**A DOCUMENT ON WEB FILTERING**

**Overview**

This article describes Sophos Firewall's web filtering basics.  
  
The following sections are covered:

* [HTTPS decryption](https://support.sophos.com/support/s/article/KB-000036518?language=en_US#HTTPS)
* [Web categorization](https://support.sophos.com/support/s/article/KB-000036518?language=en_US#Categorization)
* [Web policies](https://support.sophos.com/support/s/article/KB-000036518?language=en_US#Policies)
* [Malware scanning](https://support.sophos.com/support/s/article/KB-000036518?language=en_US#Scanning)

**Product and Environment**

Sophos Firewall - All supported versions



**Information**

**HTTPS decryption**

* Use the traditional proxy or the later deep packet inspection (DPI) mode.
* In proxy mode, HTTPS decryption is configured in the firewall rule.
* In DPI mode, HTTPS decryption is configured under **Rules and policies** > [**SSL/TLS inspection rules**](https://docs.sophos.com/nsg/sophos-firewall/Latest/help/en-us/webhelp/onlinehelp/index.html?contextID=TLSInspectionRuleManage).
* If configured, the web traffic is decrypted and scanned for malware.

**Web categorization**

* We categorize millions of websites into 70+ categories.
* Sophos Firewall does category lookups (with local cache) to its cloud web servers.
* Custom categories can be created based on the domain or keywords found in the URL.
* URL groups are another way of specifying domains that should be grouped for use in policies.
* Categories, URL groups, and file types can be grouped in "User Activities" to make them more convenient to use.
* For HTTPS connections, categorization is done on the server name that is in the SNI header of the TLS connection.
* Categorization is based on the full URL for decrypted HTTP and HTTPS traffic.
* Website categories can be used in web policies to allow or block traffic to types of websites and in web exceptions and SSL/TLS inspection rules (DPI mode) to decide if sites should be HTTPS decrypted.

**Web policies**

* List what website categories or user activities should be allowed or blocked while allowing or blocking access to the rest.
* Policy rules can show a "Warn", a block page that can be clicked through, or "Quota", allowing access for a limited time per day.
* Policy rules can be specific to users, groups, and times of the day.
* Can enforce Safeseach and Youtube restrictions. For more information, see [Sophos Firewall: Add a web policy](https://docs.sophos.com/nsg/sophos-firewall/Latest/help/en-us/webhelp/onlinehelp/index.html?contextID=WebProfileEdit).

**Malware scanning**

* In the firewall rule, you can configure whether the traffic matching the rule will be scanned for malware (antivirus scan)
* Sophos Firewall has two malware scan engines, Sophos and Avira.
* In **Web** > **General settings**, you can configure the scan engine to use or if the traffic scanning is either by batch or real-time mode. More information about the modes is found on [Sophos Firewall: Malware and content scanning](https://docs.sophos.com/nsg/sophos-firewall/Latest/help/en-us/webhelp/onlinehelp/index.html?contextID=WebSettingProtectionEdit#malware-and-content-scanning).
* Potentially unwanted applications (PUAs) can be optionally blocked. These are not malware but can be adware or other things administrators may not want to allow.
* The maximum scan size can be configured. Malware is typically sent in small files, and large files take longer to scan. Therefore most admins allow larger files to be downloaded unscanned.

