Managing your schools web filtering with E2BN Protex Local

Contents:

1 What is E2BN Protex?

In an ideal world, our children would be able to surf the Internet without fear of discovering inappropriate material, being preyed upon by paedophiles, ripped off by con artists or ‘radicalised' by political extremists.

Sadly that is not the way of the world; the practise of filtering Internet access in school seems to be with us to stay so it's vitally important that schools choose the right system.

A school has many users with different web access requirements which a filtering system must cater for. First and foremost the filter must protect the school's youngest and most vulnerable members yet at the same time it should not unnecessarily restrict legitimate access by older students and staff.

Where some filtering products employ a “one-size fits all” approach, E2BN Protex Local comes with a range of 16 pre-configured age-appropriate 'profiles' covering Primary, Middle and Secondary students, Sixth form and Staff.

In a typical secondary school using E2BN Protex, members of staff can access all YouTube videos, while students, by default, cannot. An 'A' Level Ethics student would have access to sites about vivisection, abolition and other sensitive issues but younger students would be blocked from such material.

E2BN Protex Local filtering can be adjusted even on a per-user basis, very simply via web menus, with all changes having immediate effect.

Many filtering products protect users by simply adding sites to a blacklist; sites and URLs which are not blacklisted pass through the filter regardless of the content. This can result in either a heavy-handed over-blocking or a too-relaxed filtering policy. E2BN Protex is more flexible and more effective because it employs dynamic content checking.

While E2BN Protex does use blacklists, **Protex also examines page content**, hunting out and evaluating words and phrases from a very extensive list of suspect terms. Even when sites are unlisted, users are still protected from receiving unsuitable content.

E2BN Protex also adds a number of other protective features to student filtering such as VerySafeSearch, file type checking, and image search filtering.

The following pages are aimed at providing you with an understanding of how E2BN Protex works in practice.

2 Understanding E2BN Protex Profiles and Categories

Every time a user's device sends a website request to the Internet via E2BN Protex, a filtering profile is applied and the request is either accepted or denied based on the policies associated with that profile.

As inferred above, a profile is a set of policies that include:

- Enabled **Features** such as IP blanket block, Image filtering, YouTube for Schools, Safe Search, untrusted SSL block
- Blocked/allowed **Filtering Categories**
- Blocked/allowed **file types**
- Content-check threshold score or "**Naughtiness limit**"

Your Protex Local system is configured "out of the box" with sixteen standard E2BN profiles. It is worthwhile understanding which policy items apply to the profiles you have in use. For example "online games" is a blocked category on the E2BN Primary, Middle, and Secondary profiles only; it is not blocked on the other profiles.

You can view the profiles and compare the configuration of each via the E2BN Protex system administration menus. The table below provides a quick overview of the standard profile names and the level of filtering provided by each.

E2BN Profile	**Summary of Profile**
Banned	no internet access
Primary	School students 4-8 years
Middle	School students 9-11 years
Secondary	School Students 12-15 years
Sixth Form	School Students 16-17 years – allows games and social networking
Walled Garden profiles	School students – Trusted (whitelist) URLs and search terms only
With Games profiles	Allows "online games" sites in addition
Staff	For teachers and school staff
Library (public Libraries)	As staff but higher content-check limit
CLibrary (public Libraries)	Similar to Middle School but for Children's Librarys.

2.1 Filtering Categories

Categories provide a way of assigning blocked/allowed URLs and Search Terms so that they apply only to a particular profile or profiles. For example assigning a blocked URL to the "online games" category means that the site will only be blocked on the E2BN:Primary, E2BN:Middle and E2BN:Secondary profiles. As mentioned above, it is important therefore to understand which categories apply to each profile in use.

Here is a summary of the pre-configured categories and to which Profiles they are applied:

Block Categories	**Applied on the following E2BN Profiles**
Adult	All student profiles & Childrens Library
Adverts	Primary, Middle, Secondary and C'Library
Chat	All student profiles and C'Library
Gambling	All student profiles and C'Library
Filehosting	Primary, Middle, Secondary and C'Library
Illegal Hacking*	ALL Profiles
Illegal Drugs*	ALL Profiles
Intolerance	All student profiles & Childrens Library
KidsTimewasting	All student profiles
OnlineGames	All student profiles excluding "with games" variants
Proxy*	ALL Profiles
Pornography*	ALL Profiles
Social Networking	Primary, Middle, Secondary & C'Library
Violence	ALL Profiles
VirusInfected	ALL Profiles
LocalBlockAll	ALL Profiles
Age Specific Block Categories	**Applied on the following E2BN Profiles including "with games" variants**
Pre-9 Block	Primary,
Pre-12 Block	Primary,Middle, C'Library
Pre-16 Block	Primary,Middle,Secondary,C'Library
Pre-18 Block	Primary,Middle,Secondary,SixthForm, C'Library

Allow Categories	**Applied on**
Adult	**Staff,Library**
ArtNudes	**All**
ChildCare	**All**
Culinary	**All**
Download	**All**
Gardening	**All**
Government	**All**
HomeRepair	**All**
Hygiene	**All**
News	**All**
Radio	**All**
Teaching	**All**
Age Specific Allow Cat's	**Applied on**
Post-9 Allow	**Middle school and upwards**
Post-12 Allow	**Secondary school and upwards**
Post-16 Allow	**Sixth Form and upwards**

3 Assigning Profiles to users

This section describes options for configuring E2BN Protex so that users get the differentiated filtering level that is most appropriate to them. The online documentation describes in detail the actual configuration steps.

http://protex.e2bn.org/ - documentation tab

We recommend that you run either the Port-Based or User-Authentication method but not both. You can use the Location method alongside either of these if you wish.

3.1 Port Based Profile Assignment

The E2BN Protex Web administration menus allow tcp ports 8080 to 8089 to be mapped to E2BN filtering profiles. Users' internet browser settings should be configured to point to the E2BN Protex server on the relevant port. This option allows up to ten different profiles to be mapped.

3.2 Location Based Profile Assignment

In some situations it is more convenient to assign a particular profile to a group of computers – for example, in the Library or Staff room or maybe a "guest" wireless network. You can create locations or groups of computers by specifying their IP addresses. Once the locations have been created a filter profile can be allocated to each of them. Location based profile assignments take precedence over any other method.

3.3 User-Authentication Profile Assignment

E2BN Protex can be easily integrated with a school NTLM / Active Directory system. When a user begins browsing, Protex assigns a filtering profile by checking which user group that they belong to.

There are a number of advantages to this method.

- Map many AD groups to filtering profiles – by comparison port-based is restricted to ten.
- Single TCP proxy port (Authorisation port) applies to all browsers regardless of user type
- Enables an Acceptable Use Policy page to be displayed before users can browse
- Enables the use of timebands – filtering profiles can be automatically scheduled to change depending on time of day
- Easily implement a "sin bin" policy – allows users to be added temporarily to an AD group mapped to a more restrictive profile. If configured correctly E2BN Protex will prioritise the restricted profile over the user's normal profile.
- Proxy switcher for staff - allows teachers to test student profiles "on the fly"
- Default profile - in the event of a user without an AD membership or if the AD server fails for any reason, a default profile is available.

The E2BN Protex online documentation gives full details on how to configure all of the various methods for assigning profiles to users.

4 Active Directory Integration – related features

The following are some of the main features that can be enabled when you use User-Authentication profile assignment via NTLM/Active Directory integration on your E2BN Protex Local system. Please read the online documentation for detailed menu steps.

4.1 Time Banding

Time Bands enable you to assign a filtering profile to users depending on time of day. As an example let's say you want to allow students to access online games at lunch time only.

- Set up a timeband called "Lunch" – enter the start and finish times and days of the week it will apply.
- In the profile assignment menus, find the relevant AD group(s) that you want to allow games for. You will see the "default" profile for that AD group already mapped. If you have not already set up a mapping then do this first.
- Now click the Set Timebands button
- You'll see the default profile for the AD group listed already. Click "Add line" and select the timeband "Lunch" from the drop down and then select the "with games" variant of the profile you want to use. Save your changes.

4.2 "Sin Bin" Policy

If a user is a member of more than one AD group E2BN Protex will apply the filtering profile that is highest in the list of mapped AD groups. If you wish to set up a "Sin Bin" policy that restricts internet access temporarily as disciplinary action then do the following.

- In your AD system define a "sin bin" AD group
- In E2BN Protex, map this AD group to a restricted profile. This could be for example the E2BN:Banned or maybe E2BN:Primary_Walled_Garden or a local profile that you have created that limits users to specific categories or web sites.
- Make sure this profile is uppermost in the list of mappings. Use the Up/Down buttons to do this
- When you want to implement the policy for a user, simply add them as a member of the "sin bin" group in your AD system. As far as AD is concerned they can remain a member of their normal AD group in addition to their temporary group membership. E2BN Protex will apply the restrictive profile because the mapping for the "sin bin" group has priority.

4.3 Profile Switcher

E2BN Protex provides differentiated filtering to allow staff to get on with their online activities more or less unhampered while students get a more protected environment. Sometimes this means that staff prepare a lesson only to find that students are getting a block page when trying to access the lesson resources online.

The Profile Switcher feature enables staff to login as normal but then change their filtering profile on a temporary basis using a web drop-down menu.

To turn this feature on for an Active Directory Group [usually staff group(s)] access the profile assignment menus and tick the Override box next to the AD group profile mapping – save changes.

To access the feature the user must locate the small E2BN Protex Login Status web page within their browser. There will be a drop down menu embedded in this status page, listing the available profiles. The user selects the profile they wish to test. They can then quickly switch back to their normal profile.

5 HTTPS Content Inspection – new in version 4.0 and 4.0r

In Protex version 3.x and prior, content inspection of HTTPS/SSL traffic did not take place. Protex could only filter based on the URL of the request and even then only on the (sub) domain and not the complete URL. This limitation led us to introduce a default (blanket) block on untrusted domains and urls when requested over SSL via student profiles. (See 8.1)

In version 4.0 Protex has the capability to do full URL and content checking for both http **and** https traffic.

5.1 E2BN Root CA Browser Certificate – Important

If you are about to purchase E2BN Protex Local or you are upgrading from v3.x to 4.x you will need to install the E2BN Protex Root CA certificate onto every device that will access the internet via the filtering system.

See http://protex.e2bn.org/certs for details. You **must do this** before installing a new system or when upgrading otherwise users will get browser certificate warnings every time they go to use an https site. We can provide support should you run into problems or unexpected issues with this procedure.

5.2 Default offering – Google Search SSL inspection

By default all new Protex systems carry a restricted version of the new software called 4.0r which enables SSL content checking for Google Search only. This is a direct response to Google removing their old “no-ssl” search facility. In 4.0r, all other untrusted SSL traffic for students is subject to the blanket block policy.

5.3 Optional offering – Full SSL content inspection

Protex Local customers will have the option (additional payment required) to carry out a further upgrade from the base offering and this will enable SSL content inspection and full URL analysis of ALL https traffic. When completed this will also turn off the blanket SSL block feature for students.

6 Making List Changes

Here are some basic principles to understand before you begin making filtering changes.

6.1 Global and Local Lists

When you first download your Protex Local software your staff and students are protected immediately they start using the internet. This is because the software is already configured with the latest "global" filtering lists.

E2BN Protex is a "community" system. There is a master management server that holds and distributes a standard set of "global" filtering lists to all subscribing Protex systems in schools and Local Authorities. You will notice that in the system they are actually called **Blacklists or RBC lists or Regional Lists.** They are called regional lists because the original system was intended for use only by schools in the East of England. These global lists are distributed to all ProtexLocal systems as central updates occur. Delta changes are sent every 15 minutes during the day and there is a complete download overnight.

The main concept and feature of Protex Local is that your school can tailor the standard filtering to suit your own circumstances and preferences. The first time you make a **list change** on your ProtexLocal system you are in fact creating "local" lists. These **local lists take precedence over the global lists**.

So if you want to allow "faceblog.com" for students or block "e-buy.com" for staff then you can, without affecting any other schools. The web admin menus allow you to add a block/allow entry and if you want to undo this you can simply remove the change. You can also use the logging menus to keep track of all list changes made on your system.

All the list changes that you make require a "soft" restart of Protex – this does not affect service but simply loads the new local lists and puts your changes into effect immediately.

6.1.1 Audit Trail

All list changes that are made on your Protex Local system are logged locally and also sent to the E2BN central management server database. The log shows the date, time, username, IP address and the change that was made. E2BN staff review these logs daily. If we see a list change that may benefit the whole community e.g. you block a new online games site then we can "adopt" your change and add it to the "global" lists.

6.2 Content check and Trusted – what do they mean?

Whenever you make a list change to allow a URL there is the option of making it Content-Check or Trusted. Trusted means that you trust the site completely and no filtering of any sort will take place; E2BN Protex will not inspect the page contents and it won't apply the file type checks.

Content-check means that you want to unblock a banned URL but E2BN Protex will still inspect the page contents and apply the file type checks associated with the user's profile.

As a general rule its good practice to use Content-Check when allowing a URL unless you need to overcome an "overblocking" issue; or add a https site – See below under **SSL Blanket block**.

Overblocking can be said to occur when the E2BN content-check features prevent the user from accessing a bona-fide URL due to "phrase limits" or where the user needs to download a "forbidden" file type from a bona-fide site. In that case then the URL/site would need to be added as Trusted in order to overcome the content-check blocking.

6.2.1 Emergency Categories – handle with care*

E2BN Protex has some special "emergency" filtering categories. When anybody makes a change in these categories that change is **automatically rolled out to ALL E2BN Protex systems within 15 minutes**. The idea behind this is that if for example one school discovers and then blocks a pornographic site this should be blocked on all systems as soon as possible. By automating the process, students and staff on all E2BN Protex systems are protected quickly without the need for further human intervention.

Consequently, care should be taken when adding sites in the following categories:

- Pornography
- Proxy (anonymous proxy sites)
- Illegal Drugs
- Illegal Hacking

It should be noted that these block categories apply to all profiles. When creating a **Local Profile** they cannot be turned off.

If a school wishes to block a site or search term to all users, the **Local Block All** category should be used instead UNLESS the site falls into one of above the emergency categories.

6.2.2 Age related categories

A URL or search term may not necessarily fall into a particular "type" category but may be particularly suited only for certain age-group(s). There are pre-configured age-specific categories. These are useful where a school may have a wide age range of students utilising for example the Middle School, Secondary and Sixth Form profiles. Example:

> You want to allow a blocked tabloid newspaper site for the Sixth Form only.
>
> Add the site to the Post-16 allow category.

6.2.3 Special Categories

The **Local Block All** category is applied to all E2BN standard profiles. It allows you to add an item outside of the 4 "emergency" categories that will be blocked to all users including staff. For example: your school wishes to bar "e-buy.com" to all staff. The site is not pornography,

proxy, illegal drugs or illegal hacking. Add the site using the LocalBlockAll category and "e-buy.com" will be blocked on all of the E2BN:Profiles.

Per-Local-Profile Category – this is a block/allow category that is automatically generated and applied individually to each local profile that you create. It allows you to have very bespoke filtering for special groups of users. See examples below under **Local Profiles.**

7 Local Profiles

The provision of 16 standard E2BN Profiles combined with the ability to change the filtering lists to suit local circumstances is more than adequate for most schools.

However it is not possible to carry out a wholesale switch on/off of the various policy items within a standard profile. For example it is not possible to switch off the block on all Chat sites within the pre-configured E2BN student profiles.

In order to give complete flexibility E2BN Protex allows schools to create their own profiles.

The Local Profiles feature allows you to make a copy of any of the standard E2BN profiles then edit and save as a Local Profile.

Here's an example of where you would need to use a Local Profile:

> A school is using the E2BN:Staff profile for all staff and teachers because it's the most appropriate out of the 16 available. You are asked to block all Social Networking and Chat sites for school admin staff only. In this case you can create a local profile based on the E2BN:Staff profile and edit the applied categories. Tick the Chat and Social Networking Block categories then save your local profile as myschool:admin. Next make sure you change the profile assignment mappings to point your admin staff browsers at the myschool:admin local profile.

Another example:

> The Network Manager wants to restrict most staff from downloading zip files and other files that sometimes cause problems; but he/she still wants the IT Team to be able to download pretty much anything. The E2BN Protex administrator can create a local profile based on E2BN:Staff and switch off any file type that is not required. All staff except the IT team would browse via the restricted local profile.

Local profiles also allow you to block or allow specific URLs and search terms for "exception" sets of users. Each local profile automatically get's its own unique category:

> An upper school has a three year groups Yr9 to Yr11. All students are browsing via the E2BN:Secondary profile. The Head wants to allow Yr11 only to use a social networking site. If the site is added into any of the standard allowed categories then it would be available to

the whole school. To get around this, create a local profile based on the E2BN:Secondary. It will be called something like myschool:Yr11. Now go to list management and add the site as allowed. In the category drop-down list there will be a myschool:Yr11 "category". Select this and then the site will be allowed only for students who browse via this local profile.

8 Other E2BN Protex filtering features

8.1 Blanket SSL Block for Students

As previously outlined, the content-check feature of E2BN Protex is enforced on all non trusted domains and URLs. Content checking protects users against dubious content even though the site may not be in any blacklist. However, if the site or URL is accessed via the https protocol the content is encrypted and content-check is ineffective. There is a strong argument therefore to actually block requests via https unless the domain is in a trusted list. E2BN Protex Version3 implements this principle on all student profiles.

Unlike normal http traffic, E2BN Protex does not put up a block page when an https block is imposed. The protocol response header will contain a 403 error but depending on the browser the user will see:

- Internet Explore cannot display the page
- The proxy server is refusing connections

Or some similar message

You can check the Protex detailed logs when this type of issue occurs and you should find an entry such as this

```
https://yahoo.com:443
BLOG : *DENIED* Blocked site: HTTPS access is only allowed to trusted sites.
```

If you want to unblock a site that requires https access, use the list management menus to add the domain as a trusted site in the appropriate category.

8.2 YouTube for Schools

E2BN Protex has a built in YouTube for Schools feature that enforces a redirect to YouTube's education site whenever a request to YouTube is made via a student profile. By default a special header code is included in the request that links the request to E2BN's own "channel".

ProtexLocal enables your school to set up its own YouTube for Schools account and insert that header code in place of the default thus providing access to your schools YouTube for Schools "channel". If teachers want their students to access specific YouTube videos that are outside of

the education site then the administrator of you school's YouTube for Schools account can add them into your "channel" and the students will then be able to access them.

If you do not wish to set up your own YouTube for schools account but wish instead to add videos to the E2BN "channel" then please use the list request form at:

http://protex.e2bn.org/listrequest

Be sure to specify the url of the video – it will be something like

http://www.youtube.com/watch?v=hLdKsKep1og

8.2.1 Allowing "normal" YouTube for Students

If you wish to allow the standard YouTube site for any students then you will need to create a Local Profile, turn off the YouTube for schools feature in the profile and then use the list management menus to allow YouTube on that profile. See **Per-Local Profile Categories.**

9 Bring Your Own Device and Mobile Device Configuration

There is a growing trend toward mobile computing, and allowing staff and students to bring their own devices into school.

When "unknown" devices and non-Windows devices need to connect to the internet it can be a challenge as to how to enable them to browse safely with a minimum of hands-on configuration.

Methods available for auto-configuration include Web-Auto-Proxy-Discovery (WPAD) and use of Proxy-Auto-Configuration files or PAC.

E2BN Protex Local has some features that compliment the use of these protocols.

9.1 WPAD/PAC file hosting

WPAD stands for Web Proxy Automatic Discovery. When clients that support WPAD connect to a wireless network or when client browsers are configured to "Automatically Detect Proxy Settings" the client will send out a query for the location of a host on the network called "wpad" and then attempt to download a PAC file called wpad.dat.

This file contains a series of statements that tell the client browser how to behave. Typically it can be used to configure "proxy bypass" settings and to specify which proxy address (es) and port(s) to use.

A variation on this is to use an MDM system to configure the mobile device as to where to find the file. This is useful when WPAD is not supported by the client but the network manager still wishes employ a PAC file for mobile devices.

E2BN Protex Local (Virtual Appliance only) has a **WPAD configuration menu** that provides a wpad.dat (PAC) file store and allows the administrator to configure this file by altering the default text.

9.2 Transparent Proxy (http)

Transparent proxying is a method for intercepting and filtering internet traffic when there is no means of configuring a proxy setting on a device. The typical method used is that the client device is configured to use the filtering device as its "default gateway". The filtering device then listens on the normal internet ports (80/443) and redirects this to an internal filtering port, allowing other traffic from the client to pass through to the internet.

Setting the default gateway on a client device can be achieved via automated network settings that all devices support (DHCP).

E2BN Protex currently supports transparent proxy of http port 80 traffic only.

The filtering device, whether this is a cache box or Protex Local VA must be configured to either block or allow https port 443 traffic to pass straight through unmodified.

9.2.1 Configuring E2BN Protex for Transparent Proxy

The Equiinet TINA Pilot cache supports transparent proxy of http port 80 traffic. This is achieved by defining a filtering port as a service and then port-forwarding port 80 internet requests toward the filtering IP:port. When the client uses the box as its network gateway Port 80 traffic gets redirected via the Protex Local profile associated with the chosen port. The TINA Pilot can be configured to allow or deny other traffic to pass through.

The E2BN Protex VA (Virtual Appliance) can also be configured to act as a transparent proxy for http port 80 traffic. Currently this requires the assistance of free remote support services provided by E2BN.

9.3 Login on demand (LoD)

The E2BN Protex Local Login-on-demand feature requires the use of the User-Authentication Profile assignment method (NTLM/AD integration). By turning on LoD, authentication becomes optional instead of mandatory for users browsing the internet. This facilitates the ability to provide a default level of filtering to "unknown" devices/users whilst allowing optional authentication in order to:

a) Raise the device/user permissions
b) Begin logging by username

9.3.1 Configuring Login on Demand

Use the E2BN Protex Local login options menus to set and save the Login on Demand option.

Using direct configuration, or WPAD/PAC, or transparent proxy, configure/force the client browser to use the E2BN Protex Local authentication tcp port. The browser will automatically receive the level of filtering defined by the Default Profile setting.

When a block page is encountered, the page displayed contains a login button. Clicking on this button enables the user to enter their user credentials in order to obtain the level of filtering set for their user group under Assign Profiles by NTLM menus.

10 Further Information

For further information please see our web site:

http:// protex.e2bn.org

Or contact us at filtering@e2bn.org - 01462 834588