Configuring NTLM Authentication for URL Filtering and Browsing

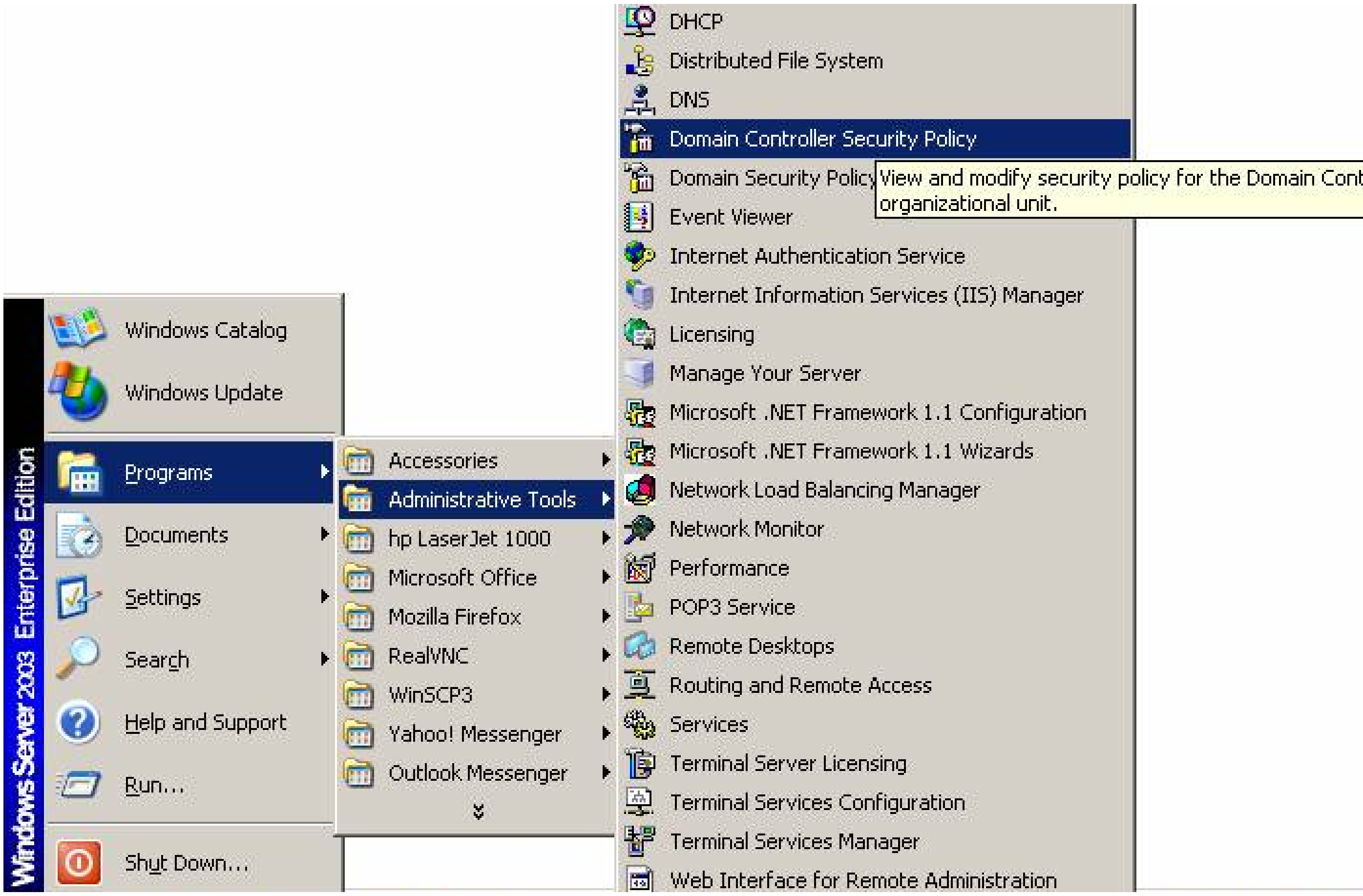
You will learn to configure NTLM Authentication with GajShield UPTM in this guide.

GajShield supports a wide variety of user authentication for the browsing users. The authentication supported are NTLM, Active Directory, LDAP, Radius & Tacas+. You can define policies for URL filtering based on users and groups. These users would authenticate with GajShield UPTM, before they are allowed to browse internet. For this authentication you can configure GajShield UPTM to integrate with Microsoft NTLM

Steps to Configure NTLM Authentication

Step 1

On the Windows 2003 server Click on Start – Programs – Administrative Tools – Default Domain Controller Security Policy

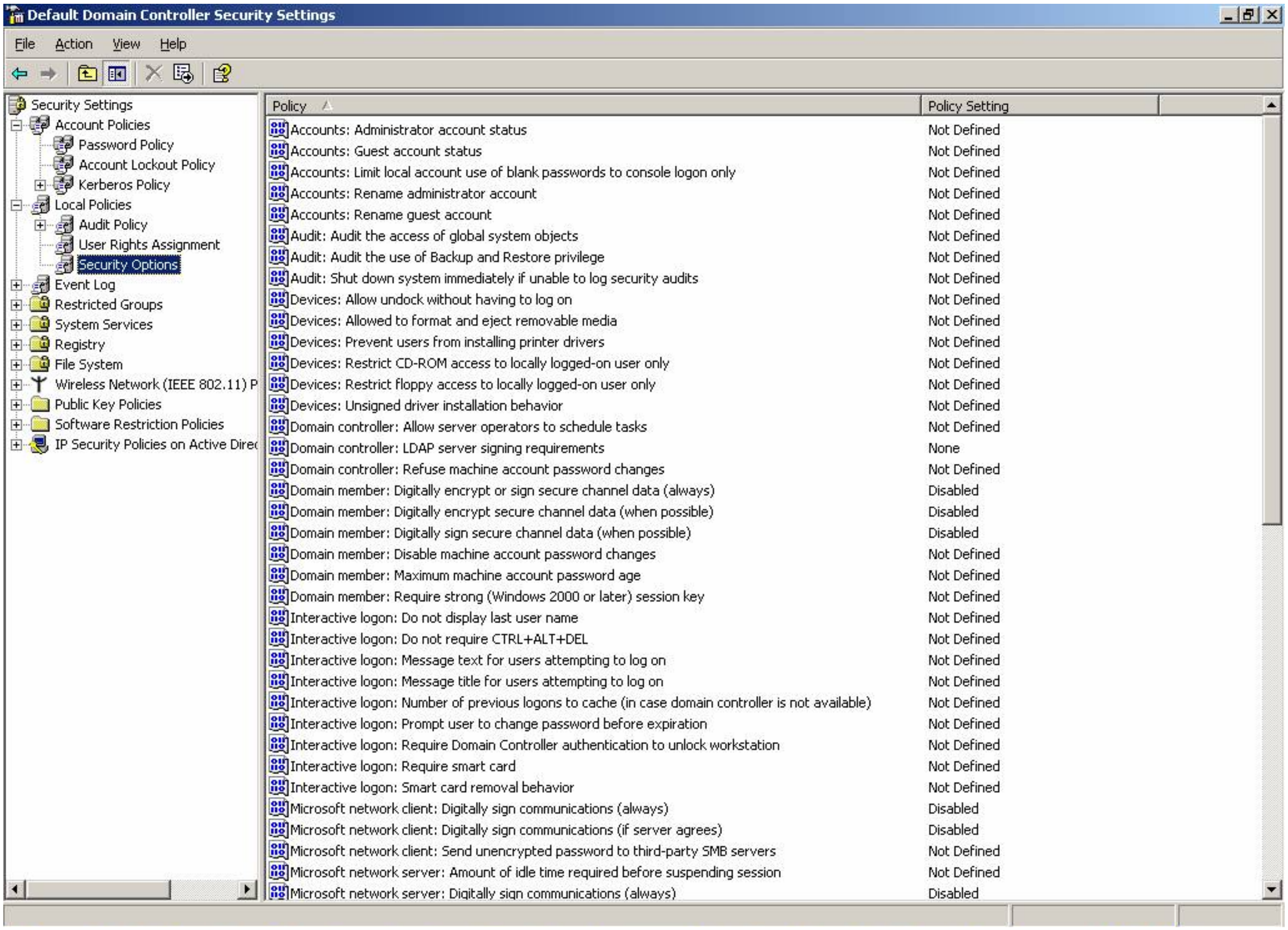


View and modify security policy for the Domain Cont
organizational unit.

Windows Server 2003 Enterprise Edition
Windows Catalog
Windows Update
Programs
Documents
Settings
Search
Help and Support
Run...
Shut Down...
Accessories
Administrative Tools
hp LaserJet 1000
Microsoft Office
Mozilla Firefox
RealVNC
WinSCP3
Yahoo! Messenger
Outlook Messenger
DHCP
Distributed File System
DNS
Domain Controller Security Policy
Domain Security Policy
Event Viewer
Internet Authentication Service
Internet Information Services (IIS) Manager
Licensing
Manage Your Server
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Network Load Balancing Manager
Network Monitor
Performance
POP3 Service
Remote Desktops
Routing and Remote Access
Services
Terminal Server Licensing
Terminal Services Configuration
Terminal Services Manager
Web Interface for Remote Administration

Step 2:

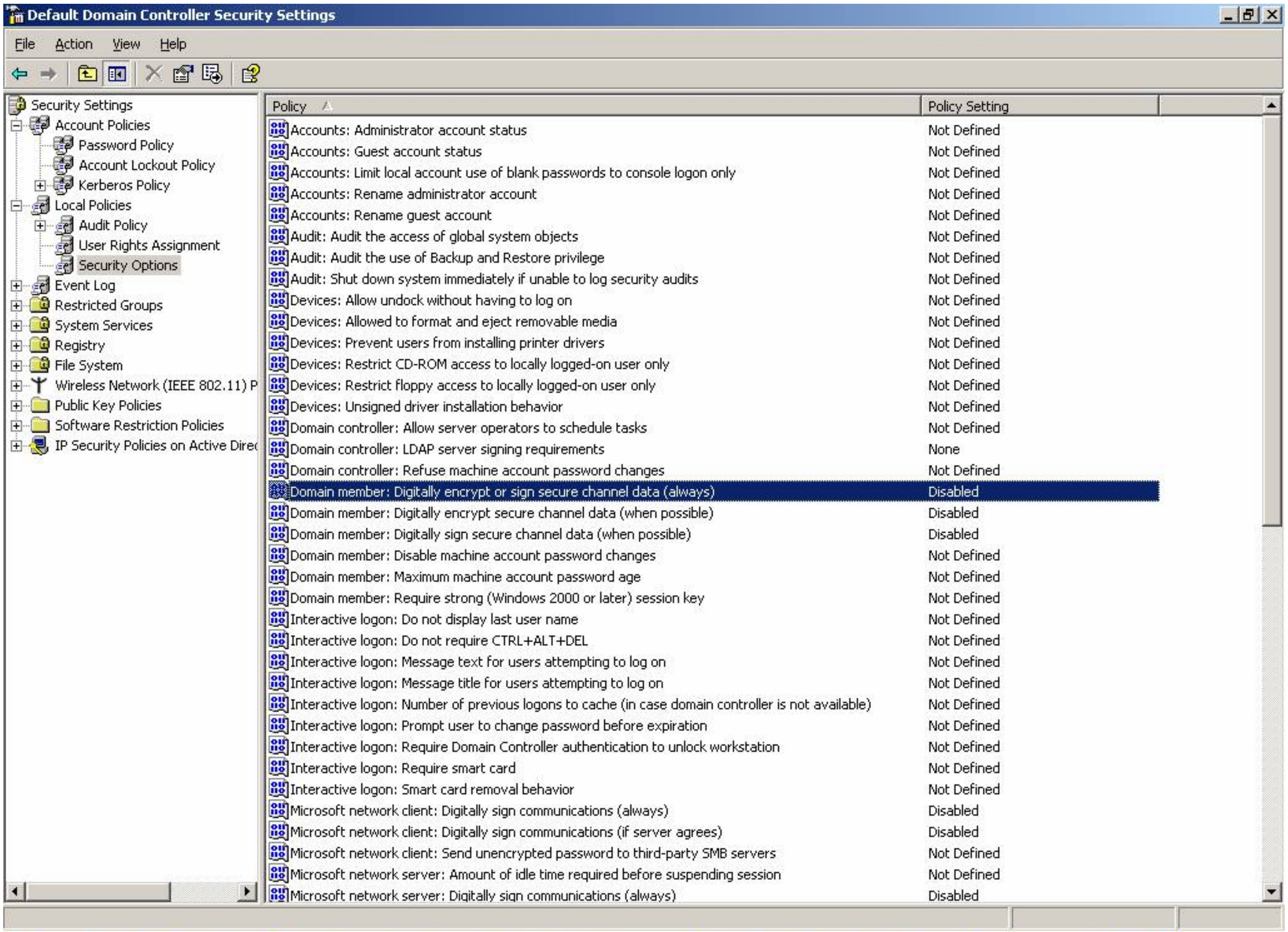
In Domain Controller Security Policy click on Local Policy – Security options



Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to console logon only	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Shut down system immediately if unable to log security audits	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Devices: Unsigned driver installation behavior	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	None
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Disabled
Domain member: Digitally encrypt secure channel data (when possible)	Disabled
Domain member: Digitally sign secure channel data (when possible)	Disabled
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Disabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Not Defined
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled

Step 3:

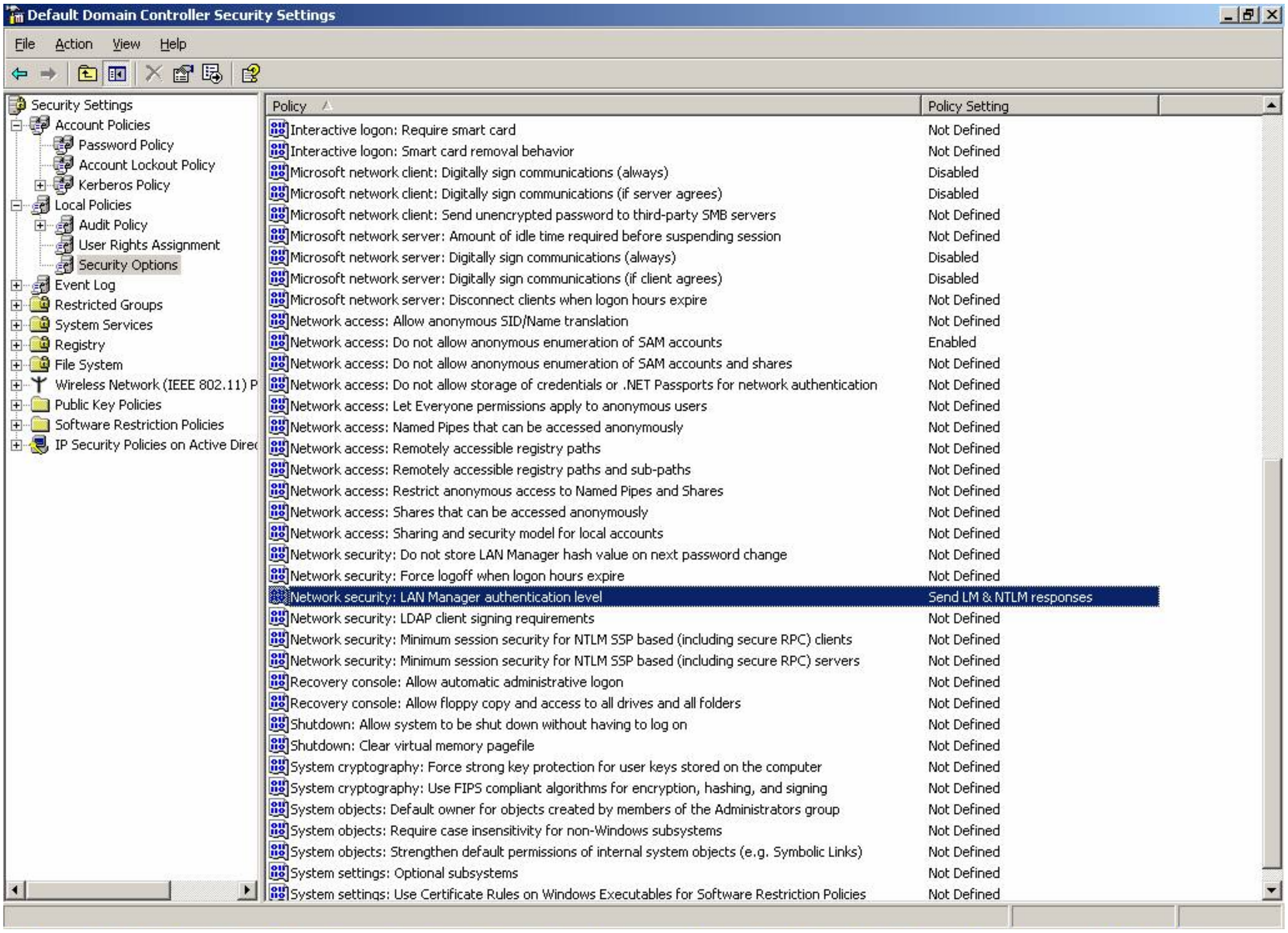
In Security Options select **Domain Member: Digitally encrypt…..** Right click and disable this option



Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to console logon only	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Shut down system immediately if unable to log security audits	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Devices: Unsigned driver installation behavior	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	None
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Disabled
Domain member: Digitally encrypt secure channel data (when possible)	Disabled
Domain member: Digitally sign secure channel data (when possible)	Disabled
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Disabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Not Defined
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled

Step 4:

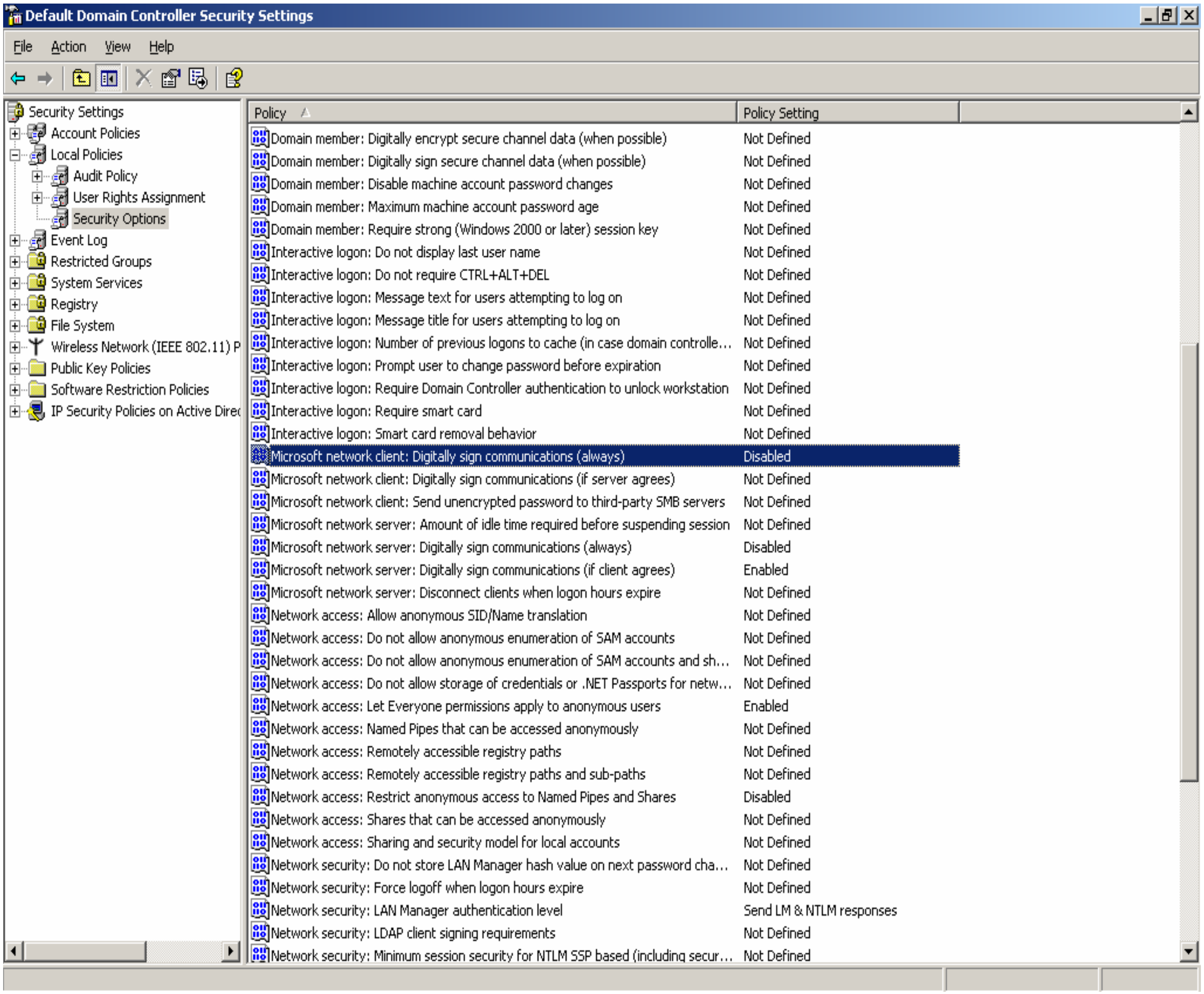
In Security Settings: Local Policy - Select Security Options - Select **Network Security: LAN Manager Authentication** Right click and select Send LM & NTLM responses



Policy	Policy Setting
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Disabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Not Defined
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Not Defined
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Not Defined
Network access: Let Everyone permissions apply to anonymous users	Not Defined
Network access: Named Pipes that can be accessed anonymously	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub-paths	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Not Defined
Network security: Force logoff when logon hours expire	Not Defined
Network security: LAN Manager authentication level	Send LM & NTLM responses
Network security: LDAP client signing requirements	Not Defined
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Not Defined
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Not Defined
Recovery console: Allow automatic administrative logon	Not Defined
Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
Shutdown: Allow system to be shut down without having to log on	Not Defined
Shutdown: Clear virtual memory pagefile	Not Defined
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Not Defined
System objects: Default owner for objects created by members of the Administrators group	Not Defined
System objects: Require case insensitivity for non-Windows subsystems	Not Defined
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Not Defined
System settings: Optional subsystems	Not Defined
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Not Defined

Step 5:

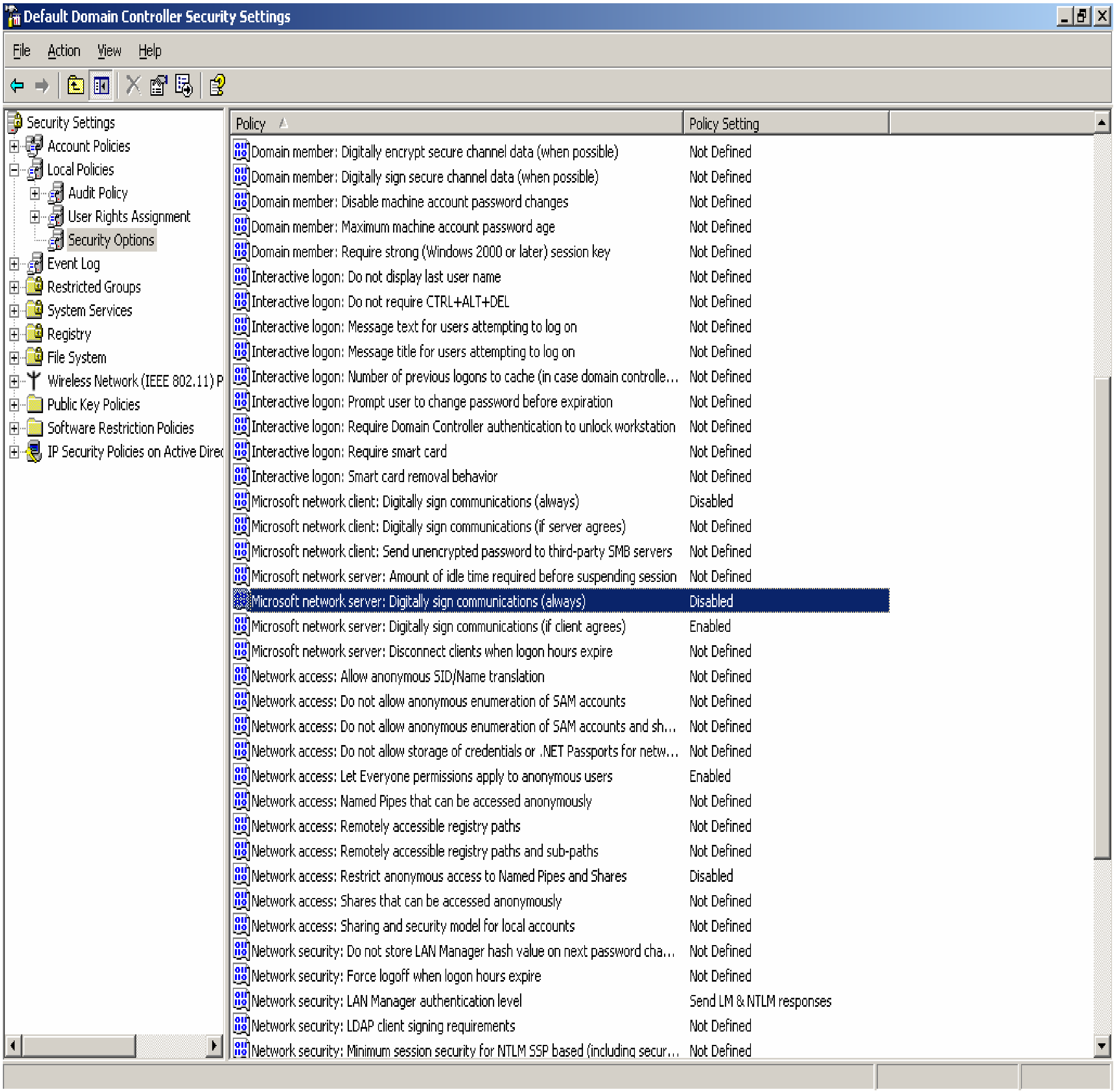
In Security Settings: Local Policy - Select Security Options - Select **Microsoft network Client: Digitally sign Communication (Always)** Right click and disable this option



Policy	Policy Setting
Domain member: Digitally encrypt secure channel data (when possible)	Not Defined
Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controlle...	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Not Defined
Microsoft network client: Send unencrypted password to third-party SMB servers	Not Defined
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts and sh...	Not Defined
Network access: Do not allow storage of credentials or .NET Passports for netw...	Not Defined
Network access: Let Everyone permissions apply to anonymous users	Enabled
Network access: Named Pipes that can be accessed anonymously	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub-paths	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Disabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Not Defined
Network security: Do not store LAN Manager hash value on next password cha...	Not Defined
Network security: Force logoff when logon hours expire	Not Defined
Network security: LAN Manager authentication level	Send LM & NTLM responses
Network security: LDAP client signing requirements	Not Defined
Network security: Minimum session security for NTLM SSP based (including secur...	Not Defined

Step 6:

In Security Settings: Local Policy - Select Security Options - Select **Microsoft network Server: Digitally sign Communication(Always)** Right click and disable this option



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wireless Network (IEEE 802.11) P
  - Public Key Policies
  - Software Restriction Policies
  - IP Security Policies on Active Direc

Policy	Policy Setting
Domain member: Digitally encrypt secure channel data (when possible)	Not Defined
Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controlle...	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Not Defined
Microsoft network client: Send unencrypted password to third-party SMB servers	Not Defined
Microsoft network server: Amount of idle time required before suspending session	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Network access: Allow anonymous SID/Name translation	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts and sh...	Not Defined
Network access: Do not allow storage of credentials or .NET Passports for netw...	Not Defined
Network access: Let Everyone permissions apply to anonymous users	Enabled
Network access: Named Pipes that can be accessed anonymously	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub-paths	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Disabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Not Defined
Network security: Do not store LAN Manager hash value on next password cha...	Not Defined
Network security: Force logoff when logon hours expire	Not Defined
Network security: LAN Manager authentication level	Send LM & NTLM responses
Network security: LDAP client signing requirements	Not Defined
Network security: Minimum session security for NTLM SSP based (including secur...	Not Defined

Step 7:

Rule on Firewall

To configure the NLTM rules on GajShield UPTM you need to create the services group of the services used by NTLM. These services are available in GajShield UPTM hence please select them and create a service group.

Create a Service Group on GajShield UPTM :

ServiceGroupName	ServiceName	Sorce Port	Destination Port	Type
NTLM	Microsoft-smbtcp	1024:65535	445	Tcp
	Netbios-dgmtcp	138	138	Tcp
	Netbios-dgmudp	138	138	Udp
	Netbios-nstcp	137	137	Tcp
	Netbios-ssntcp	1024:65535	139	Tcp
	Netbios-ssnudp	1024:65535	139	Udp
	Netbios-udp-ns	1024:65535	137	Udp
	Netbios-nsudp	137	137	Udp

Add the rule on GajShield :

Now create the rules for allowing NTLM service through the GajShield UPTM from the Policy menu

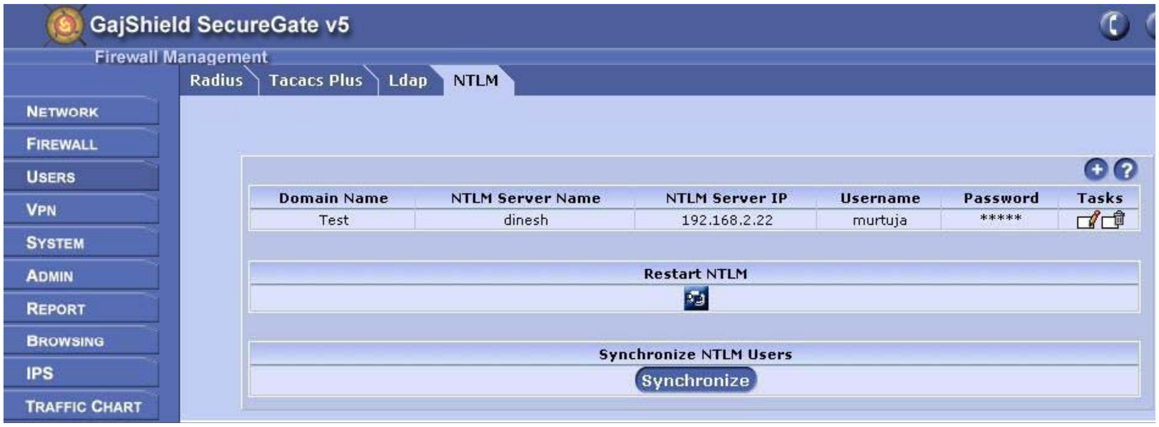
Direction	Source	Service	Destination
Secure to Secure	Fwip-secure	NTLM	NTLM-Server

Note : Please install policies after the above rules have been added.

Step 8:NTLM setting on the Firewall :

Configure the NTLM settings on GajShield UPTM under USERS - NTLM. Click on Add button + and provide the following information

Domain Name: Domain Name of the NTLM Server (e.g. Test)
NTLM Server Name: Netbios Name of the NTLM server.
NTLM Server IP: IP of the NTLM server.
Username: User which is created on NTLM server for GajShield
(**Note:** This user should have Administrative rights on NTLM server).
Password: Password of the user created for the user.



Domain Name	NTLM Server Name	NTLM Server IP	Username	Password	Tasks
Test	dinesh	192.168.2.22	murtuja	*****	

Restart NTLM

Synchronize NTLM Users

After adding the above information restart the NTLM service.

Then Click on Synchronize NTLM Users to synchronize users from NTLM server to GajShield.