Port Knocking for Security

LearnMikroTik.com
Network Training & Consulting

Introduction

- Steve Discher - 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

LearnMikroTik.com
Network Training & Consulting

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

Port Knocking for Security

LearnMikroTik.com
Network Training & Consulting

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 1st attempt and 2nd is within a specified time then the requester IP will be allowed to access the router

Knocking Port
PORT 1234
PORT 4321

LearnMikroTik.com
Network Training & Consulting

Firewall Chain Review

LearnMikroTik.com
Network Training & Consulting

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.

LearnMikroTik.com
Network Training & Consulting

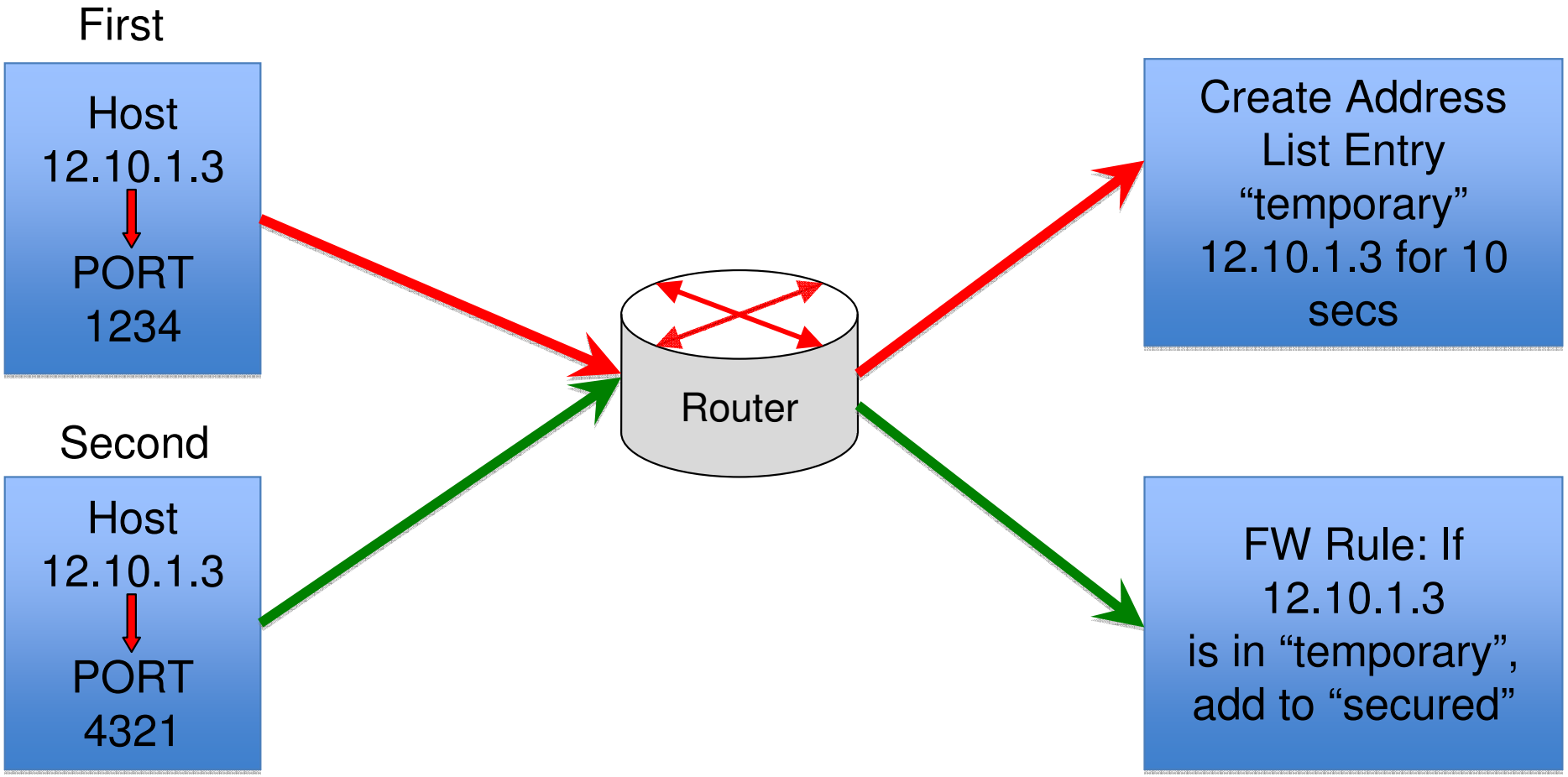
Output Chain

- 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”.

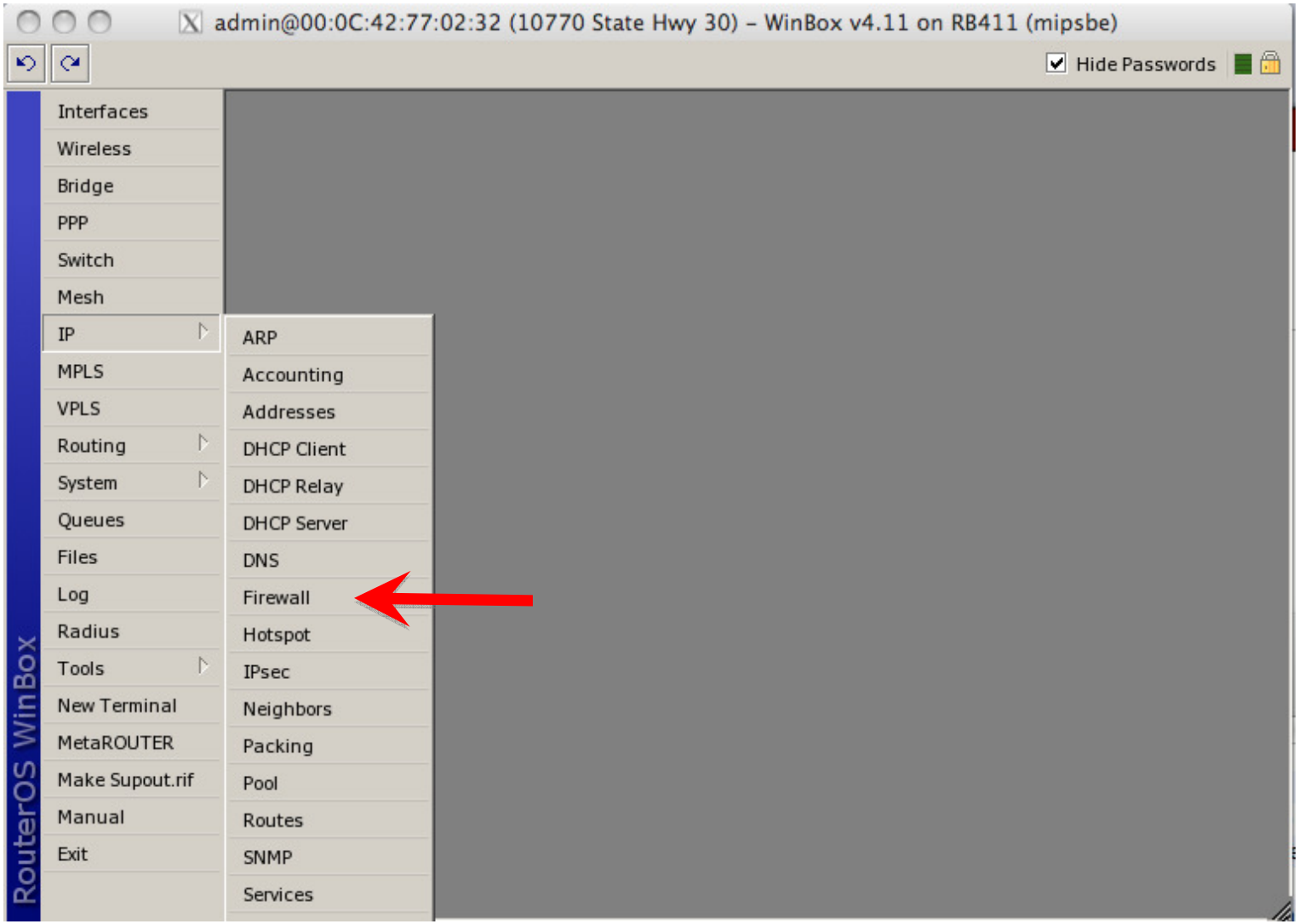
Port Knocking Strategy



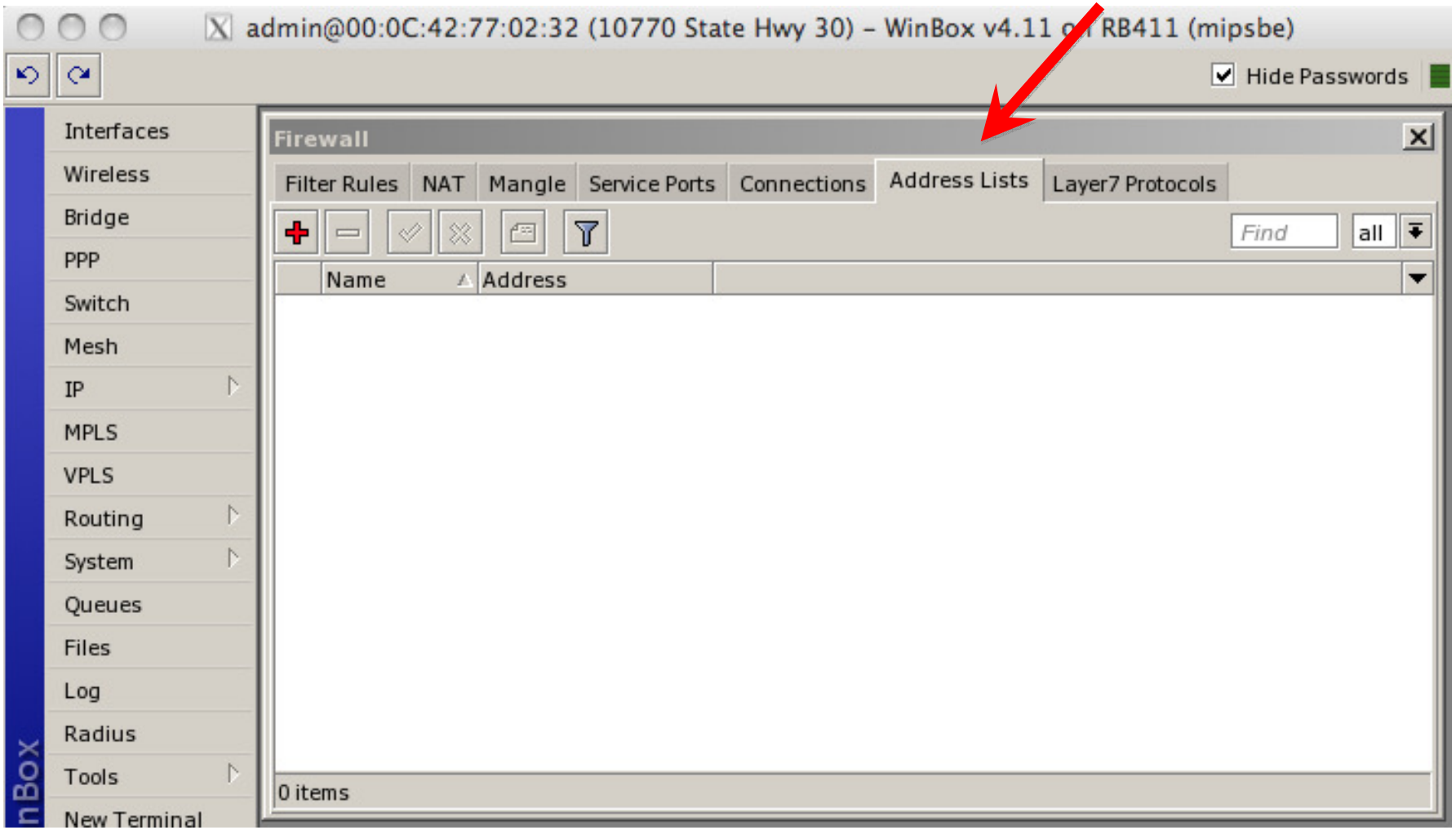
Address Lists

- 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…

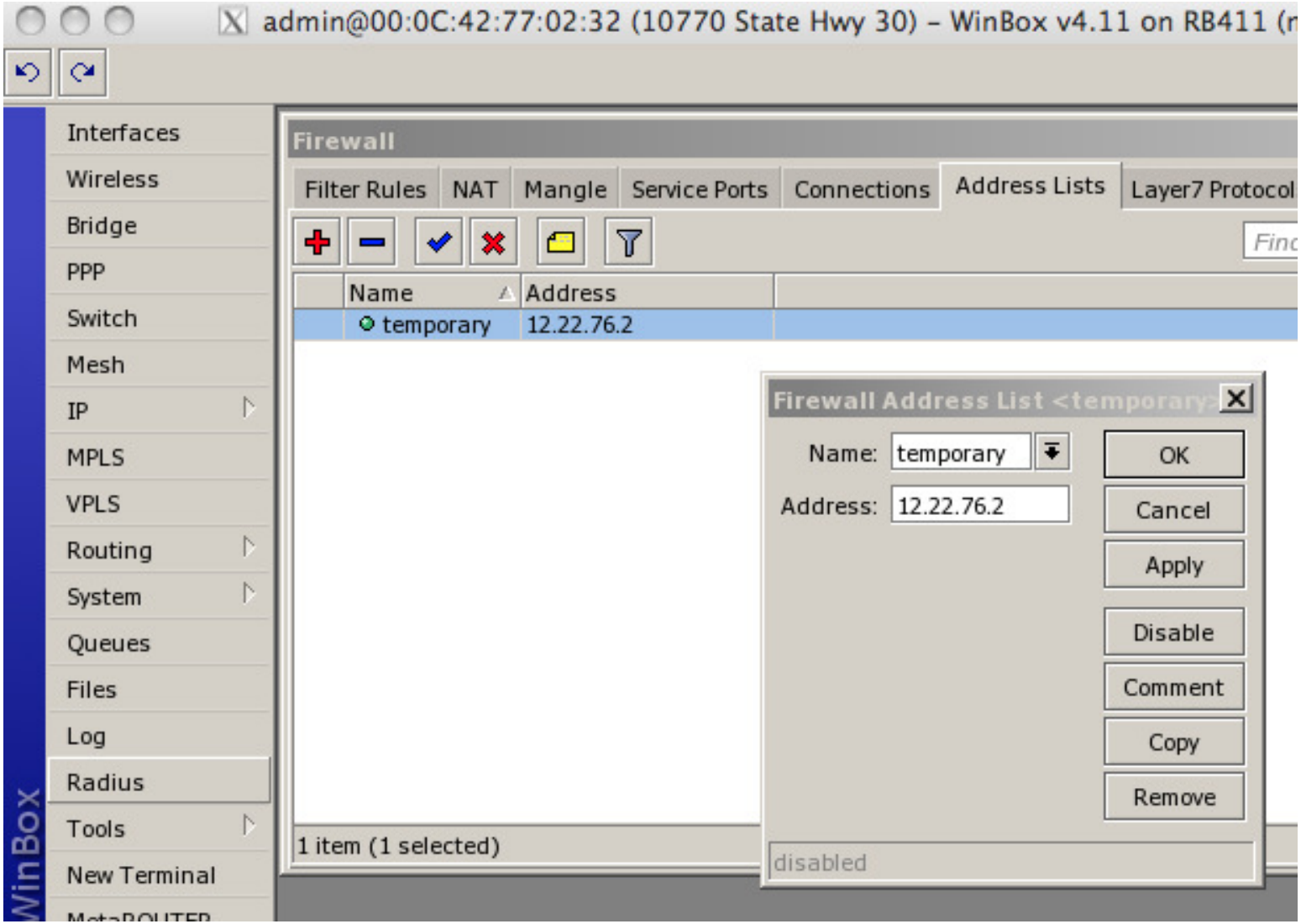
Address Lists



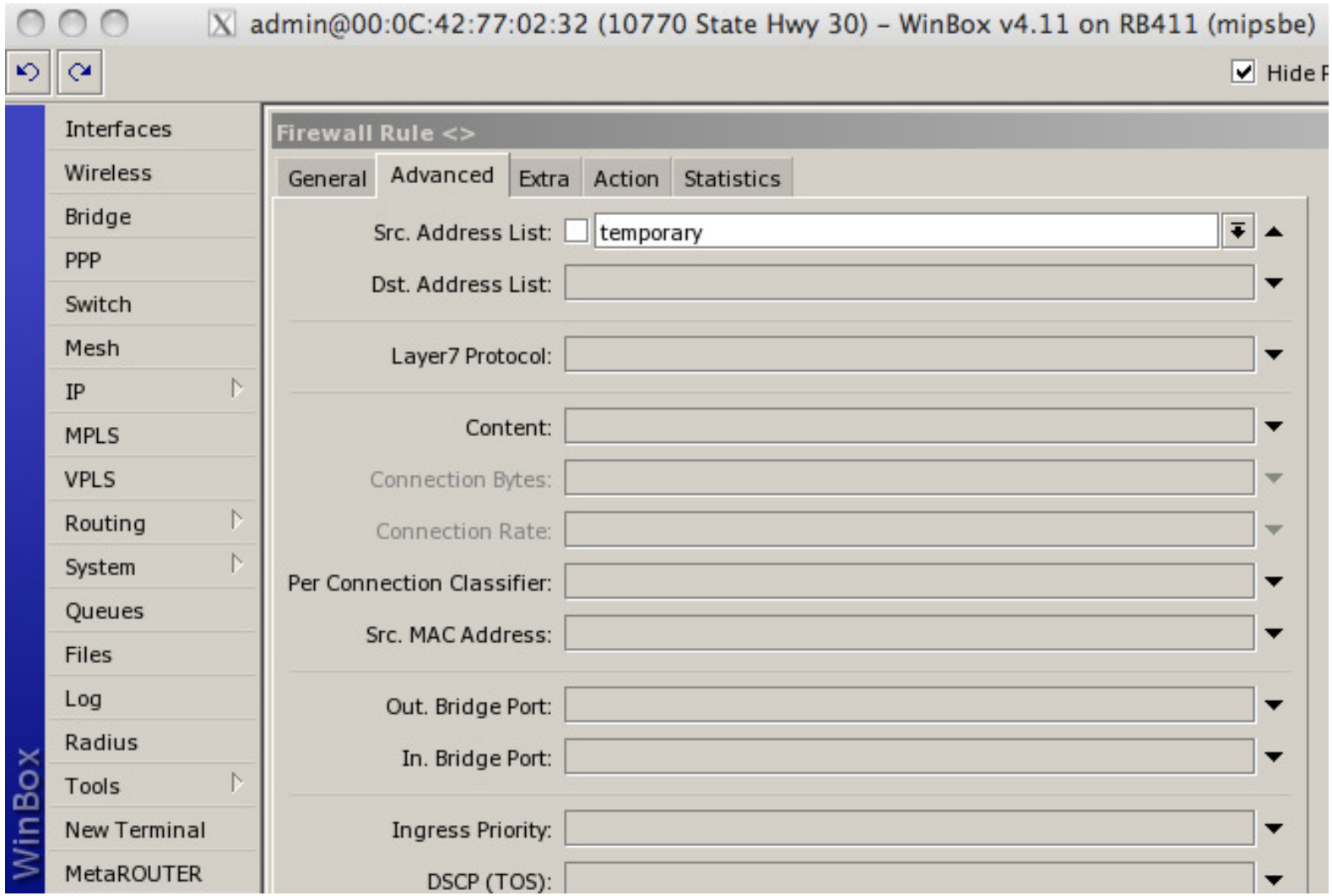
Address Lists



Address Lists



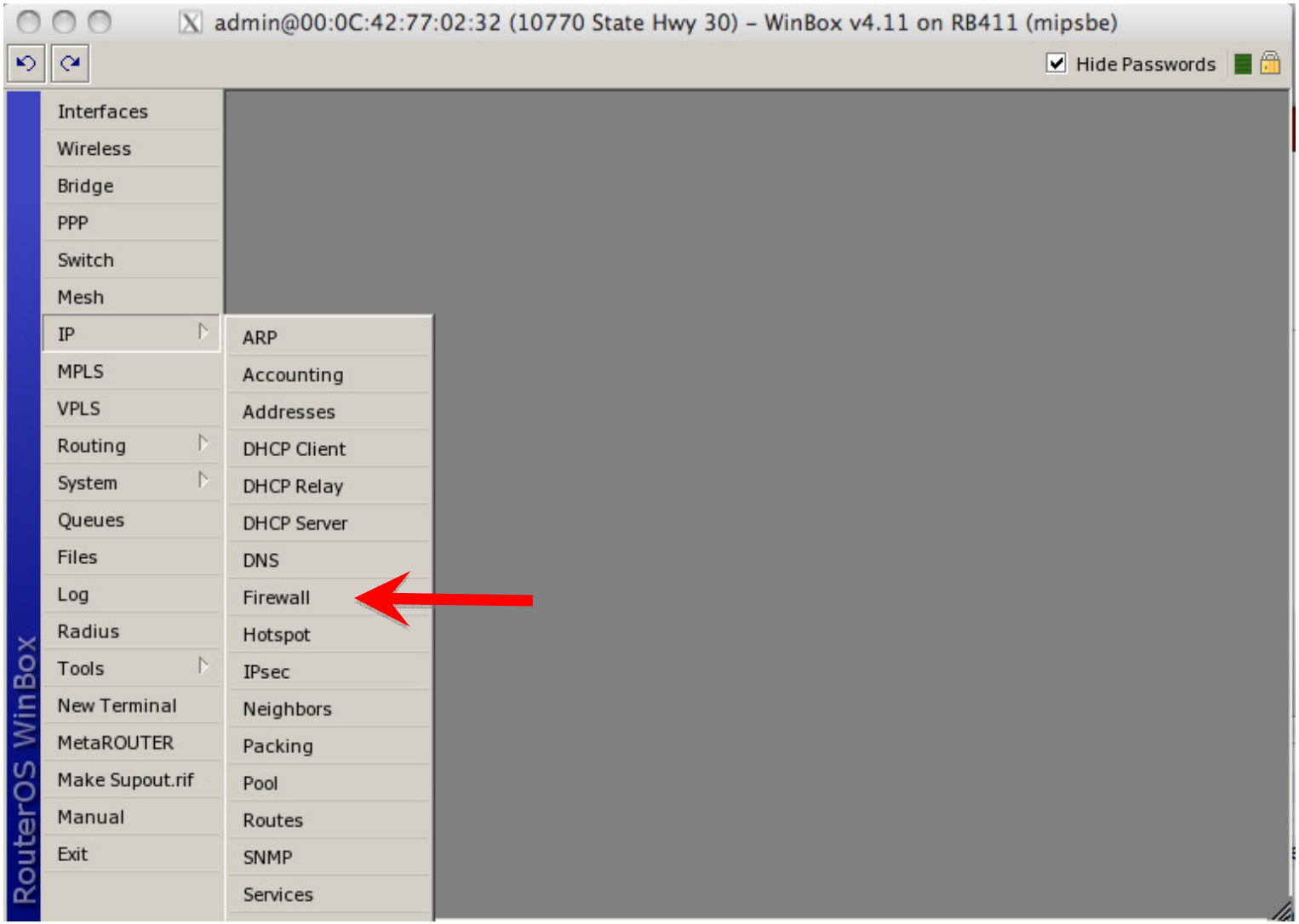
Address Lists



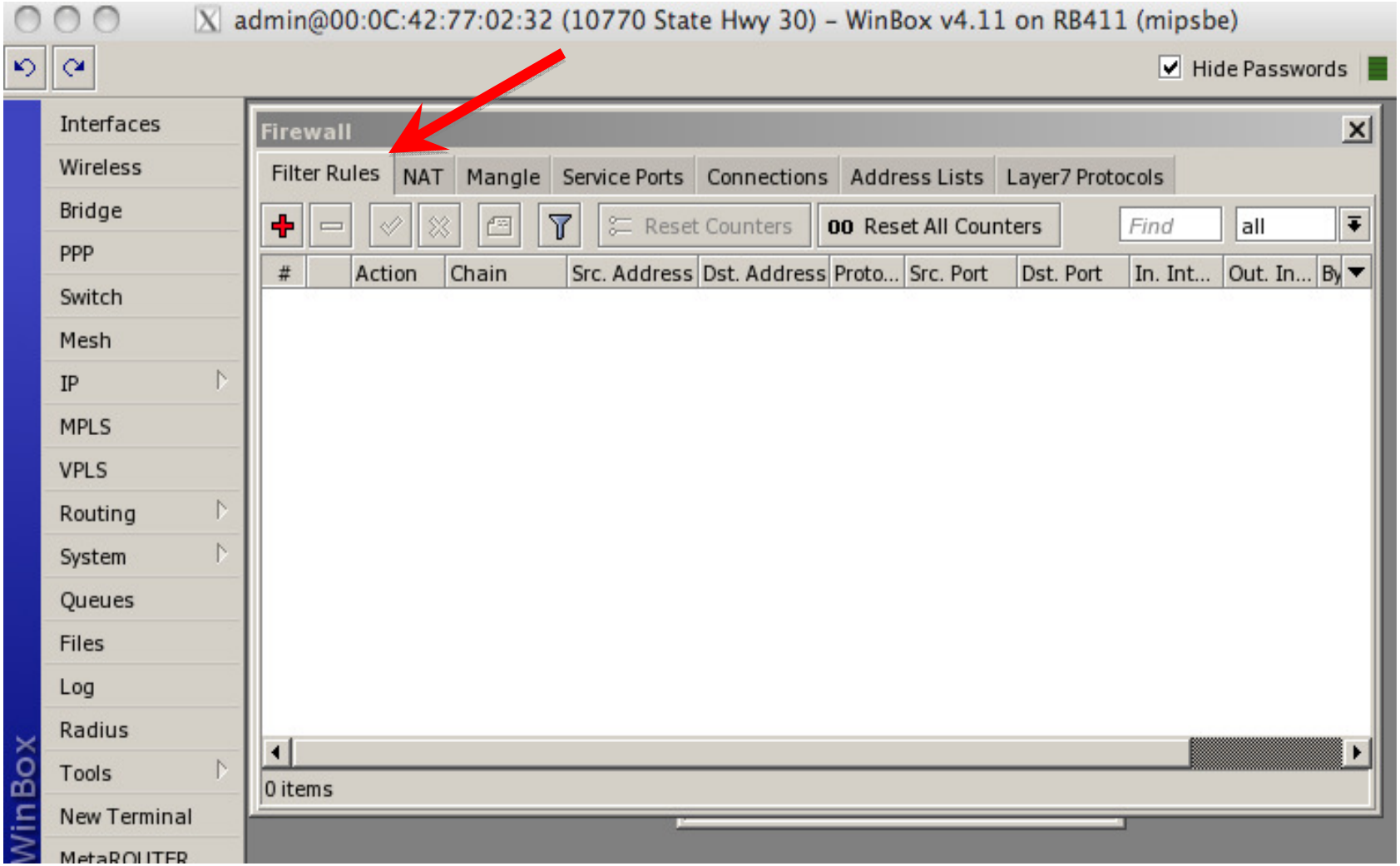
Port Knocking Strategy

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

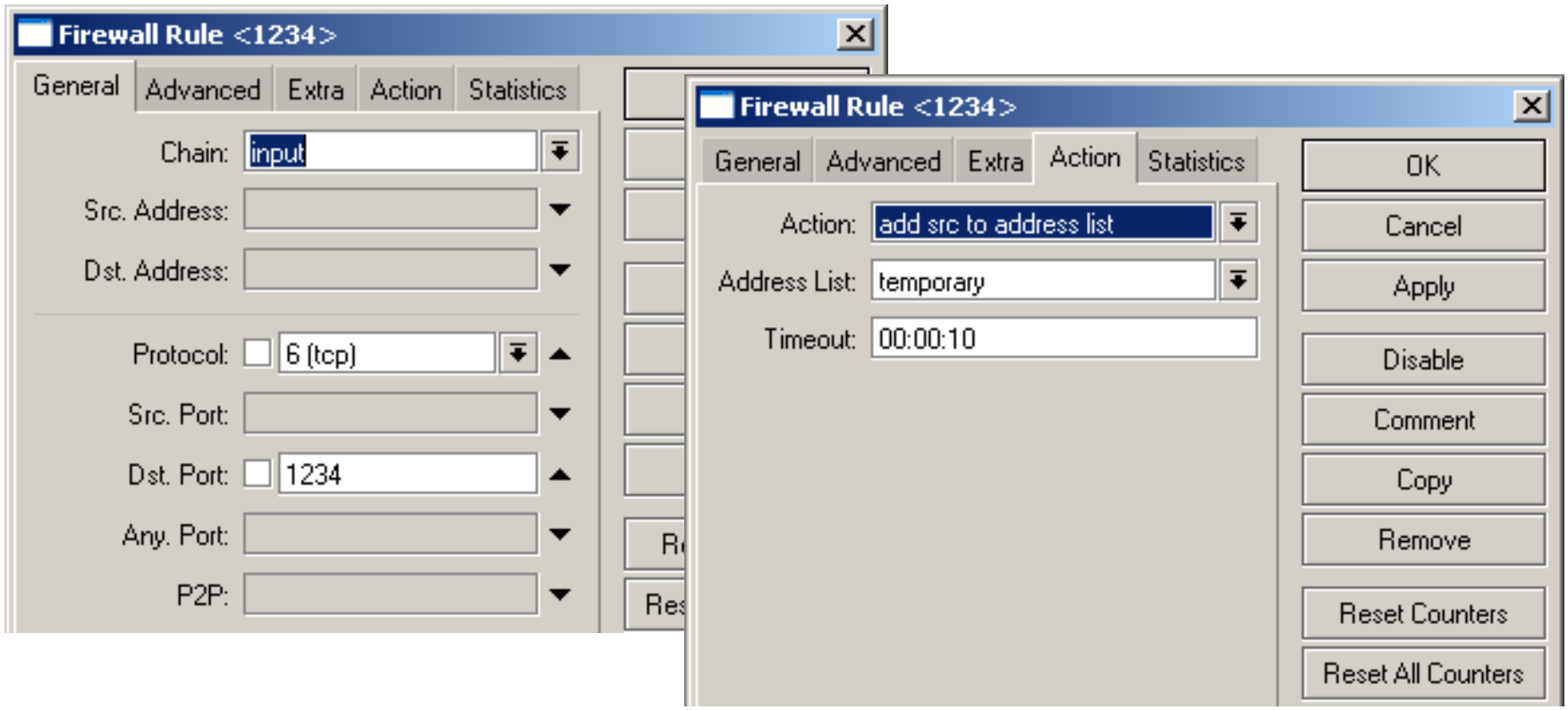


Configuration – Step 1



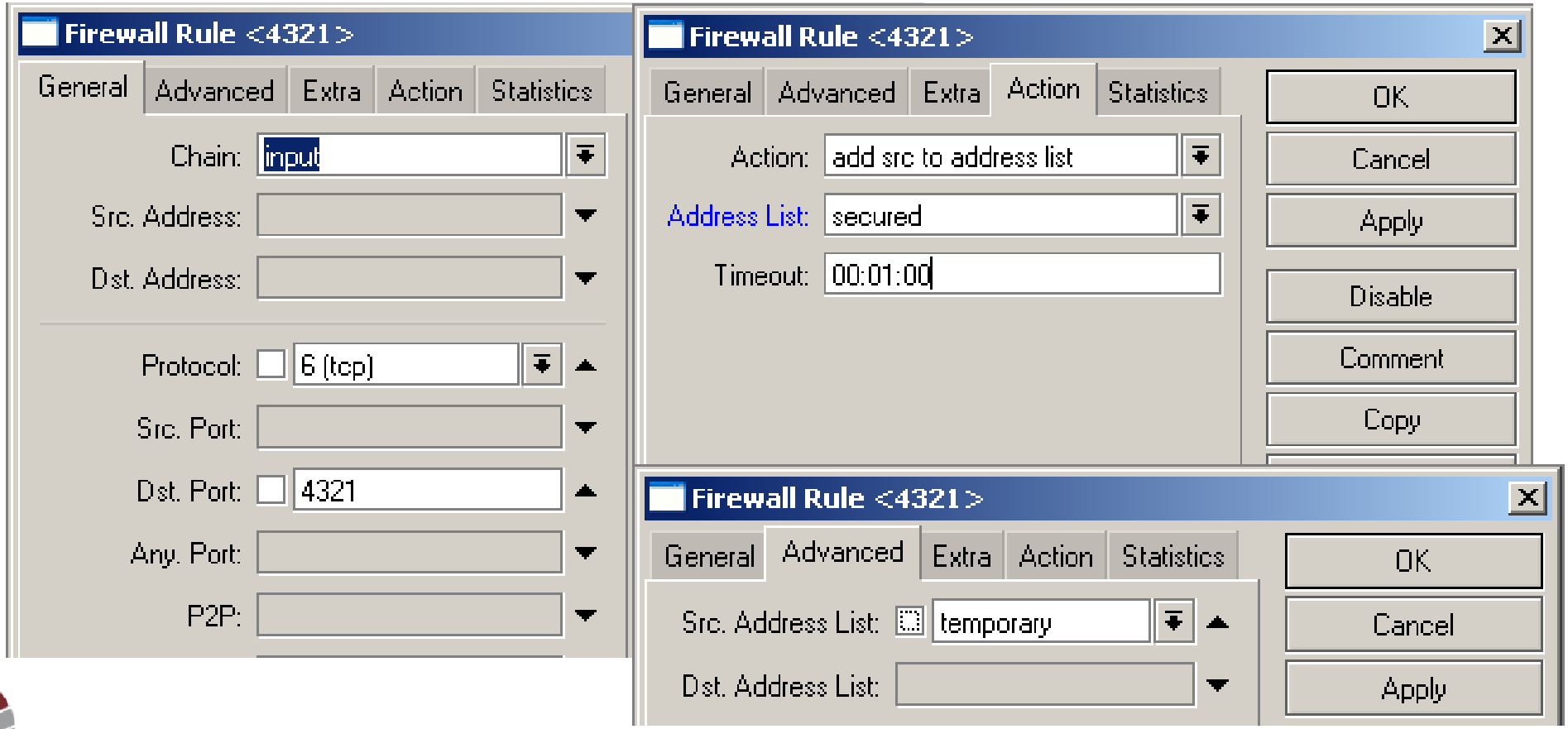
Configuration – Step 1

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



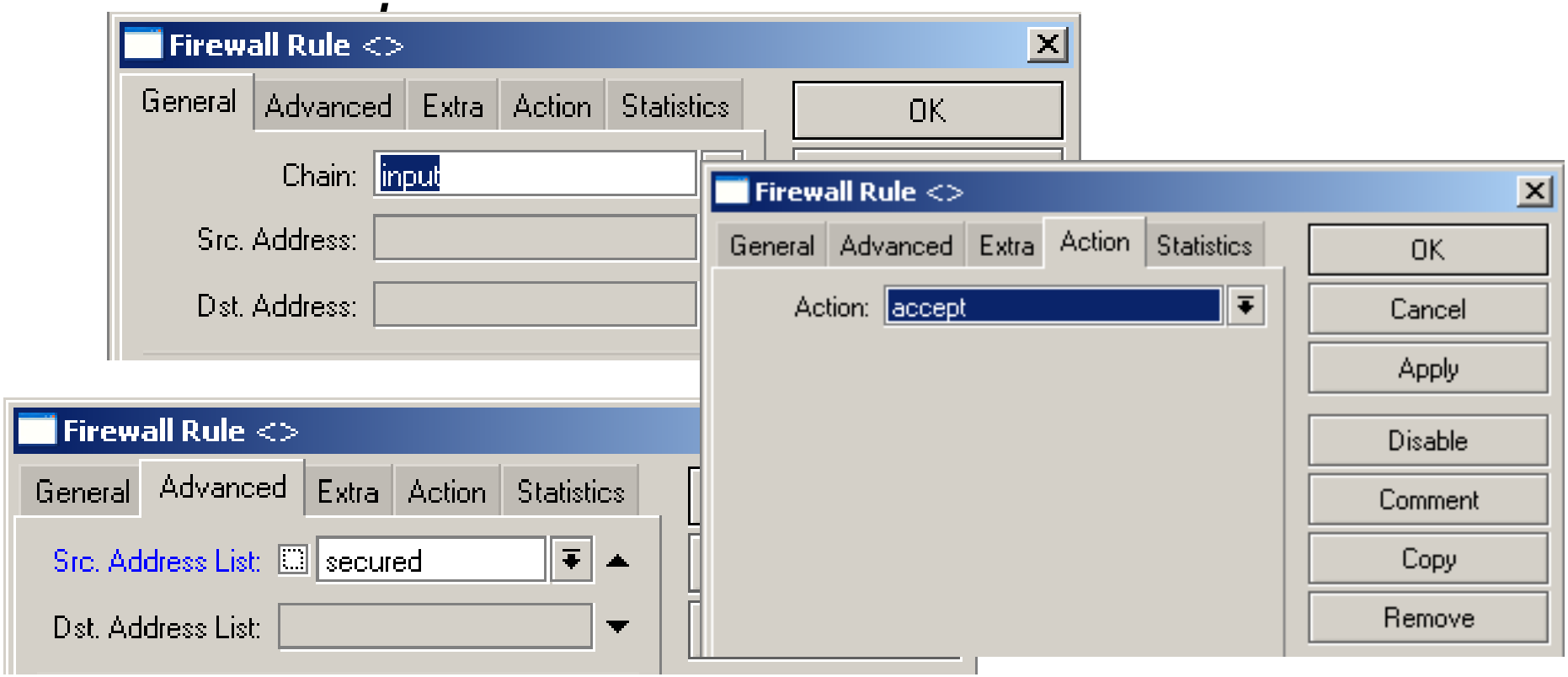
Configuration – Step 2

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



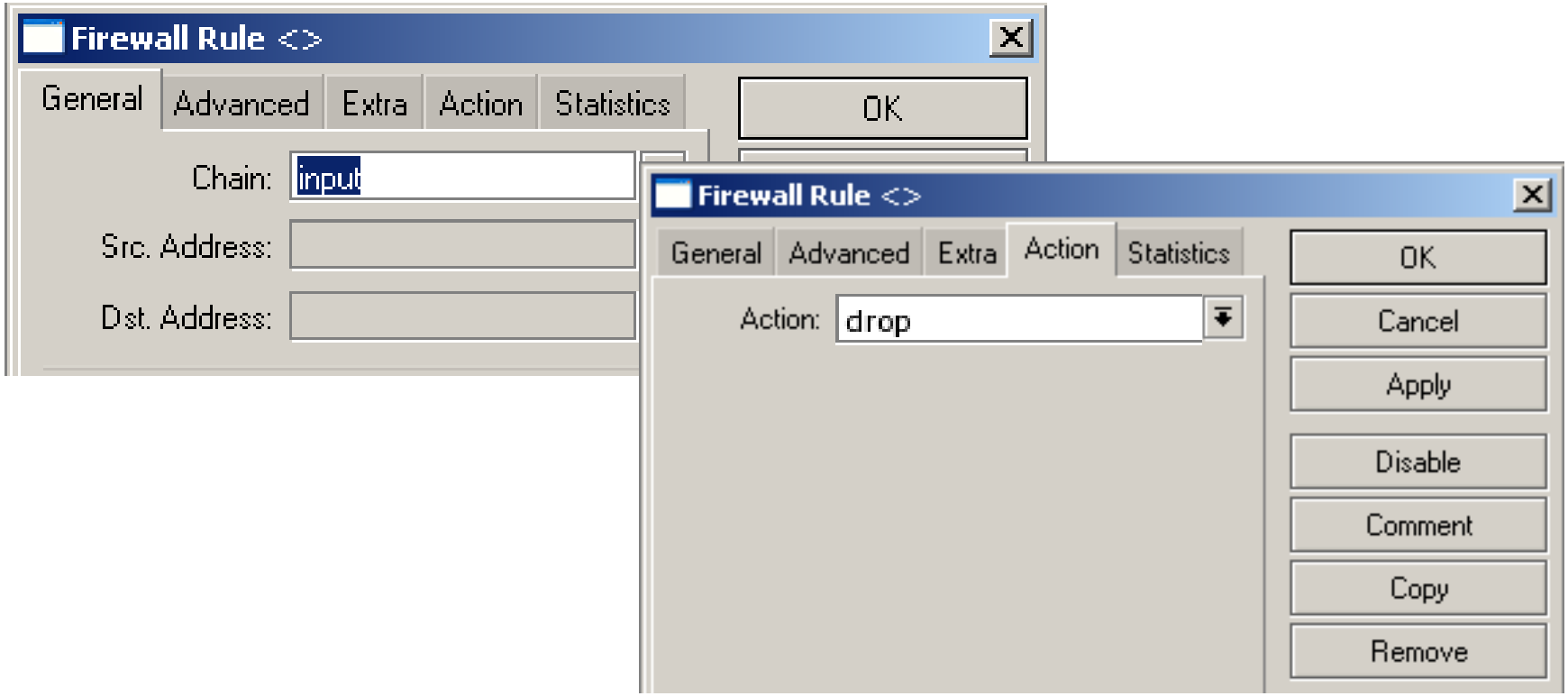
Configuration – Step 3

- Allow access from src-address-list

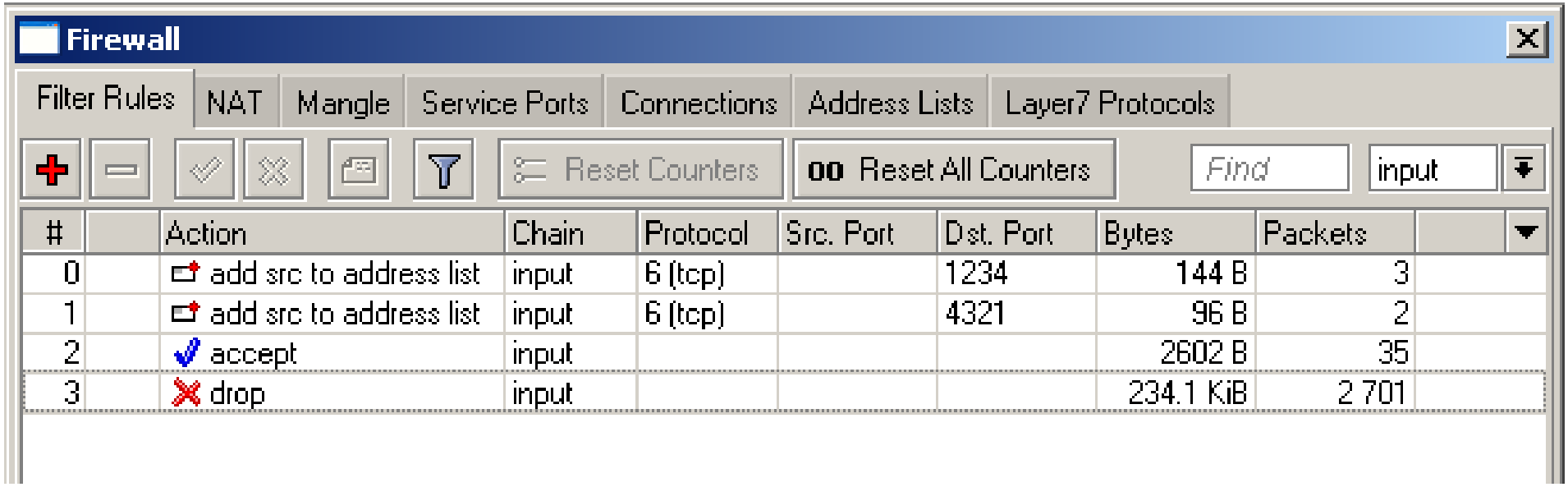


Configuration – Step 4

- Drop everything else



Configuration – Summary



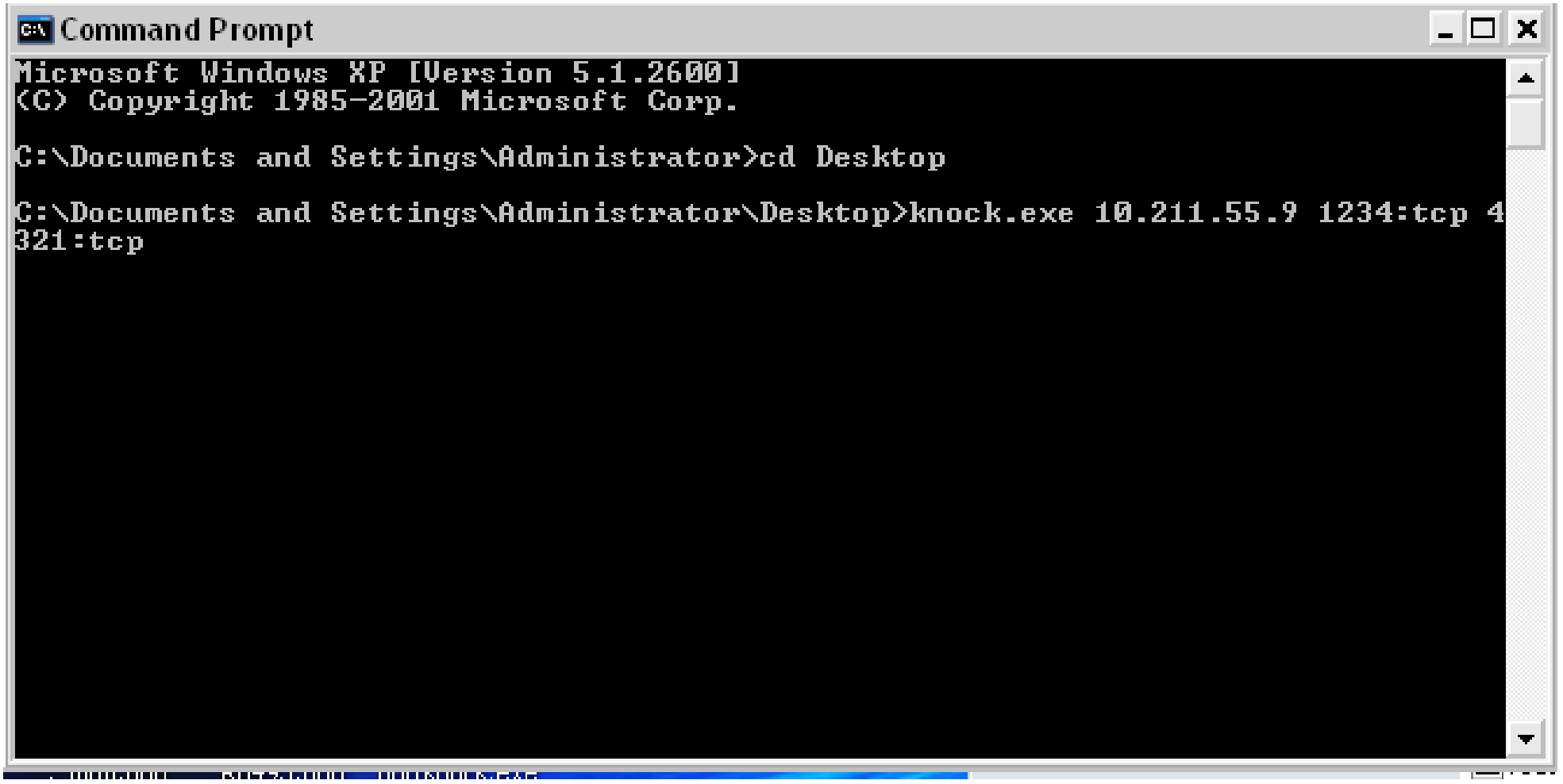
Generating The Knock

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

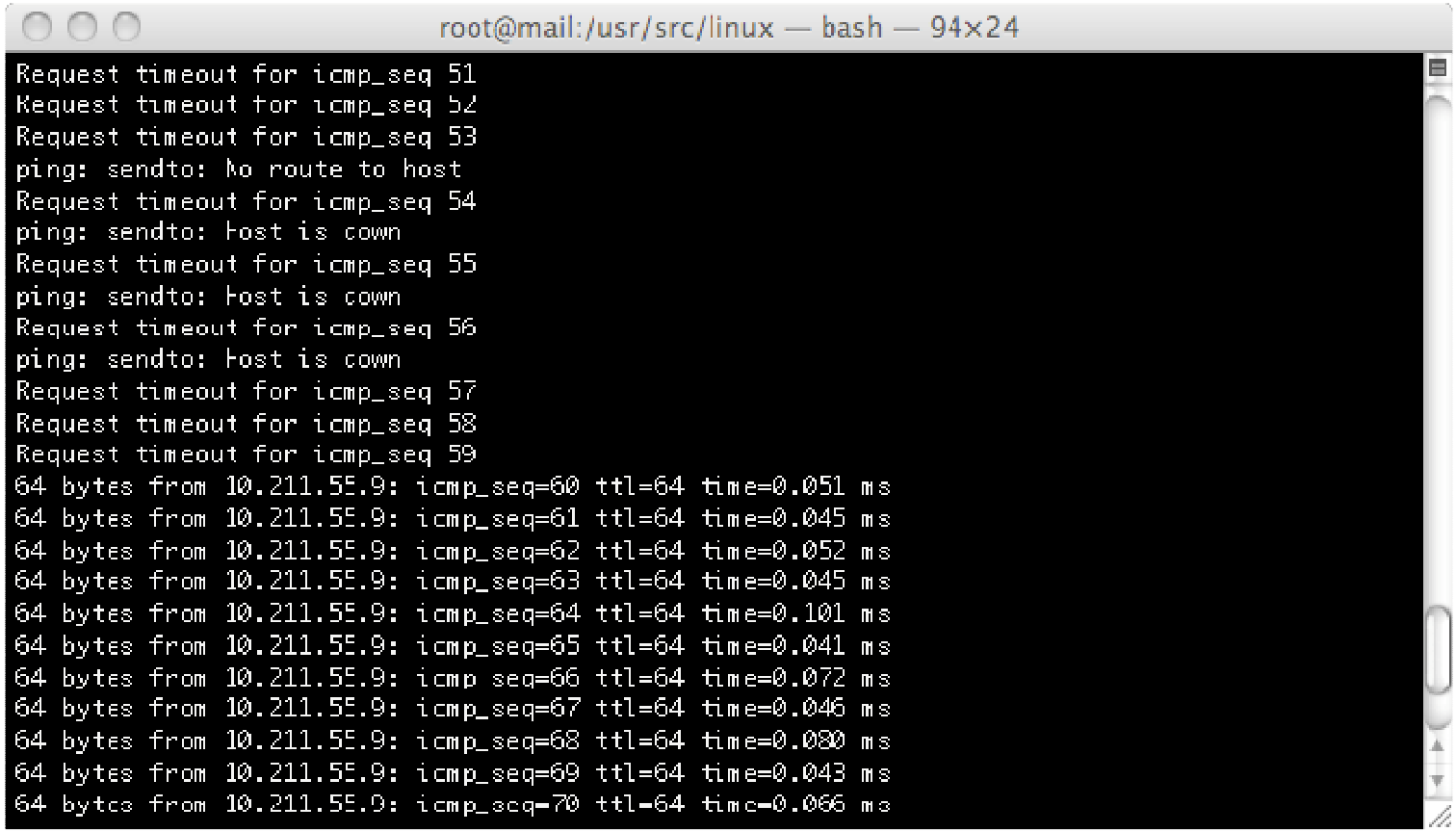
Knock.exe
http://www.zeroflux.org/proj/knock/files/knock-cygwin.zip

Or, build your own!

Generating The Knock



Knock Is Complete!



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), 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:

```
UDPStartup()
$socket = UDPOpen("10.0.1.1", 1234)
 $status = UDPSend($socket, "supersecretpassword1")
 UDPCloseSocket($socket)
$socket = UDPOpen("10.0.1.1", 4321)
 $status = UDPSend($socket, "supersecretpassword2")
 UDPCloseSocket($socket)
 UDPShutdown()
```

Create Layer 7 Rules – Step 2

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

LearnMikroTik.com
Network Training & Consulting

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?

LearnMikroTik.com
Network Training & Consulting

Thank You

LearnMikroTik.com
http://www.LearnMikroTik.com
info@LearnMikroTIk.com

LearnMikroTik.com
Network Training & Consulting