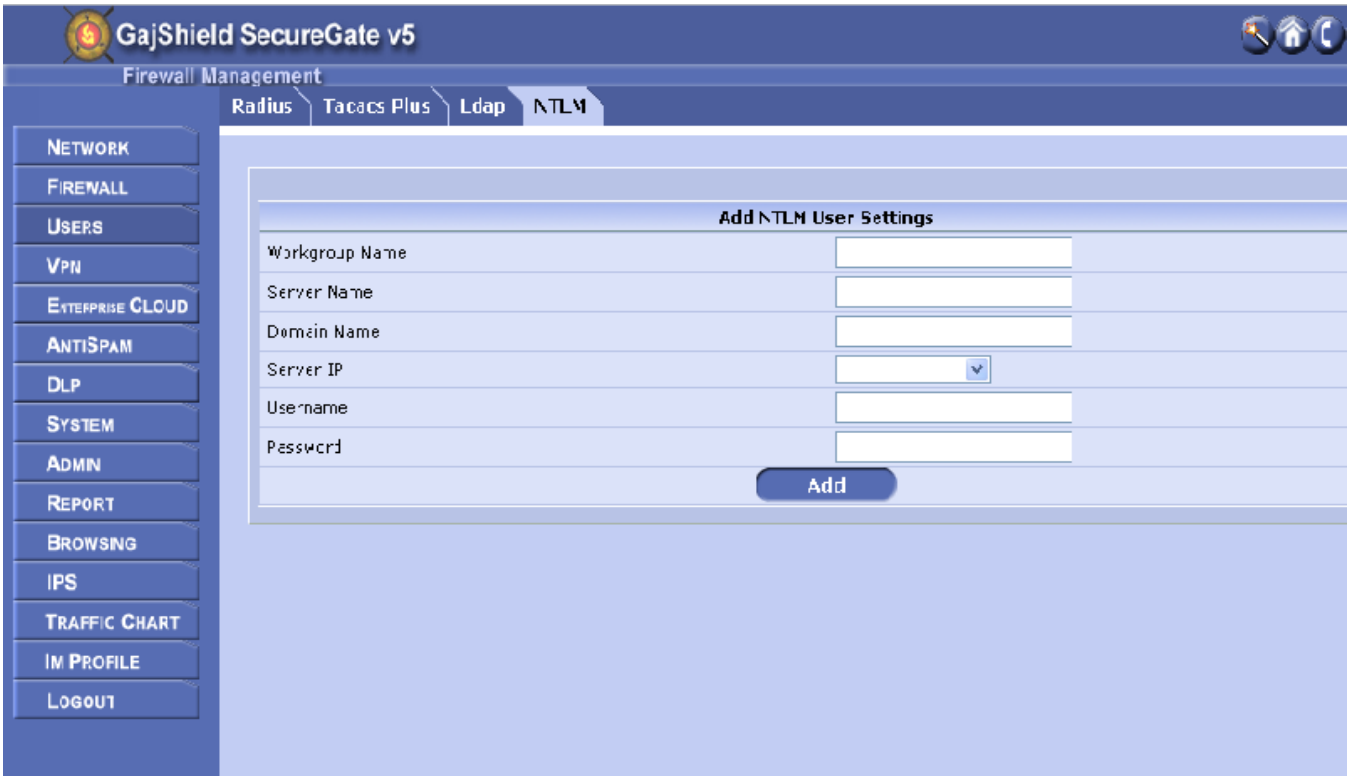
NTLM also know as **NT LAN Manager** is a suite of Microsoft® security protocols that provides authentication, integrity, and confidentiality to users. This screen helps you configure the NTLM service on GajShield.

Go To GajShield Firewall Web Frontend:

1. Go to **Users > NTLM >** and provide below information.



Workgroup Name: Type you domain name without abbreviation.
(Example: Domain name is **testdc.com**, only insert **testdc**)

Server Name: Insert the host name / NetBIOS name of the server.

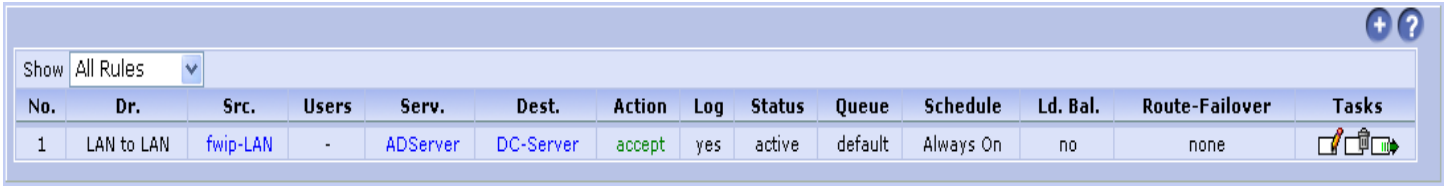
Domain Name: Insert Domain name.
(Example: Domain name is **testdc.com**, insert the same)

Server IP: Select the Domain controller LAN IP.
(Create IP host in firewall by going on **Firewall > Networks > Hosts**)

Username: Provide username of an administrator or any user with administrative right.
(Recommended is administrator user)

Password: Insert password of the user in the Username field.

Note: You will need to add a rule by going on **Firewall > Policies > Rules,** use **ADServer** in services tab & destination will be Active Directory server IP address, this will allow the firewall to access the Active Directory server. Example on how to create a rule is show below for reference.



Show All Rules

No.	Dr.	Src.	Users	Serv.	Dest.	Action	Log	Status	Queue	Schedule	Ld. Bal.	Route-Failover	Tasks
1	LAN to LAN	fwip-LAN	-	ADServer	DC-Server	accept	yes	active	default	Always On	no	none	

2. Before you click on **Restart NTLM & Synchronize NTLM Users**, go on **Browsing > Setup > Browsing Options**, under **Select Proxy Authentication Scheme** select **NTLM.**

Browsing Setup

Enter Proxy Port	8080
URL Blocker Instance	4
Enforce Strict Search on	Google Images : Yahoo Images :
Virus Scanning	
Enable Https	Https Port 8080
GajShield userSense Login Timeout Setup	5 mins.
Download Default Policy	Default Allow
Select Proxy Authentication Scheme	User (Login/Password) Authentication
	Local
	Radius
	TACACS+
	LDAP
	NTLM
	No User Authentication
	Transparent Mode
	GajShield userSense
	Local
	Radius
	TACACS+
	LDAP
	NTLM

Setup

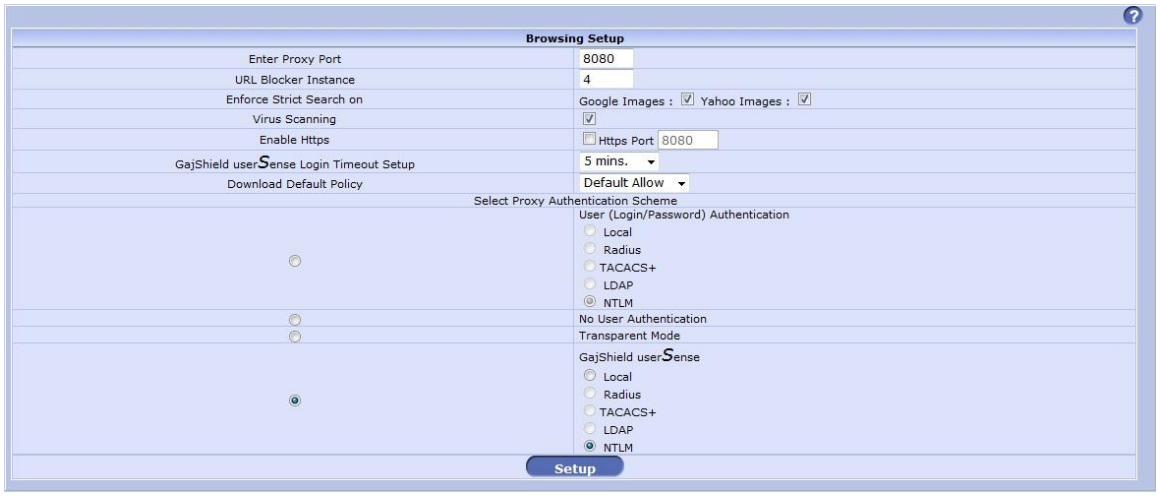
3. Go to **Firewall > Policies > Rules** click on  , create the below rule for NTLM browsing & it is also used for single sign on (SSO), when using NTLM. Port to be used in firewall rule **8080,** which was used in the earlier image next to **Enter Proxy Port.**

Show All Rules

No.	Dr.	Src.	Users	Serv.	Dest.	Action	Log	Status	Queue	Schedule	Ld. Bal.	Route-Failover	Tasks
1	LAN to LAN	fwnet-LAN	-	squid	fwip-LAN	accept	yes	active	default	Always On	no	none	
2	WAN to WAN	fwip-WAN	-	http https	any	accept	yes	active	default	Always On	no	none	

NOTE: When you select Proxy Authentication for NLTM on GajShield firewall, you will have to insert proxy settings in your Web Browser. Use the same port used in **Enter Proxy Port**.

OR



4. Under **GajShield userSense** select **NTLM**. When using usersense, user will be asked for authentication when they try to browse.
5. Click on the **Setup** button.
6. Go to **Start Proxy** Tab next to Browsing Options & click on  (Restart Proxy Button).

For further assistance please Contact GajShield Support on +91 22 66607450 / 51/ 52/ 53

Email: support@gajshield.com