

# GajShield Training – URL Filtering

# URL Filtering

- In this training session you will learn
  - How to setup Proxy
  - Transparent mode/Proxy Mode
  - Authentication (User/IP)
  - URL allowing/blocking
  - User Scheduling
  - Mime policy
  - Category blocking

# Assumptions

- You have cleared the module on 'Basic Setup of GajShield UPTM'

# URL Filtering

- Transparent Mode
  - Browser proxy settings not required
  - All Internet traffic should flow through the firewall
  - User authentication not possible
- Proxy Mode
  - Setup the browser to use the proxy settings of the firewall
  - It is not required that all Internet traffic should flow through the firewall
  - User authentication can be enabled.

# URL Filtering: Transparent

The screenshot shows the GajShield SecureGate v5 Firewall Management interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows "https://192.168.2.176/cgi-bin/mainmenus.ggi". The interface has a navigation menu on the left with categories like NETWORK, FIREWALL, USERS, and SYSTEM. The main content area is titled "Firewall Management" and includes tabs for "Quick Setup", "Rules", "Bandwidth", "Install Policies", "Backup Rules", and "Admin Ips".

The "Quick Rules" section is expanded, showing a table of services and their filtering options:

Quick Rules				
<input type="checkbox"/>	Name Services (DNS)			
<input checked="" type="checkbox"/>	Browse(HTTP,HTTPS)	<input checked="" type="checkbox"/>	With Virus Scanning	<input checked="" type="checkbox"/> With URL Filtering <a href="#">Advance Rule</a>
<input type="checkbox"/>	Sending Mails (SMTP)	<input type="checkbox"/>	With Virus Scanning	
<input type="checkbox"/>	Receiving Mails (POP3)	<input type="checkbox"/>	With Virus Scanning	
<input type="checkbox"/>	File Transfer (FTP)	<input type="checkbox"/>	With Virus Scanning	
<input type="checkbox"/>	Remote Login (Telnet,SSH)			
<input type="checkbox"/>	Network Services (Ping, Traceroute,SNMP)			
<input type="checkbox"/>	IPSEC VPN (IPSEC)			
<input type="checkbox"/>	PPTP VPN (PPTP,GRE)			

An "Apply" button is located at the bottom of the "Quick Rules" section.

At the bottom of the interface, there is a footer with the text "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and a status bar showing "Done" and the IP address "192.168.2.176".

# URL Filtering: Proxy Mode

The screenshot displays the GajShield SecureGate v5 Firewall Management interface within a Mozilla Firefox browser window. The browser's address bar shows the URL `https://192.168.2.176/cgi-bin/mainmenus.ggi`. The interface features a sidebar with navigation options: NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING (selected), Users Setting, Site Policy, MimePolicy, Category, Setup, TRAFFIC CHART, IPS, and LOGOUT. The main content area is titled "Firewall Management" and includes tabs for "Browsing Options", "Start Proxy", "Restart ICAP", and "Restart ProxyLog". A "Browsing Setup" dialog box is open, containing the following configuration fields:

Browsing Setup	
Enter Proxy Port	3128
URL Blocker Instance	10
Virus Scanning	<input checked="" type="checkbox"/>
Select Proxy Authentication Scheme	
User (Login/Password) Authentication	
<input checked="" type="radio"/> Local	
<input type="radio"/> Radius	
<input type="radio"/> TACACS+	
<input type="radio"/> LDAP	
<input type="radio"/> NTLM	
<input type="radio"/> No User Authentication	
<input type="radio"/> Transparent Mode	
<b>Setup</b>	

At the bottom of the interface, the copyright notice reads "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved." and the status bar shows "Done" on the left and "192.168.2.176" on the right.

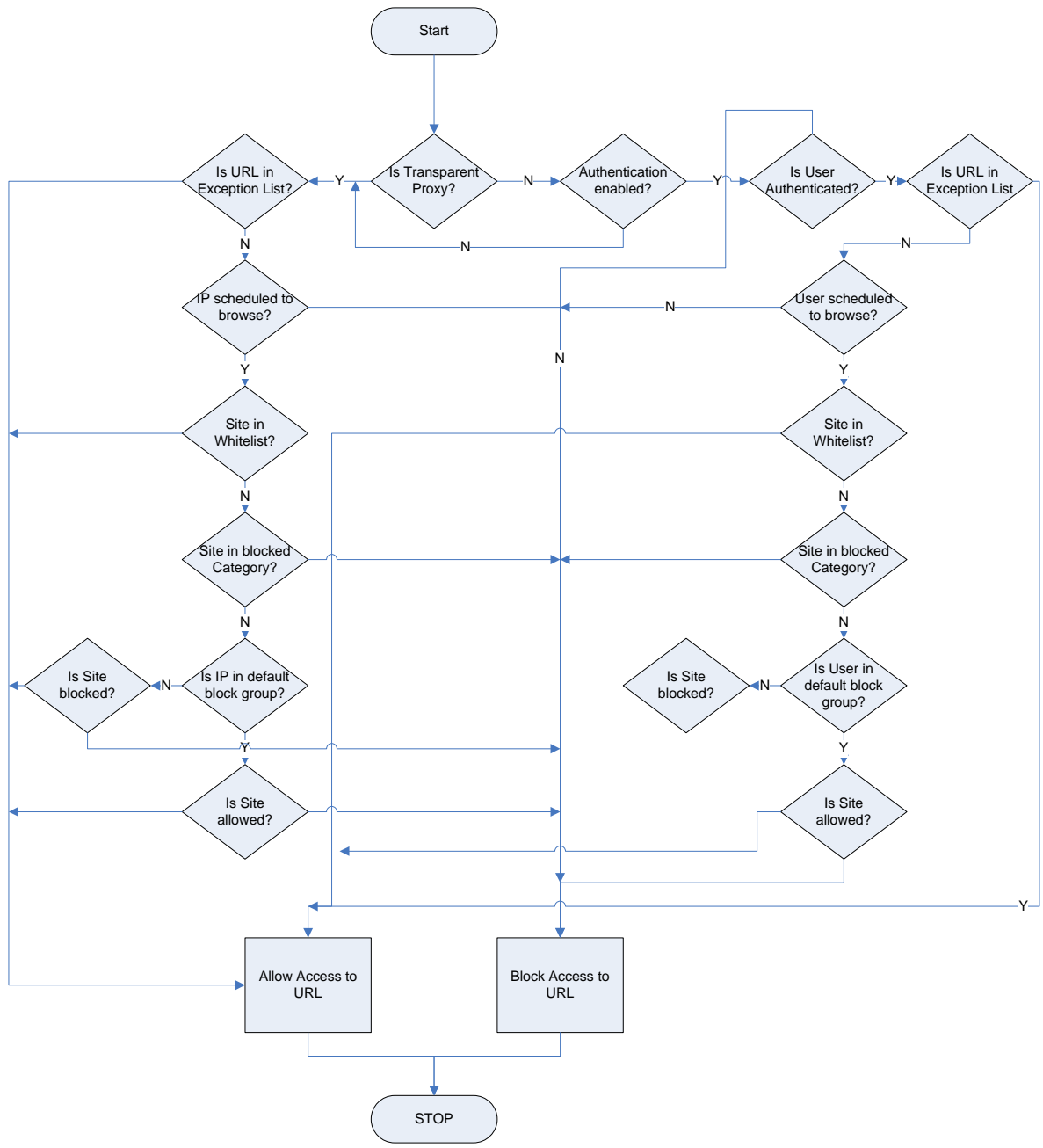
# URL Filtering: Proxy Mode

The screenshot shows a web browser window displaying the GajShield SecureGate v5 administration interface. The browser's address bar shows the URL `https://192.168.2.176/cgi-bin/mainmenuus.ggi`. The interface has a blue header with the title "GajShield SecureGate v5" and "Firewall Management". Below the header, there are tabs for "Browsing Options", "Start Proxy", "Restart ICAP", and "Restart ProxyLog". The "Start Proxy" tab is currently selected. On the left side, there is a vertical navigation menu with categories: NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. Under the BROWSING category, sub-items include Users Setting, Site Policy, MimePolicy, Category, and Setup. The main content area features a "Service Options" section with a blue play button icon on the left and a red stop button icon on the right. The status bar at the bottom of the browser shows "Done" on the left and the IP address "192.168.2.176" on the right. A copyright notice "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" is visible in the footer of the application.

# Proxy Mode: Authentication

- You can enable user authentication for web browsing. Each user will have to first authenticate to the firewall and only then will he be allowed to browse, if he is allowed by the other policies.
- Flow chart





# Proxy mode: User Authentication

The screenshot displays the GajShield SecureGate v5 web-based administration interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenus.ggi". The interface features a navigation menu on the left with options: NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. The main content area is titled "Firewall Management" and includes tabs for Radius, Tacacs Plus, Ldap, and NTLM. The "Ldap" tab is active, showing a form titled "Add Ldap User Settings". The form contains the following fields:

Add Ldap User Settings	
Name	<input type="text"/>
Server IP	<input type="text"/>
Server Port	389
Distinguished Name	<input type="text"/>
Login Attribute	<input type="text"/>
BindDN	<input type="text"/>
Password	<input type="text"/>
Scope	<input type="text"/>

Below the form is an "Add" button. The footer of the interface contains the text "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and the IP address "192.168.2.176".

# Proxy mode: User Authentication

The screenshot shows the GajShield SecureGate v5 web interface in Mozilla Firefox. The browser title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenus.cgi". The interface has a blue header with the title "GajShield SecureGate v5" and "Firewall Management" tabs for "Radius", "Tacacs Plus", "Ldap", and "NTLM". A left sidebar contains menu items: NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. The main content area displays the "Add Ldap User Settings" form with the following fields:

Add Ldap User Settings	
Name	localldap
Server IP	192.168.2.3
Server Port	389
Distinguished Name	o=ldapdb
Login Attribute	uid
BindDN	cn=manager, o=ldapdb
Password	*****
Scope	

Below the form is an "Add" button. The footer of the interface contains the text "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and the IP address "192.168.2.176".

# User Policies

- If you have configured URL filtering in transparent mode or selected 'No User Authentication' in proxy setup, all user policies will be imposed on IP address from where the user is browsing
- If you have selected 'User Authentication' and configured the selected database, all policies will be implemented on login ids or usernames

# User Policies: Creating Users

- Create users on the firewall
  - Click on 'Browsing' -> 'User Settings' -> Users to add users in the database
    - Note: Even if you have selected an external database, like LDAP or Radius, you will still need to add users here.
    - Note: If you have selected transparent mode or no user authentication, then you will need to add IP's as users

# User Policies: Creating Users



















The screenshot shows a web browser window with the title "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar displays "https://192.168.2.176/cgi-bin/mainmenuus.ggi". The main content area is titled "GajShield SecureGate v5 Firewall Management" and has two tabs: "Users" and "User Groups". A left-hand navigation menu includes options like NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. Under "BROWSING", "Users Setting" is selected. The main area contains an "Add Users" form with the following fields:

Add Users	
Login ID	<input type="text"/>
Password	<input type="password"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>

Below the form is an "Add" button. The footer of the page contains the text "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and the IP address "192.168.2.176".

# User Policies: User List

The screenshot displays the GajShield SecureGate v5 Firewall Management interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenuus.ggi". The interface features a navigation menu on the left with options like NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. The main content area is titled "Users" and contains a table of user entries. Each entry includes a Login ID, First Name, Last Name, and a Tasks column with icons for adding, editing, and deleting users. A link "Add from CSV File" is visible at the bottom of the table.

Login ID	First Name	Last Name	Tasks
administrator	administrator	administrator	  
dinesh	dinesh	dinesh	  
guest	guest	guest	  
krbtgt	krbtgt	krbtgt	  
support_388945a0	support_388945a0	support_388945a0	  
vimal	vimal	vimal	  

[Add from CSV File](#)

Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved

Done 192.168.2.176

# User Policies: User Groups

The screenshot displays the GajShield SecureGate v5 Firewall Management web interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenu.ggi". The interface features a navigation menu on the left with options like NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. The main content area is titled "Firewall Management" and has tabs for "Users" and "User Groups". The "User Groups" tab is active, showing a dialog box titled "Add User Group".

The "Add User Group" dialog box contains the following fields and controls:

- Group:** A text input field.
- Available Users:** A list box containing "administrator", "dinesh", "guest", "krbtgt", "support\_388945a0", and "vimal".
- Selected Users:** An empty list box.
- Navigation:** ">" and "<" buttons between the user lists.
- Site Policy:** A dropdown menu set to "Default Allow".
- Mime Policy:** A dropdown menu set to "Default Allow".
- Maximum Download Size (KB):** A text input field with the value "0".
- Buttons:** An "Add" button at the bottom.

At the bottom of the interface, there is a copyright notice: "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved." and a status bar showing "Done" and the IP address "192.168.2.176".



# User Policies: Category Policy

The screenshot displays the GajShield SecureGate v5 Firewall Management web interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenuus.ggi". The interface features a navigation menu on the left with categories like NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. The main content area is titled "Firewall Management" and includes tabs for "Block Category", "White List", and "Trusted Domain". A "Blocked Category Options" dialog box is open, containing a "Select the Group" dropdown menu with "vimalgroup" selected and a "Blocked" button. The footer of the interface includes the copyright notice "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and the IP address "192.168.2.176".

# User Policies: Category Policy

The screenshot displays the GajShield SecureGate v5 Firewall Management web interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenus.cgi". The interface has a blue header with the product name and navigation icons. A left sidebar contains a menu with categories like NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. The "BROWSING" category is expanded, showing sub-items: Users Setting, Site Policy, MimePolicy, Category, and Setup. The main content area is titled "Firewall Management" and has three tabs: "Block Category", "White List", and "Trusted Domain". The "Block Category" tab is active, showing a configuration window for a group named "vimalgroup". This window has two columns: "Available Category" and "Blocked Category". The "Available Category" list includes Aggressive, ArmsWeapon, Audio-Video, Banking, ChildCare, Clothing, Cooking, Dating, Dialers, and Drugs. The "Blocked Category" list includes Ads, ArtNudes, CellPhones, and Chat. There are right-pointing and left-pointing arrow buttons between the lists, and a "Modify" button at the bottom.

Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved

Done 192.168.2.176

# User Policies: Mime Policy

The screenshot displays the GajShield SecureGate v5 Firewall Management web interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenuus.ggi". The interface features a navigation menu on the left with categories like NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. The main content area is titled "Firewall Management" and has two tabs: "Mimetype Block" (selected) and "Mimetype Allow". A "Mimetype Block Settings" dialog box is open, containing a "Select the Group" label, a dropdown menu with "vimalgroup" selected, and a "Show" button. The footer of the interface includes the copyright notice "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and the IP address "192.168.2.176".

# User Policies: Mime Policy

The screenshot shows the GajShield SecureGate v5 Firewall Management interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenuus.ggi". The interface has a blue header with the GajShield logo and the text "GajShield SecureGate v5". Below the header, there are two tabs: "Mimetype Block" and "Mimetype Allow". The "Mimetype Allow" tab is active. On the left side, there is a navigation menu with the following items: NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING (with sub-items: Users Setting, Site Policy, MimePolicy, Category, Setup), TRAFFIC CHART, IPS, and LOGOUT. The main content area shows a table with two columns: "Mimetype" and "Select Options". The "Mimetype" column contains the text "Mimetype Name". The "Select Options" column contains a dropdown menu with the selected value "application/andrew-inset (ez)". Below the table is an "Add" button. At the bottom of the interface, there is a copyright notice: "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved". The status bar at the bottom left shows "Done" and the bottom right shows the IP address "192.168.2.176".

GajShield SecureGate v5  
Firewall Management

Mimetype Block    Mimetype Allow

Mimetype	Select Options
Mimetype Name	application/andrew-inset (ez)

Add

Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved

Done    192.168.2.176

# User Policies: Site Policy

The screenshot displays the GajShield SecureGate v5 web-based administration interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenuus.ggi". The interface features a navigation menu on the left with categories like NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. The main content area is titled "Firewall Management" and includes tabs for "Site Block", "Site Allow", "Schedule", "Exception Sites", and "User To Ip". The "Site Block" tab is active, showing a "Blocked Sites Options" section with a dropdown menu labeled "Select the Group" set to "vimalgroup" and a "Show" button. The footer contains the copyright notice "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and the IP address "192.168.2.176".

# User Policies: Site Policy

The screenshot displays the GajShield SecureGate v5 web-based administration interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenuus.ggi". The interface features a navigation menu on the left with categories like NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. Under BROWSING, "Users Setting" is expanded to show "Site Policy", "MimePolicy", "Category", and "Setup". The main content area is titled "Firewall Management" and has tabs for "Site Block", "Site Allow", "Schedule", "Exception Sites", and "User To Ip". The "Site Block" tab is active, showing a form to add a blocksite. The form includes a "Blocksite Name" label, a text input field containing "gajshield.com", and an "Add" button. A copyright notice at the bottom reads "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved". The status bar at the bottom shows "Done" and the IP address "192.168.2.176".

# User Policies: Schedule

The screenshot displays the GajShield SecureGate v5 Firewall Management web interface. The browser window title is "Gajshield: Web based Administration and Management Tool - Mozilla Firefox". The address bar shows the URL "https://192.168.2.176/cgi-bin/mainmenuus.ggi". The interface features a navigation menu on the left with categories like NETWORK, FIREWALL, USERS, VPN, SYSTEM, ADMIN, REPORT, BROWSING, TRAFFIC CHART, IPS, and LOGOUT. The main content area is titled "Firewall Management" and includes tabs for "Site Block", "Site Allow", "Schedule", "Exception Sites", and "User To Ip". The "Schedule" tab is active, showing a form for adding a blocksite. The form has a "Blocksite Name" label and a text input field containing "gajshield.com". An "Add" button is positioned below the input field. The footer of the interface contains the text "Copyright © GajShield Infotech (I) Pvt. Ltd. All rights reserved" and the IP address "192.168.2.176".

# URL Filtering: Exercise

- Configure the GajShield UPTM in proxy mode. Run the proxy on 8080 port and enable local user authentication in it.
- Create the following users
  - Username=abc,Password=take1234,Firstname=AB,Lastname=C
  - Username=xyz,Password=take1234,Firstname=XY,Lastname=Z
  - Username=qwert,Password=take1234,Firstname=QW,Lastname=ERT



# URL Filtering: Exercise

- Configure groups as follows
  - Sales with the following users abc,qwert with default site policy as 'Default Allow' and Mime policy as 'Default Block' and no download restrictions
  - BO with xyz with default site policy as 'Default Block' and Mime policy as 'Default Allow' and a restriction of download of 10MB
- Block the following categories for Sales
  - ArmsWeapon
  - ArtNudes
  - Chat

# URL Filtering: Exercise

- Allow the following mime types for Sales
  - application/x-dosexec (exe)
  - application/pdf
- Block the following URLs for Sales
  - rediffmail.com
  - hotmail.com
- Allow BO to browse only between 9 am to 6 pm