MikroTik Router

Setup and Secure Your RouterOS 6.x Device

Last Updated: 2021/4/25

Table of Contents

Prerequisites

1. MikroTik Device or VM with the latest version of RouterOS installed.
    a. *Update to the latest version will be performed after initial login to the physical device or VM.*
    b. *Version 6.48.2 is the latest version as of 2021/04/25.*
2. Download of the most recent version of WinBox (32-bit or 64-bit)
    a. *Version 3.27 is the latest version as of 2021/04/25.*
3. PC or laptop connected to the router will need to be configured for DHCP.
4. Network connection to any port other than Port 1 on the device will be established with the computer used for setup.
5. Internet access to external links which will be referenced for WinBox procedures (where applicable).

Initial Setup

Processes documented within this body of work assume that all prerequisites have been met. The system connected to the device being configured will have a copy of the most recent version of WinBox available on a local drive or external device that is accessible by the system.

- The device that is connected to the router or switch will obtain a DHCP address of *192.168.88.x*.
- The default address of MikroTik devices will be 192.168.88.1.

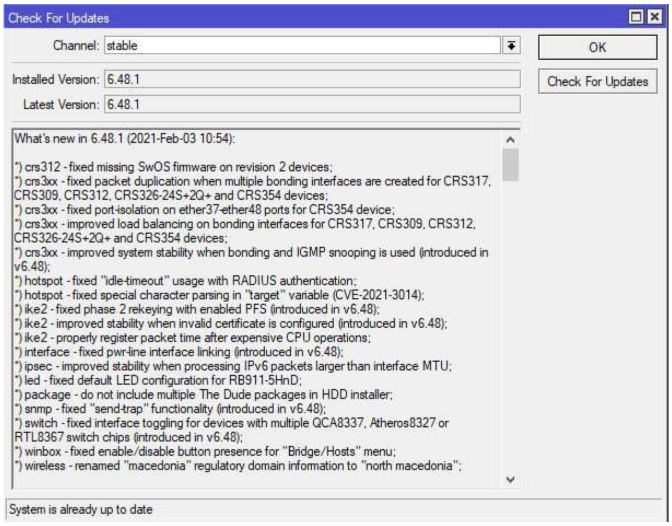
Executing WinBox on the system connected to the device that is being configured will show the MAC Address of the device in question. In the **Connect To:** field, the MAC Address or default IP address may be used to initialize the session. Default credentials will consist of the following components:

- *User ID*: admin
- *Password*: leave this field blank as the default administrator account does not have a password assigned to it.

With the appropriate values having been populated in the **Connect To:** and **Login** fields, **left click** on the **Connect** button to establish the WinBox session. The very first task involves updating the installed firmware to the most recent release. This will ensure that any known vulnerabilities that existed in prior releases have been addressed. Additionally, performing the update will provide bug fixes or may enhance the operation of existing features.

WinBox GUI – System Update

In the GUI, **left click** on the **Quick Set** navigation element on the left-hand side of the window. This will open a new window within the interface that shows the configured mode of the device, its MAC address, bridge configuration, VPN Access, a name for the system (default is *MikroTik*) and fields to change the default password (which is blank). Underneath System are buttons for **Check for Updates** and **Reset Configuration**. **Left click** on the **Check for Updates** button to spawn the Check for Updates window.



Channel: stable

Installed Version: 6.48.1

Latest Version: 6.48.1

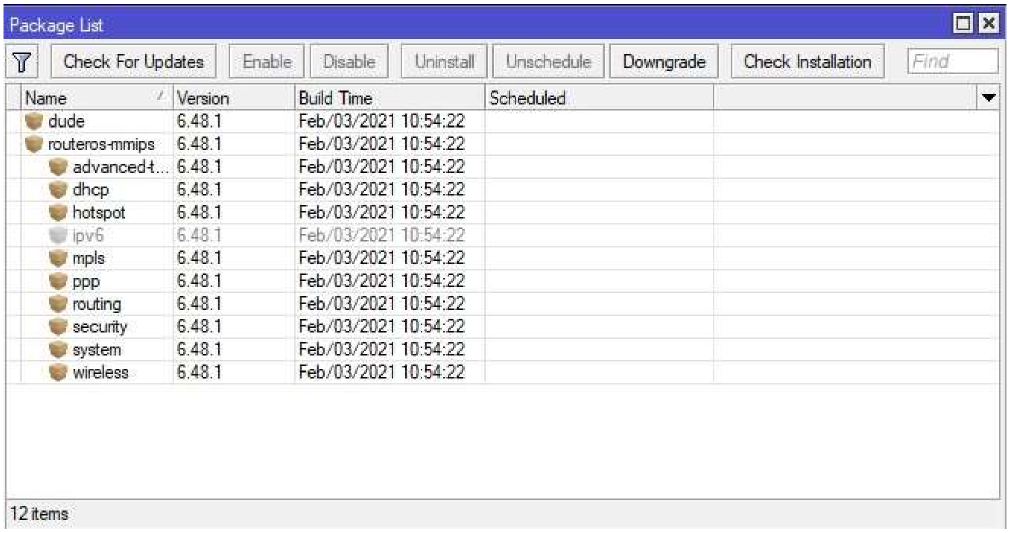
```
What's new in 6.48.1 (2021-Feb-03 10:54):

*) crs312 - fixed missing SwOS firmware on revision 2 devices;
*) crs3xx - fixed packet duplication when multiple bonding interfaces are created for CRS317,
CRS309, CRS312, CRS326-24S+2Q+ and CRS354 devices;
*) crs3xx - fixed port-isolation on ether37-ether48 ports for CRS354 device;
*) crs3xx - improved load balancing on bonding interfaces for CRS317, CRS309, CRS312,
CRS326-24S+2Q+ and CRS354 devices;
*) crs3xx - improved system stability when bonding and IGMP snooping is used (introduced in
v6.48);
*) hotspot - fixed "idle-timeout" usage with RADIUS authentication;
*) hotspot - fixed special character parsing in "target" variable (CVE-2021-3014);
*) ike2 - fixed phase 2 rekeying with enabled PFS (introduced in v6.48);
*) ike2 - improved stability when invalid certificate is configured (introduced in v6.48);
*) ike2 - properly register packet time after expensive CPU operations;
*) interface - fixed pwr-line interface linking (introduced in v6.48);
*) ipsec - improved stability when processing IPv6 packets larger than interface MTU;
*) led - fixed default LED configuration for RB911-5HnD;
*) package - do not include multiple The Dude packages in HDD installer;
*) snmp - fixed "send-trap" functionality (introduced in v6.48);
*) switch - fixed interface toggling for devices with multiple QCA8337, Atheros8327 or
RTL8367 switch chips (introduced in v6.48);
*) winbox - fixed enable/disable button presence for "Bridge/Hosts" menu;
*) wireless - renamed "macedonia" regulatory domain information to "north macedonia";
```

System is already up to date

To apply a newer release (when available) within the stable channel, **left click** the **Download&Install** button in order to obtain and apply the noted updates. Upon completion of installation, the device will reboot. A disconnect will occur within WinBox after the update has been completed. Reconnect to the device once it is online and reappears in the **Neighbors** tab.

Alternately, this same procedure may be initiated by **left clicking** on **System -> Packages**. Once the **Package List** window opens, **left click** on the **Check for Updates** button near the top of the window.



Name	Version	Build Time	Scheduled
dude	6.48.1	Feb/03/2021 10:54:22	
routeros-mmips	6.48.1	Feb/03/2021 10:54:22	
advanced-t...	6.48.1	Feb/03/2021 10:54:22	
dhcp	6.48.1	Feb/03/2021 10:54:22	
hotspot	6.48.1	Feb/03/2021 10:54:22	
ipv6	6.48.1	Feb/03/2021 10:54:22	
mpls	6.48.1	Feb/03/2021 10:54:22	
ppp	6.48.1	Feb/03/2021 10:54:22	
routing	6.48.1	Feb/03/2021 10:54:22	
security	6.48.1	Feb/03/2021 10:54:22	
system	6.48.1	Feb/03/2021 10:54:22	
wireless	6.48.1	Feb/03/2021 10:54:22	

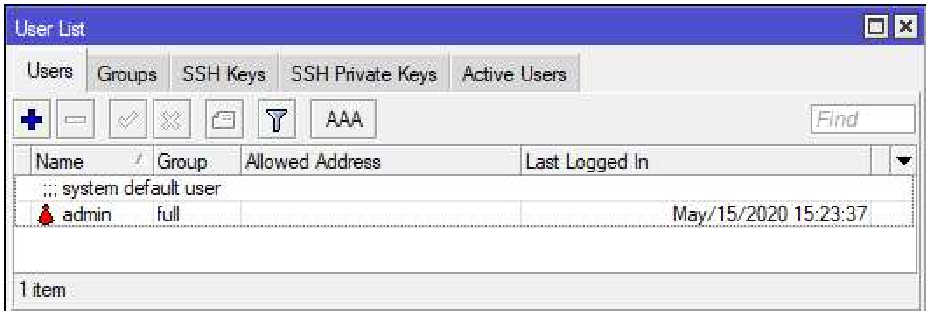
12 items

WinBox GUI – Securing the Router

The processes included in MikroTik's Wiki will be followed but will be completed via the WinBox graphical user interface (GUI) rather than using a Terminal session. While the Terminal will be more efficient from the perspective of not having to navigate through the various elements of the user interface, we are focused on providing a path that will allow individuals who are more accustomed to a GUI to achieve the same results without incurring the frustration of having to try and figure out where the configuration settings are buried sans any other formal reference.

Modifying the Administrative Credentials

The commands provided for the *Access username* and *Access password* sections of MikroTik's Wiki can be modified through the WinBox GUI by navigating to **System – Users**.



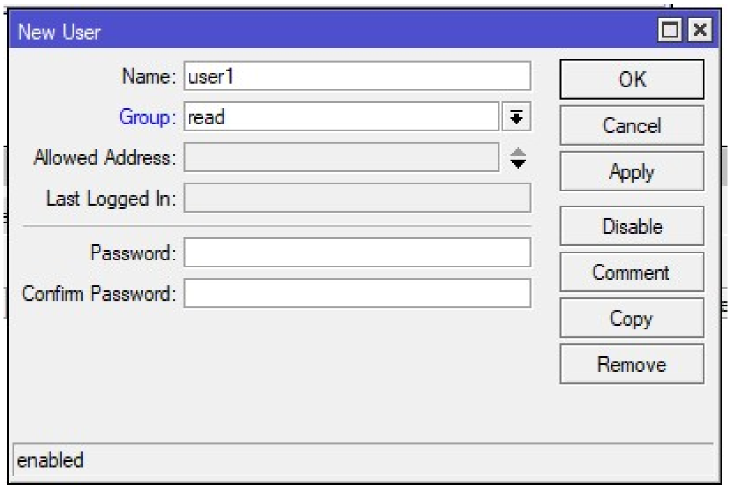
Name	Group	Allowed Address	Last Logged In
;;; system default user			
admin	full		May/15/2020 15:23:37

1 item

As you can see in the provided screenshot, the default credential of admin resides here. To replicate the actions taken within the Wiki, a new account will be created with a strong password. With the **User List** window active, we have one of three options available to create the new account.

1.) **Right-click** in the white space below the **admin** account and **left click** on **Add** on the context menu.
2.) Press the **INS** key on the keyboard.
3.) **Left click** the **+** button above the **system default user** comment shown in the screenshot.

Any of the methods listed above will spawn a **New User** window which is shown below.



Name: user1
Group: read
Allowed Address:
Last Logged In:
Password:
Confirm Password:
enabled

Within this window, the values of **Name**, **Group**, **Password** and **Confirm Password** will be modified. In the **Name** field, delete the value of **user1** and enter a replacement username for the new Administrator account. Once you have entered a viable name that is not **admin**, **left click** on the downward arrow to the right of the **Group** list box. Select **full** within the list of options. While the **Allowed Address** list will ideally contain values to limit which IP addresses may be used to access the system, the design and configuration of the network has not been established at this point. This field should be left blank until the setup has been completed. Finally, a strong password will need to be entered and confirmed. If you are using a password manager, generate a strong password and enter it into the **Password** and **Confirm Password** fields.

NOTE: If you are not using a password manager, tools such as KeePass are free of charge, can generate strong passwords, and store these passwords in a local repository.

Once the new values for the account have been entered, **left click** the **OK** button. In WinBox, **left click** on the **Session** menu item and **left click** on **Disconnect**. Modify the **Login** and **Password** values to match the newly created full user account and **left click** the **Connect** button. A successful login will confirm that the password was entered and confirmed correctly. Return to the **User List** window by **left clicking** on **System -> Users**. Select the default **admin** account in the **User List** window and **left click** on the minus button to delete the default account.

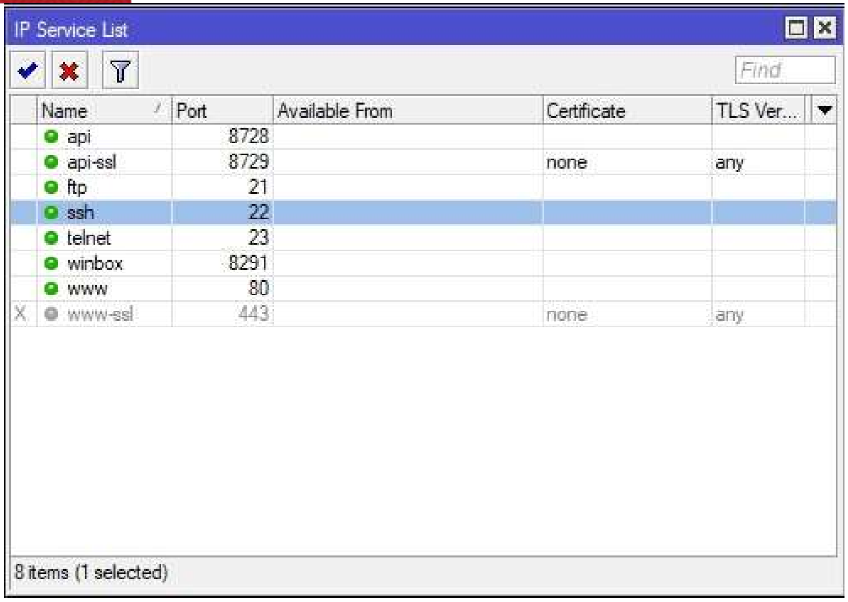
NOTE: It is possible to simply rename the default administrator account and assign it a strong password. Any error in the entry of modifications to the default credential may result in the inability to access the device via WinBox. The process that has been provided leaves room for error and prevents the need to force a factory reset early in the configuration process.

Securing Router Services

By default, there are numerous services enabled by default to facilitate access and detection of MikroTik products within a given network. As per the previously noted MikroTik Wiki, many of these services are designed to ease administration of MikroTik equipment. Leaving all services enabled with the applicable default configurations will run counter to best security practices. These services will be grouped using the same classifications contained within the Wiki: RouterOS Services, RouterOS MAC-access, Neighbor Discovery, Bandwidth Server, DNS Cache, and Other Clients Services.

RouterOS Services

The list of enabled services that are identified using the */ip service print* from a Terminal or SSH session can be found by **left clicking** on **IP -> Services**. A screenshot of the default IP Service list is provided below.



IP Service List

	Name	Port	Available From	Certificate	TLS Ver...
	● api	8728			
	● api-ssl	8729		none	any
	● ftp	21			
	● ssh	22			
	● telnet	23			
	● winbox	8291			
	● www	80			
X	● www-ssl	443		none	any

8 items (1 selected)

The Wiki uses a singular command of */ip service disable telnet,ftp,www,api,api-ssl* to efficiently disable these self-descriptive services in one pass. Understanding the functions of these services will better enable you, as the Administrator of the network, to determine if you will utilize these services.

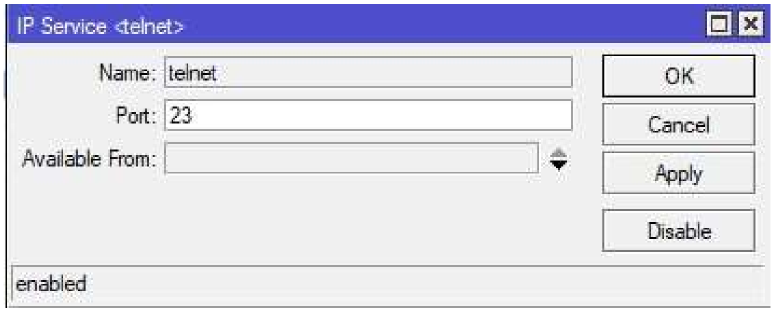
Telnet

At its core, telnet is an insecure protocol which may be used for interacting with RouterOS. With the availability of SSH in the platform, an extremely fringe use case would be required to justify keeping this service enabled. The Wiki recommendation should be followed in most use cases. To disable the service, **left click** on **telnet** once. With the service highlighted, **left click** on the red **X** button near the top of the **IP Service List** window. If the active indicator and telnet service name turns grey, the service will be successfully disabled.

If a fringe use case exists within your environment where telnet access to the device is warranted, the following modifications should be made to limit the potential for abuse of this service.

- Utilize a non-default port for the service (Port 23 is default).
- Utilize the **Available From** field to limit which IP addresses or IP ranges can access the service.

Making the necessary modifications involves selecting and **double clicking** the **telnet** service in the list to access the configuration interface that is shown below.



IP Service <telnet>

Name: telnet

Port: 23

Available From:

enabled

The text field for **Port** value will be modified. **Left click** the downward facing arrow at the end of the **Available From** field to generate an editable value. Enter the required IP address that will interface with the device via telnet. Further selection of the downward facing arrow will allow additional addresses or ranges to be defined for permitted access to the service. Once the appropriate values have been entered, **left click** the **OK** button to commit the modifications to the telnet service.

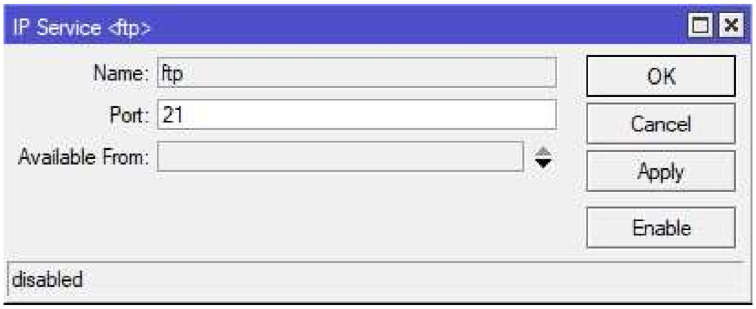
FTP

The FTP service may be used as part of maintenance-related processes for backing up configuration files or other miscellaneous data from the device. While basic authentication, default port modification, and IP address restrictions can be enabled for the service, best practices would involve utilizing SFTP (which is available since RouterOS 6.45 beta 50) for associated transfers. The Wiki recommendation should be followed in most use cases. To disable the service, **left click** on **ftp** once. With the service highlighted, **left click** on the red **X** button near the top of the **IP Service List** window. If the active indicator and ftp service name turns grey, the service will be successfully disabled.

If a fringe use case exists within your environment where FTP access to the device is warranted, the following modifications should be made to limit the potential for abuse of this service.

- Utilize a non-default port for the service (Port 21 is default).
- Utilize the **Available From** field to limit which IP addresses or IP ranges can access the service.

Making the necessary modifications involves selecting and **double clicking** the **ftp** service in the list to access the configuration interface that is shown below.



IP Service <ftp>

Name: ftp
Port: 21
Available From:

disabled

The text field for **Port** value will be modified. **Left click** the downward facing arrow at the end of the **Available From** field to generate an editable value. Enter the required IP address that will interface with the device via FTP. Further selection of the downward facing arrow will allow additional addresses or ranges to be defined for permitted access to the service. Once the appropriate values have been entered, **left click** the **OK** button to commit the modifications to the FTP service.

WWW/WWW-SSL

The WWW service plays a critical role in enabling WebFig access to the device in question. WebFig's design enables a WinBox experience within a web browser. While this would simplify administration of equipment on non-Windows platforms, the service is not appropriately secured by default. If WebFig will be used within your environment, we would encourage taking the extra steps involved with enabling the secured iteration of the service (**www-ssl**, which is disabled by default). The Wiki recommendation should be followed in all use cases. To disable the service, **left click** on **www** once. With the service highlighted, **left click** on the red **X** button near the top of the **IP Service List** window. If the active indicator and www service name turns grey, the service will be successfully disabled.

The secure variant of WebFig is disabled by default. A valid certificate will need to be generated and placed within the RouterOS file system to enable this functionality. If you do not have a valid or dedicated certificate solution for your environment and plan to utilize Let's Encrypt for this purpose, the following GitHub repository will be useful in automating the renewal process: https://github.com/gitpel/letsencrypt-routeros. Contrary to other blogs or procedures that may be discovered when searching the Internet, presenting the **www-ssl** service on the external interface (WAN) without any additional layers of monitoring, security controls, or event management will be discouraged.

API/API-SSL

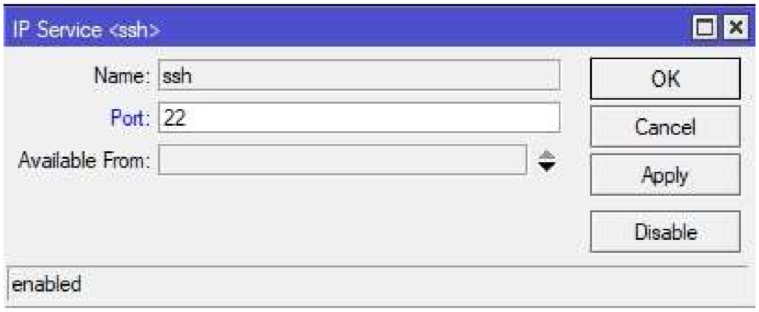
The api and api-ssl services enable the use of Restful APIs to interface with the device in question. If this functionality will be used within your environment, we would encourage taking the extra steps involved with enabling the secured iteration of the service (**api-ssl**). The Wiki recommendation should be followed in most use cases. To disable the service, **left click** on **api** once. With the service highlighted, **left click** on the red **X** button near the top of the **IP Service List** window.

Repeat this process after highlighting the **api-ssl** service. If the active indicator and api/api-ssl service names turns grey, the service will be successfully disabled.

SSH

The SSH service is a self-explanatory solution for enabling a secured shell session with the target device. The use of the WinBox GUI and Terminal within this body of work is selected to enable individuals that may not be familiar with performing administration and configuration functions solely via the command line (CLI). This does not fully eliminate the need to take the time to learn the CLI. As previously noted, disabling these service and further configuration elements that will be addressed throughout this body of work may be completed in a faster manner with the CLI. Keeping the SSH service enabled will simplify administration and future configuration changes once familiarity with the CLI is achieved. The primary recommendation involves modifying the default port from 22 to a non-standard port.

Making the necessary modifications involves selecting and **double clicking** the **ssh** service in the list to access the configuration interface that is shown below.



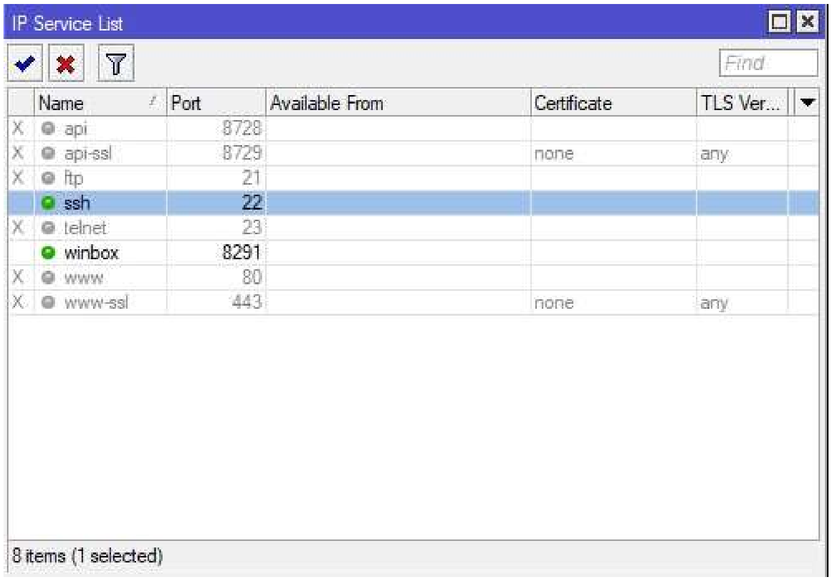
IP Service <ssh>

Name: ssh
Port: 22
Available From:

enabled

The text field for **Port** value will be modified. For enhanced security, **left click** the downward facing arrow at the end of the **Available From** field to generate an editable value. Enter the required IP address that will interface with the device via SSH. Further selection of the downward facing arrow will allow additional addresses or ranges to be defined for permitted access to the service. Once the appropriate values have been entered, **left click** the **OK** button to commit the modifications to the SSH service.

If all RouterOS services that are recommended to be disabled as per the Wiki have been modified by the WinBox GUI, the result will appear like the screenshot provided below.



IP Service List

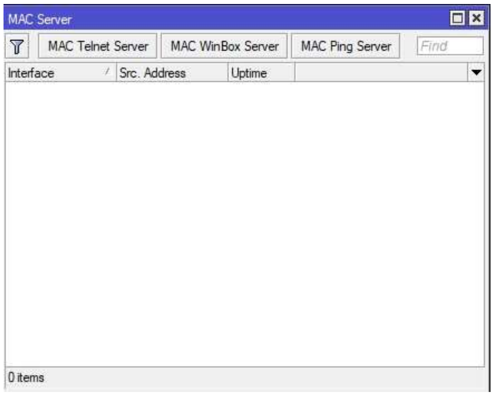
	Name	Port	Available From	Certificate	TLS Ver...
X	● api	8728			
X	● api-ssl	8729		none	any
X	● ftp	21			
	● ssh	22			
X	● telnet	23			
	● winbox	8291			
X	● www	80			
X	● www-ssl	443		none	any

8 items (1 selected)

NOTE: While this screenshot shows the ssh service running on the default port, the recommendation in the SSH procedure to change the port number will result in the port value being different than what is displayed in this example.

RouterOS MAC-Access Services

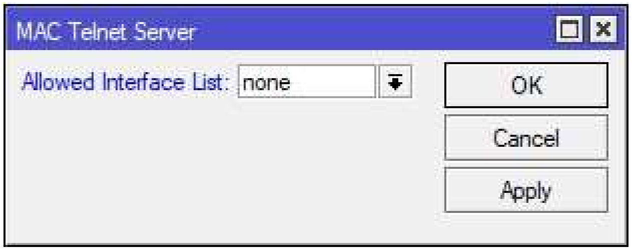
The MAC-Access Services provide a method to interface with the RouterOS-based device when it does not have an IP address established. While these services are beneficial during initial setup and configuration, they should be disabled once setup and configuration has been completed. Modification of these services within the WinBox GUI is one of the few areas where the GUI may be faster than manually entering the commands using the Terminal or an SSH session. All three services can be found by **left clicking** on **Tools -> MAC Server** in the WinBox GUI. The window shown below will appear with clearly labeled buttons near the top of the window for the three services that are in scope for modification.



NOTE: The procedures to disable these services are organized within this body of work in alignment with the MikroTik Wiki. The recommendation involves keeping the **MAC WinBox Server** and **MAC Ping Server** enabled until the configuration of the RouterOS device has been completed and validated. Without these services being enabled as a potential fallback to reconnect to the device in the event of an erroneous configuration change, the recovery option to access the device may involve a full system reset.

MAC-Telnet

The MAC-Telnet service provides the capability to establish a telnet connection with a target device that does not have an assigned IP address. Modification of the service changes the network used for this communication. **Left click** the **MAC Telnet Server** button to access the configuration interface that is shown below.

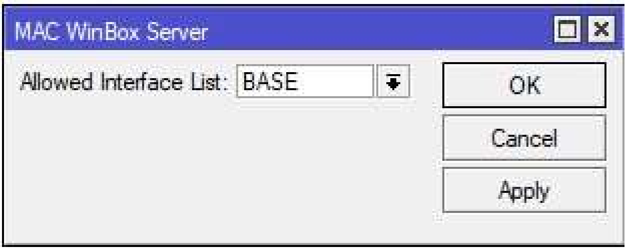


Allowed Interface List: none

As shown in the image above, modify the value of the **Allowed Interface List** by **left clicking** the list box arrow at the end of the field. **Left click** on the value of **none**. This default interface sets the associated service to not use any of the internal or external connections available to the device. **Left click** the **OK** button to commit the change.

MAC-WinBox

The MAC-WinBox service provides the capability to establish a WinBox connection with a target device that does not have an assigned IP address. Modification of the service changes the network used for this communication. **Left click** the **MAC WinBox Server** button to access the configuration interface that is shown below.

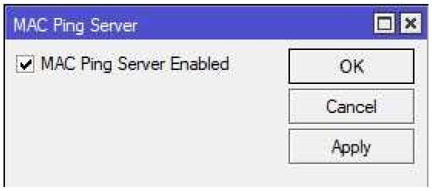


Allowed Interface List: BASE

Modify the value of the **Allowed Interface List** by **left clicking** the list box arrow at the end of the field. **Left click** on the value of **none**. This default interface sets the associated service to not use any of the internal or external connections available to the device. **Left click** the **OK** button to commit the change.

MAC-Ping

The MAC-Ping service provides the capability to test the connection with a target device using the MAC address of the device in lieu of an assigned IP address. Modification of the service involves disabling it. **Left click** the **MAC Ping Server** button to access the configuration interface that is shown below.

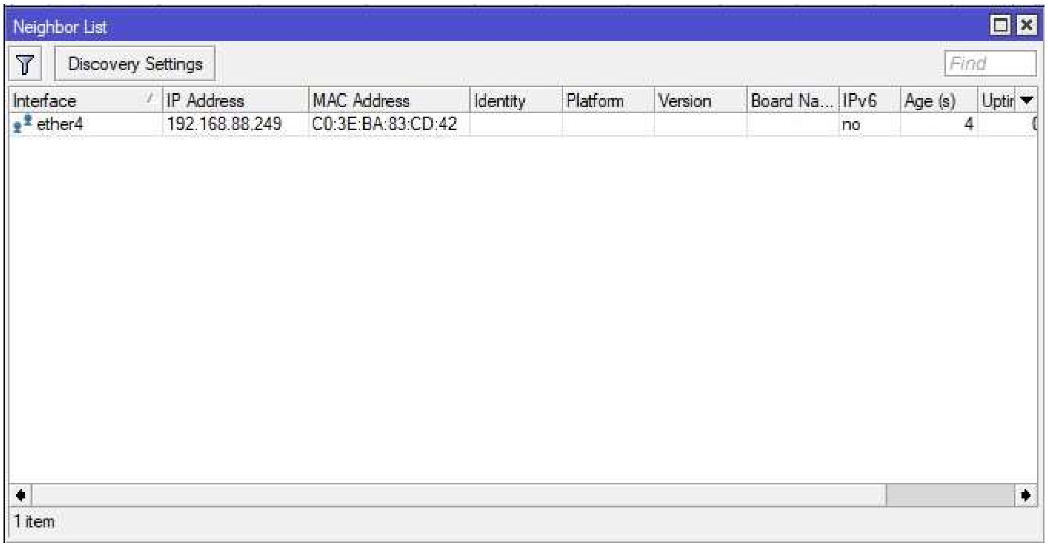


☑ MAC Ping Server Enabled

Left click the check box next to **MAC Ping Server Enabled** and **left click** the **OK** button to commit the change.

Neighbor Discovery Services

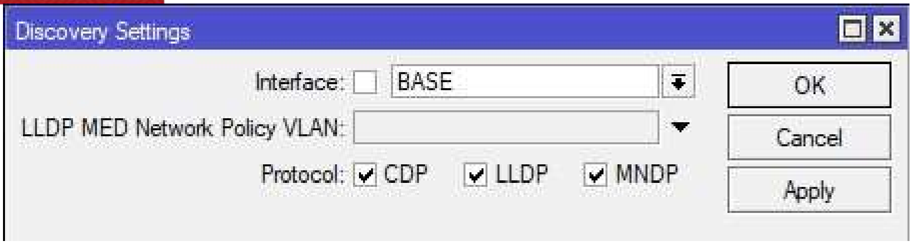
The Neighbor Discovery Services provide a method to show and recognize other RouterOS-based devices running on the same network. Modifying the utilized interface will need to be performed to disable this service. Within WinBox, **left click** on **IP -> Neighbors**. The **Discovery Settings** button near the top of the window contains the graphical interface for making the necessary modifications.



Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptir
ether4	192.168.88.249	C0:3E:BA:83:CD:42					no	4	(

1 item

Left click on the **Discovery Settings** button. The configuration window shown below will appear.


Discovery Settings

Interface: □ BASE

LLDP MED Network Policy VLAN:

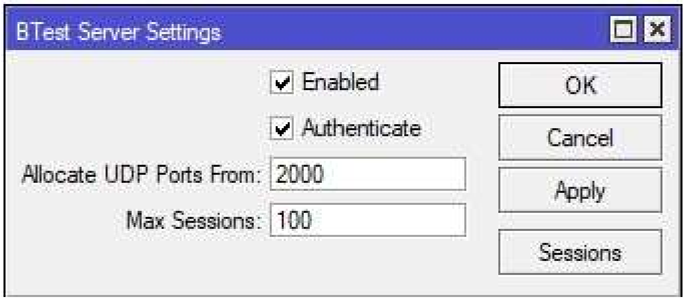
Protocol: ☑ CDP ☑ LLDP ☑ MNDP

Near the bottom of the list, there are three discovery protocols that are enabled. The first option pertains to the Cisco Discovery Protocol (**CDP**). This may be useful if Cisco hardware that utilizes this protocol will be part of the network stack. The second option is the vendor-neutral Link Layer Discovery Protocol (**LLDP**). Support for this protocol exists across multiple vendors. Finally, the third option is the MikroTik Network Discovery Protocol (**MNDP**). For many smaller networks or networks which will not mix hardware from multiple vendors, disabling the ability for this service to be abused will provide the ideal security profile.

To disable discovery, **left click** on the list box arrow at the end of the **Interface** row. Select the option of **none**. **Left click** the **OK** button to commit the change.

Bandwidth Server Service

The Bandwidth Server Service enables throughput testing between two RouterOS-based devices. This will be useful for performance validation and troubleshooting efforts yet does not need to be persistently enabled in production environments. Within WinBox, **left click** on **Tools -> BTest Server**. The **BTest Server Settings** window will appear.


BTest Server Settings

☑ Enabled

☑ Authenticate

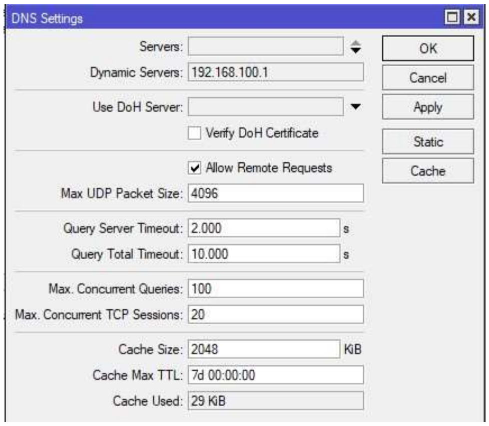
Allocate UDP Ports From: 2000

Max Sessions: 100

To disable this service, **left click** the checkbox next to **Enabled**. **Left click** the **OK** button to commit the change.

DNS Cache Service

The DNS Cache Service reduces resolution time for DNS requests from network endpoints to remote servers. This service will only require modification if caching is not required on the router or if an alternative network component fulfills this purpose. If caching is not required on the RouterOS device, it can be disabled by **left clicking** on **IP -> DNS** within WinBox. The **DNS Settings** window shown below will appear.


DNS Settings

Servers:

Dynamic Servers: 192.168.100.1

Use DoH Server:

□ Verify DoH Certificate

☑ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

Max. Concurrent Queries: 100

Max. Concurrent TCP Sessions: 20

Cache Size: 2048 KiB

Cache Max TTL: 7d 00:00:00

Cache Used: 29 KiB

Left click on the check box next to **Allow Remote Requests** to disable caching. **Left click** the **OK** button to commit the change.

Other Clients Services

The balance of services addressed in this section pertain to the MikroTik caching proxy, the MikroTik socks proxy, the MikroTik UPNP service, and the MikroTik dynamic domain name service or IP cloud service.

IP Proxy

The IP Web Proxy Service is disabled by default in RouterOS. To confirm disablement via the WinBox GUI, **left click** on **IP -> Web Proxy**. The **Enabled** check box will not be selected by default.

Socks Proxy

The Socks Proxy Service is disabled by default in RouterOS. To confirm disablement via the WinBox GUI, **left click** on **IP -> Socks**. The **Enabled** check box will not be selected by default.

UPnP Service

The Universal Plug and Play (UPnP) Proxy Service is designed to allow devices on the network to make the necessary modifications to a router or firewall for enabling communication between on-premises endpoints and cloud or remotely hosted services. Due to the potential for abuse of this service, best practices dictate that it should be disabled. Fortunately, this service is disabled by default in RouterOS. To confirm disablement via the WinBox GUI, **left click** on **IP -> UPnP**. The **Enabled** check box will not be selected by default.

Dynamic DNS (DDNS)/IP Cloud Service

The Dynamic DNS (DDNS)/IP Cloud Service aids in facilitating access to the device when the WAN connection is established using a non-persistent IP address. This functionality can come in handy if you are providing remote support for family members and want to establish a site-to-site virtual private network (VPN) between two MikroTik routers at different locations. **Left click** the **MAC Ping Server** button to access the configuration interface that is shown below. Although competing solutions may contain provisions to establish a fully qualified domain name (FQDN) of your choosing within the system, RouterOS is a bit more rigid with how this is handled. Specifically, the host name of the router is fixed in nature and will consist of the device MAC address followed by a DNS suffix of *sn.mynetname.net*. The fully qualified domain name for your router can be obtained by **left clicking** on **Quick Set** within WinBox and scrolling down to the **VPN** section of the **Quick Set** window. You will also see that the **VPN Access** service is disabled by default. Configuration of this service will not be addressed in this section. With the FQDN being known, the DDNS service can be found by **left clicking** on **IP -> Cloud**. By default, the DDNS service is disabled. If you require use of the service, **left click** the deselected check box next to **DDNS Enabled** and **left click** the **OK** button.

Enhancing SSH Security

Unfortunately, neither WinBox nor WebFig contain a graphical element to enforce strong cryptography for SSH sessions within RouterOS. At a minimum, the Wiki recommends enforcing strong-crypto. Depending on your security posture and standards, you may require a larger key size than the default of 2048. In either event, the terminal will be required to enable the necessary changes.

Within WinBox, **left click** on **New Terminal**. The Wiki command of */ip ssh set strong-crypto=yes* provides a singular step for enforcing the desired configuration setting. However, as this is the first mention of a native terminal/SSH workflow within this document, we will step through this in increments.

1.) Within the **Terminal** window, type **/ip ssh** and press **Enter** on the keyboard.

2.) Notice that the path has changed. Prior to entry of the command, the only elements behind the **>** were your user id @ the name of the router. After pressing Enter, we are now within the SSH configuration. Type **print** and press **Enter** on the keyboard.

3.) The configuration items and defined values for the SSH service will be listed with current settings. The third element that is displayed will be *strong-crypto: no*. In order to modify this value as a step in the process, type **set strong-crypto=yes** and press **Enter** on the keyboard.

4.) Confirmation of this settings modification can be obtained by typing **print** and pressing **Enter** on the keyboard.

5.) The third line printed out will now read *strong-crypto: yes*.

6.) (Optional) If you require a larger key size, type **set host-key-size=4096** (or whatever larger value meets your requirements and standards). Press **Enter** to enforce the change. Type **print** one more time and press **Enter** on the keyboard. The *host-key-size* line will be updated with the value you have set.

Securing Router Interfaces

Many MikroTik routers will be equipped with a significant quantity of Ethernet ports. Higher end models will also include an SFP or SFP+ port. Disabling unused interfaces will provide an additional layer of physical security that prevents an errant connection from being established.

NOTE: Complex network stacks may utilize additional ethernet or SFP/SFP+ ports to present designated network(s) to downstream switches or wireless access points. Recommendations for disabling interfaces contained within this document will hew to a more simplistic design where only two ports are required: one port for WAN connectivity and one port for downstream switch gear.

Ethernet/SFP Interfaces

The list of enabled services that are identified using the */interface print* command within a Terminal or SSH session can be found by **left clicking** on **Interfaces** in the WinBox GUI. Numbered ports on the router will correspond to like numbered ether# interfaces in WinBox. In a scenario where Port 1 is used for the WAN connection and Port 5 is used for the presentation of networks to downstream equipment, disabling ether2 through ether4 involves **double clicking** on the unused interface(s), one at a time, to access the port configuration. On the right side of the Interface <*ether#*> window will be a **Disable** button. **Left click** the **Disable** button and **left click** the **OK** button to disable the port. Repeat this process for all unused interfaces. If the available ports will be used for wired connections, this process will not be used.

LCD

Advanced and more powerful models within the MikroTik product portfolio may contain a small touchscreen LCD display on the top or the front of the unit. Depending on the configuration of the module, it may actively display details about the network. At a minimum, MikroTik recommends setting a PIN for the display to limit who may access the available information using this mechanism. Alternatively, the display can be disabled entirely. If your device is equipped with an LCD display, the WinBox GUI will contain an **LCD** interface under the **New Terminal** entry on the left-hand menu. **Left click** on **LCD** to open the configuration options. Achieving the same results as the Terminal-based command of */lcd set enabled=no* involves **left clicking** on the check box next to **Enabled** in the LCD window. Once the check box has been cleared, **left click** on the **OK** button to commit the change.

Firewall

NOTE: By default, IPv6 is disabled in RouterOS 6. Within the WinBox GUI, **left click** on **System -> Packages**. The **IPv6** package will appear in light grey font to indicate that it is disabled. Procedures contained in this section will focus on firewall configurations for IPv4. If IPv6 is a requirement for your environment, you will need to enable the package and configure sufficient rules to provide the necessary protections. The CLI references and settings for the IPv6 settings are available in the MikroTik Wiki.

The general concepts provided by MikroTik for performance and security considerations focus on establishing address lists that will be paired with filtering rules to provide a security baseline for clients on the network. The examples provided within their Wiki and newer documentation make the following assumptions:

- The default 192.168.88.0/24 will be the only network in scope for establishing filters.
- IP addresses within the RFC 6890 (Special-Purpose IP Address Registries) specification will not be accessed by devices inside of the network.
- Dissimilar labels for interfaces or functions will require analyzing the proposed commands or recommendations and understanding how these commands will need to be modified.
    - (i.e., the default label for the Bridge interface is bridge. Some Wikis and external references will use this standard in their commands, while other resources may represent the bridge using different names or labels within the same process).

Additional steps may be required if your network design includes multiple virtual LANs (VLANs) to properly segregate or isolate untrusted devices or Internet of Things-related endpoints. These concepts and the execution within the WinBox GUI may be added to a future revision of this document.

IPv4 Firewall to a Router

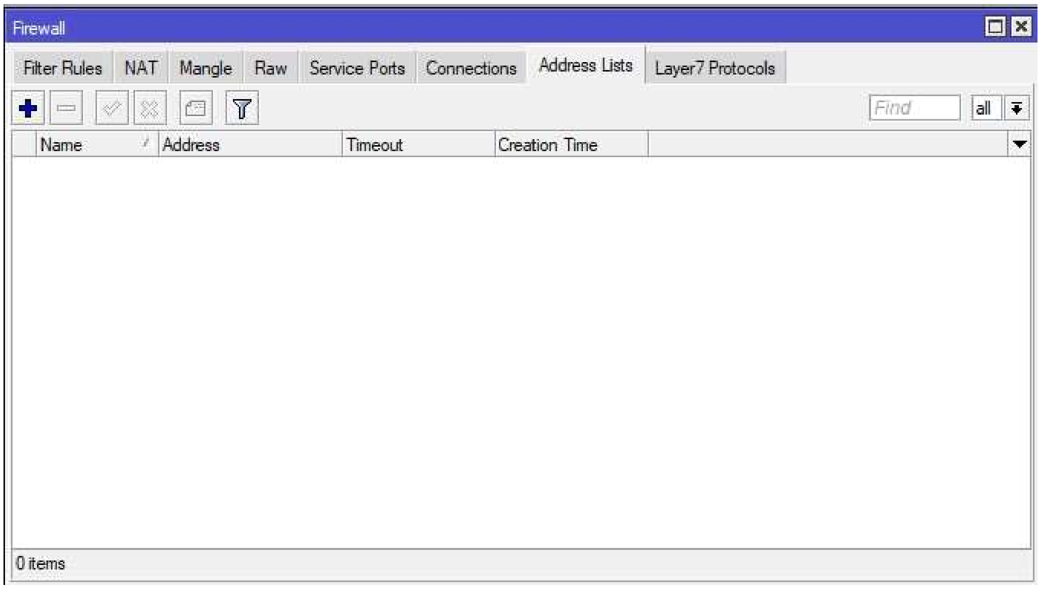
The objective of the filtering rules provided by MikroTik involves minimizing router load, establishing lists of IP addresses with an applicable label to simplify rule creation, and execution of an optional step for enabling ICMP access. The procedure provided below will cover establishing the following Terminal/SSH block of code using the WinBox GUI.

First, we will create the address lists of networks or IP ranges that can utilize the router. The Terminal/SSH commands for establishing this capability with the default network are provided below.

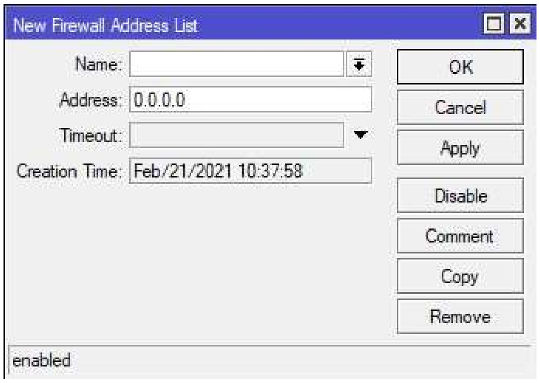
```
/ip firewall address-list
add address=192.168.88.2-192.168.88.254 list=allowed_to_router
```

Address List Definition

To perform this function using the WinBox GUI, **left click** on **IP -> Firewall**. Once the **Firewall** window appears, **left click** on the **Address Lists** tab within the window. The image below shows the default configuration where no lists have been defined.



Left click the **+** button below the tabs to access the **New Firewall Address List** window that is shown on the next page.


New Firewall Address List

Name:

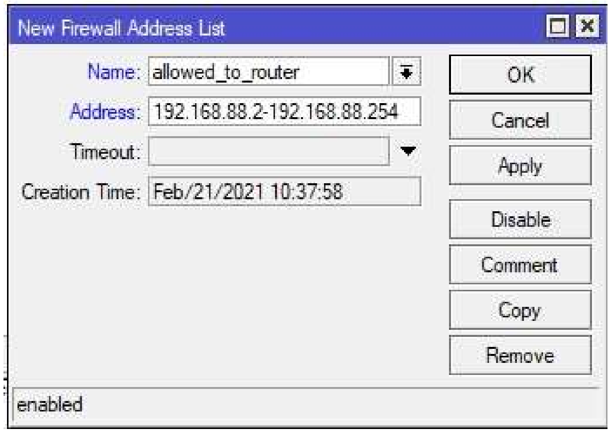
Address: 0.0.0.0

Timeout:

Creation Time: Feb/21/2021 10:37:58

enabled

Based on the second command noted on the prior page, the reference within the Wiki is defined as *allowed_to_router*. Within the **Name** field, we will use this list naming standard and type in **allowed_to_router**. Next, the list of IP addresses contained within the second command was *192.168.88.2-192.168.88.254*. In the Address field, type in **192.168.88.2-192.168.88.254**. An optional step will involve establishing a comment for the address list. This comment can consist of a longer-form explanation of the purpose of the list. **Left click** the **Comment** button. In this example, type **Default Network – Permit Routing** and **left click** the **OK** button. With all modifications made, the result of the New Firewall Address List will appear as shown below.


New Firewall Address List

Name: allowed_to_router

Address: 192.168.88.2-192.168.88.254

Timeout:

Creation Time: Feb/21/2021 10:37:58

enabled

Left click the **OK** button to establish the Address List. The comment that was entered will appear above the entry in the Address Lists. If you have defined additional networks and DHCP servers to support ranges beyond the default configuration, the subsequent additions to the **allowed_to_router** list can be made by selecting the established name in the drop-down list and entering the additional network(s) that have been established.

Firewall Rule Filters

The second part of this process involves implementing filter rules that comply with the commands provided in the Wiki.

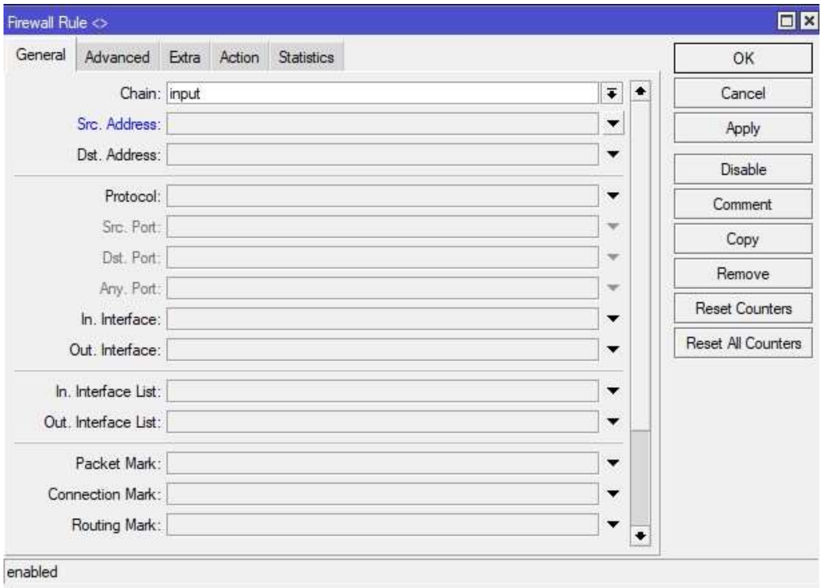
```
/ip firewall filter
add action=accept chain=input comment=”Default Configuration” connection-state=established,related
add action=accept chain=input src-address-list=allowed_to_router
add action=accept chain=input protocol=icmp
add action=drop chain=input
```

These commands switch to the Filter Rules section of the firewall and establish four rules with associated actions. In a fresh “out of the box” environment, there will be eleven filter rules which already exist. Within the **Firewall** window, **left click** the **Filter Rules** tab. The table provided below summarizes the order, intent, and actions of these default configuration rules.

	Rule Number	Chain	Action
Special dummy rule to show fasttrack counters	0	forward	passthrough
Accept established,related,untracked	1	input	accept
Drop invalid	2	input	drop
Accept ICMP	3	input	drop
Accept to local loopback (for CAPsMAN)	4	input	accept
Drop all not coming from LAN	5	input	drop
Accept in IPSec Policy	6	forward	accept
Accept out IPSec Policy	7	forward	accept
Fasttrack	8	forward	fastrrack
Accept established,related,untracked	9	forward	accept
Drop invalid	10	forward	drop
Drop all from WAN not DSTNATed	11	forward	drop

Excluding rule zero, the balance of these initial "out of the box" rules have the listed comments or purpose prefixed with *defconf*. This abbreviation indicates a default configuration. In order comply with the minimum recommendations in the filter command block of the Wiki, the easiest method using the WinBox GUI involves modifying rule one and determining whether your environment will benefit from the continued enablement of rule three.

Double click on rule one in the **Filter Rules** list to access the **Firewall Rule** configuration window shown below.



Chain: input

enabled

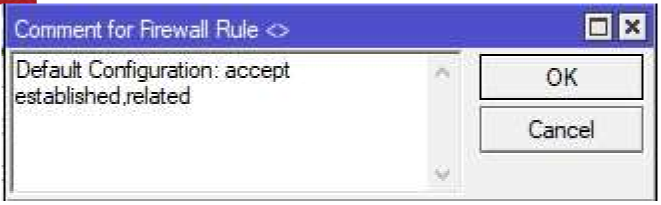
To the right of the text fields in the **General** tab is a scroll bar. Scrolling further down toward the bottom will provide visibility for the **Connection State** line. In this line, the check boxes for **established, related,** and **untracked** are selected. The following line in the Wiki code block is slightly more secure than the default configuration as it excludes untracked connections.

add action=accept chain=input comment="Default Configuration" connection-state=established,related

Modifying rule number one will provide the intended outcome with less effort. To align the settings to the desired state, **left click** on the checkbox next to **untracked** to de-select permitting this state. Once the untracked option is disabled, **left click** on the **Comment** button to modify the default comment. This comment will exist with the following verbiage.

defconf: accept established,related,untracked

At a minimum, delete the second comma and the word **untracked** from the text box. If you prefer to spell out "Default Configuration" as part of the comment, you may delete **defconf** and type **Default Configuration** in its place.

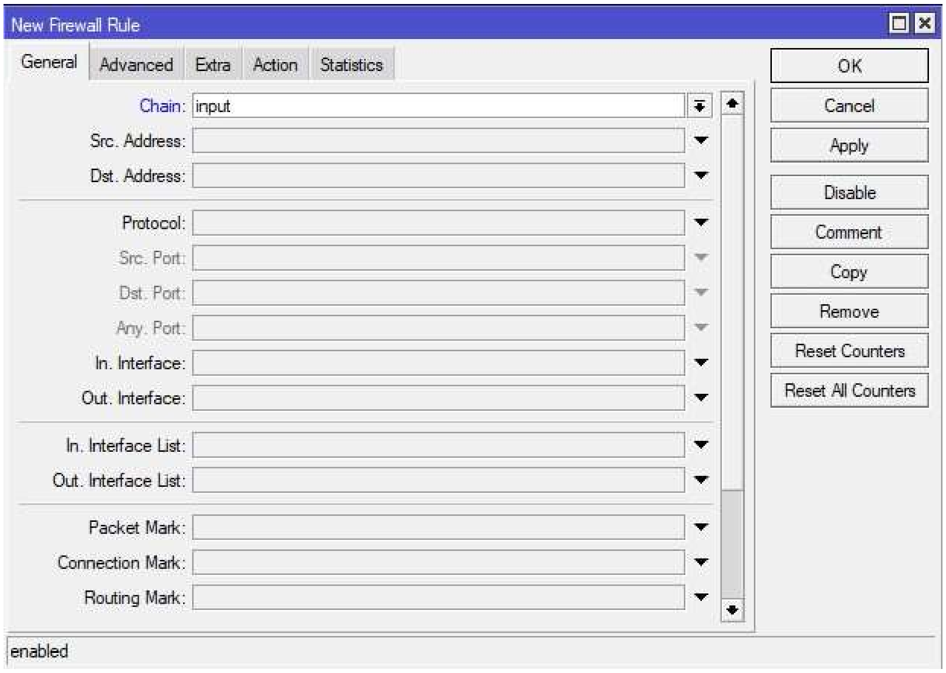


Default Configuration: accept established,related

Once the comment has been updated to reflect the removal of untracked connections being accepted, **left click** the **OK** button on the **Comment for Firewall Rule** window and **left click** the **OK** button on the **Firewall Rule** window. The second command offered within the Wiki leverages the previously created **allowed_to_router** address list to accept input connections.

add action=accept chain=input src-address-list=allowed_to_router

This rule does not exist by default and will need to be created. **Left click** the **+** button below the **Filter Rules** tab in the **Firewall** window. A **New Firewall Rule** window will appear. Modify the **Chain** value using the list box control to the right of the field. **Left click** on **input**.



Chain: input

enabled

Left click the **Advanced** tab and **left click** the downward arrow at the end of the **Src. Address List** row. This will provide a list box selector. **Left click** the list box control and **left click** on **allowed_to_router** to select the desired list. If a comment is desired, **left click** the **Comment** box and enter an intelligible comment for the rule. **Left click** the **OK** button in the **Comment for New Firewall Rule** window and the **New Firewall Rule** window. This will create a new rule (number twelve) in the list. **Left click** on the rule and drag it to the position of rule number two. In order to align our rules with the balance of commands established in the Wiki, drag rule number four into the place where rule number three resides. Once this has been done, the Filter Rules list should match the table below.

	Rule Number	Chain	Action
Special dummy rule to show fasttrack counters	0	forward	passthrough
Accept established,related,untracked	1	input	accept
<New rule to accept input for allowed_to_router>	2	input	accept
Accept ICMP	3	input	accept
Drop invalid	4	input	drop
Accept to local loopback (for CAPsMAN)	5	input	accept
Drop all not coming from LAN	6	input	drop
Accept in IPSec Policy	7	forward	accept
Accept out IPSec Policy	8	forward	accept

Fasttrack	9	forward	fastrrack
Accept established,related,untracked	10	forward	accept
Drop invalid	11	forward	drop
Drop all from WAN not DSTNATed	12	forward	drop

Rule number three specifically focuses on allowing and accepting ICMP traffic. This will be useful for monitoring and troubleshooting purposes yet may not be necessary depending upon your standards. If this optional rule is not required, **left click** on the Accept ICMP rule and **left click** the red **X** button to disable it. The final rule defined in the Wiki is already established as rule number four.

IPv4 Firewall for Clients

The objective of the client-related filtering rules provided by MikroTik involves improving data throughput, dropping invalid connections or connections defined within another to-be-implemented address list, blocking connections that are not utilizing network address translation (NAT), and preventing packets on the LAN from transferring if they do not originate from an endpoint with a valid LAN IP Address. Further logging provisions are implemented as part of the client rules. The procedure provided below will cover establishing the following Terminal/SSH block of code using the WinBox GUI.

```
/ip firewall filter
add action=fasttrack connection chain=forward comment=FastTrack connection-state=established,related
add action=accept chain=forward comment=”Established, Related” connection-state=established,related
add action=drop chain=forward comment=”Drop invalid” connection-state=invalid log=yes log-prefix=invalid
add action=drop chain=forward comment=”Drop tries to reach non-public addresses from LAN” dst-address-
list=not_in_internet in-interface=bridge log=yes log-prefix=!public_from_LAN out-interface=!bridge
add action=drop chain=forward comment=”Drop incoming packets that are not NATted” connection-nat-state=!dstnat
connection-state=new in-interface=ether1 log=yes log-prefix=!NAT
add action=drop chain=forward comment=”Drop incoming from Internet which are non-public IPs” in-interface=ether1
log=yes log-prefix=!public src-address-list=not_in_internet
add action=drop chain=forward comment=”Drop packets from LAN that do not have LAN IP” in-interface=bridge log=yes
log-prefix=LAN_!LAN src-address=!192.168.88.0/24
```

```
/ip firewall address-list
add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet
add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet
add address=10.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet
add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet
add address=192.0.0.0/24 comment=RFC6890 list=not_in_internet
add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet
add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet
add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet
add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet
add address=224.0.0.0/4 comment=Multicast list=not_in_internet
add address=192.88.99.0/24 comment=”6to4 Relay Anycast [RFC 3068]” list=not_in_internet
```

There is much to unpack in the client-side code block. Beginning with the creation of the new Address Lists and designated ranges will be easier than implementing or modifying the listed filter rules in the WinBox GUI.

- If the Firewall window has been closed in the WinBox GUI, **left click** on **IP -> Firewall**. **Left click** on the **Address Lists** tab.
- If the Firewall window is still open in the WinBox GUI, **left click** on the **Address Lists** tab.

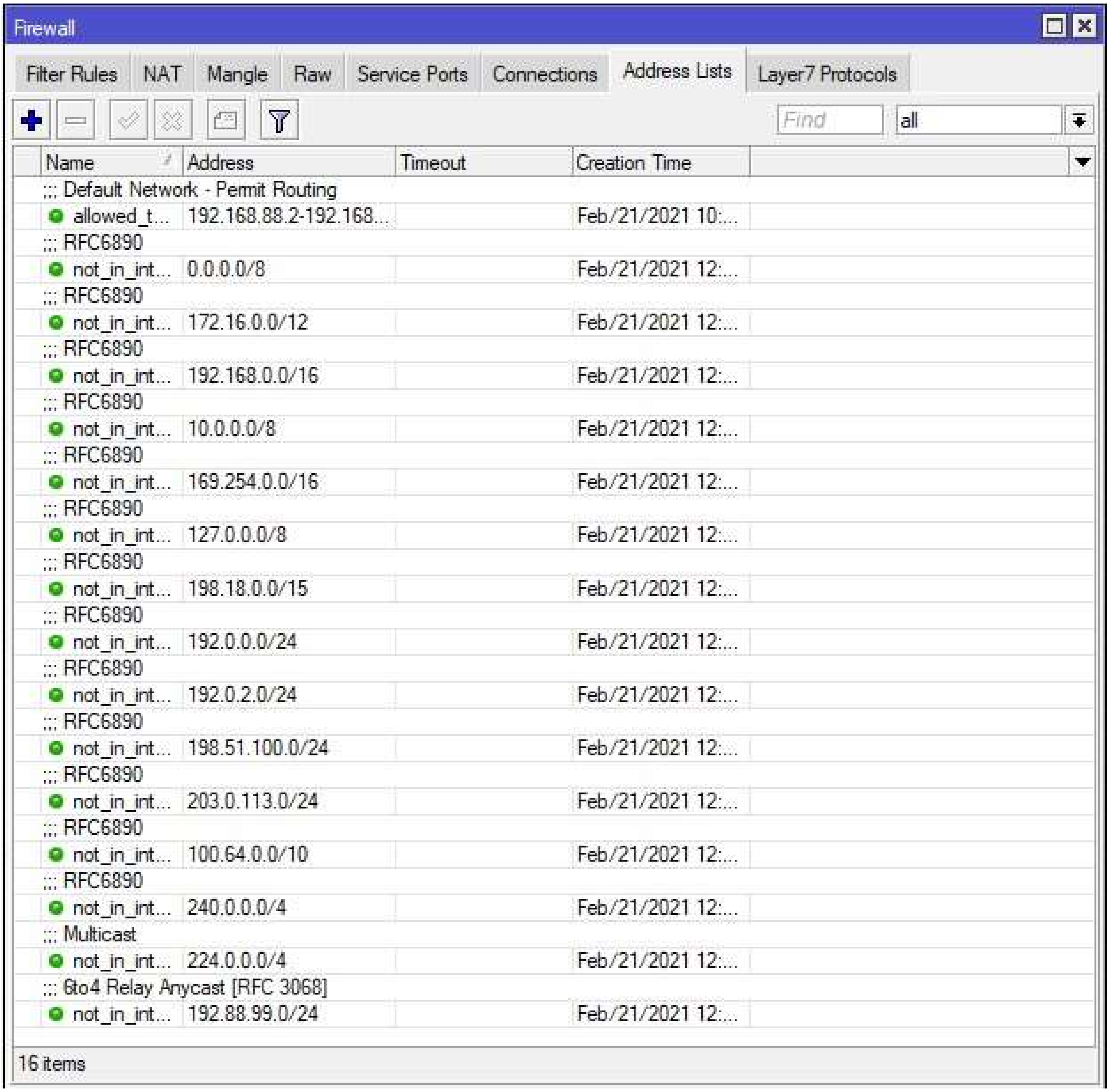
If we look at all the entries under the *ip firewall address-list* code block, the first thirteen have the same comment while the last two items have a different comment. This will result in a cluttered list within the WinBox GUI. By comparison, applying the comment to the first item in the list and opting to skip identical comments will make the list appear as appropriately grouped in the default view. Conversely, using Comment filters would return an incomplete list of applicable address ranges without the use of the comment for all associated entries.

Address List Definition

With the quantity of addresses that will be added to the *not_in_internet* list, it will be much faster to copy the command block and paste it into a Terminal window.

NOTE: Pressing Ctrl-V to paste within the Terminal window in the WinBox GUI will enable auto-completion for commands within the session. Utilize a **right click** and select **paste** for commands being copied from this body of work. If you've accidentally enabled auto-completion, pressing **Ctrl-V** will revert the session to using tab-based auto-completion.

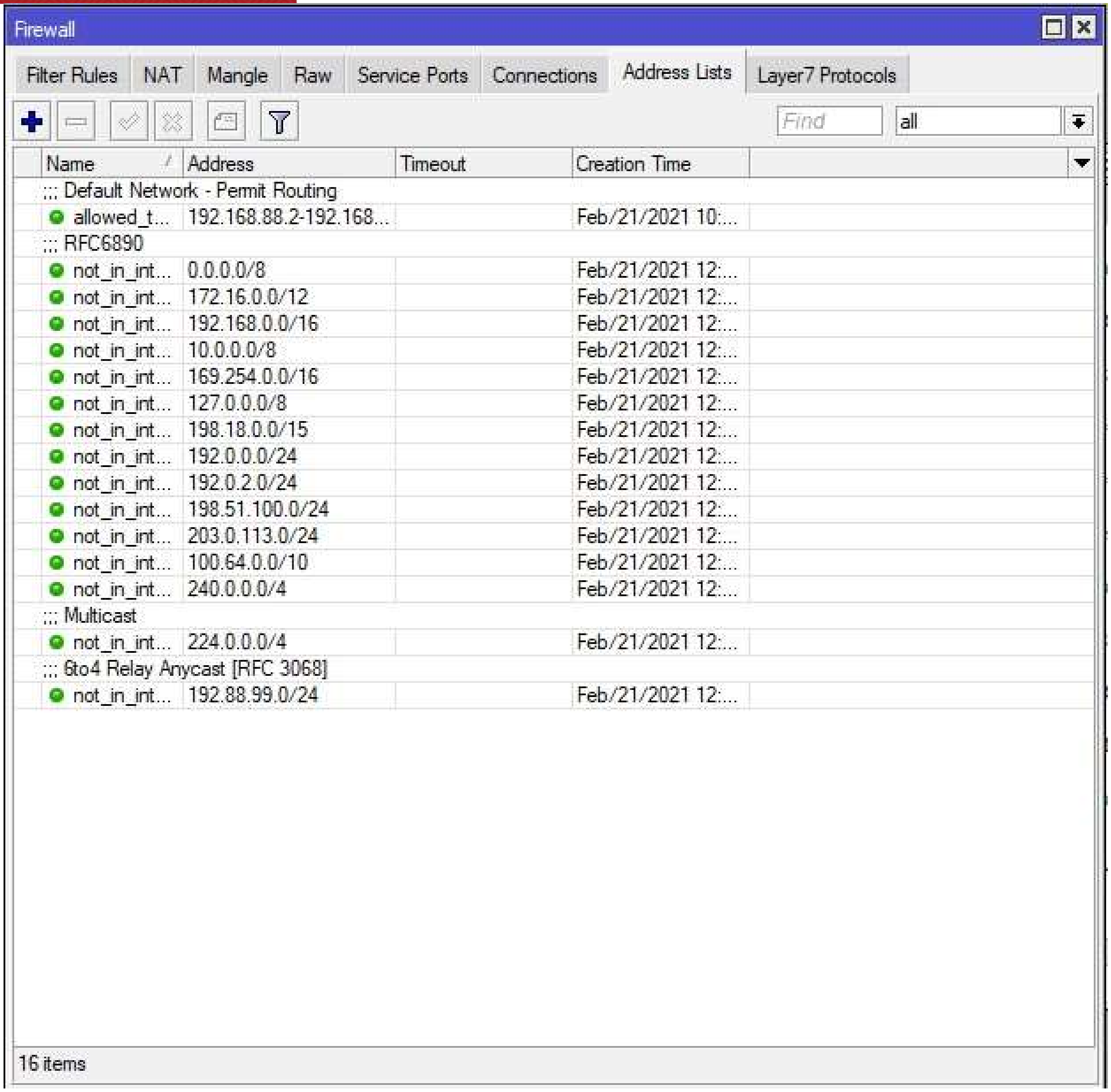
With comments implemented for each entry, the **Address Lists** tab will appear as pictured below.



Name	Address	Timeout	Creation Time
;;; Default Network - Permit Routing			
● allowed_t...	192.168.88.2-192.168...		Feb/21/2021 10:...
;;; RFC6890			
● not_in_int...	0.0.0.0/8		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	172.16.0.0/12		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	192.168.0.0/16		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	10.0.0.0/8		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	169.254.0.0/16		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	127.0.0.0/8		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	198.18.0.0/15		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	192.0.0.0/24		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	192.0.2.0/24		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	198.51.100.0/24		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	203.0.113.0/24		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	100.64.0.0/10		Feb/21/2021 12:...
;;; RFC6890			
● not_in_int...	240.0.0.0/4		Feb/21/2021 12:...
;;; Multicast			
● not_in_int...	224.0.0.0/4		Feb/21/2021 12:...
;;; 6to4 Relay Anycast [RFC 3068]			
● not_in_int...	192.88.99.0/24		Feb/21/2021 12:...

16 items

If the command block is altered to only contain a comment for the first *not_in_internet* range, the *Multicast* range, and the *6to4 Relay Anycast [RFC 3068]* range, then the resulting presentation in the **Address Lists** tab will appear as shown below.



Name	Address	Timeout	Creation Time
;;; Default Network - Permit Routing			
allowed_t...	192.168.88.2-192.168...		Feb/21/2021 10:...
;;; RFC6890			
not_in_int...	0.0.0.0/8		Feb/21/2021 12:...
not_in_int...	172.16.0.0/12		Feb/21/2021 12:...
not_in_int...	192.168.0.0/16		Feb/21/2021 12:...
not_in_int...	10.0.0.0/8		Feb/21/2021 12:...
not_in_int...	169.254.0.0/16		Feb/21/2021 12:...
not_in_int...	127.0.0.0/8		Feb/21/2021 12:...
not_in_int...	198.18.0.0/15		Feb/21/2021 12:...
not_in_int...	192.0.0.0/24		Feb/21/2021 12:...
not_in_int...	192.0.2.0/24		Feb/21/2021 12:...
not_in_int...	198.51.100.0/24		Feb/21/2021 12:...
not_in_int...	203.0.113.0/24		Feb/21/2021 12:...
not_in_int...	100.64.0.0/10		Feb/21/2021 12:...
not_in_int...	240.0.0.0/4		Feb/21/2021 12:...
;;; Multicast			
not_in_int...	224.0.0.0/4		Feb/21/2021 12:...
;;; 6to4 Relay Anycast [RFC 3068]			
not_in_int...	192.88.99.0/24		Feb/21/2021 12:...

16 items

The reduction in comments allows the initially commented range to serve as an organization heading. All ranges that are not commented under the **RFC6890** commented line appear to be part of the same group. The list name, **not_in_internet**, is still the same and would function as intended for all filter rules that rely upon the list. This is ultimately a matter of personal preference that will be clearer based on the provided examples.

Firewall Rule Filters

Evaluating the client IP filter code block will aid in identifying default rules that may need to be modified. In the absence of default rules, new rules will need to be created.

- If the Firewall window has been closed in the WinBox GUI, **left click** on **IP -> Firewall**. **Left click** on the **Filter Rules** tab.
- If the Firewall window is still open in the WinBox GUI, **left click** on the **Filter Rules** tab.

At the end of the router rules configuration section, the table below highlights what exists from the combination of “out of the box” defaults and modifications made thus far.

	Rule Number	Chain	Action
Special dummy rule to show fasttrack counters	0	forward	passthrough
Accept established,related,untracked	1	input	accept
<New rule to accept input for allowed_to_router>	2	input	accept
Accept ICMP	3	input	accept
Drop invalid	4	input	drop
Accept to local loopback (for CAPsMAN)	5	input	accept
Drop all not coming from LAN	6	input	drop
Accept in IPSec Policy	7	forward	accept
Accept out IPSec Policy	8	forward	accept
Fasttrack	9	forward	fastrrack
Accept established,related,untracked	10	forward	accept
Drop invalid	11	forward	drop
Drop all from WAN not DSTNATed	12	forward	drop

Examination of the Wiki recommendations will be compared to the balance of default rules in the configuration. Color-coded highlighting will be used on the command block below and the table above to match rules that do not need to be created.

```
/ip firewall filter
add action=fasttrack connection chain=forward comment=FastTrack connection-state=established,related
add action=accept chain=forward comment=”Established, Related” connection-state=established,related
add action=drop chain=forward comment=”Drop invalid” connection-state=invalid log=yes log-prefix=invalid
add action=drop chain=forward comment=”Drop tries to reach non-public addresses from LAN” dst-address-list=not_in_internet in-interface=bridge log=yes log-prefix=!public_from_LAN out-interface=!bridge
add action=drop chain=forward comment=”Drop incoming packets that are not NATted” connection-nat-state=!dstnat connection-state=new in-interface=ether1 log=yes log-prefix=!NAT
add action=drop chain=forward comment=”Drop incoming from Internet which are non-public IPs” in-interface=ether1 log=yes log-prefix=!public src-address-list=not_in_internet
add action=drop chain=forward comment=”Drop packets from LAN that do not have LAN IP” in-interface=bridge log=yes log-prefix=LAN_!LAN src-address=!192.168.88.0/24
```

We can see that four of the seven recommended rules exist within some capacity as part of the default “out of the box” configuration. Examining what each rule does and validating the base implementation will be performed to confirm functionality and associated logging options.

Filter rule number nine, which is the Default FastTrack rule, uses the fasttrack-connection action for forwards that are established or related. **Double clicking** on the rule in the WinBox GUI and scrolling down the general tab confirms alignment with the proposed settings.

- Chain is set to forward.
- Check boxes for an **established** or **related** Connection State are enabled.
- Selecting the **Action** tab shows the **fasttrack connection** value indicated in the command block.

NOTE: Differences between processes and labels or naming conventions established within the default configuration exist for this rule. The Wiki documents the intended action as *fasttrack-connection* yet this option is defined in the RouterOS default configuration as **fasttrack connection**. While the label differs, the intended function and action is identical. Mismatched labels or names will return errors in the Terminal or SSH session if relying upon an external script.

Left click the **Cancel** button to close the window. **Double-click** rule number ten to compare the default settings to the recommended configuration. The following modifications will need to be made to rule number ten.

- **Left click** on the check box next to **Untracked** to disable use of this connection state.
- **Left click** on the **Comment** button. Delete the last comma and the word *untracked*.
- **Left click** the **OK** button on the **Comment for Firewall Rule** window and the **Firewall Rule** window to commit the changes.

Filter rule eleven will require modification from the default configuration. The basic implementation does not provide logging, yet the recommendation involves logging the drops with a prefix of *invalid*. **Double-click** rule number eleven to open the **Firewall Rule** window. Make the following modifications to rule number eleven.

- **Left click** on the **Action** tab.
- **Left click** on the check box next to **Log** to enable logging.
- **Left click** on the downward facing arrow at the end of the **Log Prefix** field to activate the text field.
- Type **invalid** into the **Log Prefix** text field and **left click** on the **OK** button to commit the modification to the filter rule.

Filter rule number twelve, which is the default Drop all from WAN not DSTNATed, aligns with the objectives of the security principle yet differs for the following configuration items.

- The proposed hardening rule in the code block defines the in-interface as *ether1*, yet the default rule uses *WAN*. The **Interface List** tab within the **Interfaces** module of the WinBox GUI shows that WAN is **ether1**. Use of the Interface List name in lieu of the physical interface itself will simplify rule design and script development as networks grow in complexity. If the physical port providing WAN connectivity fails on the RouterOS device, the association with a different available port can be managed using the Interface List without having to reconfigure rules to point to a new physical ethernet port.
- As was the case with filter rule number eleven, logging is not enabled for the rule.

To bring the default configuration for filter rule number twelve into alignment with the proposed settings in the code block, perform the following actions.

- If the Firewall window has been closed in the WinBox GUI, **left click** on **IP -> Firewall**. **Left click** on the **Filter Rules** tab.
- If the Firewall window is still open in the WinBox GUI, **left click** on the **Filter Rules** tab.
- **Double click** on filter rule number twelve to open it.
- The default settings in the **General** tab match the desired configuration for **Chain** (forward), **In. Interface List** (WAN – used in lieu of binding directly to ether1 using the **In. Interface** GUI element two rows above), a **Connection State** of **new** is enabled, and the **Connection NAT State** of **not dstnat** is configured with the selection of the **dstnat** check box along with the not (**!**) qualifier preceding the two primary NAT options.
- **Left click** on the **Action** tab.
- The **drop** action is already in place. Logging will need to be added into the equation.
- **Left click** on the check box next to **Log** to enable logging.
- **Left click** on the downward facing arrow at the end of the **Log Prefix** field to activate the text field.
- Type **!NAT** into the **Log Prefix** text field and **left click** on the **OK** button to commit the modification to the filter rule.

The remaining three rules within the code block need to be implemented.

```
add action=drop chain=forward comment=”Drop tries to reach non-public addresses from LAN” dst-address-list=not_in_internet in-interface=bridge log=yes log-prefix=!public_from_LAN out-interface=!bridge
add action=drop chain=forward comment=”Drop incoming from Internet which are non-public IPs” in-interface=ether1 log=yes log-prefix=!public src-address-list=not_in_internet
add action=drop chain=forward comment=”Drop packets from LAN that do not have LAN IP” in-interface=bridge log=yes log-prefix=LAN_!LAN src-address=!192.168.88.0/24
```

The first of these remaining rules will drop connections intended for IP addresses contained within the Address List as part of the *not_in_internet* collection.

NOTE: Consumer-grade modems may utilize a management interface address which falls within the 192.168.0.0/16 address space. An example of this behavior would include Arris cable modems (192.168.100.1). Once this rule is created and enabled, the function of the rule will prevent access to this IP address.

Creating the rule requires accessing the **Filter Rules** tab.

- If the Firewall window has been closed in the WinBox GUI, **left click** on **IP -> Firewall**. **Left click** on the **Filter Rules** tab.
- If the Firewall window is still open in the WinBox GUI, **left click** on the **Filter Rules** tab.

Left click the **+** button under the **Filter Rules** tab to initialize a **New Firewall Rule** window.

add action=drop chain=forward comment="Drop tries to reach non-public addresses from LAN" dst-address-list=not_in_internet in-interface=bridge log=yes log-prefix=!public_from_LAN out-interface=!bridge

- *chain=forward*: The second element of the command block attempts to set the chain to **forward**. This will be the default value for the **Chain** field within the **New Firewall Rule**.
- *in-interface=bridge*: The fifth element of the command block defines the inbound interface as the bridge. Within the **General** tab, **left click** the downward facing arrow at the end of the **In. Interface** row. **Left click t**he list box selector that appears at the end of the text field and **left click** on the **bridge** element within the list.
- *out-interface=!bridge* The final element of the command block defines the outbound interface as not the bridge. Within the **General** tab, **left click** the downward facing arrow at the end of the **Out. Interface** row. **Left click t**he list box selector that appears at the end of the text field, **left click** on the **bridge** element within the list, and **left click** the tick box in front of **bridge** to establish the **not (!)** operator.
- *dst-address-list=not_in_internet*: The fourth element of the command block will force the rule to be evaluated against the previously defined *not_in_internet* records in the Address List. **Left click** the **Advanced** tab. **Left click** the downward facing arrow at the end of the **Dst. Address List** row. **Left click t**he list box selector that appears at the end of the text field and **left click** on the **not_in_internet** element within the list.
- Actions performed against matching patterns or data flows, along with associated logging definitions, are all contained within the **Action** tab. The following three elements of the code block will be addressed in this single step.
    - *add action=drop*
    - *log=yes*
    - *log-prefix=!public_from_LAN*
- **Left click** the **Action** tab. **Left click** on the list box selector at the end of the **Action** row to view all options. **Left click** on **drop** within the list to establish the documented action.
- **Left click** the empty check box next to **Log** to enable logging. **Left click the** downward facing arrow at the end of the **Log Prefix** line to activate the text field. Type **!public_from_LAN** into the text field.
- Finally, **left click** the **Comment** button on the right-hand side of the **New Firewall Rule** window. Within the **Comment for New Firewall Rule** window, type **Drop tries to reach non-public addresses from LAN**. **Left click** the **OK** button to commit the comment to the rule.
- **Left click** the **OK** button in the **New Firewall Rule** window to implement this rule.

A new rule will appear as active and implemented at the bottom of the list. A similar process will be leveraged for the final two rules contained within the Wiki.

Left click the **+** button under the **Filter Rules** tab to initialize a **New Firewall Rule** window for the code block listed below.

add action=drop chain=forward comment="Drop incoming from Internet which are non-public IPs" in-interface=ether1 log=yes log-prefix=!public src-address-list=not_in_internet

- *chain=forward*: The second element of the command block attempts to set the chain to **forward**. This will be the default value for the **Chain** field within the **New Firewall Rule**.
- *in-interface=ether1*: The fifth element of the command block defines the inbound interface as the ether interface that contains the WAN connection. Within the **General** tab, **left click** the downward facing arrow at the end of the **In. Interface** row. **Left click t**he list box selector that appears at the end of the text field and **left click** on the **ether1** element within the list.
- *dst-address-list=not_in_internet*: The fourth element of the command block will force the rule to be evaluated against the previously defined *not_in_internet* records in the Address List. **Left click** the **Advanced** tab. **Left click** the downward facing arrow at the end of the **Src. Address List** row. **Left click t**he list box selector that appears at the end of the text field and **left click** on the **not_in_internet** element within the list.
- Actions performed against matching patterns or data flows, along with associated logging definitions, are all contained within the **Action** tab. The following three elements of the code block will be addressed in this single step.
    - *add action=drop*

    - *log=yes*
    - *log-prefix=!public*
- **Left click** the **Action** tab. **Left click** on the list box selector at the end of the **Action** row to view all options. **Left click** on **drop** within the list to establish the documented action.
- **Left click** the empty check box next to **Log** to enable logging. **Left click the** downward facing arrow at the end of the **Log Prefix** line to activate the text field. Type **!public** into the text field.
- Finally, **left click** the **Comment** button on the right-hand side of the **New Firewall Rule** window. Within the **Comment for New Firewall Rule** window, type **Drop incoming from Internet which are non-public IPs**. **Left click** the **OK** button to commit the comment to the rule.
- **Left click** the **OK** button in the **New Firewall Rule** window to implement this rule.

Left click the **+** button under the **Filter Rules** tab to initialize a **New Firewall Rule** window for the final code block listed below.

```
add action=drop chain=forward comment=”Drop packets from LAN that do not have LAN IP” in-interface=bridge log=yes
log-prefix=LAN_!LAN src-address=!192.168.88.0/24
```

- *chain=forward*: The second element of the command block attempts to set the chain to **forward**. This will be the default value for the **Chain** field within the **New Firewall Rule**.
- *in-interface=bridge*: The fifth element of the command block defines the inbound interface as the bridge. Within the **General** tab, **left click** the downward facing arrow at the end of the **In. Interface** row. **Left click t**he list box selector that appears at the end of the text field and **left click** on the **bridge** element within the list.
- *src-address=!192.168.88.0/24*: The final element of the command block defines the parameters for source addresses. Within the **General** tab, **left click** the downward facing arrow at the end of the **Src. Address** row. Type **192.168.88.0/24** in the editable text field and **left click** the tick box in front of the Src. Address text field to establish the **not (!)** operator.
- Actions performed against matching patterns or data flows, along with associated logging definitions, are all contained within the **Action** tab. The following three elements of the code block will be addressed in this single step.
    - *add action=drop*
    - *log=yes*
    - *log-prefix=LAN_!LAN*
- **Left click** the **Action** tab. **Left click** on the list box selector at the end of the **Action** row to view all options. **Left click** on **drop** within the list to establish the documented action.
- **Left click** the empty check box next to **Log** to enable logging. **Left click the** downward facing arrow at the end of the **Log Prefix** line to activate the text field. Type **LAN_!LAN** into the text field.
- Finally, **left click** the **Comment** button on the right-hand side of the **New Firewall Rule** window. Within the **Comment for New Firewall Rule** window, type **Drop packets from LAN that do not have LAN IP**. **Left click** the **OK** button to commit the comment to the rule.
- **Left click** the **OK** button in the **New Firewall Rule** window to implement this rule.

After these steps have been completed, there will be fifteen filter rules established within the firewall. The updated table below contains the summary of rules.

	Rule Number	Chain	Action
Special dummy rule to show fasttrack counters	0	forward	passthrough
Accept established,related,untracked	1	input	accept
<New rule to accept input for allowed_to_router>	2	input	accept
Accept ICMP	3	input	accept
Drop invalid	4	input	drop
Accept to local loopback (for CAPsMAN)	5	input	accept
Drop all not coming from LAN	6	input	drop
Accept in IPSec Policy	7	forward	accept
Accept out IPSec Policy	8	forward	accept
Fasttrack	9	forward	fastrack
Accept established,related,untracked	10	forward	accept
Drop invalid	11	forward	drop
Drop all from WAN not DSTNATed	12	forward	drop

Drop tries to reach non-public addresses from LAN	13	forward	drop
Drop incoming from Internet which are non-public IPs	14	forward	drop
Drop packets from LAN that do not have LAN IP	15	forward	drop

At this point, the router has been brought into compliance with the recommendations provided within the Wiki. Further rules may need to be established to meet your specific requirements. However, execution of these tasks within the WinBox GUI will improve familiarity with this option. Additional references and links contained within the next section will aid in further enhancing the security and capabilities of your network.

References and Acknowledgements

MikroTik Securing Your Router Wiki: https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

Let’s Encrypt RouterOS Scripts and Processes: https://github.com/gitpel/letsencrypt-routeros

Using RouterOS to VLAN your network: https://forum.mikrotik.com/viewtopic.php?t=143620

MikroTik IP/Firewall/Filter Wiki: https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter