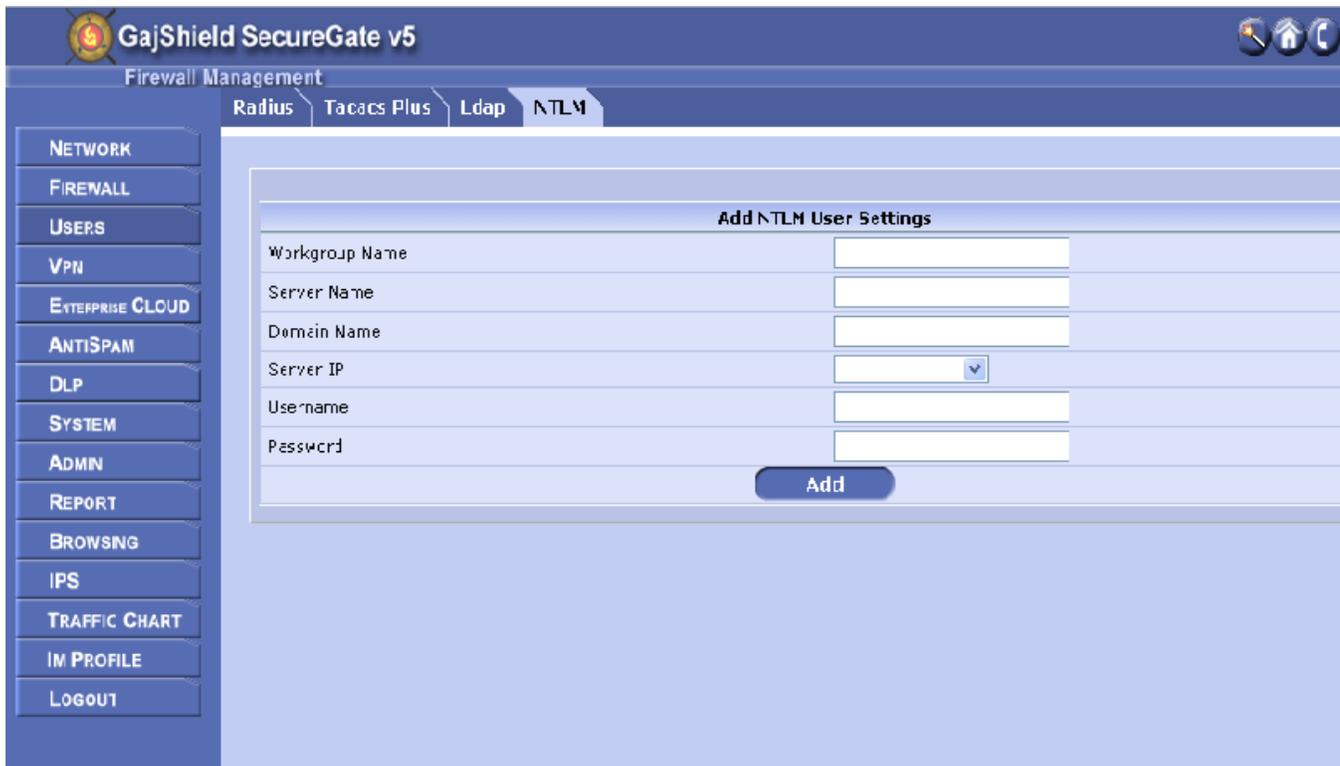


NTLM also know as **NT LAN Manager** is a suite of Microsoft® security protocols that provides authentication, integrity, and confidentiality to users. This screen helps you configure the NTLM service on GajShield.

Go To GajShield Firewall Web Frontend:

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



The screenshot shows the GajShield SecureGate v5 Firewall Management web interface. The top navigation bar includes 'Radius', 'Tacacs Plus', 'Ldap', and 'NTLM'. The left sidebar contains a menu with options: NETWORK, FIREWALL, USERS, VPN, ENTERPRISE CLOUD, ANTI SPAM, DLP, SYSTEM, ADMIN, REPORT, BROWSING, IPS, TRAFFIC CHART, IM PROFILE, and LOGOUT. The main content area is titled 'Add NTLM User Settings' and contains the following fields:

Add NTLM User Settings	
Workgroup Name	<input type="text"/>
Server Name	<input type="text"/>
Domain Name	<input type="text"/>
Server IP	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>

Below the form is an 'Add' button.

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.

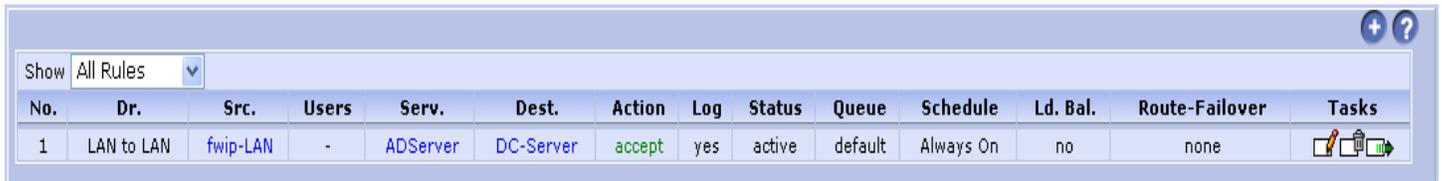
Domain Name: Insert Domain name.
(Example: Domain name is **testdc.com**, insert the same)

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.

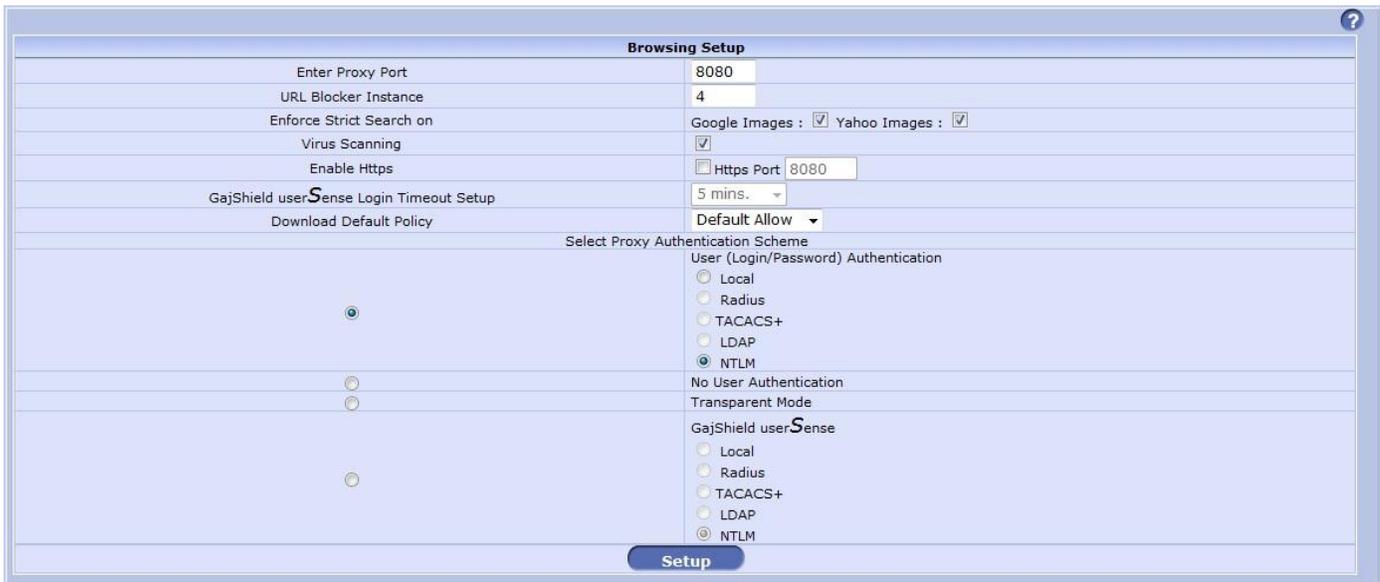
Note: You will need to add a rule by going on **Firewall > Policies > Rules**, use **ADServer** in services tab & destination will be Active Directory server IP address, this will allow the firewall to access the Active Directory server. Example on how to create a rule is show below for reference.



A screenshot of a web interface showing a table of firewall rules. The table has columns for No., Dr., Src., Users, Serv., Dest., Action, Log, Status, Queue, Schedule, Ld. Bal., Route-Failover, and Tasks. The first rule is highlighted.

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**.



A screenshot of the 'Browsing Setup' configuration page. The 'Select Proxy Authentication Scheme' section is expanded, showing radio button options for Local, Radius, TACACS+, LDAP, NTLM, No User Authentication, and Transparent Mode. The NTLM option is selected.

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**.

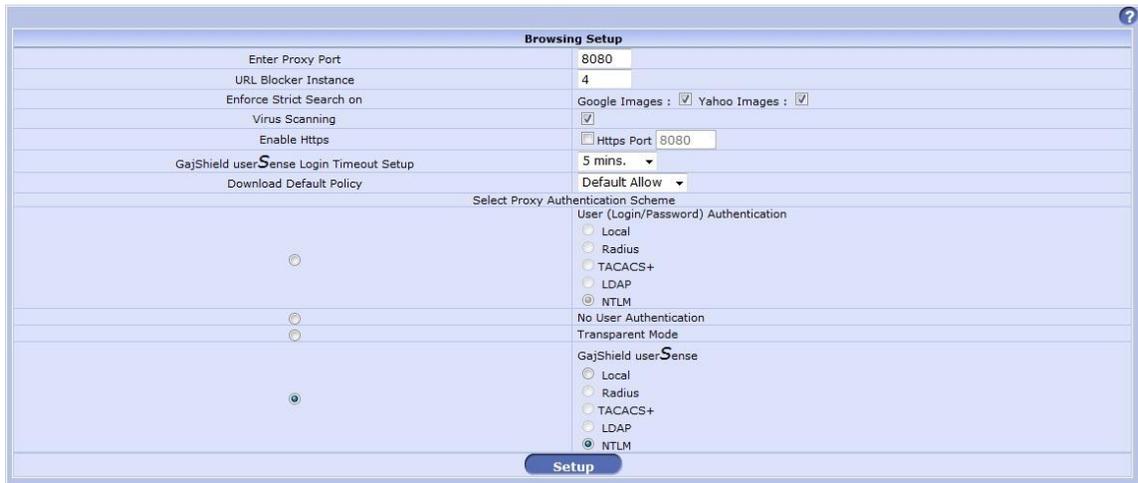


A screenshot of a web interface showing a table of firewall rules. The table has columns for No., Dr., Src., Users, Serv., Dest., Action, Log, Status, Queue, Schedule, Ld. Bal., Route-Failover, and Tasks. Two rules are listed.

No.	Dr.	Src.	Users	Serv.	Dest.	Action	Log	Status	Queue	Schedule	Ld. Bal.	Route-Failover	Tasks
1	LAN to LAN	fwip-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



The screenshot shows the 'Browsing Setup' configuration window in GajShield. The 'Enter Proxy Port' field is set to 8080. The 'URL Blocker Instance' is set to 4. The 'Enforce Strict Search on' section has 'Google Images' and 'Yahoo Images' checked. 'Virus Scanning' is checked. 'Enable Https' is unchecked, with the 'Https Port' set to 8080. 'GajShield userSense Login Timeout Setup' is set to 5 mins. 'Download Default Policy' is set to 'Default Allow'. Under 'Select Proxy Authentication Scheme', 'User (Login/Password) Authentication' is selected, and 'NTLM' is chosen. Under 'GajShield userSense', 'NTLM' is also selected. A 'Setup' button is at the bottom.

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