Seguridad en Tiempos Difíciles

Protección de Redes de datos v1

Costa Rica - 20 Julio 2018

Robert Delgado Reinoso - XTERCOM SRL

Robert Delgado Reinoso

Consultor Certificado Mikrotik

Fundador XTERCOM SRL,
República Dominicana

Experiencia Mikrotik desde 2012

Certificaciones Mikrotik

MTCNA | MTCRE | MTCTCE | MTCINE

XTERCOM
DATA CARRIER EXPERTS

Integradores de Soluciones de TI:

- Centrales Telefónicas IP
- Enlaces PtP/PtMP
- VPN Site to Site
- Transporte de Datos
- Fibra óptica

@ robert@xtercom.net
@robertdelgado
fb.me/robertdelgadoreinoso

"La desconfianza es la madre de la seguridad."
Aristófanes

Los dispositivos Mikrotik recién sacados de la caja, al igual que otras marcas, requieren un endurecimiento de la seguridad para reducir las posibilidades de que sean comprometidos una vez conectados a la red.

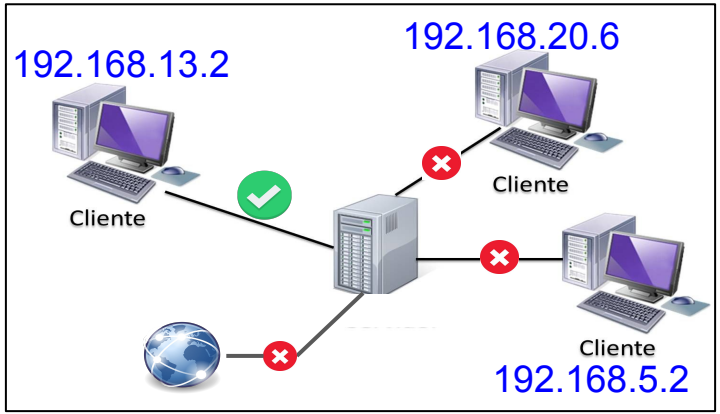
Algunas cambios básicos pueden ser implementados de inmediato para reducir la posibilidad de ser vulnerados mientras se aplican mejores implementaciones de seguridad en nuestro dispositivo.

El acceso al Router debe ser restringido a las áreas o subredes que tiene este privilegio.

Cuando encienda el equipo haga esto:

- Crear un Nuevo Usuario y con su contraña
- Eliminar/Deshabilitar Usuario “admin”
- Deshabilitar MAC Server y Discovery en Interfaces Innecesarias
- Deshabilite los servicios que no utiliza en ip->services
- Actualizar RouterOS
  - Es de suma importancia mantener su sistema actualizado
- No comparta su clave 

Permita el acceso a puertos deseados, puede usar una VLAN o Interfaz de administración.



Crear Address List con direcciones Permitidas

/ip firewall address-list

add address=192.168.13.0/24 list=IT_Depto

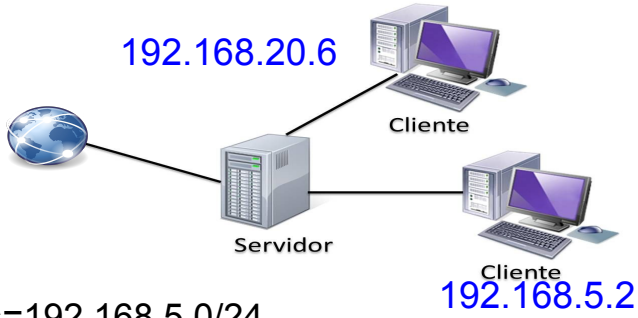
Permita puertos deseados, no deje el campo **dst-port** vacío.

ip firewall filter
add action=accept chain=input disabled=no in-interface=**ether3 dst-port**=22,8291 protocol=tcp \
src-address-list=**IT_Depto**

add action=drop chain=input comment="Drop All" disabled=no

ip service set address=192.168.13.0/24 winbox

Bloqueo de Hosts y Subredes



ip firewall filter

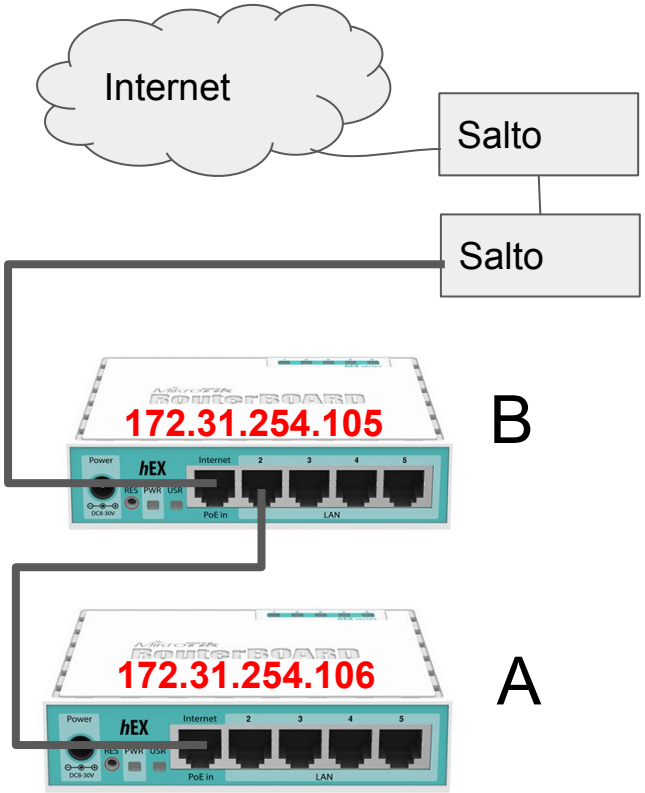
add action=drop chain=**forward** dst-address=192.168.20.0/24 src-address=192.168.5.0/24

#Bloquear a host de una red hablar con hosts de otra red

add action=drop chain=**input** dst-address=192.168.20.0/24 src-address=192.168.5.0/24

add action=drop chain=**input** dst-address=192.168.5.0/24 src-address=192.168.20.0/24

#previene que host hablen con puertas de enlaces contrarias



Traceroute

Traceroute To:	1.1.1.1
Packet Size:	56
Timeout:	1000
Protocol:	icmp
Port:	33434
	Use DNS
Count:	
Max Hops:	
Src. Address:	
Interface:	
DSCP:	
Routing Table:	

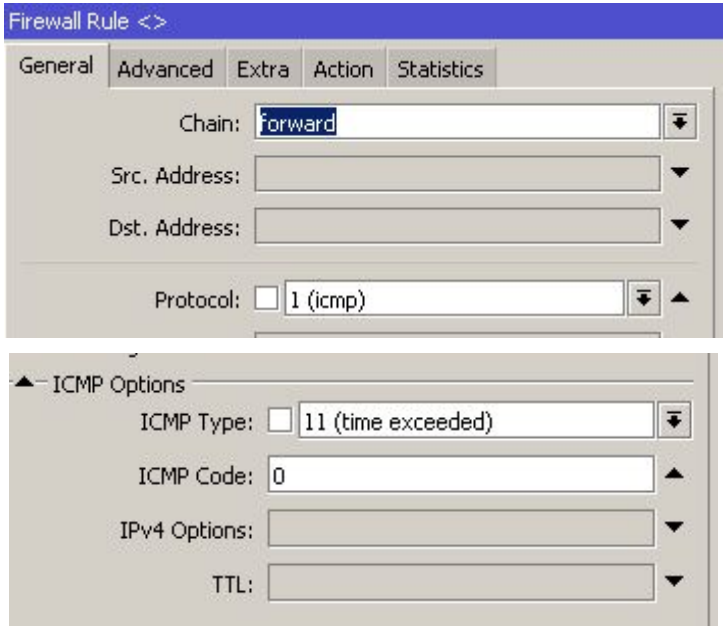
Hop	Host	Loss	Sent	Last
1	172.31.254.105	0.0%	2	0.1ms
2	190.6.140.1	0.0%	2	1.6ms
3	172.17.254.243	0.0%	2	4.0ms
4	172.17.255.57	0.0%	2	3.5ms
5	172.17.255.162	0.0%	2	3.8ms
6	172.17.255.161	0.0%	2	3.8ms
7	172.17.22.200	0.0%	2	4.3ms
8	172.17.255.158	0.0%	2	44.5ms
9	172.17.255.182	0.0%	2	42.1ms
10	80.239.160.174	0.0%	2	53.6ms
11	1.1.1.1	0.0%	1	41.6ms

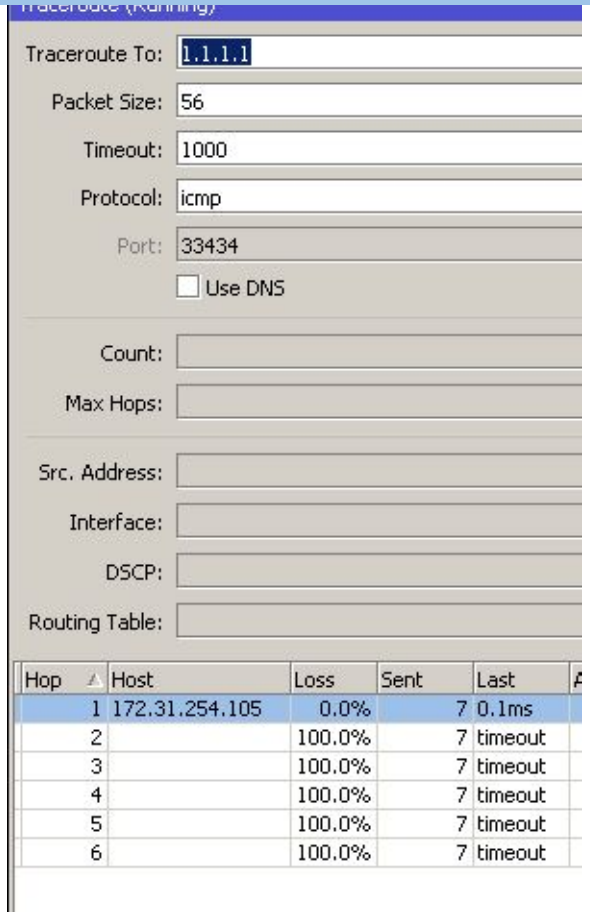
Ocultando saltos

TRACEROUTE REALIZADO DESDE ROUTER A

Ocultando Saltos

ip firewall filter
add action=accept chain=forward icmp-options=11:0 protocol=icmp

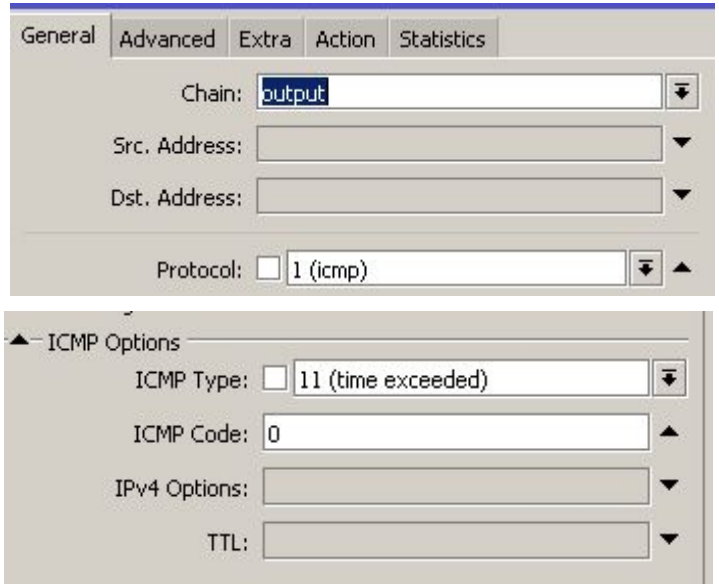


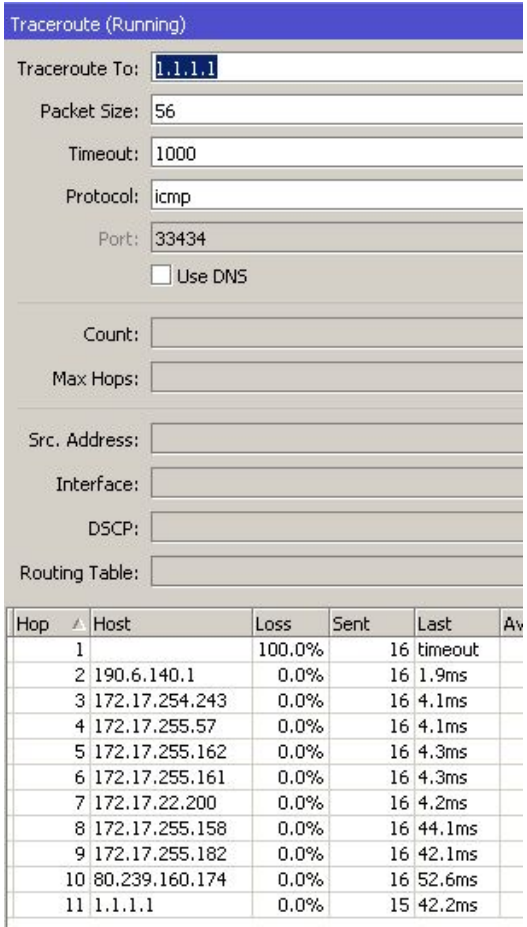


Ocultamiento de los hops después del Router

Ocultamiento de hops

ip firewall filter
add action=accept chain=output icmp-options=11:0 protocol=icmp





Hop	Host	Loss	Sent	Last	Av
1		100.0%	16	timeout	
2	190.6.140.1	0.0%	16	1.9ms	
3	172.17.254.243	0.0%	16	4.1ms	
4	172.17.255.57	0.0%	16	4.1ms	
5	172.17.255.162	0.0%	16	4.3ms	
6	172.17.255.161	0.0%	16	4.3ms	
7	172.17.22.200	0.0%	16	4.2ms	
8	172.17.255.158	0.0%	16	44.1ms	
9	172.17.255.182	0.0%	16	42.1ms	
10	80.239.160.174	0.0%	16	52.6ms	
11	1.1.1.1	0.0%	15	42.2ms	

Ocultamiento del Router visualizando los hops detras de este puede agregar un DROP al ICMP completo para que el router no repsonda a Ping

Restricción de Acceso basado en el Pais de Origen de la Dirección IP.

Escenario: ¿Cuando se conecta de forma remota a su Router / Red con o sin VPN, lo hace desde los servicios de Internet de su Pais, por que responde peticiones a direcciones IP de Origen en Otro punto de la Geografia global distinto al suyo?

Creamos un Address List con los CIDR que queremos filtrar y los Filtros de firewall.

ip firewall filter

1 - add chain=**input** in-interface=ether1 src-address-list=**GeoIP_list** action=**accept**
2 - add chain=**forward** in-interface=ether1 src-address-list=**GeoIP_list** action=**accept**
3 - add chain=**input** in-interface=ether1 action=**drop**

1 = Destinado al Router | 2 = Destinado a la redes detras del router (Ej: Port Forward)
3 = Drop a Todo lo que entre por ether1 (WAN)

Creando los Address List con los CIDR para GeoIP

En Internet hay Muchos recursos con los cuales podemos obtener los CIDR de los Países, Regiones y provincias que podemos agregar a nuestros address list según la necesidad y el escenario que tengamos.

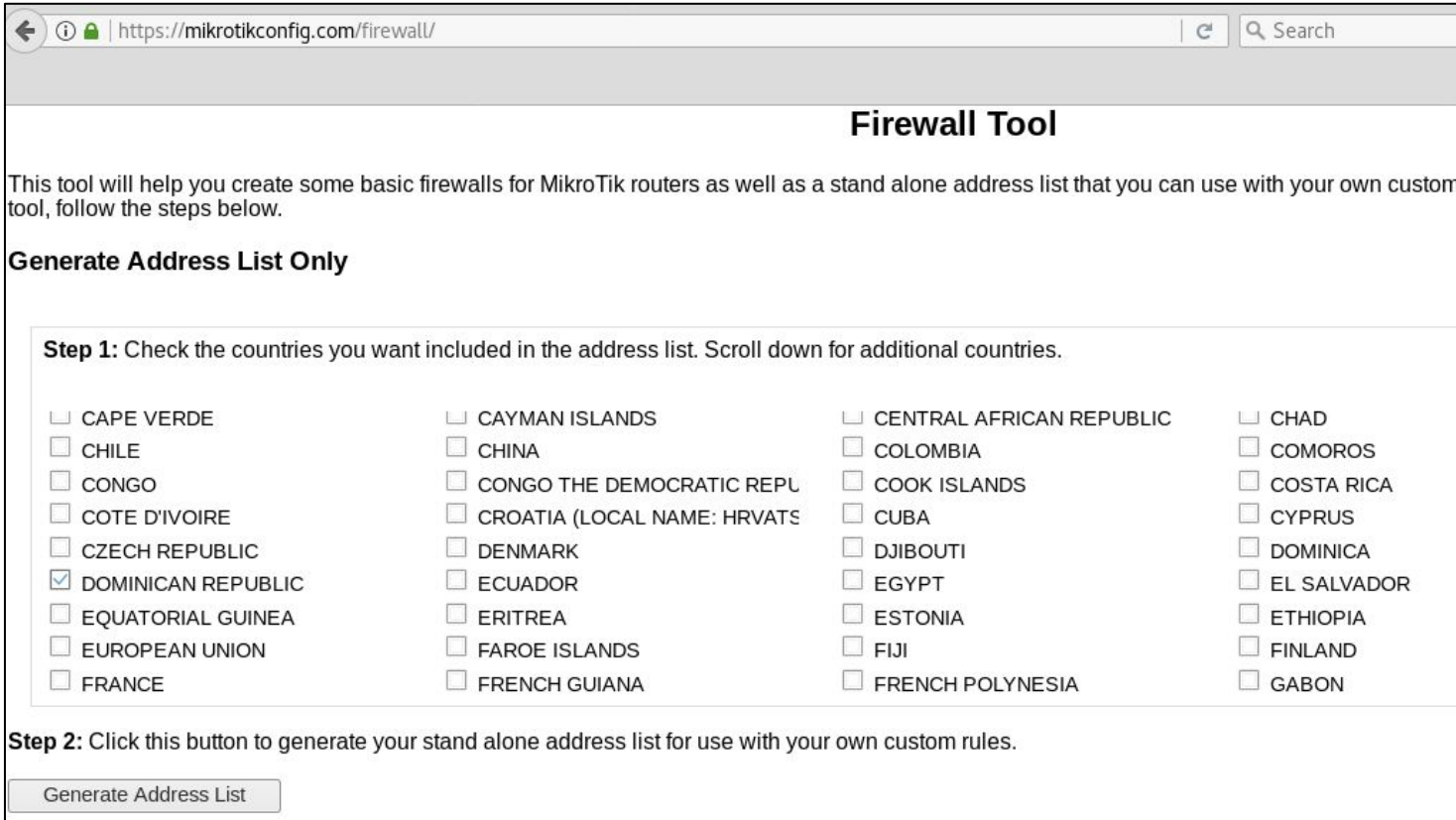
Hay sitios que ofrecen los Address List para Mikrotik ya Generados para que solo debas importarlo a RouterOS y Otros sitios que Ofrecen una Base de datos en Formato TXT o CSV que para algunos casos están mejor actualizados script ya realizados (Generalmente de pago).

Estas Bases de datos de Direcciones IP pueden ser adquiridas de forma gratuita o de pago, dependiendo de la necesidad que desea cubrir puede elegir la opción más conveniente, Bloques de IP por Pais, Region, Provincia, etc, pues con esas bases de datos puede realizar desde restricción de acceso hasta ofrecer ciertas rutas u contenido distinto para usuarios que procedan desde cierto punto geográfico, filtrado en base a su dirección IP de Origen.

Creando los Address List con los CIDR para GeoIP

Elegimos los Paises que deseamos incluir a nuestra lista y luego damos Clic en **Generate Address List.**

Se Descargará un **archivo.rsc** que solo debe importar a su RouterOS.



Address List con CIDR

Open | IP-Firewall-Address-List.rsc | /tmp/mozilla_root0 | Sa

```
/ip firewall address-list
add address=205.233.76.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=64.32.64.0/18 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=66.98.0.0/18 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=66.98.64.0/19 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=131.221.4.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=138.36.24.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=138.97.248.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=138.99.236.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=138.255.248.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=143.0.24.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=143.137.80.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=143.208.164.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=148.0.0.0/16 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=148.101.0.0/16 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=148.103.0.0/16 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=148.255.0.0/16 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=152.0.0.0/16 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=152.166.0.0/15 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=179.43.192.0/18 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=179.49.80.0/20 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=179.51.64.0/20 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=179.52.0.0/15 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=181.36.0.0/15 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
add address=181.224.168.0/22 comment="DOMINICAN REPUBLIC" list=CountryIPBlocks
```

En el archivo descargado, se indica por defecto que los CIDR se agregará al **Address List** Llamado **CountryIPBlocks,** en el comentario de cada linea Agrega el Nombre del Pais que pertenece el CIDR.

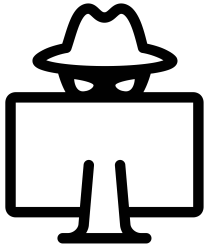
Estos datos pueden ser modificados a su conveniencia de forma masiva con un editor de texto, por ejemplo, el **list=CountryIPBlocks** podemos reemplazarlo por **list=GeoIP_list**, siendo esta última la lista utilizada en nuestros ejemplos anteriores.

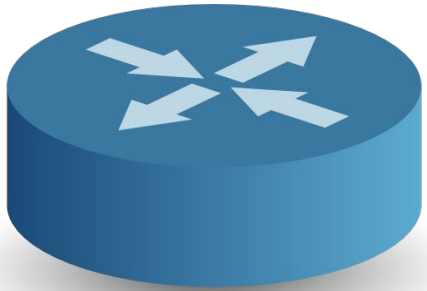
Port Knoking

= DROP

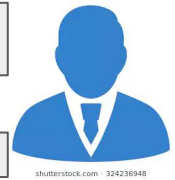
TCP 22

TCP 9000





TCP/7000 - TCP/8000 - TCP/9000



TCP/22, TCP/8291

La estrategia del port knocking se basa en detectar una conexión a un puerto y agregarlo a un address List temporal, luego detecta una conexión a un segundo puerto y verifica si la IP de origen está en el primer address List y lo coloca en un segundo Address List temporal también, Luego Detecta una conexión a un tercer puerto y verifica si la IP esta en la segunda lista y lo agrega a un address List Definitivo por tiempo limitado si así se desea.

ip firewall filter

Aceptar conexiones a puertos TCP 22, TCP 8291 a quien supere el Port Knoking.
add action=accept chain=input src-address-list=portknock-3 protocol=tcp dst-port=22,8291

3ra Etapa, una vez tocado el TCP 9000 se agrega por 1 hora a Address List que es tomado en cuenta arriba
add action=add-src-to-address-list address-list=portknock-3 address-list-timeout=1h chain=input **dst-port=9000** \
in-interface=ether1 protocol=tcp src-address-list=portknock-2

2ra Etapa, Quien superó la primera etapa y golpea el TCP 8000 se agrega por 10s a un address List.
add action=add-src-to-address-list address-list=portknock-2 address-list-timeout=10s chain=input **dst-port=8000** \
in-interface=ether1 protocol=tcp src-address-list=portknock-1

1ra Etapa, quien toque el TCP 7000 es agregado a un address List por 10s, este puede avanzar a la 2da etapa.
add action=add-src-to-address-list address-list=portknock-1 address-list-timeout=10s chain=input **dst-port=7000** \
in-interface=ether1 protocol=tcp

Drop a todo lo que entre por la WAN
add chain=**input** in-interface=ether1 action=**drop**

- Reducir timeouts en address lists
- Combinar otros Protocolos, UDP/ICMP

Brinda mejor protección

Prevención de ataques de fuerza bruta

Estrategia

- Capturar cada nueva conexión hacia un determinado puerto del Router

  Agregando a un address list temporal la IP del host que realiza una conexión por cada intento de login, fallido o no, al completar 4 intento se agrega a un blacklist donde se hace drop por 15 dias.
  Ejemplo: Winbox, SSH, Web, otros

- Para servicios de texto plano, se puede capturar textualmente la respuesta del router en el intento de Login, capturando explícitamente el texto respondido por el Router al host y tomando una decisión al respecto. Es recomendable limitar la cantidad de conexiones por minutos realizadas.
  Ejemplo: FTP, Telnet

Podemos hacer que los atacantes que figuren en un BlackList, no puedan realizar conexiones con los clientes, cambiando el Chain Input por forward en el Router.

Capturando cada Nueva Conexion

#Ejemplo con Winbox.
/ip firewall filter

add chain=input protocol=tcp dst-port=8291 **src-address-list=winbox_blacklist** action=drop \
comment="Drop Winbox brute forcers" disabled=no

add chain=input protocol=tcp dst-port=8291 connection-state=new src-address-list=winbox_login3 \
action=**add-src-to-address-list address-list=winbox_blacklist** address-list-timeout=15d disabled=no

add chain=input protocol=tcp dst-port=8291 connection-state=new src-address-list=winbox_login2\
action=**add-src-to-address-list address-list=winbox_login3** address-list-timeout=1m disabled=no

add chain=input protocol=tcp dst-port=8291 connection-state=new src-address-list=winbox_login1 \
action=a**dd-src-to-address-list address-list=winbox_login2** address-list-timeout=1m disabled=no

add chain=input protocol=tcp dst-port=8291 connection-state=new action=**add-src-to-address-list \
address-list=winbox_login1** address-list-timeout=1m disabled=no

Para Telnet

```
add chain=input protocol=tcp dst-port=23 src-address-list=telnet_blacklist action=drop \
comment="drop telnet brute forcers"
```

#Permite solo unos intentos de login por minuto

```
add chain=output action=accept protocol=tcp src-port=23 content="Login failed, incorrect username or password" dst-limit=3/1m,0,dst-address/1m

add chain=output action=add-dst-to-address-list src-port=23 protocol=tcp content="Login failed, incorrect username or password" \
address-list=telnet_blacklist address-list-timeout=3h
```

Para FTP, cambiar content="530 Login incorrect”

Gracias