Mikrotik Firewall

Securing Your Router With Port Knocking

Introduction

- Name : Akbar
- Mikrotik User Since : Mid 2005
- IT Manager @ Agung Sedayu Group
- Trainer For Ufoakses Mikrotik Training
- www.forummikrotik.com
- akbar@forummikrotik.com

What is Port Knocking ?

- Port Knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports
- Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host which sent the connection attempts to connect over specific port(s)

Port Knocking Process

Connection Attempt to Router with Winbox or Telnet or SSH

Connection Attempt Rejected / Drop

Knock : Connection Attempt to Pre **Defined Port**

Firewall Rules Dynamically Modified to Allow Access From That Host

Connection Attempt to Router with Winbox or Telnet or SSH

Connection Granted



Router with **Firewall**





Host

Why Port Knocking ?



 The primary purpose of port knocking is to prevent an attacker from scanning a system for potentially exploitable services by doing a port scan, because unless the attacker sends the correct knock sequence, the protected ports will appear closed.

When to Use Port Knocking ?



- When you need to do remote configuration or monitoring from remote area
- When you try to decrease brute force attack

How to Apply Port Knocking in Mikrotik ?



- Using :
 - Firewall Filter
 - Address List
 - Knock Application

Please download the application from : www.zeroflux.org



The Basic of Firewall Filter

Interfaces	-											
Wireless	Firewall											
Bridge	Filter Rules NAT 1	Mangle Ser	vice Ports C	onnections A	Address L	ists Layer7	Protocols					
PPP		0 7	I Recei	Counters	o Resel	All Counters						
		(ain	Stc. Address	Dst. Address	Proto	Src. Port	Dst. Port	In Inter	Out. Int	Bytes	Packets	
IP F	Addresses	ward								0		0
Routing	Routes	ward								0		0
Ports	Pool	input								0		0
Queues	ARP	input			17 (u		64872			0		0
Drivers	Frewall	input			6 (tcp)		64872-64			0		0
System 🗈	Socks	unauth			6 (tcp)					0		0
Files	UPnP	unauth			-					0	-	0
Log	Traffic Flow	unauth-to								0	8	0
SNMP	Accounting	used hs								0	B	0
Users	Services	N.			6 (tcp)		1337			64	В	1
Radius												
Tools	Packing											
	Neighbors											
New Terminal	DNS											
Teinet	Web Proxy											
Password	DHCP Client											
Certificates	DHCP Server											
Make Supout.nif	DHCP Relay											
Manual	Hotspot											
Exit	IPsec											

The Basic of Firewall Filter

- Firewall Filter is used for packet filtering
- Firewall Filter consist of IF-THEN rules
 IF <conditions> THEN <action>
- Firewall Filter is done in sequential top to bottom
- Firewall Filter are organized in chains

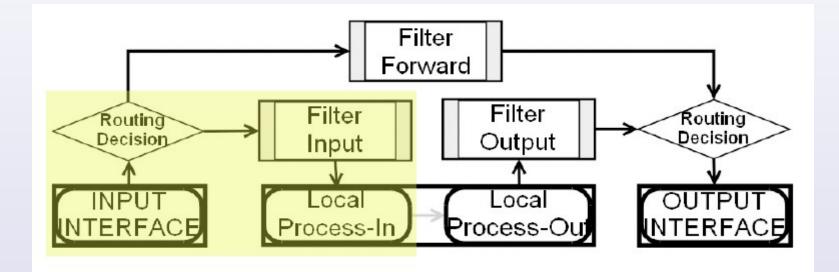
The Basic of Firewall Filter



- Input : Processes packets addressed to the router itself
- Output : Processes packets sent by the router itself
- Forward : processes traffic sent through the router

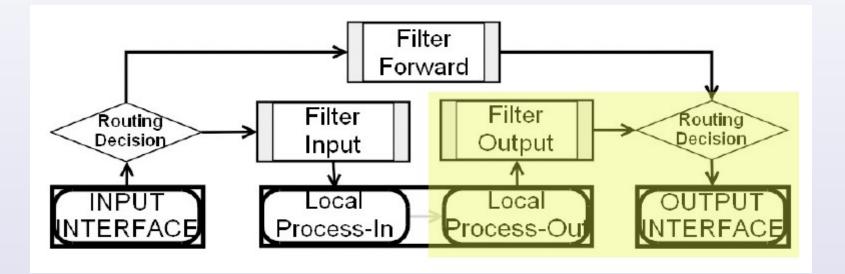
Chain Input





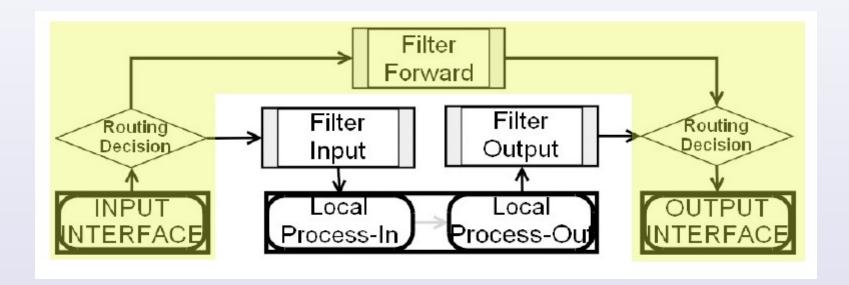
Chain Output







Chain Forward





Firewall Filter Action

- Accept accept the packet. No action is taken, I.e the packet is passed thourgh and no more rules applied to it
- Add-dst-to-address-list adds destination address of an IP packet to the address list specified by address-list parameter
- Add-src-to-address-list adds source address of an IP packet to the address list specified by address-list parameter
- **Drop** silently drop the packet (without sending the ICMP reject messege))
- Jump jump to the chain specified by the value of the jump-targetparameter
- Log each match with this action will add a messege to the system log
- Passthrogh ignores this rule and goes on the next one
- Reject reject the packet and send an ICMP reject messege
- **Return** passes control back to the chain where the jump took place
- **Tarpit** captures and hold incoming TCP connections (replies with SYN/ACK to the inbound TCP SYN packet



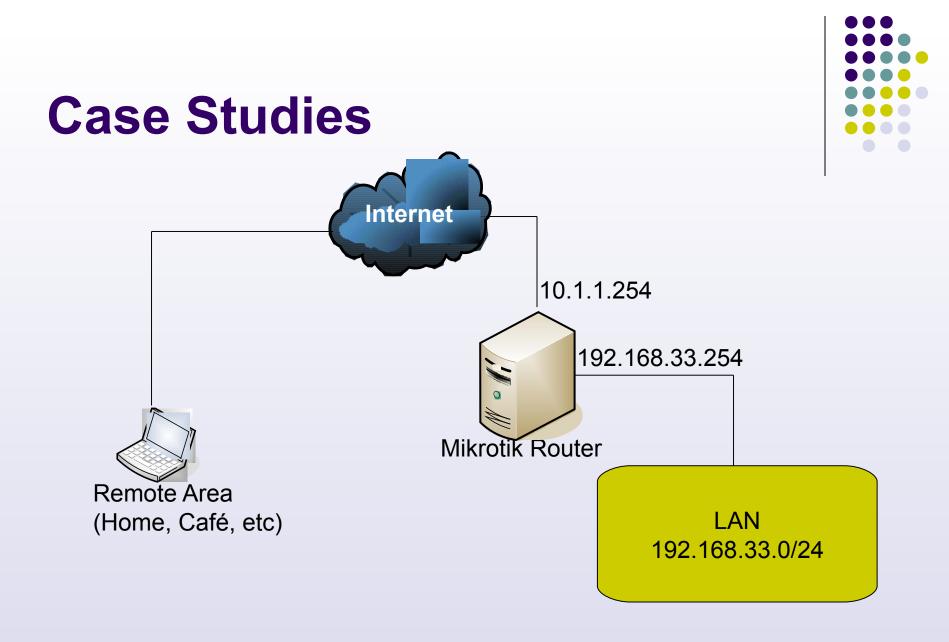
IP Address List

- You can also define group of IP address using "IP address List"
- IP address List can be used in Firewall Rules to apply certain action
- You can use mangle or firewall filter rule to dynamicly add IP address to IP address List certain time limit

Eirewall						×
Filter Rules NAT N	Mangle Service F	Ports	Connections	Address Lists		
+- ~ ×	<u>~</u>				all	⊡
Name 🔺	Address					~
 nice 	58.65.240.0/24					
 nice 	58.65.241.0/24					
 nice 	58.65.242.0/24					
 nice 	58.65.243.0/24		lew Firewa	ll Address Lis	t 🔀	
 nice 	58.65.244.0/24					
 nice 	58.65.245.0/24	Na	ame: nice	-	ок	
 nice 	58.65.246.0/24					
nice	58.65.247.0/24	Addr	ess: 0.0.0.0		Cancel	
nice	58.145.168.0/24				Analy	
nice	58.145.171.0/24				Apply	
nice	58.145.173.0/24					
nice	58.145.174.0/24				Enable	
 nice 	58.147.184.0/24				Comment	
nice	58.147.185.0/24				Common	
nice	58.147.186.0/24				Сору	
nice	58.147.187.0/24					
nice	58.147.188.0/24				Remove	
nice	60.253.96.0/24					
 nice 	60.253.97.0/24	disab	led			
nice	60.253.98.0/24					
 nice 	60.253.99.0/24					
nice	60.253.100.0/24					
nice	60.253.101.0/24 60.253.102.0/24					
nice nice	60.253.102.0/24 60.253.103.0/24					~
	160 /53 (03 0//4		1			



Let's Start Implementing Port Knocking in Mikrotik Router OS...



Case Studies



- We only allowed access to router only from several IP from LAN :
 - 192.168.33.10 Until 192.168.33.20
- Different IP from LAN have to knock first before gain access to router
- Remote area from Internet have to knock first before gain access to router

Case Studies



- We will only allowed access to router from address list named "Safe Haven"
- Other have to knock first to :
 - Protocol TCP, Port 1337
 - Protocol UDP, Port 17954

Adding Allowed LAN Address to Address List



🗖 New Firewall Address	List 🛛 🔀	🗖 Firewa	u				
Name: Save Haven Final Address Address: 10-192.168.33.20	List X OK Cancel Apply Disable Comment Copy	Filter Rules	NAT M	angle	Service Ports Y Address 192.168.33	Connections 10-192.168.33	ists Layer7 Protocols
disabled	Remove						

add address=192.168.33.10-192.168.33.20 comment="" disabled=no list=\ "Save Haven"

Knock Rules 1

🗖 New Firewall Rule		🗖 New Firewall Rule	
General Advanced Extra Action Statistics	ОК	General Advanced Extra Action Statistics	OK
Chain: input 🔻	Cancel	Action: add src to address list	Cancel
Src. Address:	Apply	Address List: knock-knock	Apply
Dst. Address:	Disable	Timeout: 00:00:15	Disable
Protocol: 🗌 6 (tcp) 🐺 🔺	Comment		Comment
Src. Port:	Сору		Сору
Dst. Port: 🗌 1337 🔺	Remove		Remove
Any. Port:	Reset Counters		
P2P:	Reset All Counters		
In. Interface: 📃 🔻			
Out. Interface:			

add action=add-src-to-address-list address-list=knock-knock address-listtimeout=15s chain=input comment="Knock 1" disabled=no dst-port=1337 protocol=tcp



Knock Rules 2

Tirewall Rule <17954>	X	Firewall Rule <17954>	X
General Advanced Extra Action Statistics	ОК	General Advanced Extra Action Statistics	ОК
Chain: input ∓	Cancel	Action: add src to address list	Cancel
Src. Address:	Apply	Address List: Save Haven	Apply
Dst. Address:	Disable	Timeout: 03:00:00	Disable
Protocol: 🗌 17 (udp) ∓ 🔺	Comment		Comment
Src. Port:	Сору		
Dst. Port: 17954	Remove		
Any. Port:	Reset Counters		
P2P:	Reset All Counters		
In. Interface: 📃 🔻			
Out. Interface:			

add action=add-src-to-address-list address-list="Save Haven" address-listtimeout=3h chain=input comment="Knock 2 - OK" disabled=no dst-port=17954 protocol=udp src-address-list=knock-knock

Only Allowing "Save Haven" to Connect to the router

$\bullet \bullet \bullet \bullet \bullet$

🗖 New Firewall Rule		🗖 New Firewall Rule	×
General Advanced Extra Action Statistics	ОК	General Advanced Extra Action Statistics	OK
Chain: input	Cancel	Src. Address List: 🖾 Save Haven 🔻 🔺 🛛	Cancel
Src. Address:	Apply	Dst. Address List:	Apply

🗖 New Firewall Rule 🛛 🔀							
General	Adv	anced	Extra	Action	Statistics		ОК
Ac	tion:	accept			₹		Cancel
							Apply

add action=accept chain=input comment="Only Allow Access from Save Haven" disabled=no src-address-list="Save Haven"



Drop Everything Else

🗖 Firewall Rule <>		
General Advanced Extra Action Statisti	cs OK	
Chain: input	Cancel	
Src. Address:	▼ Apply	
	🔲 Firewall Rule <>	
	General Advanced Extra Ac	tion Statistics
	Action: drop	₹



add action=drop chain=input comment="Drop Everything Else" disabled=no



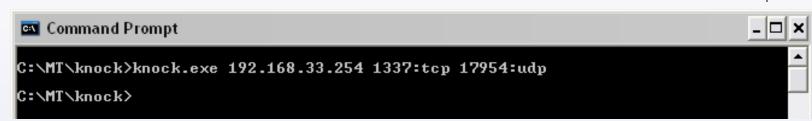
Configuration

T Firewall											
Filter Rules	NAT	Mangle	Service Ports	Connections	Address Li	sts Layer	7 Protocols				
+ -	</th <th></th> <th>🍸 🔚 Re</th> <th>set Counters</th> <th>oo Reset</th> <th>All Counter</th> <th>s</th> <th></th> <th></th> <th></th> <th></th>		🍸 🔚 Re	set Counters	oo Reset	All Counter	s				
# A	ction	Chain	Src. Addre	ss Dst. Addre	ss Proto	Src. Port	Dst. Port	In. Inter	Out. Int	Bytes	Packets
;;; Knock	1										
0 0	🕈 add	input			6 (top)		1337			64 B	1
;;; Knock	2-0K										
1 0	🕈 add	input			17 (u		17954			29 B	1
;;; Only A	llow Acc	ess from S	ave Haven								
2 •	🥖 acc	input								85.4 KiB	715
;;; Drop E	verythin	g Else									
3	drop	input								77.0 KiB	388

Here's the configuration for port knocking. Just make sure you don't change the sequence or this will not worked



Knock Attempt



- Hosts have to Knock the correct ports
- Hosts IP Address that have knocked the correct ports will be put in dynamically to "Save Haven" Address List
- Hosts can access router

Closing



- Port Knocking is useful for securing the router
- Port Knocking is also useful to decrease a brute force attack
- Port Knocking has it's weakness also:
 - It's possible to spy out the knocking sequence by sniffing the network
 - It's necessary to have a special knocking-client
- Port Knocking is only one method to secure the router, best to combine this with other methods.



Thank You

Your Question Will be Appreciated