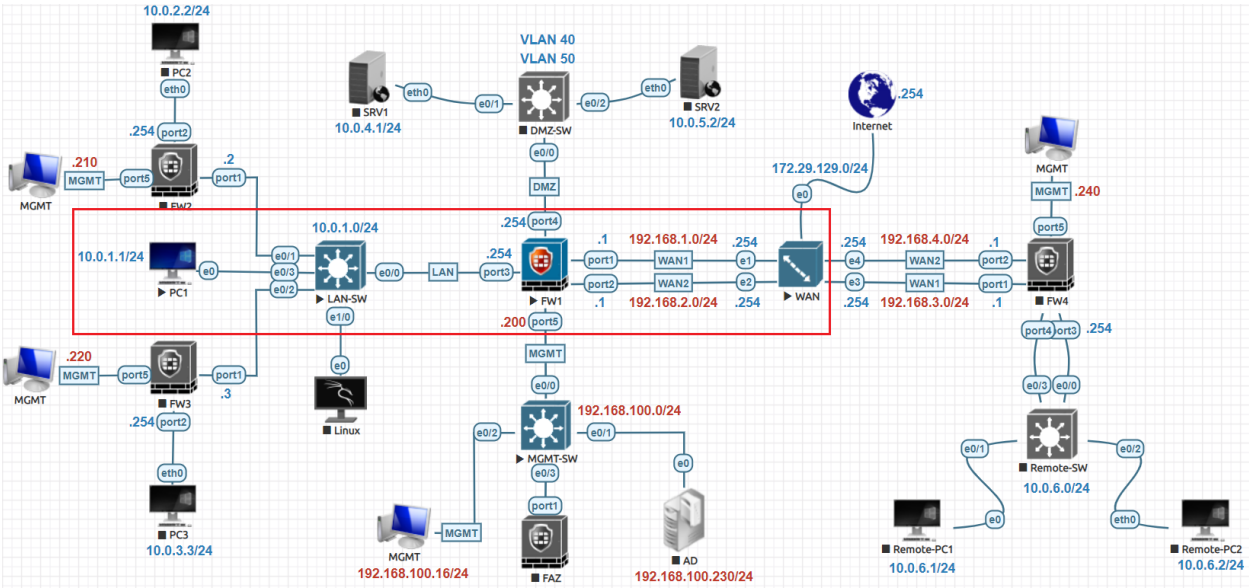
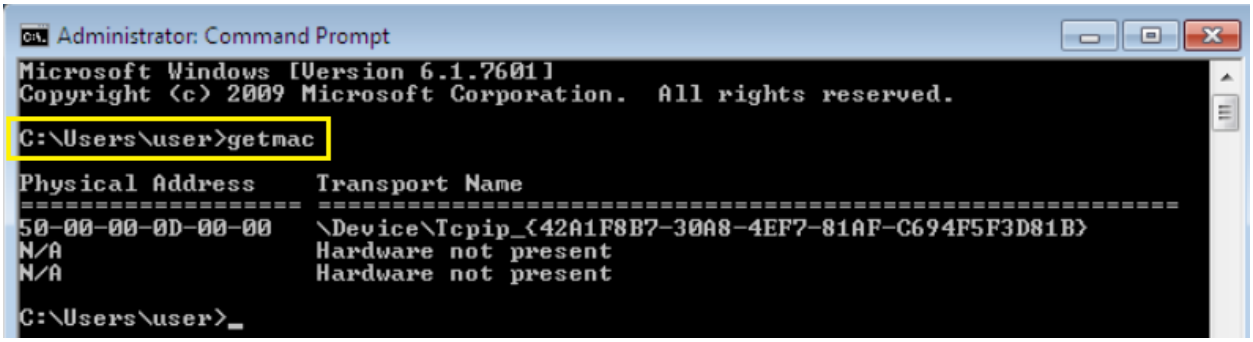
MAC Address-Based Policies:

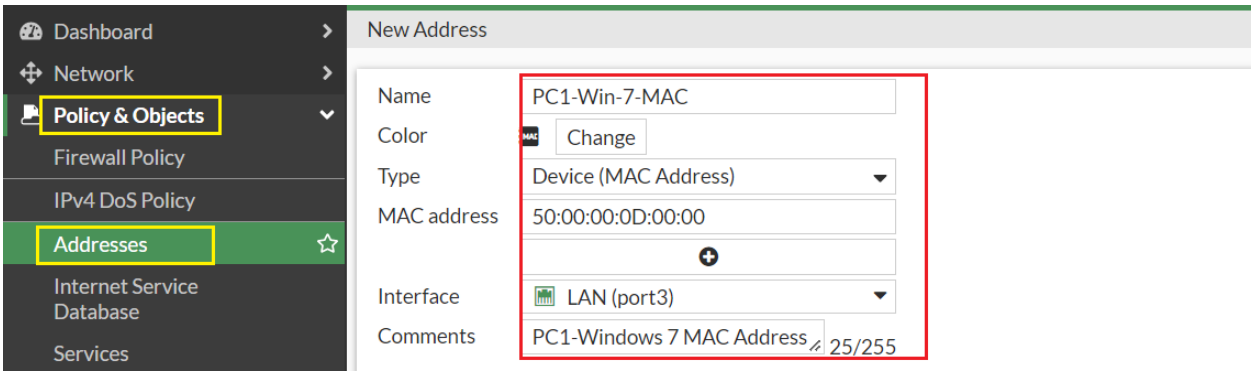


MAC Address-Based Policies:

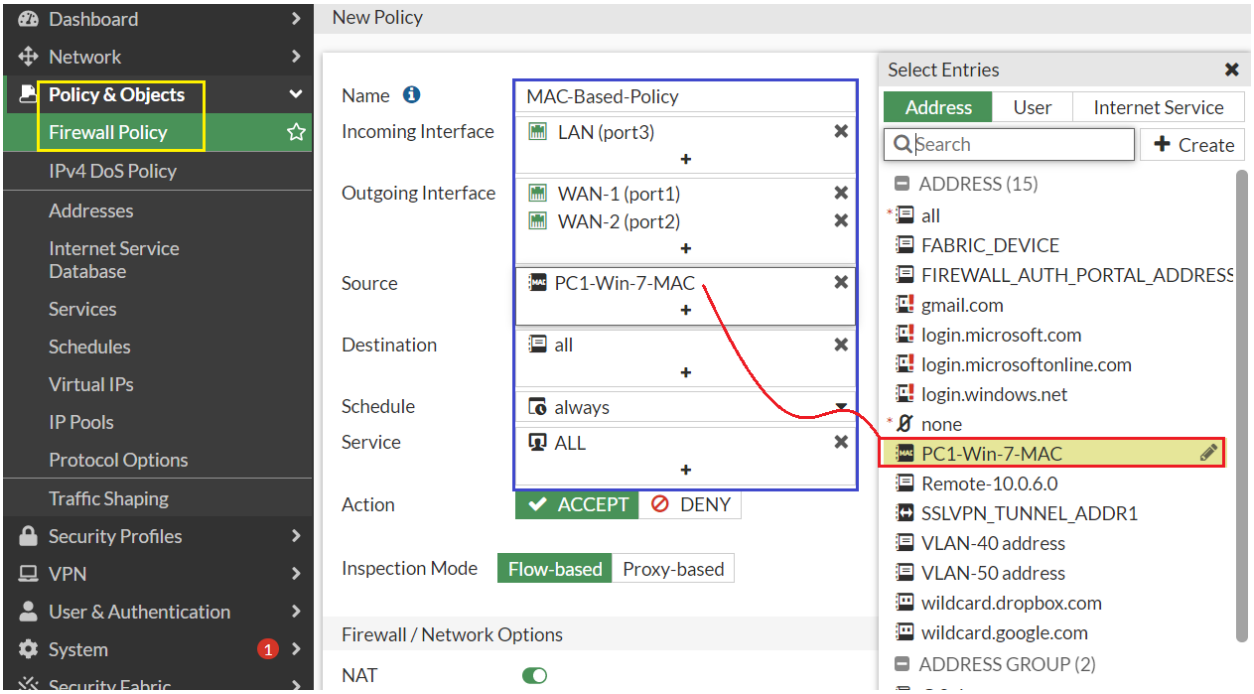
First get the MAC address of the user system or PC, Type getmac in CMD to display.



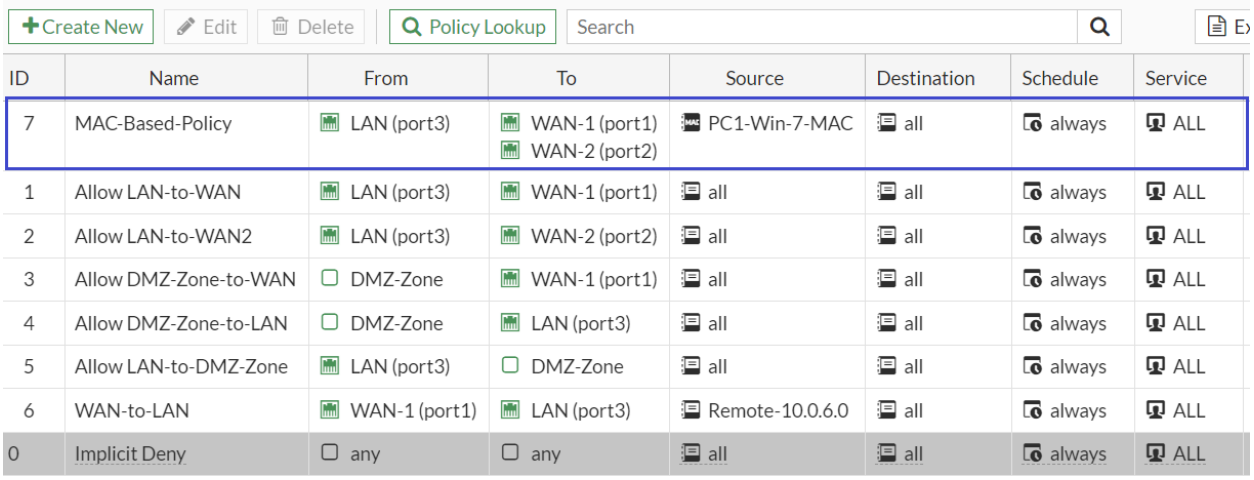
Go to Policy & Objects -> Addresses -> Created new -> Address -> Select Type as Device (MAC Address). Specify the name and MAC address of the respective users.



Go to Policy & Objects -> Firewall Policy -> Create new -> specify the Source as the MAC address created in the Addresses Click OK.



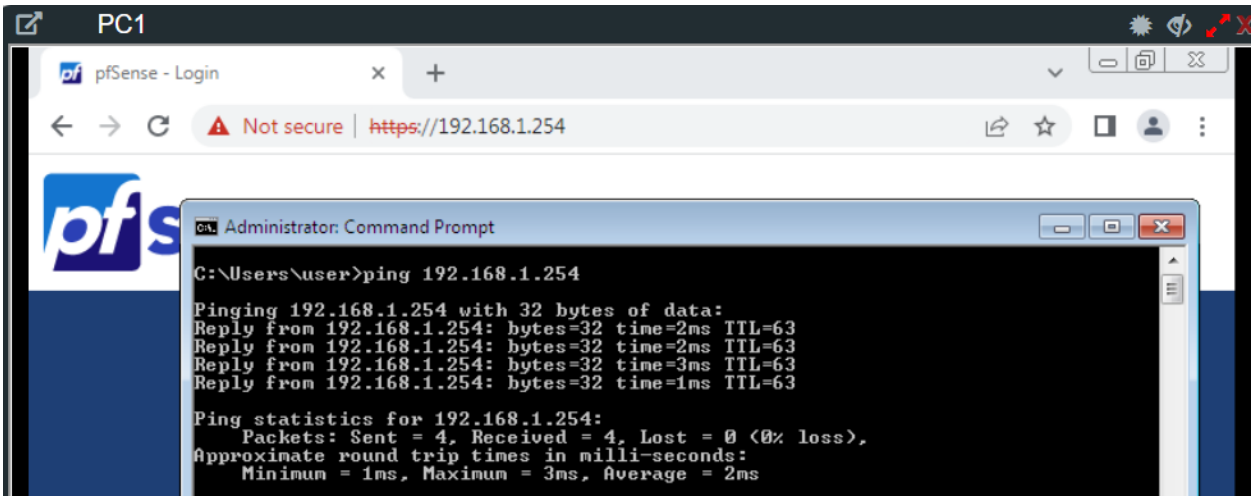
Let's put the policy on the top to test it.



ID	Name	From	To	Source	Destination	Schedule	Service
7	MAC-Based-Policy	LAN (port3)	WAN-1 (port1) WAN-2 (port2)	PC1-Win-7-MAC	all	always	ALL
1	Allow LAN-to-WAN	LAN (port3)	WAN-1 (port1)	all	all	always	ALL
2	Allow LAN-to-WAN2	LAN (port3)	WAN-2 (port2)	all	all	always	ALL
3	Allow DMZ-Zone-to-WAN	DMZ-Zone	WAN-1 (port1)	all	all	always	ALL
4	Allow DMZ-Zone-to-LAN	DMZ-Zone	LAN (port3)	all	all	always	ALL
5	Allow LAN-to-DMZ-Zone	LAN (port3)	DMZ-Zone	all	all	always	ALL
6	WAN-to-LAN	WAN-1 (port1)	LAN (port3)	Remote-10.0.6.0	all	always	ALL
0	Implicit Deny	any	any	all	all	always	ALL

Test and Verification:

From Windows 7 PC1 in the internal network, attempt to browse or ping the Internet.



Go to Policy & Objects -> Firewall Policy our MAC-Based-Policy are getting Hit Counts.

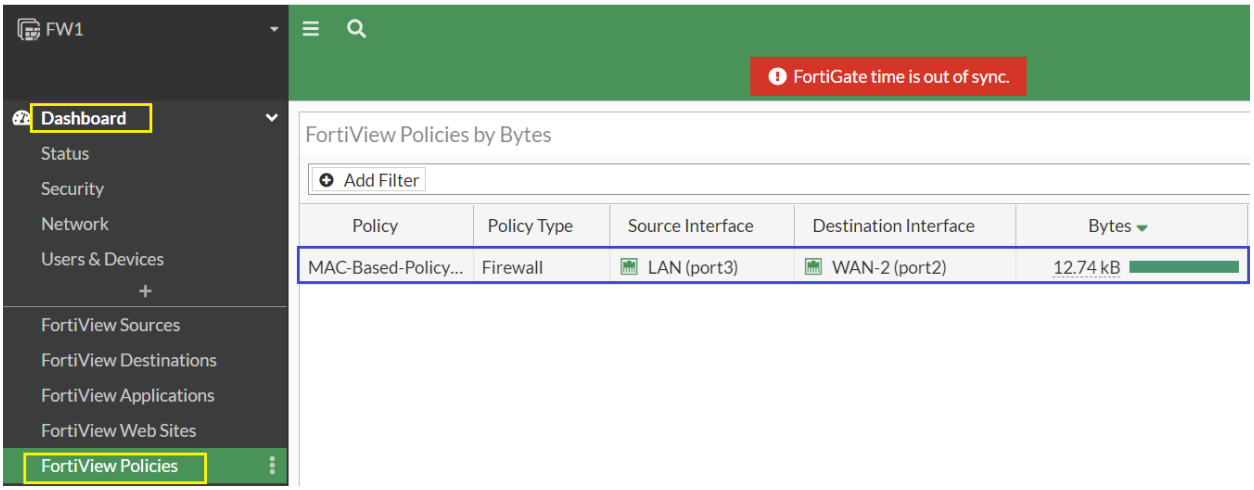
ID	Name	From	To	Source	Hit Count
7	MAC-Based-Policy	LAN (port3)	WAN-1 (port1) WAN-2 (port2)	PC1-Win-7-MAC	118
1	Allow LAN-to-WAN	LAN (port3)	WAN-1 (port1)	all	0
2	Allow LAN-to-WAN2	LAN (port3)	WAN-2 (port2)	all	109
3	Allow DMZ-Zone-to-WAN	DMZ-Zone	WAN-1 (port1)	all	0
4	Allow DMZ-Zone-to-LAN	DMZ-Zone	LAN (port3)	all	0
5	Allow LAN-to-DMZ-Zone	LAN (port3)	DMZ-Zone	all	0
6	WAN-to-LAN	WAN-1 (port1)	LAN (port3)	Remote-10.0.6.0	0
0	Implicit Deny	any	any	all	0

Log & Report -> Forward traffic -> Filter the source IP -> Check current traffic of client machine.

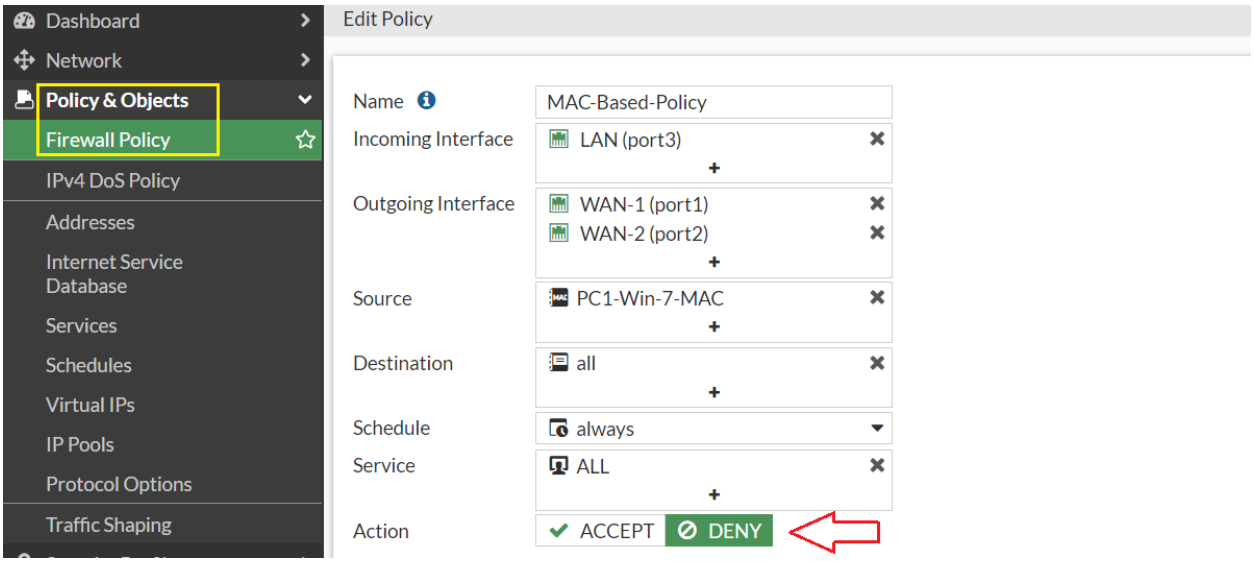
Destination: 192.168.1.254 <= >= A-B OR NOT EXACT Add Filter

Date/Time	Destination Interface	Policy ID	Source	Device	Destination
44 minutes ago	WAN-1 (port1)	MAC-Based-Policy (7)	10.0.1.1	USER-PC	192.168.1.254 (pfSense.localdomain)
45 minutes ago	WAN-1 (port1)	MAC-Based-Policy (7)	10.0.1.1	USER-PC	192.168.1.254 (pfSense.localdomain)
46 minutes ago	WAN-1 (port1)	MAC-Based-Policy (7)	10.0.1.1	USER-PC	192.168.1.254 (pfSense.localdomain)
46 minutes ago	WAN-1 (port1)	MAC-Based-Policy (7)	10.0.1.1	USER-PC	192.168.1.254 (pfSense.localdomain)
46 minutes ago	WAN-1 (port1)	MAC-Based-Policy (7)	10.0.1.1	USER-PC	192.168.1.254 (pfSense.localdomain)
47 minutes ago	WAN-1 (port1)	MAC-Based-Policy (7)	10.0.1.1	USER-PC	192.168.1.254 (pfSense.localdomain)
47 minutes ago	WAN-1 (port1)	MAC-Based-Policy (7)	10.0.1.1	USER-PC	192.168.1.254 (pfSense.localdomain)
47 minutes ago	WAN-1 (port1)	MAC-Based-Policy (7)	10.0.1.1	USER-PC	192.168.1.254 (pfSense.localdomain)

Dashboard->FortiView Polices-> here you will find MAC-Based-Policy has been used.



Let's modify the policy and deny the traffic from the given MAC Address.



This time no PING and no browse is working because of Deny by MAC Address.