept	forward													0 B	0
;;; defconf: accept out ipsec policy																	
D	7	accept	forward													0 B	0
;;; defconf: fasttrack																	
D	8	fasttrack c	forward													1064.1 KiB	10 645
;;; defconf: accept established,related, untracked																	
D	9	accept	forward													1064.1 KiB	10 645
;;; defconf: drop invalid																	
D	10	drop	forward													200 B	5
;;; defconf: drop all from WAN not DSTNATed																	
D	11	drop	forward									WAN				0 B	0
;;; Rule #0 "Trusted": allow established, related connections.																	
D	12	accept	input													0 B	0
;;; Chain: Input. Rule #1 "Drop Invalid Packet": drop packets connection state: invalid.																	
D	13	drop	input													0 B	0
;;; Chain: Input. Rule #3 "ICMP": accept icmp packets.																	
D	14	accept	input			1 (icmp)										0 B	0
;;; Chain: Input. Rule #10 "Winbox": accept Winbox port connections.																	
D	15	accept	input			6 (tcp)		30122								0 B	0
;;; Block Client Router Access																	
E	X 16	drop	input			6 (tcp)		21,22,23,80,8						!support	Routers	0 B	0
;;; defconf: accept established,related																	
D	17	accept	forward													0 B	0
;;; defconf: drop invalid																	
D	18	drop	forward													0 B	0
D	19	accept	input			17 (udp)			69							0 B	0
D	20	accept	forward			17 (udp)			69							0 B	0
;;; defconf: drop all from WAN not DSTNATed																	

Un plus de détails:

Etape 1

– Supprimer tout filtrage existant sur notre routeur.

Etape 2
– Mettre en place la politique par défaut qui consiste à tout bloquer sauf sorties du routeur

On bloque toutes trames traversant le routeur:

```
/ip firewall filter
add action=drop chain=forward comment="defconf: drop invalid" \connection-
state=invalid
```

On bloque toutes trames entrant dans le routeur:

```
/ip firewall filter
add action=drop chain=input
```

On accepte les trames sortant du routeur:

```
/ip firewall filter
add action=accept chain=output
```

Etape 3
– Autoriser le Trafic établi Le trafic établi est la réponse aux trames déjà existantes, il est important de l'autoriser. Accepter les trames établies pour toutes trames traversant, entrant ou sortant du routeur :

```
/ip firewall filter
add action=accept chain=forward comment="defconf: accept established,related"
\connection-state=established,related
add action=drop chain=forward comment="defconf: drop invalid" \connection-
state=invalid
add action=accept chain=input protocol=icmp
add action=accept chain=input connection-state=establishedadd action=accept
chain=input connection-state=relatedadd action=drop chain=input in-
interface=ether1
```

Etape 4
– Nouvelle règle : le LAN parle vers la DMZ et le LAN parle vers le WAN L'objectif est d'autoriser toutes les trames sortant du LAN afin qu'elles puissent communiquer avec toutes les zones de notre situation initiale. Accepter les trames traversant le routeur en provenance d'ether1 (LAN) :

```
add action=drop chain=forward comment=\"defconf:  drop all from WAN not DSTNATed"
connection-nat-state=!dstnat \connection-state=new in-interface=ether1
```

Etape 5
– Règle : le LAN parle au routeur Le but est d'autoriser le dialogue avec le routeur. (ex : administration du routeur) Accepter les trames en entrée du LAN vers le routeur :

```
add action=drop chain=input in-interface=ether1
```

Etape 6
– Règle : la DMZ parle vers le WAN Quand le serveur web aura besoin d'aller sur internet il pourra envoyer des paquets sur ce dernier, ce qui n'était pas possible auparavant. Accepter les trames en sortie du DMZ en direction du WAN (internet) :

```
add action=accept chain=forward comment="accept dmz to wan" \
```

Etape 7
– Règle : Autoriser les trames du WAN vers le Serveur WEB Quand le serveur web envoie des paquets il faut que le destinataire lui réponde, c'est pour cela qu'il est important que ce paramètre soit ajouté au script. Autoriser les trames traversant du WAN vers la DMZ ayant comme port 80 pour aller en direction du serveur web :

```
add action=accept chain=forward port=80 protocol=tcp
```

Etape 8
– Règle : Autoriser l'accès au serveur DNS depuis le serveur WEB Cela permettra au serveur web de pouvoir bénéficier de la résolution de noms proposée par le serveur. Filtrer et accepter toutes les trames traversant de la DMZ vers le LAN ayant comme port 53 via le protocole UDP :

```
add action=accept chain=forward port=80 protocol=tcp
```

Etape 9
- Les bogons

```
/ip firewall address-list
add address=0.0.0.0/8 comment="Self-Identification [RFC 3330]" list=Bogons
add address=10.0.0.0/8 comment="Private[RFC 1918] - CLASS A # Check if you nee\
 d this subnet before enable it" list=Bogons
add address=127.0.0.0/8 comment="Loopback [RFC 3330]" list=Bogons
add address=169.254.0.0/16 comment="Link Local [RFC 3330]" list=Bogons
add address=172.16.0.0/12 comment="Private[RFC 1918] - CLASS B # Check if you \
 need this subnet before enable it" list=Bogons
add address=192.0.2.0/24 comment="Reserved - IANA - TestNet1" list=Bogons
add address=192.88.99.0/24 comment="6to4 Relay Anycast [RFC 3068]" list=\
 Bogons
```

```
add address=198.18.0.0/15 comment="NIDB Testing" list=Bogons
add address=198.51.100.0/24 comment="Reserved - IANA - TestNet2" list=Bogons
add address=203.0.113.0/24 comment="Reserved - IANA - TestNet3" list=Bogons
add address=224.0.0.0/4 comment=\
 "MC, Class D, IANA # Check if you need this subnet before enable it" \
 list=Bogons

add action=drop chain=forward comment="Drop to bogon list" dst-address-list=\
 Bogons
```

J'ai bloqué les bogons parce que les adresses IP Bogon sont populaires dans les activités de piratage ou malveillantes et sont utilisées par les spammeurs et ceux qui lancent des attaques par déni de service distribuées.