

# Port Knocking for Security



# Introduction

- Steve Discher - [LearnMikroTik.com](http://LearnMikroTik.com)
- MikroTik RouterOS training, including MTCNA, MTCRE, MTCTCE, MTCWE and MTCUME
- Own a WISP



# Introduction

- Just completed a 10,000 mile, 100 day journey around western USA teaching RouterOS, the MikroTik Road Show





- The Road Show was a 100 day journey that started in College Station, Texas in April
- Purpose was to travel all over the western US conducting MikroTik RouterOS training in as many locations as possible



# Road Show Stats

Miles Traveled: 10,000 by motor home

3,000 by Jeep

Fuel Used: 1,111 gals of Diesel

Nights on the road: 100

Areas Traveled: 11 US states, 3 islands and 2  
Canadian Provinces



# Road Show Stats

Trainings Conducted: 5 public, 6 private, consulted with 9 different companies

MT Certifications Issued: 35

Look for the next MikroTik Road Show, Summer 2011

[www.MTRoadShow.com](http://www.MTRoadShow.com)



# Port Knocking for Security



# 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 pre-specified series of closed ports



# What is Port Knocking?

- The port "knock" itself is similar to a secret handshake and can consist of any number of TCP, UDP, or ICMP or other protocol packets to numbered ports on the destination machine



# What is Port Knocking?

- The knock may also consist of text strings sent to the device being knocked to add additional complexity and security



# Port Knocking Example



1. Send a connection to PORT-1234

2. The router stores the requester's IP for an amount of time

3. Send a connection to PORT-4321

4. The router checks to see if the IP is the same IP from the first connection (PORT-1234)

5. If the IP is the same and the time between 1<sup>st</sup> attempt and 2<sup>nd</sup> is within a specified time then the requester IP will be allowed to access the router



Knocking Port  
PORT 1234  
PORT 4321



# Firewall Chain Review



# Input Chain

- Input Chain – used to process packets entering the router through one of the interfaces with the destination IP address which is one of the router's addresses. Packets passing through the router are not processed against the rules of the input chain. Protects the router itself.



# Forward Chain

- Forward Chain - used to process packets passing through the router. Protects the clients.



# Output Chain

- Output Chain – used to process packets generated by the router. Packets passing through the router are not processed against the rules of the output chain.

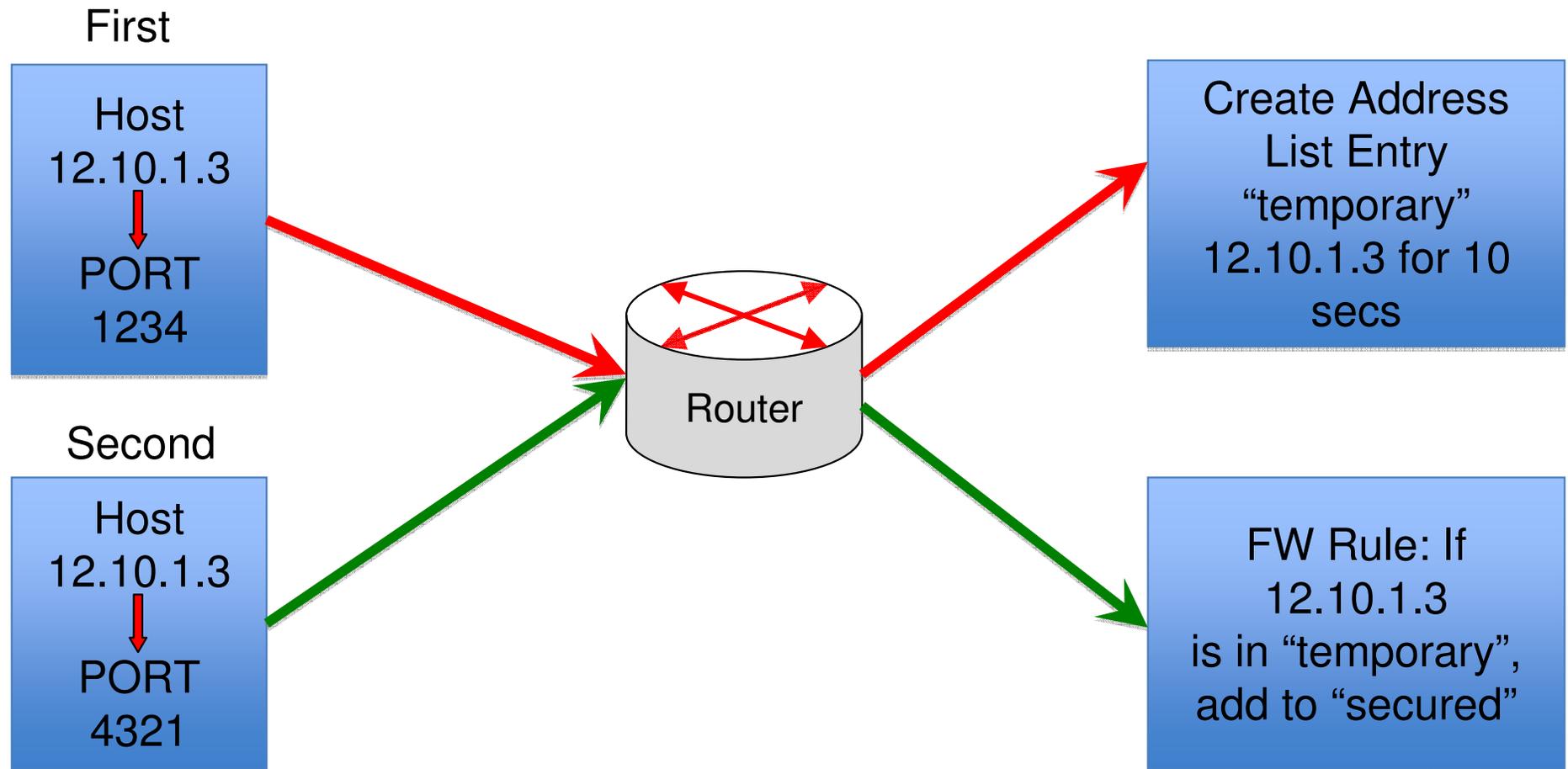


# Port Knocking Strategy

1. Detect a connection to a port and put it in an address list we will name “temporary” for 10 seconds.
2. Detect a connection to a second port and check to see if the source IP is in the address list “temporary”. If so, put in the list “secured”.
3. Allow access to the router from hosts in the address list “secured”.



# Port Knocking Strategy

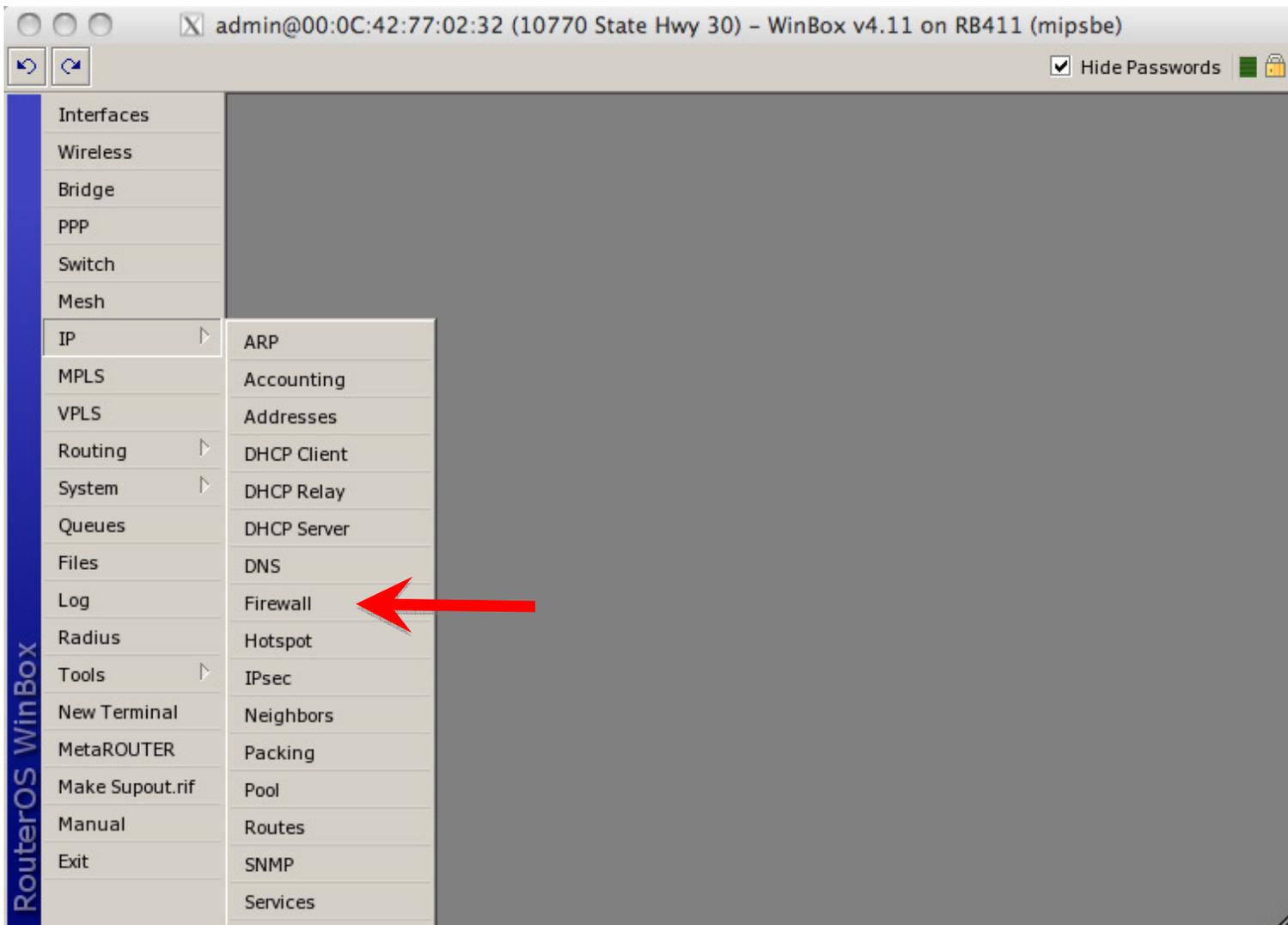


# Address Lists

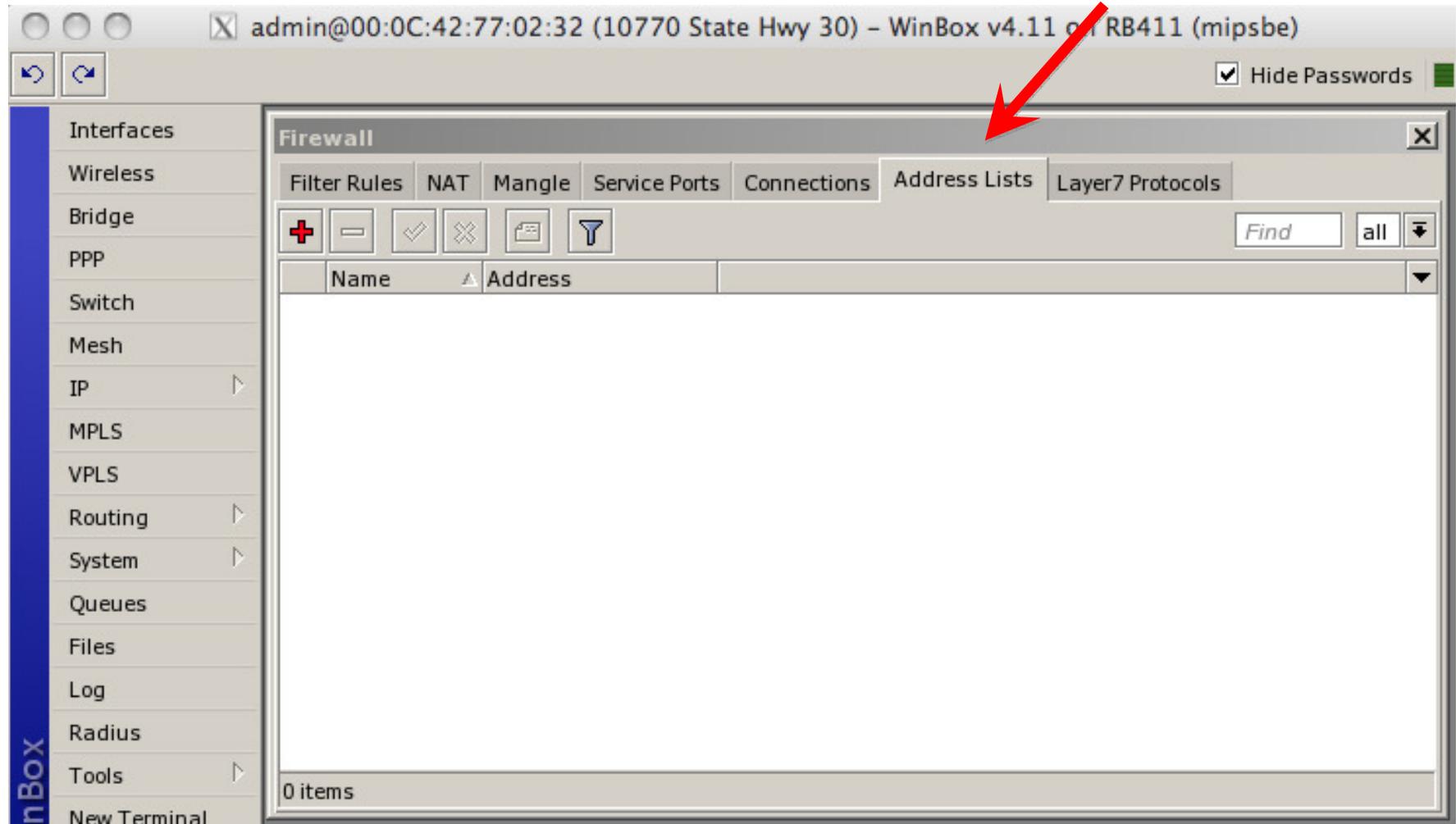
- If you have not used Address Lists in RouterOS before, you are missing a great way to reduce the number of rules in your firewall and create a much more extensible firewall device
- Let's take a look at Address Lists...



# Address Lists



# Address Lists



The screenshot shows the WinBox v4.11 interface for configuring a firewall. The main window is titled "Firewall" and has several tabs: "Filter Rules", "NAT", "Mangle", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The "Address Lists" tab is selected, and a red arrow points to it. Below the tabs, there are several icons for adding, deleting, and saving configurations, along with a search bar labeled "Find" and a dropdown menu set to "all". The main area is a table with two columns: "Name" and "Address". The table is currently empty, and the status bar at the bottom indicates "0 items".

Name	Address
------	---------



# Address Lists

The screenshot shows the WinBox interface for configuring Firewall Address Lists. The main window is titled "admin@00:0C:42:77:02:32 (10770 State Hwy 30) - WinBox v4.11 on RB411 (r". The left sidebar contains a navigation menu with items: Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, VPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, and Meta-ROUTER. The main content area is titled "Firewall" and has tabs for Filter Rules, NAT, Mangle, Service Ports, Connections, Address Lists, and Layer7 Protocol. The "Address Lists" tab is active, showing a table with one entry:

Name	Address
temporary	12.22.76.2

Below the table, it indicates "1 item (1 selected)". A modal dialog box titled "Firewall Address List <temporary>" is open, showing the configuration for the selected item. The dialog has the following fields and buttons:

- Name: temporary (dropdown menu)
- Address: 12.22.76.2 (text input)
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

The status bar at the bottom of the dialog shows "disabled".



# Address Lists

The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule. The window title is "admin@00:0C:42:77:02:32 (10770 State Hwy 30) - WinBox v4.11 on RB411 (mipsbe)". The left sidebar contains a menu with categories: Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, VPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, and MetaROUTER. The main area is titled "Firewall Rule <>" and has tabs for General, Advanced, Extra, Action, and Statistics. The "General" tab is active, showing the following configuration fields:

- Src. Address List:  temporary
- Dst. Address List:
- Layer7 Protocol:
- Content:
- Connection Bytes:
- Connection Rate:
- Per Connection Classifier:
- Src. MAC Address:
- Out. Bridge Port:
- In. Bridge Port:
- Ingress Priority:
- DSCP (TOS):

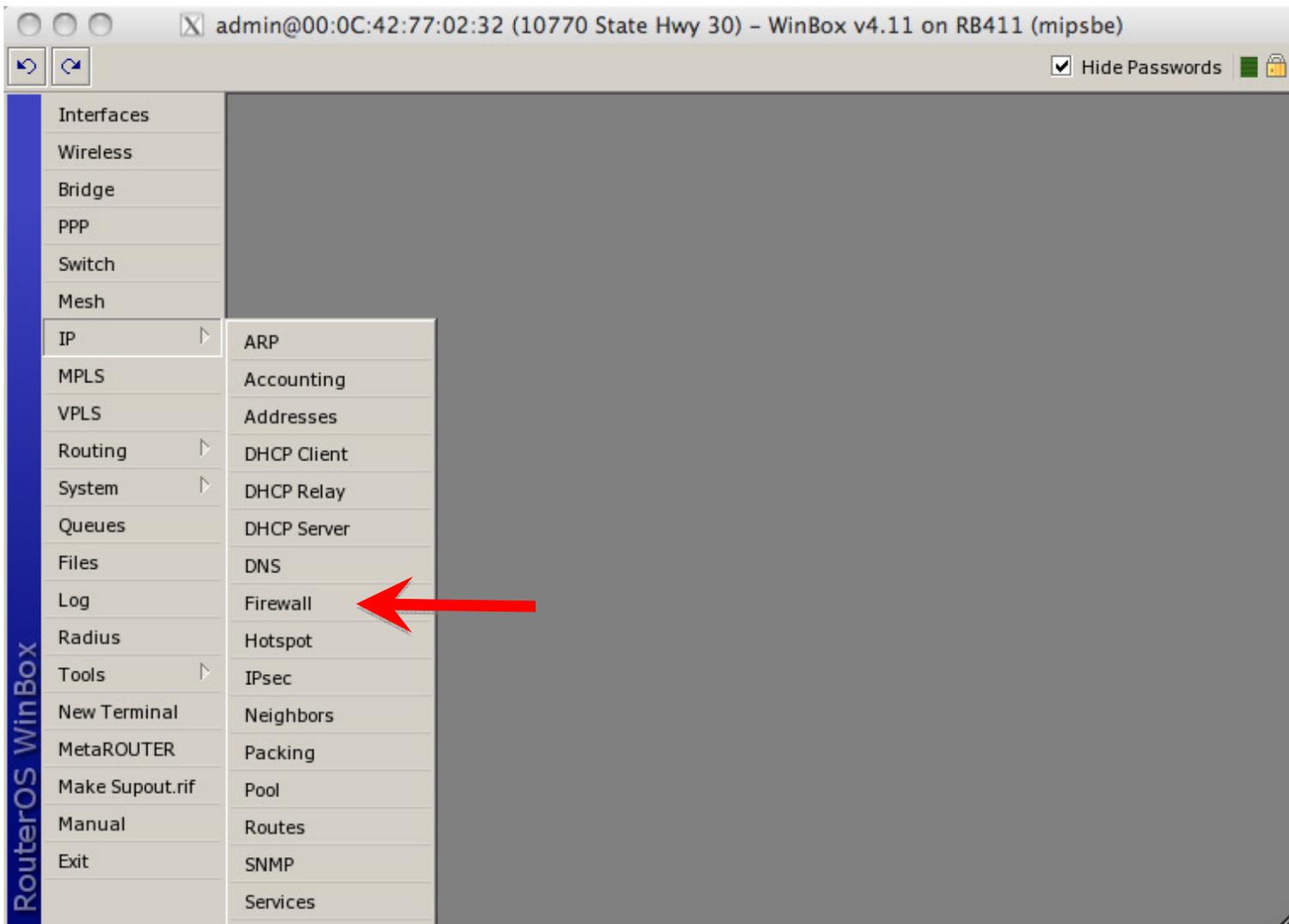


# Port Knocking Strategy

1. Detect a connection to a port and put in an address list entry “temporary” for 10 seconds.
2. Detect a connection to a second port and check to see if the source IP is in the address list “temporary”. If so, put in the list “secured”.
3. Allow access to the router from hosts in the address list “secured”.



# Configuration – Step 1



# Configuration – Step 1

The screenshot displays the WinBox v4.11 interface for configuring a firewall on an RB411 router. The 'Firewall' window is open, and the 'NAT' tab is selected, indicated by a red arrow. The interface includes a sidebar with various configuration options and a main panel for rule management. The main panel shows a table with columns for rule details, and the current view shows 0 items.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Int...	Out. Int...	By
0 items										



# Configuration – Step 1

- Trap TCP(1234) and put the source address to address-list *temporary* for 10 seconds

The image shows two overlapping windows from Mikrotik WinBox. The background window is titled "Firewall Rule <1234>" and has tabs for General, Advanced, Extra, Action, and Statistics. The "General" tab is selected, showing the following configuration:

- Chain: input
- Src. Address: (empty)
- Dst. Address: (empty)
- Protocol:  6 (tcp)
- Src. Port: (empty)
- Dst. Port:  1234
- Any. Port: (empty)
- P2P: (empty)

The foreground window is also titled "Firewall Rule <1234>" and has tabs for General, Advanced, Extra, Action, and Statistics. The "Action" tab is selected, showing the following configuration:

- Action: add src to address list
- Address List: temporary
- Timeout: 00:00:10

On the right side of the foreground window, there are several buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

# Configuration – Step 2

- Trap TCP(4321) and src-address is in *temporary*. Put it to address-list *secured*

The image displays three sequential screenshots of the Mikrotik Firewall Rule configuration interface for rule 4321, showing the progression of settings.

**Top Left Screenshot (General tab):** Shows the initial configuration with Chain: input, Protocol: 6 (tcp), and Dst. Port: 4321.

**Top Right Screenshot (Action tab):** Shows the Action: add src to address list and Address List: secured. The Timeout is set to 00:01:00.

**Bottom Screenshot (Extra tab):** Shows the Src. Address List: temporary and Dst. Address List: (empty).



# Configuration – Step 3

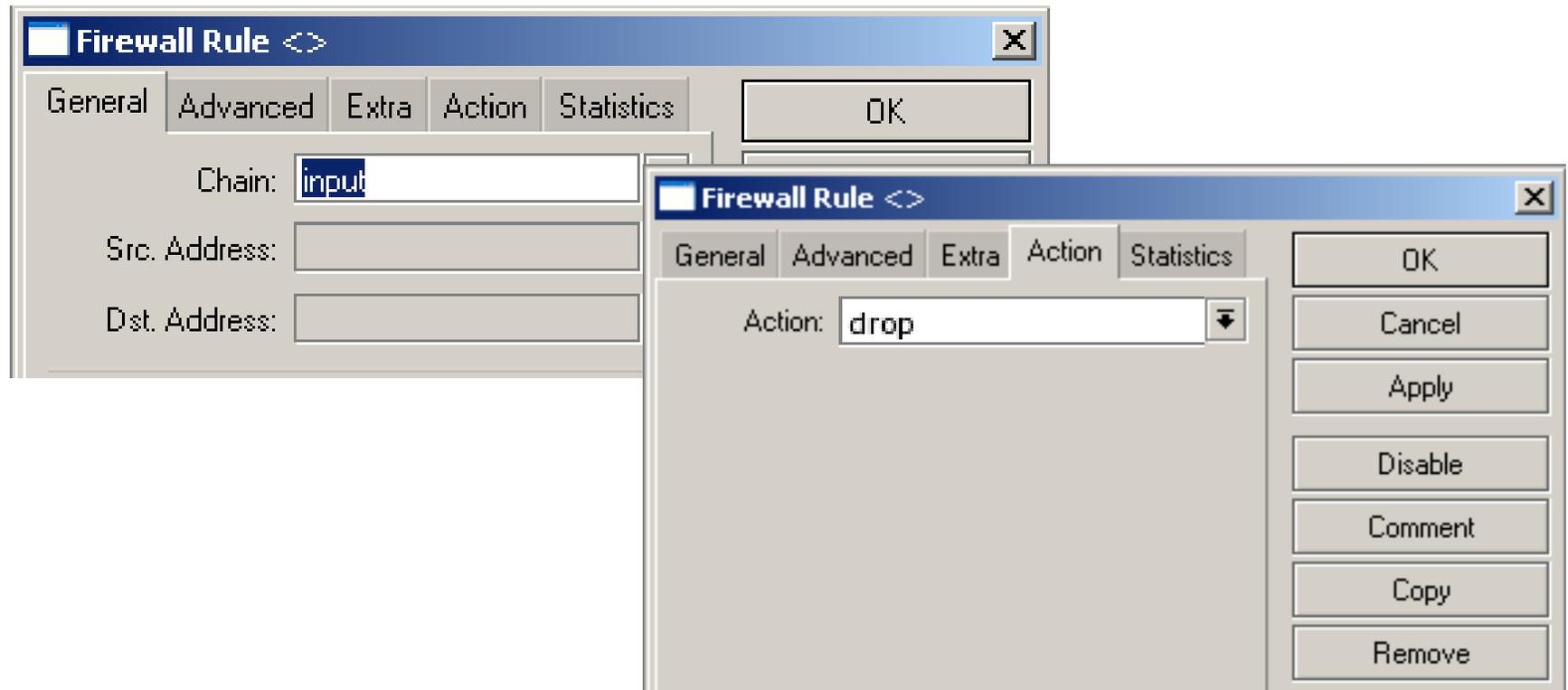
- Allow access from src-address-list

The image displays three overlapping screenshots of the Mikrotik Firewall Rule configuration interface. The top-left window shows the 'General' tab with 'Chain: input' and empty 'Src. Address' and 'Dst. Address' fields. The bottom-left window shows the 'General' tab with 'Src. Address List' set to 'secured' and an empty 'Dst. Address List' field. The right window shows the 'Action' tab with 'Action: accept' and a list of buttons: OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

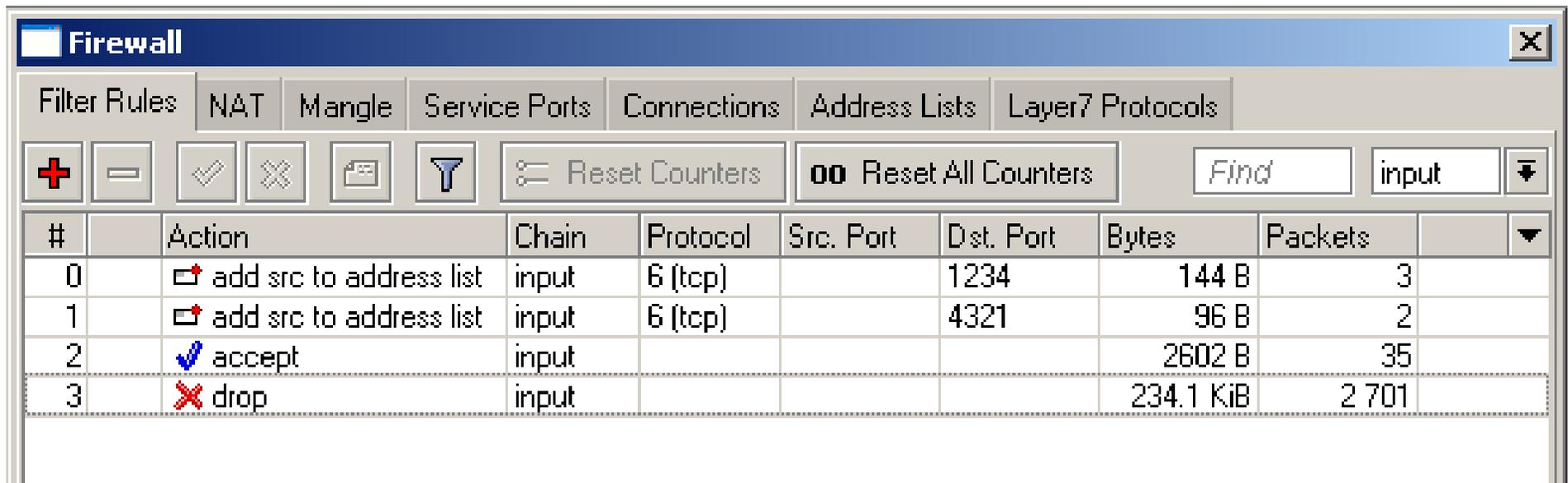


# Configuration – Step 4

- Drop everything else



# Configuration – Summary



The screenshot shows the Mikrotik WinBox Firewall configuration window. The window title is "Firewall". It has several tabs: "Filter Rules", "NAT", "Mangle", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The "Filter Rules" tab is active. Below the tabs are several control buttons: a red plus sign, a minus sign, a checkmark, a cross, a folder icon, a funnel icon, a "Reset Counters" button, a "Reset All Counters" button, a "Find" search box, and a dropdown menu currently showing "input".

#	Action	Chain	Protocol	Src. Port	Dst. Port	Bytes	Packets	
0	add src to address list	input	6 (tcp)		1234	144 B	3	
1	add src to address list	input	6 (tcp)		4321	96 B	2	
2	accept	input				2602 B	35	
3	drop	input				234.1 KiB	2 701	



# Generating The Knock

To generate the knock you need a client. There are numerous clients for download for Windows, Linux or Mac.

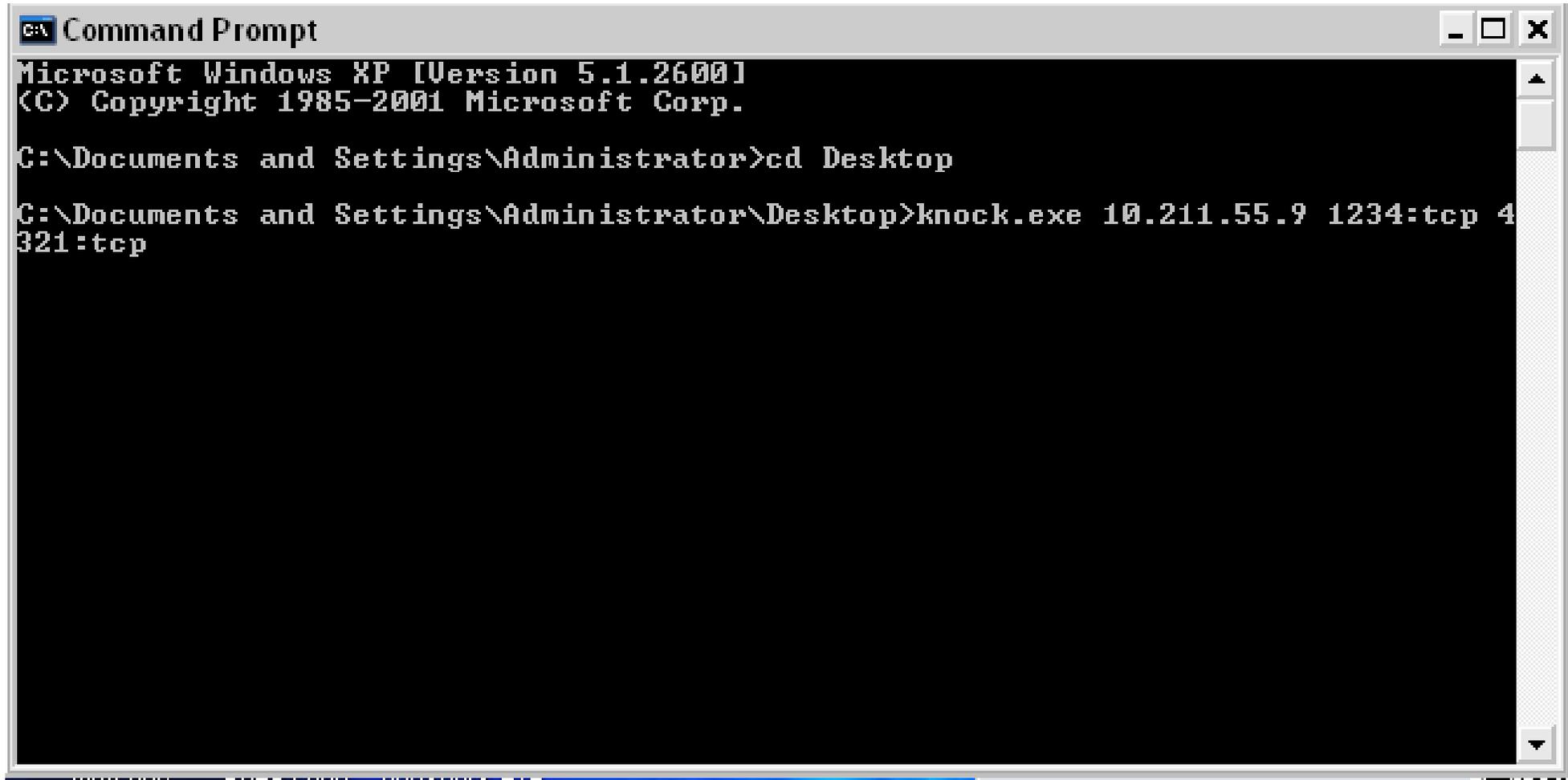
## **Knock.exe**

<http://www.zeroflux.org/proj/knock/files/knock-cygwin.zip>

Or, build your own!



# Generating The Knock



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd Desktop

C:\Documents and Settings\Administrator\Desktop>knock.exe 10.211.55.9 1234:tcp 4
321:tcp
```



# Knock Is Complete!

```
root@mail:/usr/src/linux — bash — 94x24
Request timeout for icmp_seq 51
Request timeout for icmp_seq 52
Request timeout for icmp_seq 53
ping: sendto: No route to host
Request timeout for icmp_seq 54
ping: sendto: host is down
Request timeout for icmp_seq 55
ping: sendto: host is down
Request timeout for icmp_seq 56
ping: sendto: host is down
Request timeout for icmp_seq 57
Request timeout for icmp_seq 58
Request timeout for icmp_seq 59
64 bytes from 10.211.55.9: icmp_seq=60 ttl=64 time=0.051 ms
64 bytes from 10.211.55.9: icmp_seq=61 ttl=64 time=0.045 ms
64 bytes from 10.211.55.9: icmp_seq=62 ttl=64 time=0.052 ms
64 bytes from 10.211.55.9: icmp_seq=63 ttl=64 time=0.045 ms
64 bytes from 10.211.55.9: icmp_seq=64 ttl=64 time=0.101 ms
64 bytes from 10.211.55.9: icmp_seq=65 ttl=64 time=0.041 ms
64 bytes from 10.211.55.9: icmp_seq=66 ttl=64 time=0.072 ms
64 bytes from 10.211.55.9: icmp_seq=67 ttl=64 time=0.046 ms
64 bytes from 10.211.55.9: icmp_seq=68 ttl=64 time=0.080 ms
64 bytes from 10.211.55.9: icmp_seq=69 ttl=64 time=0.043 ms
64 bytes from 10.211.55.9: icmp_seq=70 ttl=64 time=0.066 ms
```



# What's The Effectiveness?

- Because any combination of ports and transport protocols can be used, the number of possible sequences that an attacker would have to guess is very high. Even if the hacker knew only two port knocks were involved, as in the very simple example above, with 64,000 possible TCP, UDP, and ICMP ports to choose from, the resulting set of possible combinations for the hacker to try runs into the millions.



# What's The Effectiveness?

- Port scanners will be frustrated because port knocking uses closed ports to do the listening.



# What's The Effectiveness?

- The biggest advantage of all is that port knocking is platform-, service-, and application-independent: Any OS with the correct client and server software can take advantage of its protection



# What's The Effectiveness?

- Port knocking can also serve as an extra layer of security to protect high-risk remote management services, such as SSH and RDP.



# What's The Effectiveness?

- Critics often point to the fact that eavesdropping hackers might be able to capture and replay the successful port-knocking sequence or series of bytes. True, but port knocking should be just a layer on top of other types of security such as tunnels, or allowed IP addresses.



# What's The Effectiveness?

- If a hacker does manage to glean your combination, the worst-case scenario is that the intruder bypasses the port-knocking protection and now has to face your normal service security measures.



# Some Ideas

- Use port knocking to augment existing security such as VPN tunnels. For example, client must knock before you allow VPN connection.
- Extend port knocking to include sending text passphrases. Client must knock correct ports, correct protocol, correct sequence and send the right string during the sequence.



# Extending Knock - Example

- Using Autoit ([www.autoitscript.com](http://www.autoitscript.com)), create an application to send text strings to udp ports in sequence
- Use Layer 7 rules to watch for strings sent to certain ports
- Based my firewall filter rules on Layer 7 rules



# Create Knock Client App – Step 1

- Autoit script:

```
UDP Startup ()
```

```
$socket = UDP Open("10.0.1.1", 1234)
```

```
  $status = UDP Send($socket, "supersecretpassword1")
```

```
  UDP CloseSocket($socket)
```

```
$socket = UDP Open("10.0.1.1", 4321)
```

```
  $status = UDP Send($socket, "supersecretpassword2")
```

```
  UDP CloseSocket($socket)
```

```
UDP Shutdown ()
```



# Create Layer 7 Rules – Step 2

```
/ip firewall layer7-protocol  
add comment="" name=knock1  
    regexp="^supersecretpassword1\$"  
add comment="" name=knock2  
    regexp="^supersecretpassword2\$"
```



# Create Firewall Rules – Step 3

```
/ip firewall filter
```

```
add action=add-src-to-address-list address-list=temporary \  
    address-list-timeout=10s chain=input comment="" disabled=no dst-port=1234 \  
    layer7-protocol=knock1 protocol=udp  
add action=add-src-to-address-list address-list=secured address-list-timeout=\  
    10s chain=input comment="" disabled=no dst-port=4321 layer7-protocol=\  
    knock2 protocol=udp src-address-list=temporary  
add action=accept chain=input comment="" disabled=no src-address-list=secured  
add action=drop chain=input comment="" disabled=no
```



# Demonstration



# Questions?



# Thank You

LearnMikroTik.com  
<http://www.LearnMikroTik.com>  
[info@LearnMikroTik.com](mailto:info@LearnMikroTik.com)

