



### Basic MikroTik Router's Security



### Presented by:

Titas Sarker Founder (Tsoft IT) System administrator (Enosis Solutions) Certificates:(MTCNA,MTCRE,RHCE)

Agenda	Page no
Reason for security	04
How to secure our network?	05
Administrative Users credentials	06-07
Winbox default ports	08-09
MAC-access restriction	10-11
Site restriction	12-15
Virus port filtering	16-17
Log server	19-21
Reference	22
Conclusion	23



### **Reason for security**

- Remedy unauthorized people to access to the network
- Intruder detection purpose
- Taking necessary action for fix the issue.
- Protect information and infrastructure.

### How to secure our network?

- Administrative Users credentials
- Winbox default ports
- MAC-access restriction
- Site restriction
- Virus port filtering
- Log server



#### Administrative Users credentials

Mikrotik router's default username is "admin". If it is kept to the default username, it can be assumed very easily. So it is recommended to change the username and set a strong password for the admin privileged user.

### Basic MikroTik Router's Security

### **Administrative Users credentials**

#### How to change credentials?

- Log in Winbox
- Click on System
- Click on Users
- Note: user & Password

Sadmin@192.16	8.1.1 (MikroTik) - WinBox v6.34.2 on hAP lite (smips)		0	titas@192.168.	1.1 (M	likroT	Tik) - WinBox v6.34.2 on	hAP lite (smips)		
Session Settings Dashboard					Das	shboa	ard			
🖒 🍳 🛛 Safe N	lode Session: 192.168.1.1	3	5	🖓 🛛 Safe M	ode	Se	ession: 192.168.1.1			<b>a</b>
🖌 🄏 Quick Set			F	Auick Set						
🗘 CAPsMAN	User List			T CAPeMAN		- [	llear liet			
🛲 Interfaces	Users Groups SSH Keys SSH Private Keys Active Users						User Est			
T Wireless				Interfaces			Users Groups SSH	Keys SSH Private Keys	Active Users	
Bridge				🤶 Wireless			4 - V X	🗖 🍸 🗛		Find
	Name / Group Allowed Address Last Logged In			Bridge					let lees de	
	iii system derault user A admin full Mar/13/2018 08						Name A Group	Allowed Address	Last Logged in	<b>_</b>
🛫 Switch							admin full			Mar/13/2018 08
°t¦3 Mesh				₩ Switch			👗 titas 🛛 full			Mar/13/2018 08
255 IP	1			°t¦8 Mesh						
ण्डू IPv6	1			255 IP						
MPLS	N			v∮ IPv6						
🐹 Routing	N			MPLS	Þ					
🎲 System	1			🐹 Routing	Þ					
Rueues 👳				System	Þ					
E Dise	•					-				



### Winbox default ports

Usually we use Winbox application to log in to MikroTik router's admin panel. Winbox runs on default port 8291. If the default port is changed to a custom port it would require the exact port number to browse the admin panel. It will be a secured way when logging in using IP, username and password.

### Basic MikroTik Router's Security

### Winbox default ports

# How to change defaults ports numbers?

- Log in Winbox
- Click on IP
- Click on Services

🔵 admir	@192.168.88.1	(MikroTik) - WinBox v6:25 on RB941-2nD (smipi)		No. admin@192.168.1.1:	8310 (MikraTik) - WinBox v6.34.2 on hAP lite (smins)	
Session	Settings Da	shiboard				
00	Safe Mode	Session: 192.168.88.1		Session Settings Da	shboard	
10	luck Set			🂫 🍳 🛛 Safe Mode	Session: 192.168.1.1:8310	
ΞC	AP#MAN			auick Set		
jas ir	rterfaces			CAPeMAN		
ΞV	Vireless					
228	indge			Interfaces		
es P	PP	IP Service List		🧘 Wireless		
12 S	witch	1 a 7	Find	Sidge Stidge	IP Service List	
*@ N	lesh	Name / Port Available From	Cetificate 💌	🚅 PPP		Find
@F	P (*	• api 8728 • api sol 8729	none	🛫 Switch	Name / Port Available From	Certificate
40 M	IPLS P	• ftp 21		°T <sup>e</sup> Mesh	X 🛛 api 8728	
X, A	louting	esh 22			X 🛛 api-ssl 8729	none
(i) S	iystem	windox N 8291		₩ IP	X @ftp 21	
	lueues	orwww ha≹ 80.		👳 IPv6 🗈	X 9 ssh 22	
R R	ies -	X 9 www.stil 443	none	🖉 MPLS 🗈 🗈	winbox 8310	
BL	og.			🔀 Routing 🗈 🗎	X • www 80	
19 R	ladus			Cuton N	X  www-ssl 443	none
400				System		



### **MAC-access restriction**

MAC access RouterOS has built-in options for easy management access to network devices. But the particular services should be shutdown on production networks for security purpose.





### **MAC-access restriction**

#### How we can configure it?

- Log in Winbox
- Click on Tools
- Select Winbox Interfaces
- Finally disable "all"





### **Site restriction**

Mikrotik router can be used to prevent access to selected websites if required (i.e. adult sites, social media, entertainment websites etc.).

#### How to configure it?

- Log in Winbox
- Click on IP
- Click on Firewall
- Click on layer 7 Protocols '+'

<b>)</b> t	titas01717955372@	192.168.1.1 (MikroTik) - WinBox v5.18 on x86 (x86)
ю	Call Safe Mode	Hide Passwords
	Interfaces Wireless	
	PPP Mesh	Firewall     X       Filter Rules     NAT       Mangle     Service Ports       Connections     Address Lists       Layer7     Protocols
	IP Pv6 P	Name     ∠     Regexp     ▼       ● facebook     ^.+(facebook com) *\$     ▼
	MPLS F Routing F System F	Firewall L7 Protocol <facebook>     Image: King State Stat</facebook>
	Queues Files	Cancel ^.+(facebook.com).*\$
	Log Radius	Comment
	New Terminal	Remove
Box	ISDN Channels KVM	
Wir	Make Supout.rif	1 item
SC	Manual	
er(	Exit	

### Basic MikroTik Router's Security

#### **Site restriction**

- Filter rule>
- General>src addreess

<b>()</b> t	itas01717955372@	192.168.1.1 (MikroTik) - WinBox v5.18 on x	36 (x86)	-	
ю	Call Safe Mode			💌 Hi	de Passwords 📗 🛅
	Interfaces	New Firewall Rule			
	Wireless	General Advanced Extra Action Statist	cs		ОК
	Bridge	Chain: forward		₹	Cancel
	PPP	Src. Address: 192.168.1.222		•	Apply
	Mesh	Det Addresse:		_	
	IP 🗅	Dst. Address.		·	Disable
	IPv6 🗅	Protocol:		•	Comment
	MPLS N	Src. Port:		-	Сору
	Routing	Dist Port:		<b>_</b>	Remove
	System D	And Date			
	Queues	Any. Port:		×	Reset Counters
	Files	P2P:		•	Reset All Counters
	Log	In. Interface:		•	
	Radius	Out. Interface:		•	
	Tools D			_	
0	New Terminal	Packet Mark:		•	
Ô	ISDN Channels	Connection Mark:		•	
inE	KVM	Routing Mark:		•	
$\geq$	Make Supout.rif	Routing Table:		<b>-</b>	
S	Manual			_	
P D	Exit	Connection Type:		•	
ute		Connection State:		•	
Ro					

### Basic MikroTik Router's Security

**Site restriction** 

S t	itas017	717955372@	192.168.1.1 (MikroTik) - WinBox v5.18 on x86 (x86)		
5	0	Safe Mode		✓ Hi	de Passwords 📗 🕯
Interfaces		ices	New Firewall Rule		
	Wirele	ess	General Advanced Extra Action Statistics		ОК
	Bridge	•	Src. Address List:	▼	Cancel
	PPP		Dst. Address List:		Apply
	Mesh	N			Diezble
	IPv6			· · · · · · · · · · · · · · · · · · ·	Disable
	MPLS	· ·	Content:	<b>~</b>	Comment
	Routir		Connection Bytes:	<b>•</b>	Сору
	Syster	m D	Connection Rate:		Remove
	Queue	es	Per Connection Classifier		Reset Counters
	Files				Reset All Counte
	Log		Src. MAC Address:	<b>`</b>	
	Radiu	s	Out. Bridge Port:	▼	
	Tools	1	In. Bridge Port:	•	
	New 1	Terminal			
ô	ISDN	Channels	Ingress Priority:	▼	
in	KVM	0	DSCP (TOS):	▼	
$\geq$	Make	Supout.nt	TCP MSS:	▼	
OS	Fv#	ai	Packet Size:	▼	
ter	LAIL		Random:		
no			TCP Flags		
R			-▼- ICMP Options		

• Advanced>Layer7 protocol

### Basic MikroTik Router's Security

**Site restriction** 

	itas01717955372@	192.168.1.1 (MikroTik) - WinBox v5.18 on x86 (x86)	
5	Ca Safe Mode		Hide Passwords 📗 🛅
	Interfaces	New Firewall Rule	
	Wireless	General Advanced Extra Action Statistics	ОК
	Bridge	Action: drop	Cancel
	PPP		Apply
	Mesh		
			Disable
	IPV6		Comment
	Paution		Сору
	System		Remove
	Queues		Reset Counters
	Files		Reset All Counters
	Log		Hosel / II counters
	Radius		
	Tools D		
	New Terminal		
ŏ	ISDN Channels		
inB	KVM		
$\geq$	Make Supout.rif		
SC	Manual		
er(	Exit		
out			
R		enabled	

Action>drop



### **Site restriction result**

So that if he/she try to visit Facebook now. He/she will not able to visit it.





### Virus port filtering

Firewalls filter keep outside threats away from sensitive data available inside the network. Whenever different networks are joined together, there is always a threat that someone from outside of your network will break into your LAN. MikroTik router's firewall easily filter virus ports and we can drop it.

### Basic MikroTik Router's Security

### Virus port filtering

# How to block all the virus ports in MikroTik?

- Log in Winbox
- Click on IP
- Click on Firewall
- Filter rules "+"

Safe Mode	Hide Passwords
Interfaces	
Wireless	
Bridge	
PPP	
Mesh	
IP 🗅	
IPv6 ▷	
MPLS 🗅	
Routing D	Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols
System 🗅	🛉 📼 🧭 🖄 🖾 🍸 🖾 Reset Counters 00 Reset All Counters Find all 🔻
Queues	# Action Chain Src. Address Dst. Address Proto Src. Port Dst. Port In. Inter Out. Int Byter
Files	
Log	
Radius	
Tools 🗅	
New Terminal	
ISDN Channels	
KVM	
Make Supout.rif	
Manual	
Exit	
	•
	0 items

add chain=virus protocol=tcp dst-port=135-139 action=drop comment="Drop Blaster Worm" add chain=virus protocol=udp dst-port=135-139 action=drop comment="Drop Messenger Worm" add chain=virus protocol=tcp dst-port=445 action=drop comment="Drop Blaster Worm" add chain=virus protocol=udp dst-port=445 action=drop comment="Drop Blaster Worm" add chain=virus protocol=tcp dst-port=593 action=drop comment=" add chain=virus protocol=tcp dst-port=1024-1030 action=drop comment=" add chain=virus protocol=tcp dst-port=1080 action=drop comment="Drop MyDoom" add chain=virus protocol=tcp dst-port=1214 action=drop comment=" add chain=virus protocol=tcp dst-port=1363 action=drop comment="ndm requester" add chain=virus protocol=tcp dst-port=1364 action=drop comment="ndm server" add chain=virus protocol=tcp dst-port=1368 action=drop comment="screen cast" add chain=virus protocol=tcp dst-port=1373 action=drop comment="hromgrafx" add chain=virus protocol=tcp dst-port=1377 action=drop comment="cichlid" add chain=virus protocol=tcp dst-port=1433-1434 action=drop comment="Worm" add chain=virus protocol=tcp dst-port=2745 action=drop comment="Bagle Virus" add chain=virus protocol=tcp dst-port=2283 action=drop comment="Drop Dumaru.Y" add chain=virus protocol=tcp dst-port=2535 action=drop comment="Drop Beagle" add chain=virus protocol=tcp dst-port=2745 action=drop comment="Drop Beagle.C-K" add chain=virus protocol=tcp dst-port=3127-3128 action=drop comment="Drop MyDoom" add chain=virus protocol=tcp dst-port=3410 action=drop comment="Drop Backdoor OptixPro" add chain=virus protocol=tcp dst-port=4444 action=drop comment="Worm" add chain=virus protocol=udp dst-port=4444 action=drop comment="Worm" add chain=virus protocol=tcp dst-port=5554 action=drop comment="Drop Sasser" add chain=virus protocol=tcp dst-port=8866 action=drop comment="Drop Beagle.B" add chain=virus protocol=tcp dst-port=9898 action=drop comment="Drop Dabber.A-B"



### Log server

MikroTik RouterOS is capable of logging various system events and status information. As well, MikroTik router's Logging is configured for view who is visiting which website. If anyone tries to visit any unauthorized site then we can easily track it.

#### How to configure it?

- Log in Winbox
- Click on System
- Click on Logging
- Click on Actions

admin@192.168.1.1 (	MikroTik) - WinBox v6.34.2	on hAP lite (smips	)		
ession Settings Das	hboard				
Safe Mode	Session: 192.168.1.1				<b>a</b>
🔏 Quick Set					
CAPsMAN					
Interfaces					
Wireless					
📲 🖁 Bridge					
🚅 PPP				তা	
💬 Switch		tione		-	
° <mark>t</mark> ₿ Mesh	Rules Au	aions		_1	
255 IP 🗅	+ -	7	Find		
👳 IPv6 🛛 🗅	Name				
🖉 MPLS 🛛 🗅	echo	Log Action <remotion< th=""><th>3&gt;</th><th></th><th></th></remotion<>	3>		
😹 Routing 💦 🗅	* memory	Name:	remote	ОК	
🎲 System 🗅	<sup>-</sup> remote	Type:	remote Ŧ	Cancel	
🙊 Queues		Remote Address:	192 168 1 209	Apply	
Files		Nemote Address.	132.100.1.203		
K Eog		Remote Port:	514	Сору	
🖌 🧟 Radius		Src. Address:	0.0.0.0	Remove	
🗙 🔀 Tools 🛛 🗈			BSD Syslog		
New Tree in al					



### Log server

#### X admin@192.168.1.1 (MikroTik) - WinBox v6.34.2 on hAP lite (smips) Session Settings Dashboard ю. C<sup>4</sup> Safe Mode Session: 192.168.1.1 A Quick Set CAPsMAN Interfaces Wireless 😹 Bridge 🛋 PPP 💬 Switch Rules Actions °t<sup>®</sup> Mesh T × 255 IP $\mathbb{P}$ Log Rule <error> 🜿 IPv6 Topics critical Topics: 🛄 error ∓ ≑ OK MPLS erro 🐹 Routing $\mathbb{N}$ info Prefix: -Cancel warning System $\mathbb{N}$ Ŧ Action: remote Apply Queues Disable Files Copy Loa 🧟 Radius Remove $\mathbf{c}$ 🗶 Tools New Terminal enabled default 🗋 Make Supout.rif 4 items (1 selected) Manual 🔘 New WinBox

#### Steps:

- Log in Winbox
- Click on System
- Click on Logging
- Click on Rules



#### Log server's output

#### Here we are use Kiwi Syslog for view purpose

🔄 Kiwi Syslo	g Service M	anager (Free Vers	ion 9.6)		×
File Edit	View Man	age Help			
a 🖸 📾	▲ 🖪 €	Display 00 (D	efault) 💌	Compare features of the first and licensed versions	
Date	Time	Priority	Hostname	Message	
08-28-2017	01:06:20	Local7.Debug	192.168.1.1	firewall.info www.facebook.com forward: in:bridge1 out:ether1, arc-mac 2c:55:dc:71:c0:e8, proto TCP (ACK), 192.168.1.253:50294 > 157.240.7.20:443, Ion 40	
08-29-2017	01:06:20	Local7.Debug	192.168.1.1	firewall,info forward: in:bridge1 out:ether1, src-mac 2c:56:dc:7f:c0:e8, proto TCP (ACK), 192.168.1.253:50294->157.240.7.20:443, NAT (192.168.1.253:50294->192.168.102.52:50294)->157.240.7.20:443, len 40	
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewall.info www.facebook.com forward: in:bridge1 out:ether1, src-mac 2c:56:dc:71:c0:e8, proto TCP (ACK), 192.168.1.253:50294->157.240.7.20:443, NAT (192.168.1.253:50294->192.168.102.52:50294)->157.240.7.20:443, len 52	
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewalLinfo forward: in:bridge1 out:ether1, src-mac 2c:56:dc:71:c0:e8, proto TCP (ACK), 192,168.1.253:50294->157.240.7.20:443, NAT (192,168.1.253:50294->192,168.102.52:50294)->157.240.7.20:443, len 52	1
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewall.info www.facebook.com forward: in:ether1 out:bridge1, src-mac d4:ca:6d:74:46:d4, proto TCP (ACK,PSH), 157.240.7.20:443->192.168.1.253:50294, NAT 157.240.7.20:443->192.168.102.52:50294->192.168.1.253:50294], len 293	-
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewall.info www.facebook.com forward: in:bridge1 out:ether1, src-mac 2c:56:dc:7f:c0:e8, proto TCP (ACK), 192.168.1.253:50294 > 157.240.7.20:443, Ion 40	
00-29-2017	01:06:19	Local7.Debug	192.168.1.1	firewall,info forward: in:bridge1 out:ether1, src-mac 2c:56:dc:71:c0:e8, proto TCP (ACK), 192.168.1.253:50294->157.248.7.20:443, NAT (192.168.1.253:50294->192.168.102.52:50294)->157.240.7.20:443, len 40	
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewalLinfo www.facebook.com forward: in:ether1 out:bridge1, src-mac d4:ca:6d;74:46:d4, poto TCP (ACK,PSH), 157:240.7.20:443->192.168.1.253:50294, NAT 157:240.7.20:443->(192.168.102.52:50294->192.168.1.253:50294), len 293	
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewall.info www.facebook.com forward: in:bridge1 out:ether1, src-mac 2c:55:dc:7t:c0:e8, proto TCP (ACK), 192.168.1.253:50294 > 157.240.7.20:443, Ion 40	
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewall.info forward: in:bridge1 out:ether1, src-mac 2c:56:dc:71:c0:e0, proto TCP (ACK), 192.168.1.253:50294>157.240.7.20:443, NAT (192.168.1.253:50294>192.168.102.52:50294>157.240.7.20:443, len 40	
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewall.info www.facebook.com forward: in:ether1 out:bridge1, src-mac d4:ca:6d:74:46:d4, poto TCP (ACK,PSH), 157.240.7.20:443->192.168.1.253:50294, NAT 157.240.7.20:443->(192.168.102.52:50294->192.168.1.253:50294), len 293	
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewalLinfo www.facebook.com forward: in:ether1 out:bridge1, src-mac d4:ca:6d:74:46:d4, proto TCP (ACK,PSH), 157.240.7.20:443->192.168.1.253:50294, NAT 157.240.7.20:443->[192.168.102.52:50294->192.168.1.253:50294], len 303	
88-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewall.info www.facebook.com forward: in:ether1 out:bridge1, src-mac d4:cac6d:74:46:d4, proto TCP (ACK,PSH), 157.240.7.20:443->192.168.1.253:50294, NAT 157.240.7.20:443->(192.168.102.52:50294->192.168.1.253:50294), len 521	
08-28-2017	01:06:19	Local7.Debug	192.168.1.1	firewall info www.facebook.com forward: in:bridge1 out:ether1, src-mac 2c:56:dc:7f:c0:e8, proto TCP (ACK),	
				100% 3680 MRH	E

### Basic MikroTik Router's Security

### Reference

- MikroTik wiki (https://wiki.mikrotik.com/wiki/)
- MikroTik website(https://mikrotik.com/)
- MikroTik Forum (https://forum.mikrotik.com/)





### Conclusion

Awareness is the key to security.

# **THANK YOU**



www.tsoftit.com

MUM, Dhaka, Bangladesh