WEB POLICY

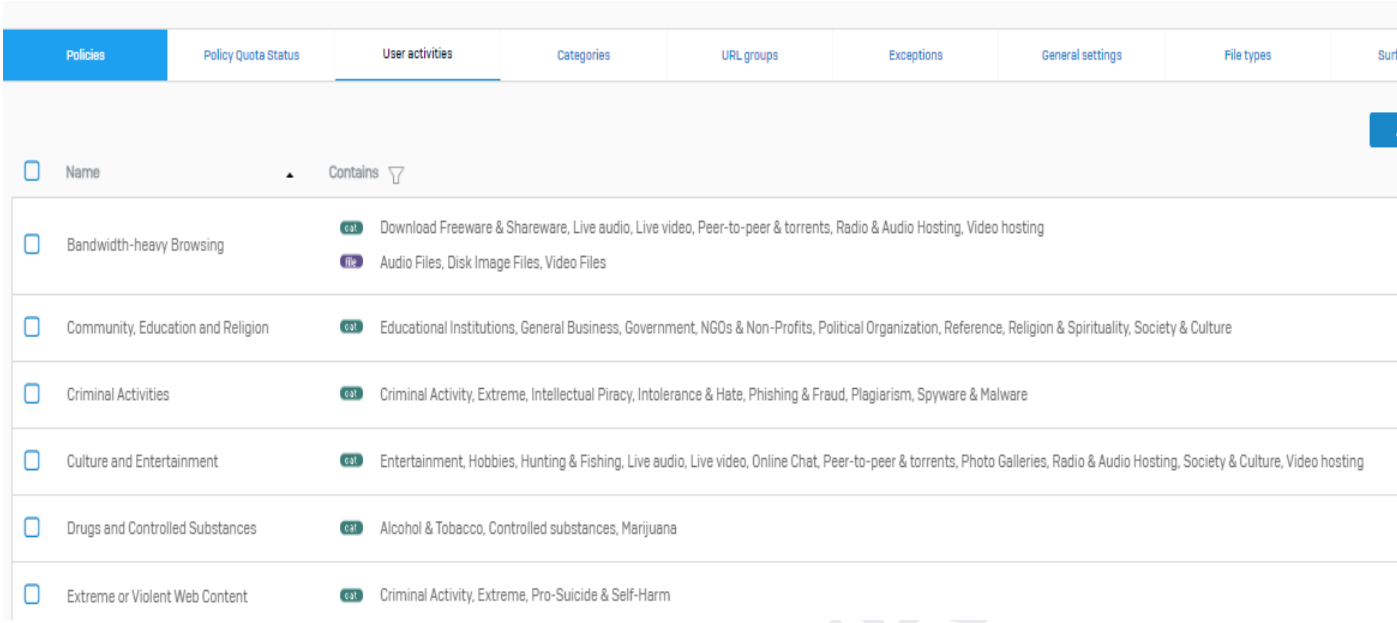
Sophos Web Filter is a security feature within the Sophos Firewall that examines internet traffic and controls access based on predefined rules and categories. It works as allowing or blocking access to specific websites or categories of websites to enhance security, productivity, and compliance.

USER ACTIVITIES:
The User Activities feature in the Web Policy section of a Sophos XGS Firewall provides detailed insights into the web browsing activities of users within the network. This functionality helps administrators monitor, manage, and enforce web usage policies effectively.

User activities combine web categories, file types, and URL groups in one container.

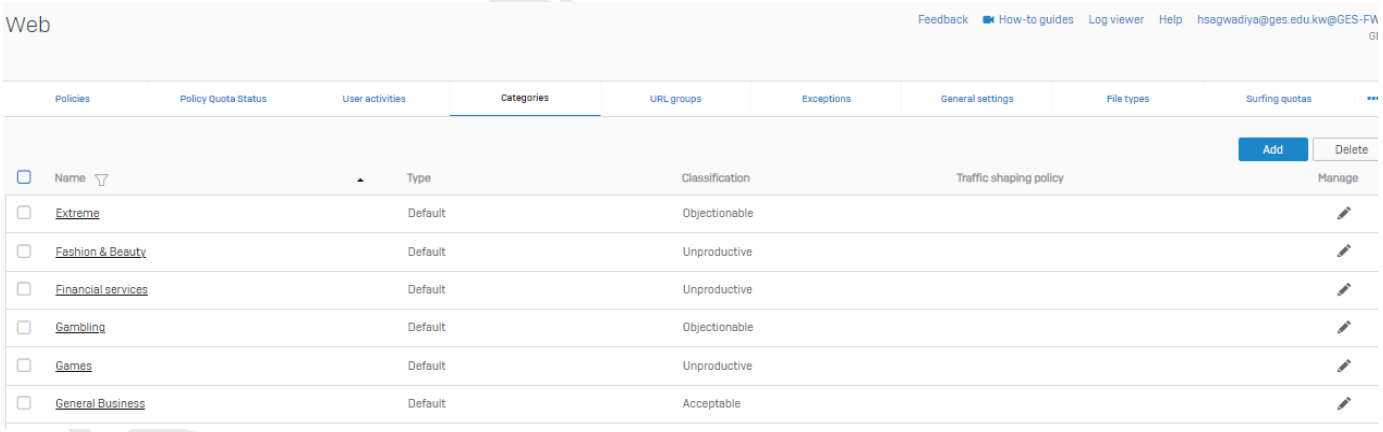
There are user activities which was created default by the Sophos are:

- Bandwidth-heavy Browsing
- Culture and Entertainment
- Drugs and Controlled Substances
- Finance & Investing
- Lifestyle
- Nudity and Adult Content
- Social Networking



They are classified as :

- Objectionable
- Unproductive
- Acceptable
- productive



CATEGORIES-

With web categories, you can organise and classify domains and keywords in a container. You can use categories within policies to control access to websites.

Within a category, you can create a list of domains and keywords specific to your organisation or import a database.

if a website is categorised incorrectly, we can also mark it as a productive category for all the sophos firewall users.

For web pages categorised as highly objectionable criminal activity, sophos will directly block those web pages and it won't add any exclusions and policy on it.

Web category descriptions

Activex - Includes all ActiveX applications. Dynamic category, see the top of the section for more information.

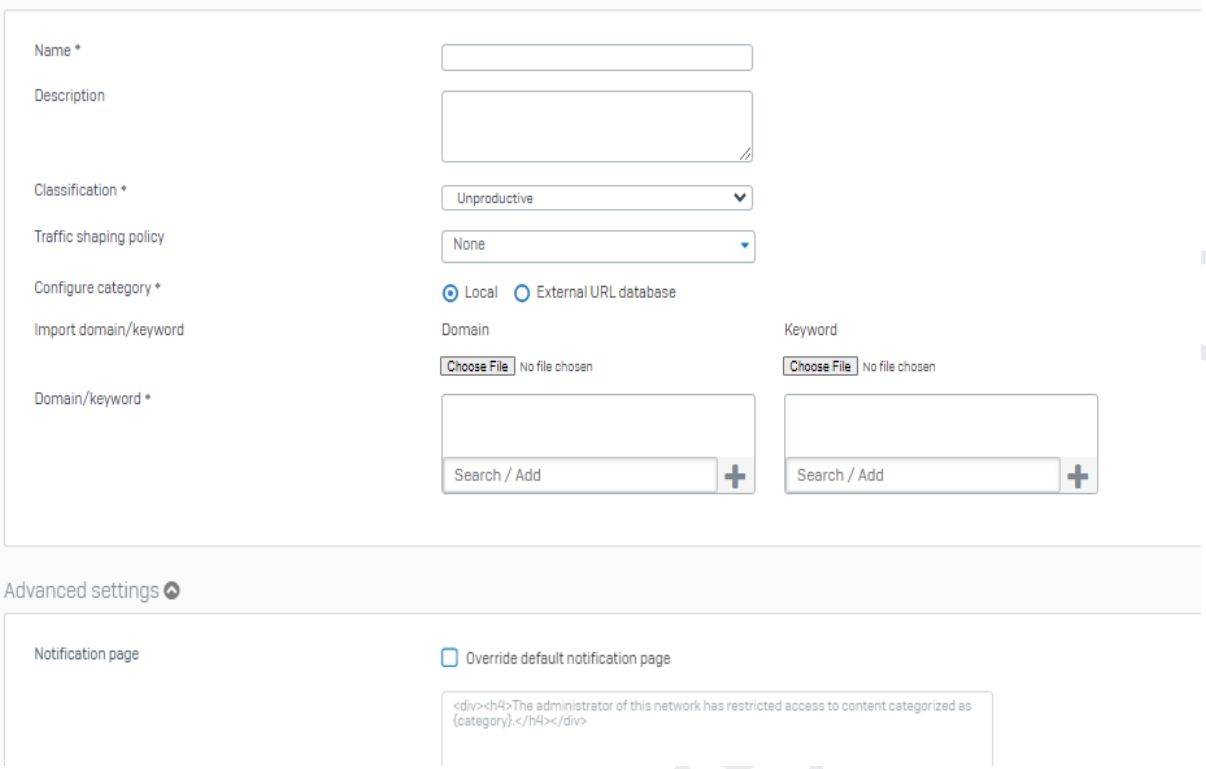
Advertisements- Includes sites of banner ad servers, sites with pop-up advertisements, and sites with known adware.

The advanced categorization of Sophos data uses the most current technical definition for adware, and thus recognizes the difference between non-malicious adware, such as cookies and more serious spyware.

Alcohol & tobacco-Includes sites that promote or distribute alcohol or tobacco products for free or for a charge.

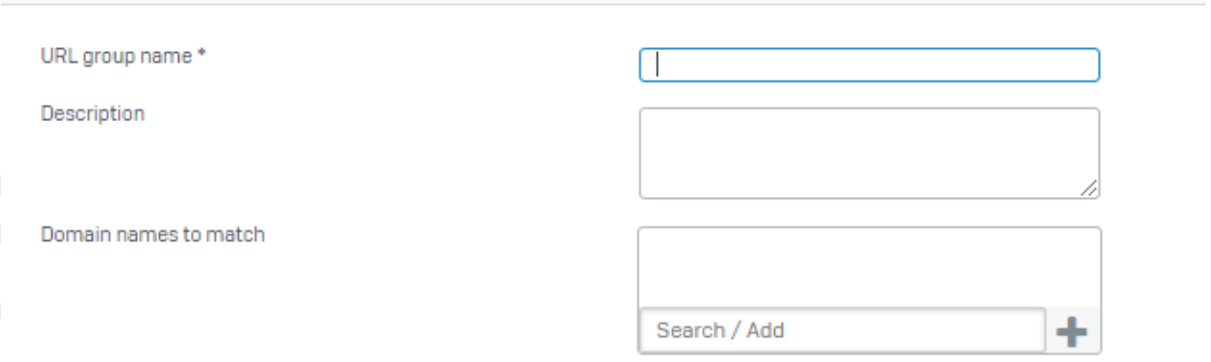
Hacking- Sites providing tools or instruction in illegal, or questionable activities to access computer systems, data or networks

Enforcing SafeSearch and additional image filters in a Sophos XGS Firewall is a way to ensure safer browsing and content filtering on your network. These settings are typically configured under the Sophos Web Policy section of the firewall's administration console. Here's a brief explanation of each:



Override default notification page- you can customise the notification page that is displayed to users when a website is blocked due to category-based filtering.

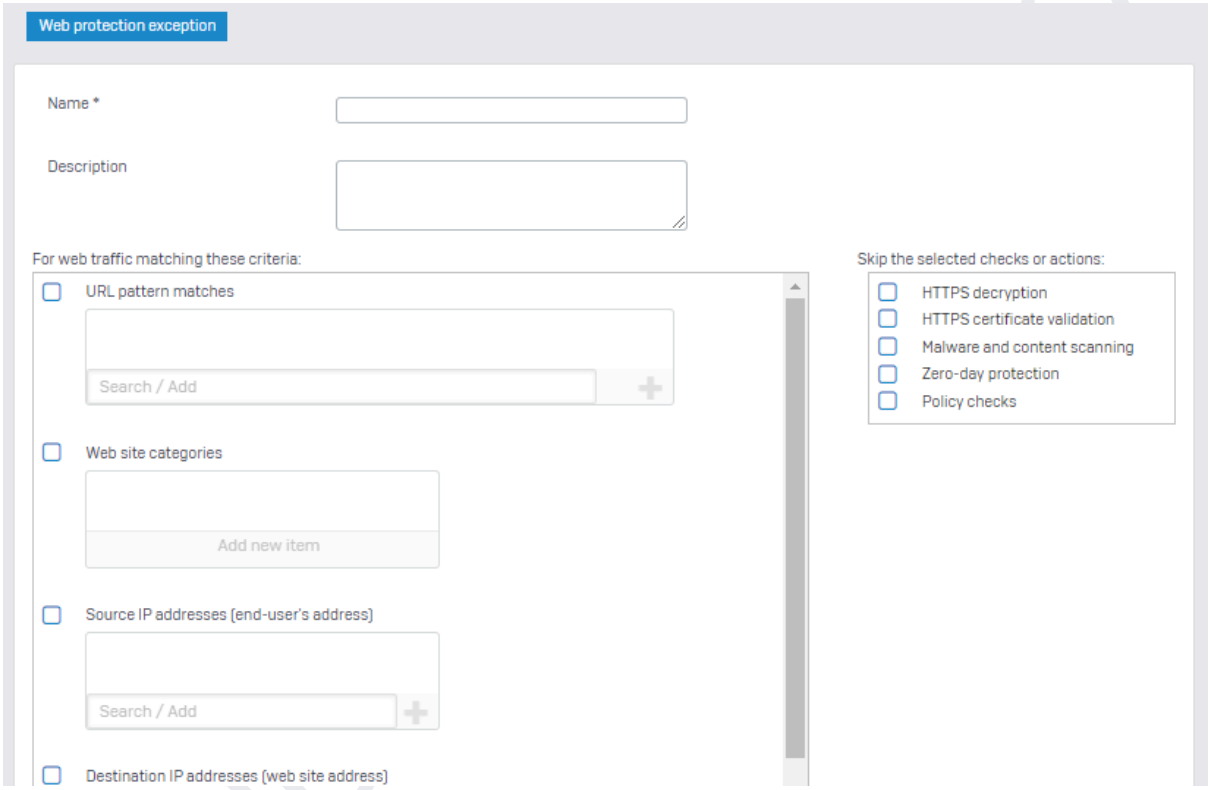
URL groups contain one or more domains that you can use in web policies to control access to websites.
A URL group can contain a maximum of 10,000 URLs.

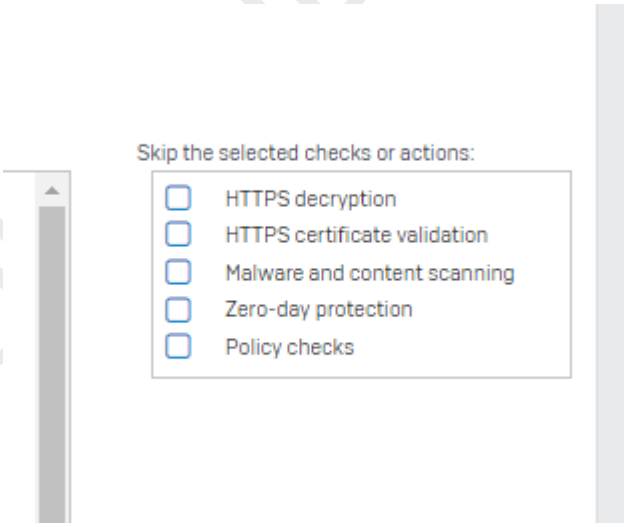


Exceptions-

With exceptions, you can override protection settings for all web traffic that matches the specified criteria, regardless of any policies or rules in effect.

For example, you can create an exception to skip HTTPS decryption for sites that contain confidential data. The default set of exceptions allows software updates and other important functions for well-known websites without being affected by web filtering.





HTTPS decryption- Select to skip decryption for HTTPS traffic that meets the specified criteria.

If you turn off HTTPS decryption, Sophos Firewall doesn't perform any other check that relies on decryption, such as malware scanning. It also allows traffic with invalid certificates if the traffic matches the exclusion criteria for HTTPS decryption.

types of websites that we can exclude are:

1. Reputable and Trusted Sites
2. privacy-sensitive Sites- sites such as financial and healthcare services.
3. Sites that must adhere to strict regulatory or compliance standards that mandate encryption without interception.

HTTPS certificate validation- the firewall will not check the validity of SSL/TLS certificates for the specified websites or categories.
This means that the firewall will not verify whether the certificates are properly signed by a trusted Certificate Authority (CA), expired, or otherwise invalid.

There are certain implications of not verifying the certificates such as MITM.

- Users might access websites that have been compromised, as the firewall won't block access based on invalid certificates.

Select to skip checks for certificate validity. If you select HTTPS decryption, Sophos Firewall automatically skips checks for certificate validity. Even when Sophos Firewall skips validity checks, it continues to decrypt traffic if it's configured to do so.

Use this if you want to allow specific websites that have invalid certificates.

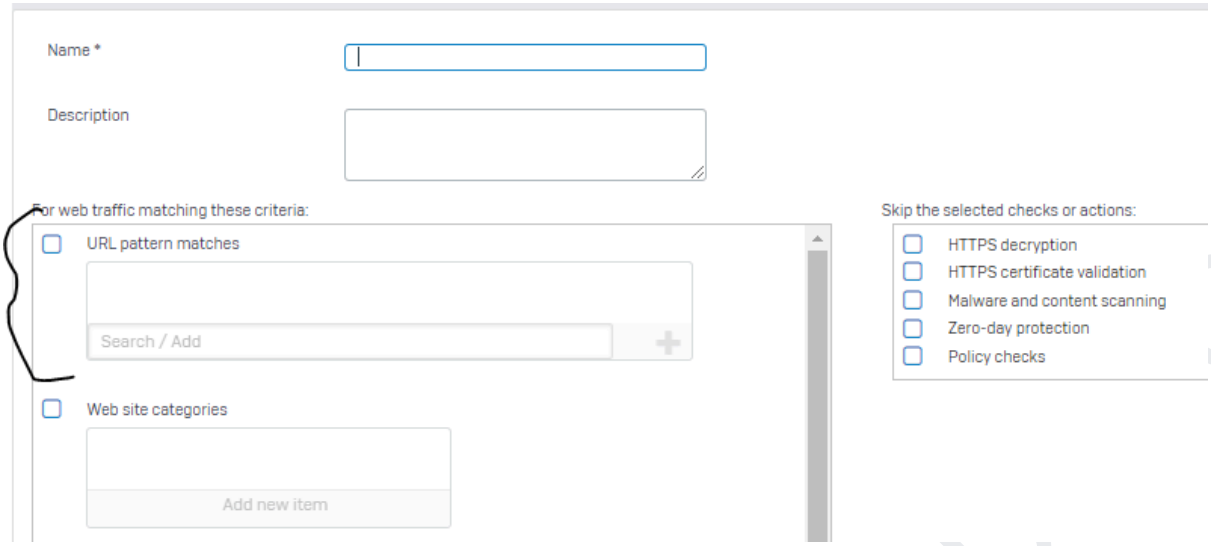
Malware and content scanning-
If you select malware and content scanning, Sophos Firewall automatically skips Zero-day protection analysis. If you skip Zero-day protection scanning, analysis reports won't be available for matching files even if malware scanning returns a positive result.

Without Zero-day protection, the firewall may not detect new, previously unknown threats that have not been identified by standard malware signatures.
You won't receive detailed analysis reports that provide insights into the nature of detected threats, which can be crucial for understanding and mitigating security risks.
Only skip Zero-day protection for highly trusted internal resources or specific applications where the security risk is minimal.

NOTE:
When you create an exception for domain eg-www.example.com and you have skipped HTTPS DECRYPTION and Certificate Validation and it will work.

When you create path based exceptions will only work when HTTP OR HTTPS traffic that has already been decrypted by the firewall.
if https decryption is not enabled for that traffic then path based exception wont work.

For example:
We have to block (www.newwebsites.com/news-day) and we want to allow (www.newwebsites.com/news-detailed)
If we have disabled https decryption , then the firewall won't see the detailed URL path but can only see the URL domain.
Therefore, path-based exceptions cannot be applied because the specific paths within the website remain hidden.

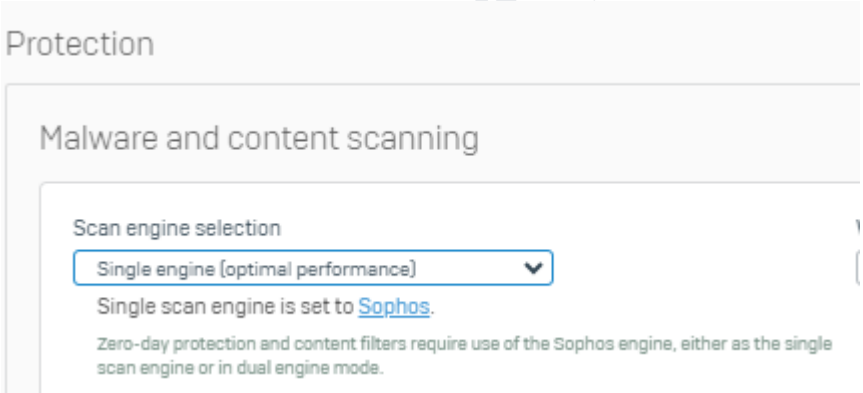


GENERAL SETTINGS

Malware and content scanning

scan engine selection-

allows you to choose the scanning engine used for various types of traffic.



Single engine: Scans traffic using the primary antivirus engine (by default, Sophos). This selection provides optimal performance.

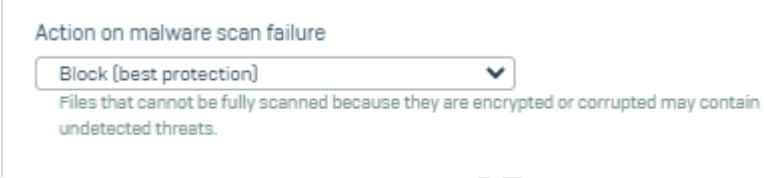
Dual engine: Scans traffic using both engines, first by the primary and then by the secondary. This selection provides maximum recognition rate and security, but may affect performance.

Web proxy scanning mode: Scanning mode for HTTP and HTTPS traffic. This option only applies to web proxy filtering. The DPI engine always uses real-time mode.

Batch: In batch mode, no part of the downloaded file is passed to the browser until the entire file has been downloaded and scanned. Batch mode offers maximum protection, but it may affect browsing performance.

Real-time: In real-time mode, the downloaded file content is passed to the browser, but won't be completed until scanned and found to be clean.

Action on Malware Scan Failure- setting determines what the firewall should do when a malware scan fails or encounters an error.



Block the Traffic:If a malware scan fails, the firewall will block the traffic and prevent it from reaching its destination.

Allow the Traffic:The firewall will allow the traffic to pass through even if the malware scan fails.

There are certain files that are compressed in more than 16 levels, files cannot be fully scanned because they are encrypted , corrupted and may contain undetected threats. **Blocking offers the best protection.**

Do not scan files larger than 30MB:
Maximum size of files to be scanned for HTTP(S), in MB. Files that exceed this size won't be scanned.

For compressed files, the firewall considers the compressed size. For example, if the scanning limit for files is 30 MB and a 500 MB file has been compressed to 5 MB, the firewall scans the file.

Maximum file scan size for FTP: Maximum size of files to be scanned for FTP, in MB. Files that exceed this size won't be scanned.

Scan audio and video files: Scans audio and video content for malware and threats. Scanning may cause issues with streaming audio and video.

Enable pharming protection: Pharming attacks redirect users from legitimate websites to fraudulent websites that have been created to look like the legitimate site. Protect users against domain name poisoning attacks by repeating DNS lookups before connecting.

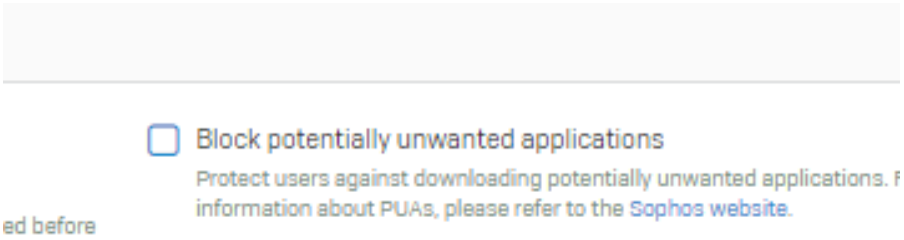
Pharming protection ensures that users are connecting to the correct websites by performing additional DNS lookups before establishing a connection.

BLOCK potentially unwanted applications

Potentially unwanted applications (PUA) are non-malicious applications such as dialers, remote administration, and hacking tools but are generally considered unsuitable for most business networks. Blocking of PUA is turned off by default.

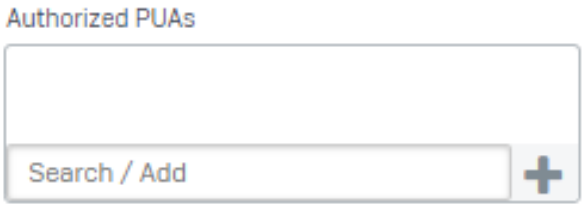
PUAs are often not outright malicious but can be undesirable because they might include adware, toolbars, or other software that can degrade system performance.

This will cause the firewall to scan for and block applications that are categorised as potentially unwanted.



Authorised PUAs

In some cases, an organisation might need to use software that is classified as a PUA for a legitimate business purpose.

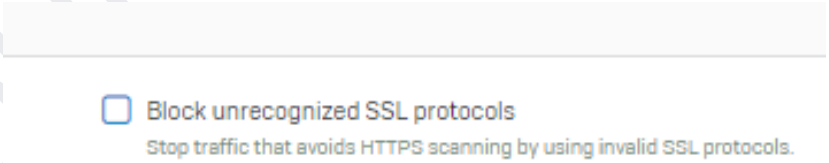


Block unrecognised SSL protocols

Blocking unrecognised SSL protocols in Sophos Firewall helps to enhance security by preventing the use of outdated or unsupported SSL/TLS protocols that might be vulnerable to attacks.

Typically, this will involve setting the firewall to only allow recognized, secure versions of SSL/TLS (such as TLS 1.2 or TLS 1.3).

Ensure that older, less secure protocols (like SSL 2.0, SSL 3.0, and older versions of TLS(TLS 1.0)



Block Invalid Certificates:

Enable the option to block invalid or untrusted certificates. This ensures that the firewall will reject connections with certificates that are not valid.

For errors and block/warn policy actions on HTTPS connections when Decrypt & Scan is disabled

In Sophos Firewall, if there is an issue with an HTTPS connection, the firewall may not be able to inspect these issues since it's not decrypting the traffic.

When the Decrypt & Scan option is disabled, Sophos Firewall can't fully inspect the content of HTTPS connections. As a result, the firewall can block entire HTTPS connections based on domain names but cannot block specific URLs or content within encrypted traffic.

When "Decrypt & Scan HTTPS" is disabled on the Sophos Firewall, the firewall's ability to filter and control HTTPS traffic is limited to domain-level actions. This means:

Policy to Block Social Media: If you set a policy in Sophos Firewall to block social media sites, like Facebook, the firewall can block access to the entire domain (e.g., www.facebook.com). This is because the firewall can see the domain name even in encrypted traffic.

Limitation on Specific Pages: However, the firewall cannot block specific pages or content within Facebook (such as a particular Facebook group or post) because that detailed information is encrypted within the HTTPS connection. Without decrypting the traffic, the firewall can’t see or act on the specific URLs or content beyond the domain name.

Enable policy override

Web policy overrides allow authorised users to provide access to otherwise blocked websites or web categories

Administrators should enable the feature, and specify users and/or user groups who are allowed to create policy override exceptions.

Blocked websites and categories

Under the Blocked websites and categories dialogue box, administrators should specify any website, URL, or website category that is to be exempted from the Web Policy override feature

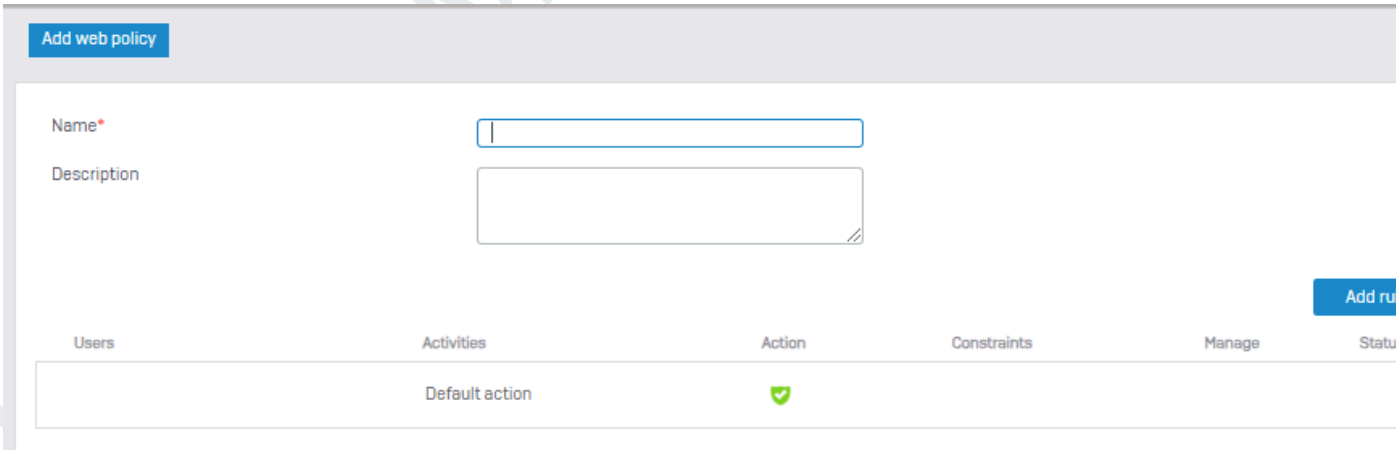
Allow manual access code

They Allow manual access code entry check box will allow authorised users to specify the password or token rather than utilise a token generated automatically by the system.

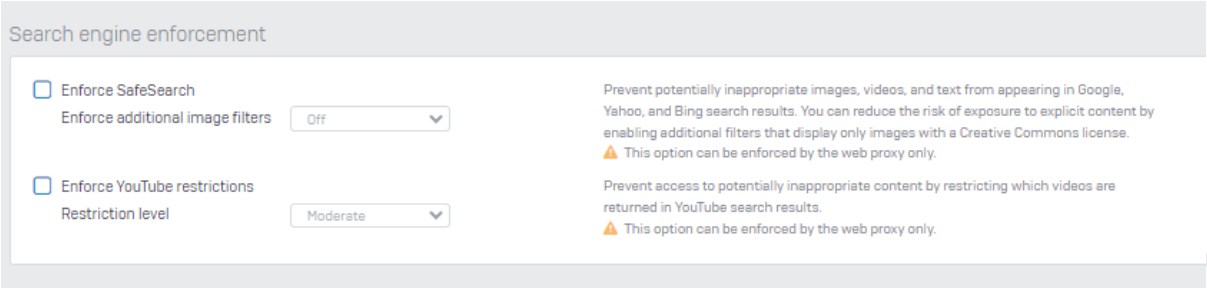
Web Content Caching

Web content caching works by storing downloaded content on the hard disk or in memory on Sophos Firewall when it is suitable for caching. When another request comes for the same content, it is served from the locally stored copy instead of downloading it again from the original web server

How to CREATE A FIREWALL WEB POLICY



Click on add rule
Select the activities you want to block



4. **Enforce SafeSearch**: SafeSearch is a feature provided by search engines like Google, Bing, and Yahoo that helps filter out explicit content from search results. Enforcing SafeSearch through your Sophos XG Firewall ensures that users on your network cannot disable this feature, providing an extra layer of protection, especially useful in environments like schools or workplaces.
5. **Additional Image Filters**: These filters provide an extra layer of content filtering by blocking or restricting access to inappropriate images. This is especially important in environments where you want to ensure that users do not encounter explicit or harmful images during their browsing sessions.
6. **Enforcing YouTube restrictions:** Enforcing YouTube restrictions and setting a restriction level on your Sophos XG Firewall can help control the type of content accessible through YouTube on your network. This is particularly useful in environments like schools or workplaces where you want to limit access to inappropriate content.

Set Restriction Level:

- You will usually find options to set the YouTube restriction level. The levels typically include:
    - **Strict Restricted Mode**: This mode filters out potentially mature content, providing a more controlled and safer browsing experience.
    - **Moderate Restricted Mode**: This mode provides a less restrictive filter compared to Strict Mode but still filters out potentially inappropriate content.

.