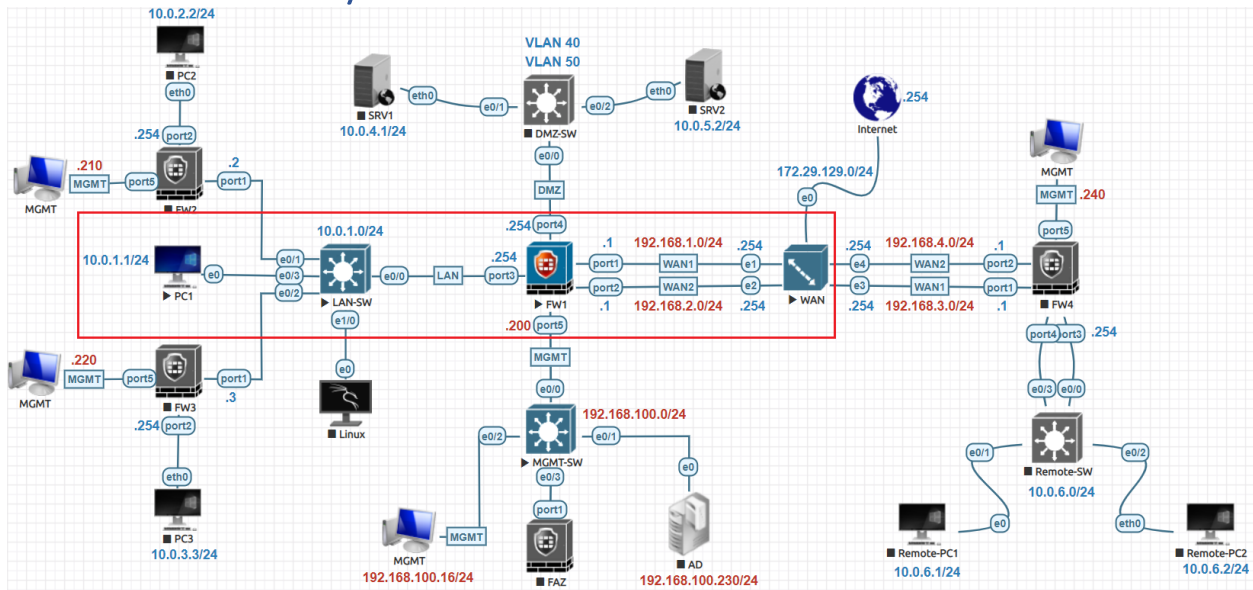
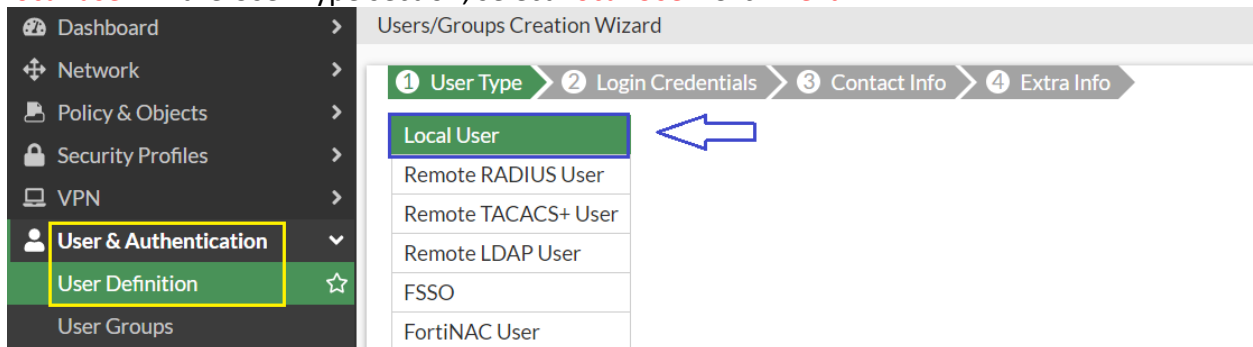


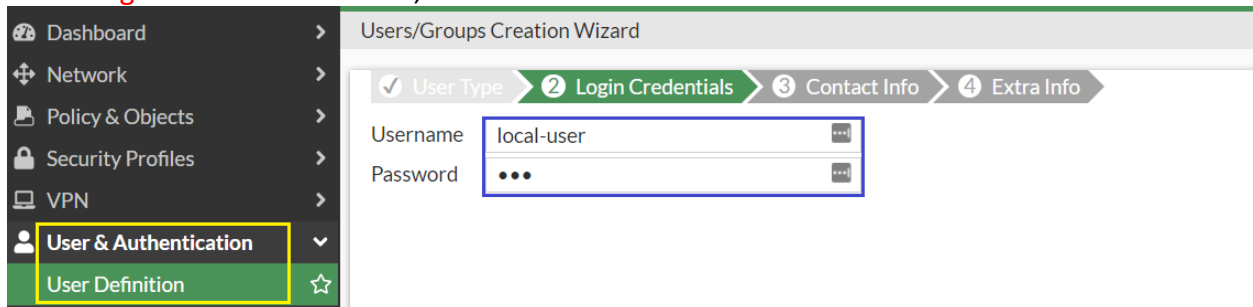
Local User and Policy:



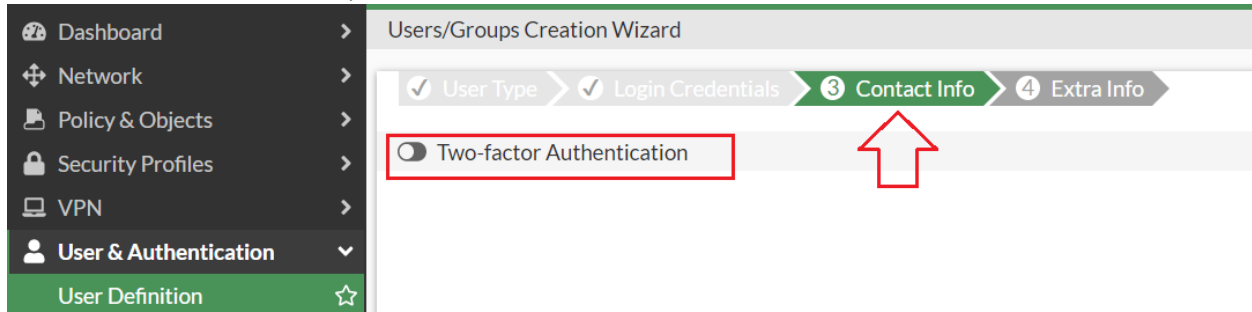
Let's Create a new user, go to **User & Authentication > User Definition** this account is called **local-user**. In the User Type section, select **Local User**. Click **Next**.



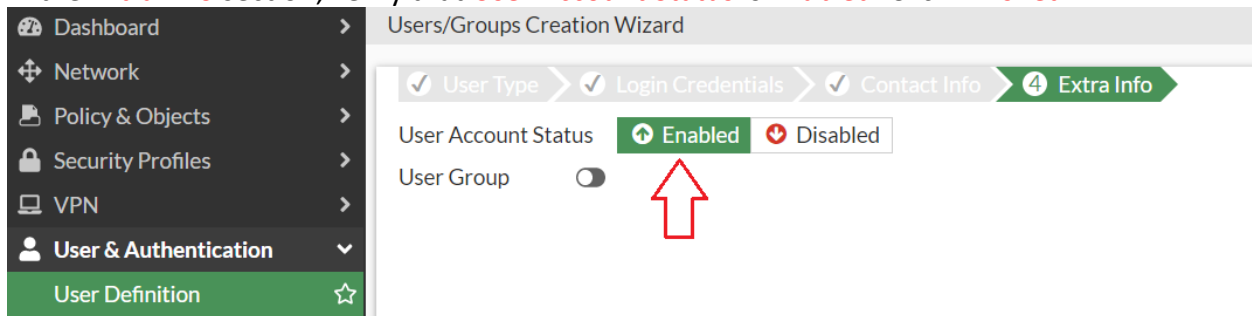
In the **Login Credentials** section, set **Username** and set a **Password**.



In the **Contact info** section, set off Two-factor Authentication.



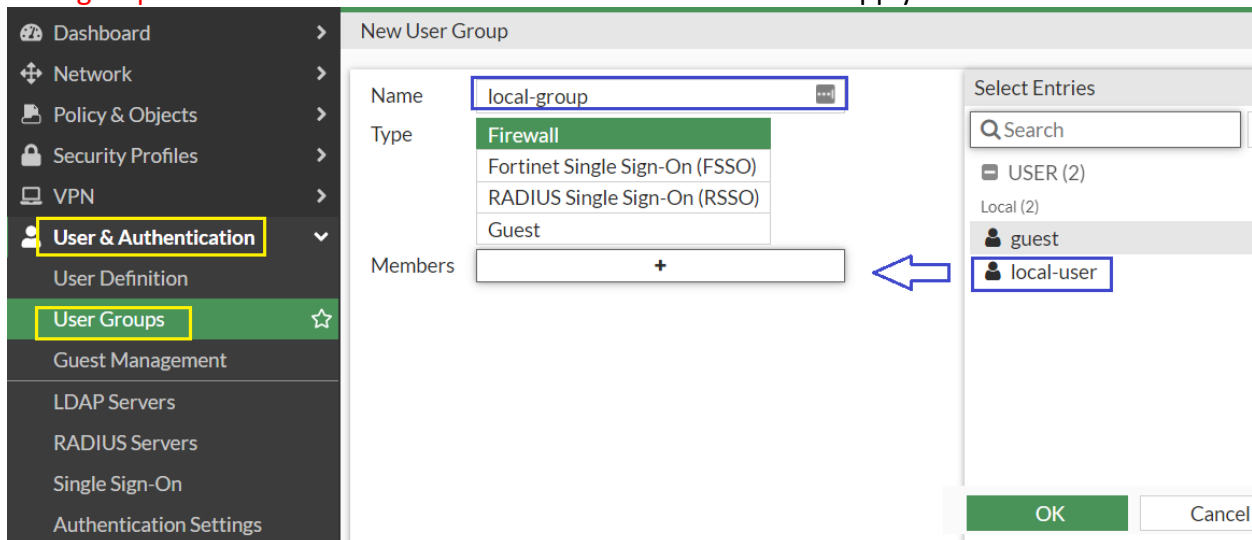
In the **Extra Info** section, verify that **User Account Status** is **Enabled**. Click **Finished**.



Your FortiGate Firewall now lists the new user.

Name	Type	Two-factor...	Groups	Status	Ref.
guest	LOCAL	✘	Guest-group	✓ Enabled	1
local-user	LOCAL	✘		✓ Enabled	0

To create a new user group, go to **User & Authentication > User Groups** this group is called **local-group**. Add user **local-user** to the **Members** list. Click **OK** to apply.



The FortiGate now lists the newly created user group with the named **local-group**.

Group Name	Group Type	Members	
Guest-group	Firewall	guest	0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1
local-group	Firewall	local-user	0

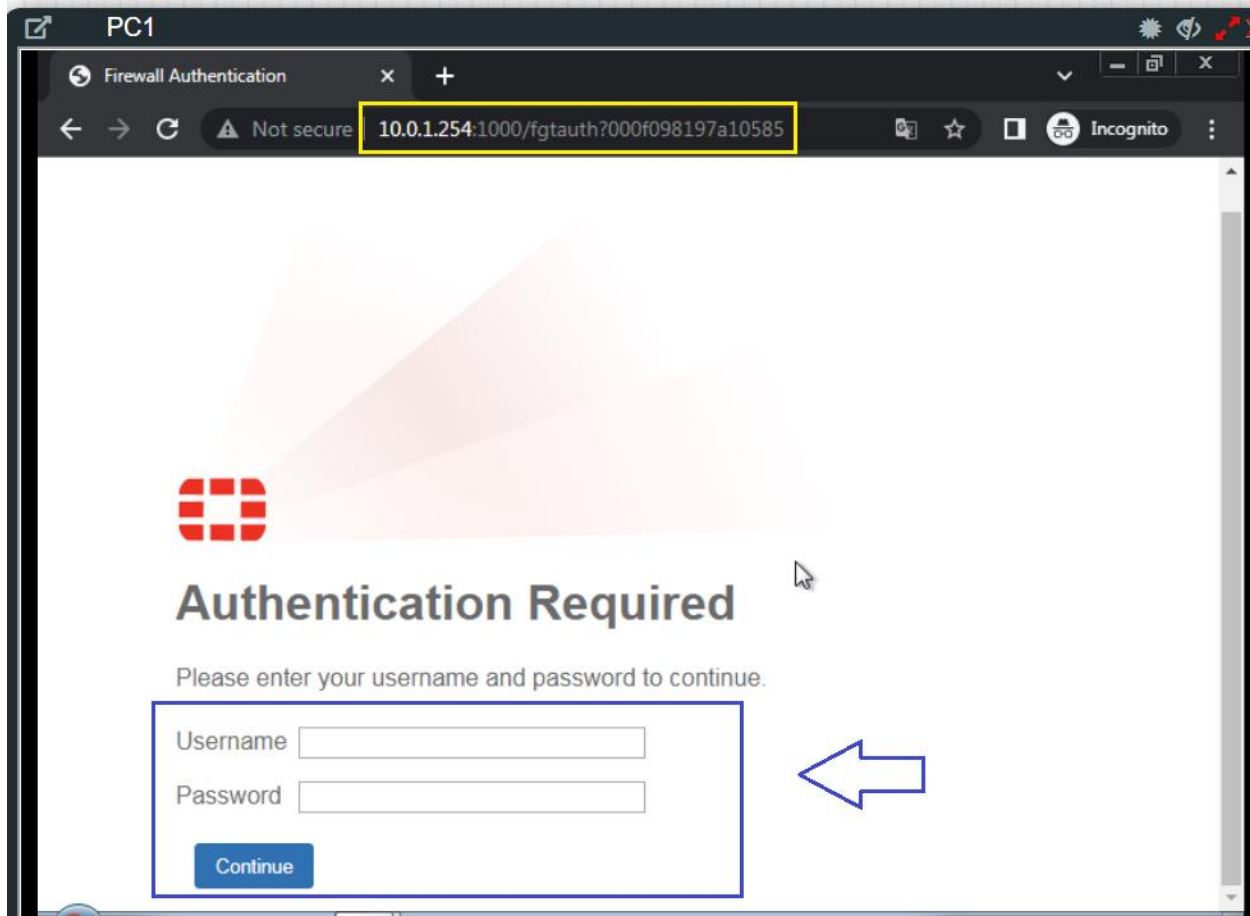
Create a policy, go to **Policy & Objects > Firewall Policy**. For **Source**, set **Address** to **all** and **User** to the **local-group** group. Under **Security Profiles**, set both to use the default profile.

To properly test disable all LAN to WAN Policies and Create Separate DNS policy on the top.

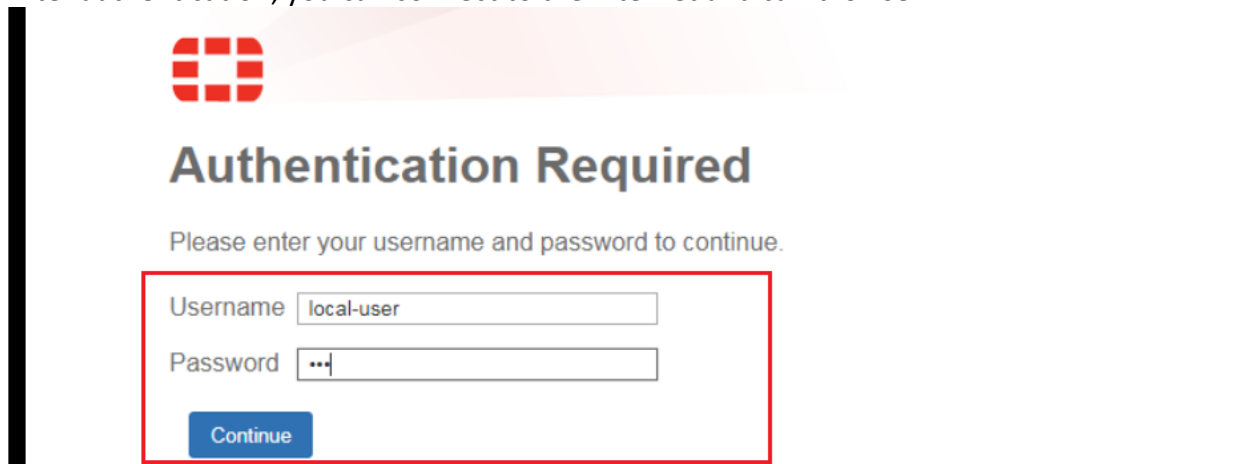
ID	Name	From	To	Source	Hit Count
9	Allow-DNS	LAN (port3)	WAN-1 (port1) WAN-2 (port2)	all	54
8	Local-User Policy	LAN (port3)	WAN-1 (port1) WAN-2 (port2)	local-user all	28
7	MAC-Based-Policy	LAN (port3)	WAN-1 (port1) WAN-2 (port2)	PC1-Win-7-MAC	0

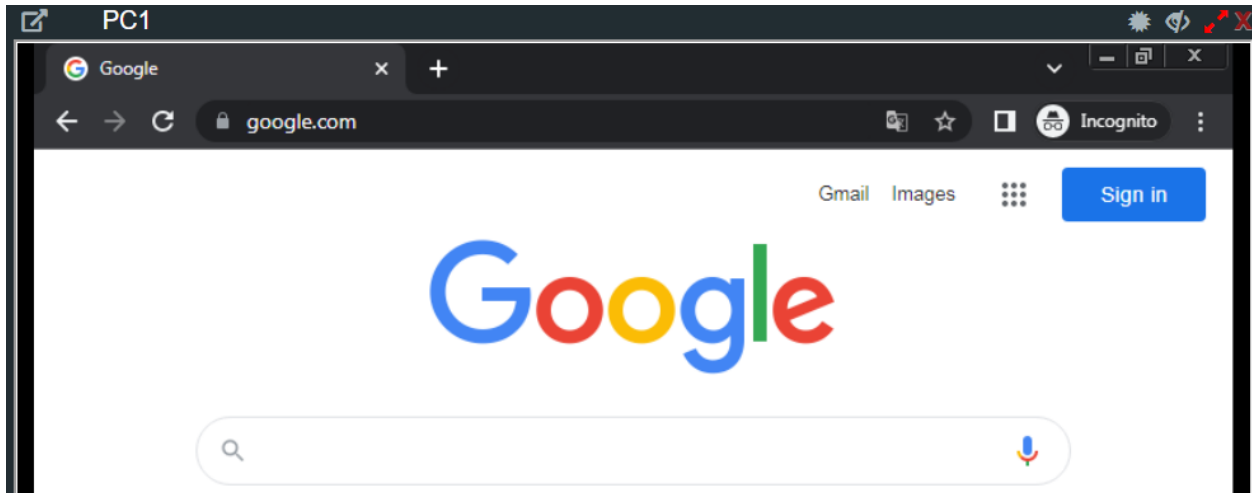
Test and Verification:

From any PC in the internal network, attempt to browse the Internet. A log in screen will appear. Use the **local-user** account to log in. After authentication, you can connect to the Internet and access the services.

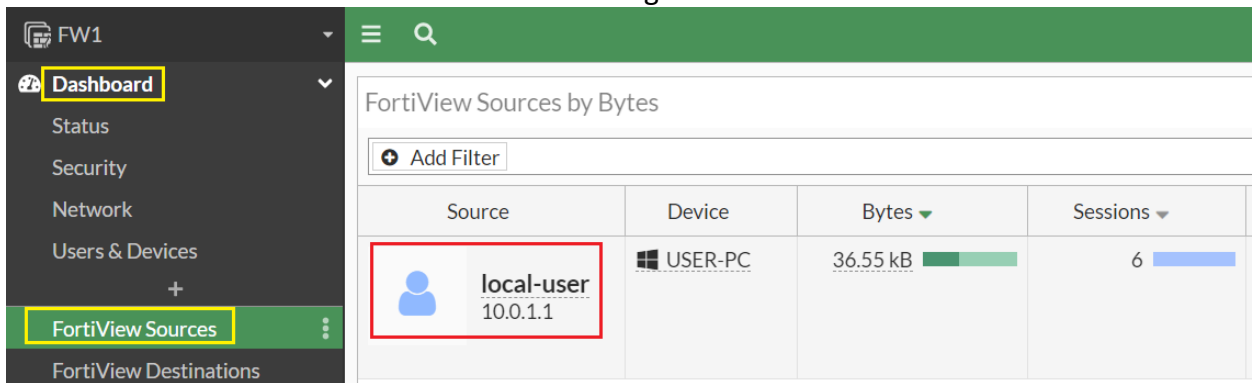


After authentication, you can connect to the Internet and can browse.

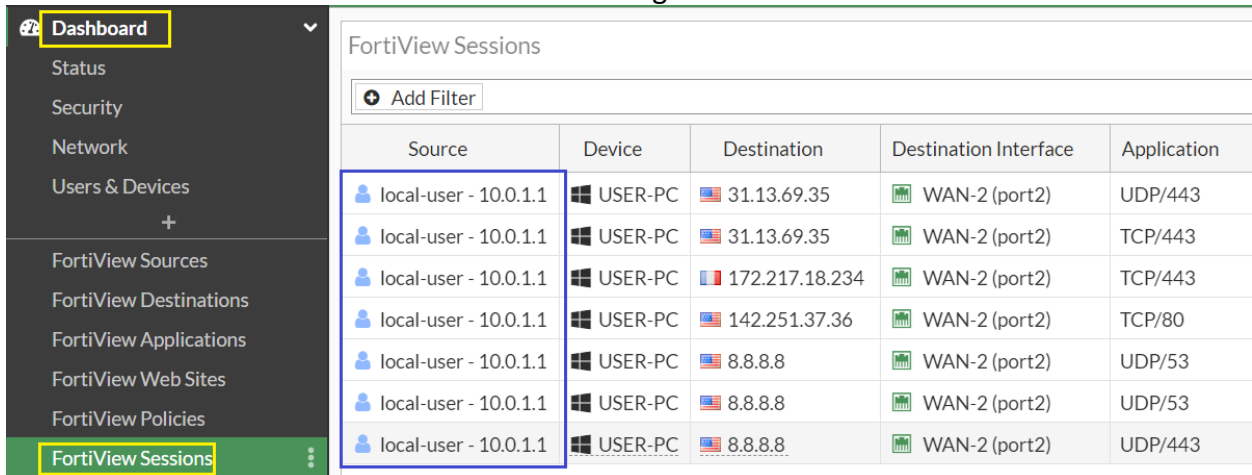




Go to **Dashboard>FortiView Sources** to see the login and authenticated user.



Go to **Dashboard>FortiView Sessions** to see the login and authenticated user sessions details.



Go to **Log & Report > Forward Traffic** to verify the login and authenticated User (local-user).

Date/Time	Source	Destination Interface	Policy ID	Device
10 seconds ago	local-user (10.0.1.1)	WAN-2 (port2)	Local-User Policy (8)	USER-PC
25 seconds ago	local-user (10.0.1.1)	WAN-2 (port2)	Local-User Policy (8)	USER-PC
47 seconds ago	local-user (10.0.1.1)	WAN-2 (port2)	Local-User Policy (8)	USER-PC
2 minutes ago	local-user (10.0.1.1)	WAN-2 (port2)	Local-User Policy (8)	USER-PC
2 minutes ago	local-user (10.0.1.1)	WAN-2 (port2)	Local-User Policy (8)	USER-PC
3 minutes ago	local-user (10.0.1.1)	WAN-2 (port2)	Local-User Policy (8)	USER-PC
4 minutes ago	local-user (10.0.1.1)	WAN-2 (port2)	Local-User Policy (8)	USER-PC
4 minutes ago	local-user (10.0.1.1)	WAN-2 (port2)	Local-User Policy (8)	USER-PC

Go to **Dashboard>Users & Devices** to see the login and authenticated users

User Name	IP Address	User Group	Duration	Traffic Volume
local-user	10.0.1.1		40 minute(s) and...	4.98 MB

Incase want to De-authenticate the user go to **Dashboard>Users & Devices** right click on username and click **Deauthneticate** or above button **Deauthneticate**

User Name	IP Address	User Group	Duration	Traffic Volume
local-user	10.0.1.1		40 minute(s) and...	4.98 MB