

## Pre-Installation Requirements

Before going to site to install a CachePilot there are a number of items to be sorted out in terms of information, access and personnel.

A number of items which make CachePilot easy to install/test/demo in a lab environment may need re-thought in a real school environment.

CachePilot is typically installed in an existing environment with which will comprise a minimum of an external firewall and perhaps a proxy server in the LEA/Service provider infrastructure, and potentially a DNS and DHCP server on the local school's LAN.

Prior to installing the CachePilot ensure the following items are resolved by someone suitably qualified – many of these items will not be the province of the CachePilot installer. Ensure these issues have been discussed before attending site or you may have a wasted journey !

Some disruption may occur when reconfiguring various elements of the network. Out of prime hours installation may be preferable.

- Required information for CachePilot
  - In which mode is the CachePilot to be used ?
    - (a) **Using External Router/Gateway'** configuration. In this mode a separate device such as a Cisco router acts as the Gateway.
    - (b) **Integrated Router/Gateway'** configuration where the CachePilot is acting as the gateway and caching device (and firewall).
  - IP Address and mask of Gateway.
  - IP address and mask for CachePilot. Needs to be on same subnet as the external Firewall/Gateway (if being used)
  - IP Address of the DNS server if CachePilot is not to act as that device.
  - Forward Proxy information if required.
  - ISP Email information (to email logs and Backup). This would include setting suitable domain name for unit to trace email source.
  - Is CachePilot to act as the DHCP server ? - Enable/Disable accordingly.

- Choices are available in terms of how CachePilot is configured e.g.:
  - Do wish to enable URL content filtering ?
    - N2H2 or NetSweeper
  - If N2H2
    - What Authentication ?
    - What categories do you wish to block ?
  - What is the N2H2/NetSweeper Server IP Address/Name and Port Number
- What Content Provider information should be pre-loaded ?
  
- The External Firewall will need to be modified to :
  - Allow Port 4000 outbound for N2H2 lookups
  - Allow CachePilot outbound access with HTTP (TCP 80), HTTPS (TCP 443) and DNS.
  - Allow inbound access to CachePilot using HTTPS (TCP 443) and SSH (TCP 22).
  - Disallow direct access from PCs to the Firewall (otherwise users will bypass N2H2 filtering)
  - Note the CachePilot uses out of hours access to update system software, and will poll out during all periods to see if software and virus updates are available.
  
- PC Client Browser Configuration
  - All PC browsers using CachePilot for N2H2 content control will need to be modified by pointing at the CachePilot as a proxy on port 8000 (if N2H2 authentication is required).
  - Browsers can be modified one at a time, so users can be moved over to the new service without too much disruption, but they will take some time/planning.