Recommended configurations for schools with Internet4schools / E2BN Broadband and Protex Web filtering

Best Practice for a Safe and Secure network

- Use the web content filtering features that Protex provides
- Assign users and devices to web filtering profiles that are age-appropriate
- Consider the benefits of Authenticated web filtering access.
- Use Group policies and device managers to lock down device configuration and user permissions
- Test your web filtering configurations regularly
- Have an acceptable use policy that everyone understands
- Know what to do and who to contact if a filtering breach happens

Firewall Controls

Where E2BN provides your broadband and web filtering solution, the firewall that sits between the school network and the internet will **not allow unfiltered web access**. The protocols used – http and https (TCP 80 and TCP 443) will be either:

a) Blocked completely
b) Filtered transparently

When schools have our latest Protex Pro Appliance we use **transparent filtering** of web traffic which forces “raw” http and https through the web filter. The default transparent filter is usually set to a profile suitable for students depending on the school lowest age group.

When schools have a different version of Protex the firewall will be set to completely block “raw” http and https traffic; all users/devices will need to have a proxy setting that directs them to a filtering profile appropriate to their age group.

QUIC Protocol

Some Google URLs including Google Search support an alternate web protocol called QUIC. This uses UDP port 80 and 443. When using the Google Chrome browser, QUIC can in certain circumstances bypass E2BN search term checking. Your E2BN managed firewall will be configured to block QUIC protocol. This forces the Chrome browser to drop back to the normal web protocols.

Proxy Setting

Although Protex Pro Appliance provides transparent filtering for un-proxied web access we strongly recommend that explicit proxy settings are deployed as widely as possible.

All school-managed devices and all student devices should be configured with a proxy setting that directs them to a filtering profile **appropriate for their age group**.

The following standard Protex filter profiles are available :

E2BN:Primary	**to age 9**
E2BN:Middle	**to age 12**
E2BN:Secondary	**to age 16**
E2BN:Sixth Form	**to age 18**
E2BN:Staff	**Adults**

The table below shows a brief overview of the standard filtering categories.

Profile	Content Check	Content Block Score	Allowed Categories – for full list see Protex Web site	File type blocking	YouTube Restricted Mode
E2BN:Primary	YES	35	Teaching ,	YES	YES
E2BN:Middle	YES	88	Teaching, Post-9	YES	YES
E2BN:Secondary	YES	100	Teaching, Post-12	YES	YES
E2BN:Sixth Form	YES	240	Teaching, Games, Social Networks, Post-16	YES	YES
E2BN:Staff	YES	300	All categories **EXCEPT** Pornography Anonymous Proxy Malware/Hacking Illegal Drugs	Some	NO

E2BN and/or your managed service provider will be able to advise you regarding proxy configuration. There are a several methods for assigning users/devices to filter profiles

- Explicitly setting a Proxy IP address and port e.g. 10.123.4.5 : 8080 , with the port indicating what profile to use. Typically Primary = 8081 or 8080, Middle = 8082, Secondary 8083, Staff 8084.

- Authenticated access – Protex can be integrated with Active Directory systems to provide per Group profile assignment and logging of usernames - requires use of a single proxy port typically 8080.

- PAC file : Internet4 schools / E2BN can provide and host Proxy Auto Configuration files for staff, student and Active Directory users that will automatically point the browser at the correct ports.

- Location based assignment – Protex can assign a filter profile based on the device IP address.

The main aim should be to ensure that users/devices use a filter profile that is safe for the age group in question.

Content Filtering and why you should use it

"Now what is the message there? The message is that there are no "knowns." There are things we know that we know. There are known unknowns. That is to say there are things that we now know we don't know. But there are also unknown unknowns. There are things we do not know we don't know. So when we do the best we can and we pull all this information together, and we then say well that's basically what we see as the situation, that is really only the known knowns and the known unknowns. And each year, we discover a few more of those unknown unknowns." Donald Rumsfeld -US Defence Secretary 2002

There are billions of web sites and URLs out there on the internet. There are people (and probably Artificial Intelligence "bots") working for companies whose job it is to categorise these sites. It can be appreciated that large numbers of sites remain as "unknowns".

Protex **standard filtering profiles** do the following:

- Block web sites that are categorised as "bad"
- Allow unconditionally sites that are known as "good"
- Checks the contents of web pages on sites that are known but remain "untrusted" (the known unknowns !)
- Check the web content on all other sites – (the unknown unknowns !!)
- Checks words and phrases entered into Google and Bing search engines.

The content-check feature allows users to safely browse the internet without being limited, confined and frustrated by the alternative ; a restricted "walled garden" list of only whitelisted sites.

When Protex performs content checking during internet browsing the resulting page "scores" are compared to the filter profile limit; the page will be blocked if over the limit. This principle applies not only to web sites visited but includes search engines such as Google – hence Protex can check (and block) words and phrases entered into searches.

Content check also includes looking at file types (extensions e.g. .exe .zip) that the browser may try to download and will block those on the banned lists.

Secure-Content Check and Browser Certificates

The majority of web browsing is done over the internet's secure protocol (https); this is designed to provide a secure, encrypted connection between the user and the web site. When content is encrypted, web filter systems can't easily perform content checking. E2BN Protex (and other systems) can de-crypt the secure connections to untrusted web sites and then inspect the un-encrypted content.

Web filter systems that de-crypt secure connections have to re-create the certificate that the web site would normally present to the client device as verification (the green padlock).

The user's device needs to trust the re-created certificate that Protex presents; this is done via a certification "tree" that leads upwards to a Root Certification Authority. To enable this Root Authority path ,**all devices** that use Protex content-check **need to install an E2BN Protex Root CA certificate** available from E2BN's Protex web site **http://protex.e2bn.org/certs**

Your IT technician , network manager or IT support will normally have enabled this across your school prior to going live with Protex filtering .

You can perform a check to see if you have the Root CA installed - go to **ca.e2bn.org**

Turning off Secure-Content Check - use with care

There may be some circumstances in which it is not possible to install the E2BN Root CA Certificate onto a device. This could be:

- "Smart" devices - printers, CCTV cameras, Wi-Fi controllers etc. that require internet access but do not have a secure certificates installer options.

- Guest devices - occasional visitors to school that need/expect to be able to connect to the internet via school wi-fi without having to install anything extra.

If you have E2BN Protex , a special local or "custom" filter profile can be configured that has secure-content check switched off. WARNING - This decreases the effectiveness of web filtering for any users/devices that are using this profile:

- Known Bad sites – still blocked
- Known Good sites – still allowed
- Web activity – still logged
- **Untrusted https sites – ALLOWED unconditionally with NO content checking**
- **Untrusted https sites -NO file type checking.**
- Google Search -not checked by Protex , will still be forced to Google Safe Search
- Inconsistent block page - http sites will show E2BN block page; https sites will show browser error.

E2BN strongly recommends that Protex profiles with content-check switched off are used only as an exception; the E2BN standard profiles should be used as widely as possible.

How to test your web filtering:

Tests of your filtering should be used to determine that:

1. Access to completely unfiltered internet is blocked.
2. Age-appropriate filtering profiles are applied.
3. Protex Content-check is active.

Carry out all three tests regularly and record the results.

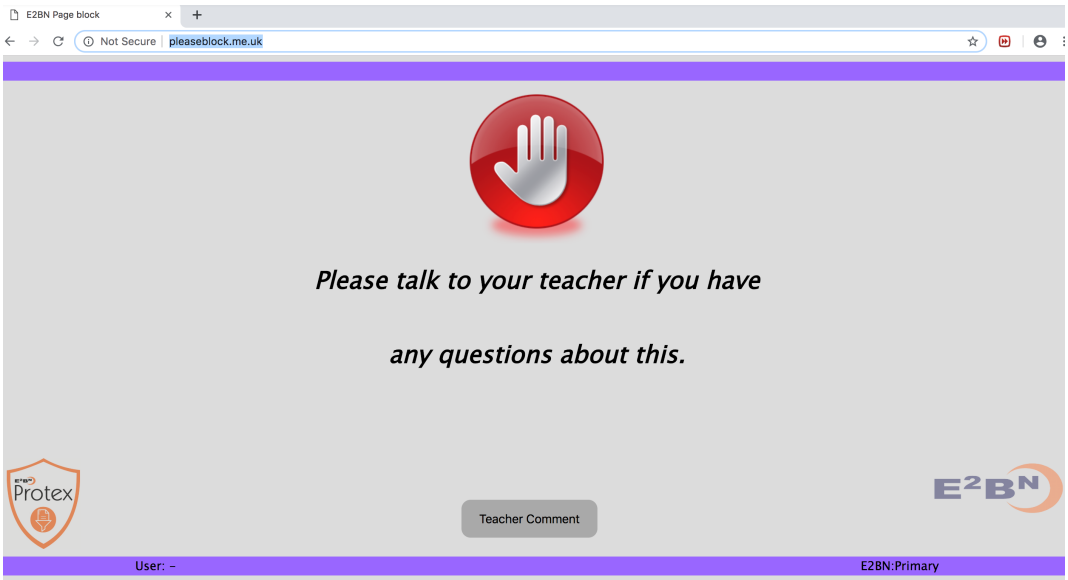
All tests should **PASS**; if they do not or if you are in any doubt please contact E2BN support via 01462 834588 or support@e2bn.org

1. Test - Unfiltered Internet is blocked by E2BN Protex/firewall

Ideally - use a test device that is connected to your main school network and that has its **proxy settings (temporarily) disabled.**

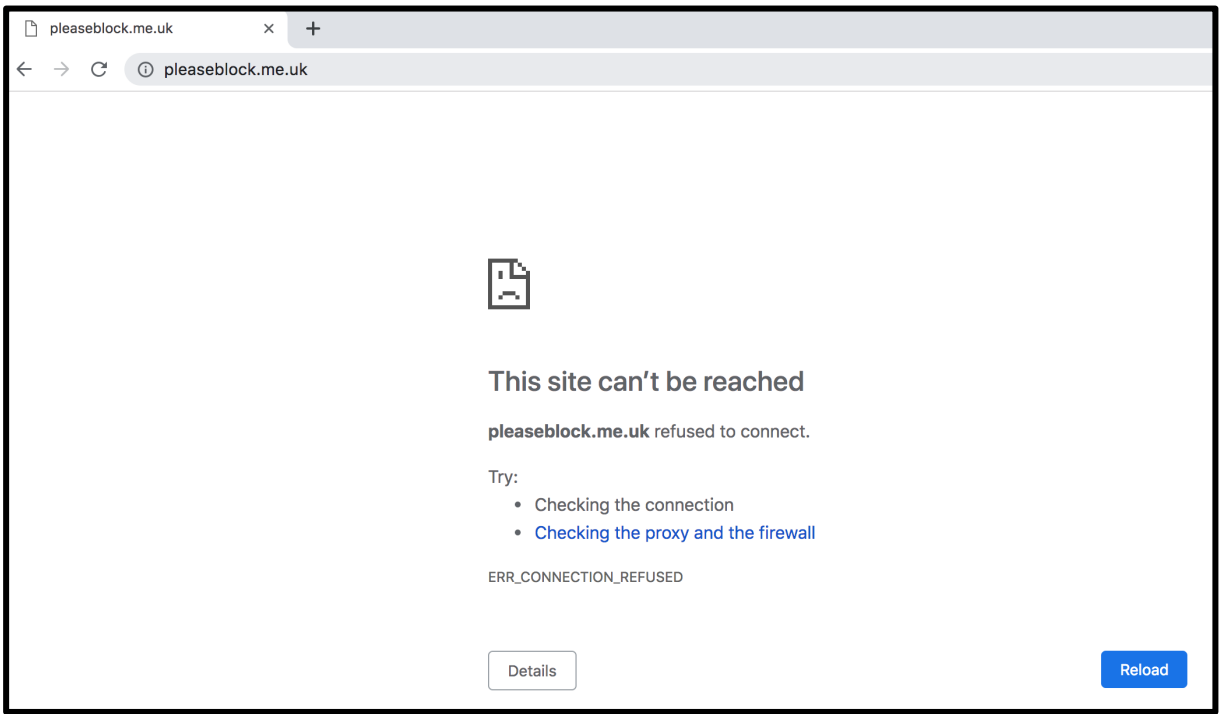
In a browser type this or copy and paste - http://pleaseblock.me.uk into a browser address bar. Press enter.

This is a real web domain owned by E2BN and is used for testing. Where your school has Protex Pro V5 you should get an E2BN Protex transparent filtering **block** page and this test has therefore **PASSED.**

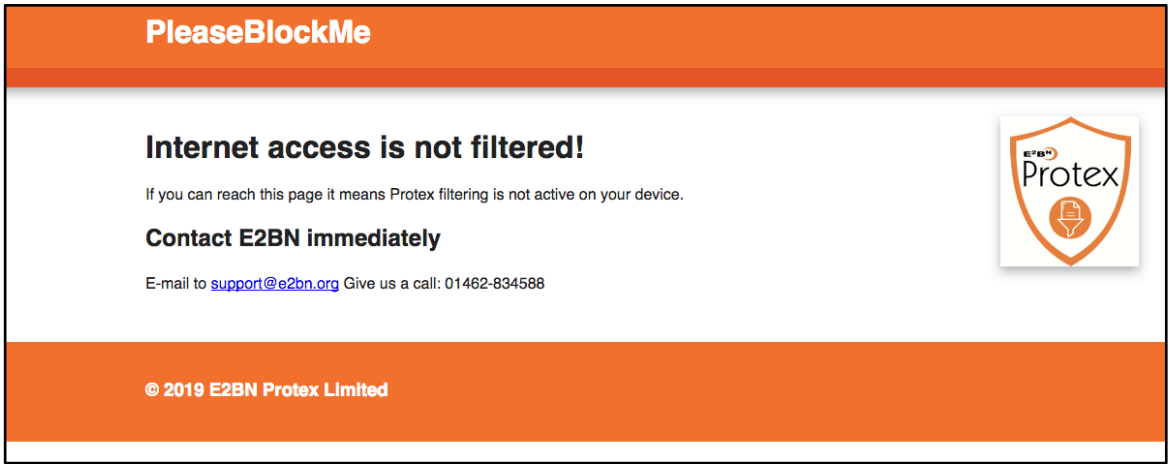


Where your school uses a different Protex version you may get a browser error when proxy settings are

disabled. **Test PASSED**



If you **do not get a block page** or **browser error** and instead get through to the domain web site as below - you should see a warning that your **Internet Access is Unfiltered**.



Test has **FAILED - please contact E2BN immediately.**

2. **Test - Age appropriate Protex filtering profiles are applied across the school.**

   Carry out the following test on a range of fixed and mobile devices using different network logins e.g. student and staff.

In a browser type this or copy and paste - http://pleaseblock.me.uk into a browser address bar. Press enter.

This domain is owned by E2BN. You should get an E2BN Protex **block** page. There will be a banner on the page that tells you which filter profile is in use. Standard profile names commence with " **E2BN:** " . Local or "custom" profiles commence with a three-letter or four-letter local site code.

If the profile name matches the age-group that you are testing for (see table above under **Proxy Setting**) the test has **PASSED.** If the profile name does not match the age group you are testing for or if you are unsure, please contact E2BN Protex for advice.

3. **Test - Protex filtering content-check is active**

Carry out the following test on a **range** of fixed and mobile devices using different network logins e.g. student and staff.

In a browser type the *exact phrase below* or copy and paste into a search engine e.g. Google or Bing.

e2bn content blocking test protex

If content-check is active you should get a **Protex block page** tailored to the profile that is in use. The test has **PASSED**

If you **do not get a block page** the test has **FAILED.** This could be due to one of the following.

- **Content check is not active on that Protex filter profile**
- **Internet access is completely unfiltered.**

To determine which of the above causes is true - carry out TEST 2 above; if you get a block page make a note of the profile name and contact E2BN support for advice. If you do not get a block page something else is wrong. **Contact E2BN support for advice.**