TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

MIGRATING A SECURITY POLICY TO THE NEW EWC URL DATABASE

Product concerned: SNS 4.3.24 LTSB and higher versions of 4.3 LTSB, SNS 4.7 and higher versions

Document last updated: December 11, 2024

Reference: sns-en-Migrating_security_policy_to_new_EWC_database-technical_note

Table of contents

Change log

Date	Description
February 13, 2024	SNS 4.3.24 LTSB release
October 30, 2023	New document

Getting started

A new URL database provider is now used on the Extended Web Control (EWC) URL classification solution from these versions onwards:

- SNS in 4.7 and later versions,
- SNS in 4.3.24 LTSB and higher versions of 4.3 LTSB.

The EWC URL database will be **automatically** changed when the firewall is updated to an SNS version that uses the new database.

IMPORTANT
Due to the new EWC URL database, the firewall's initial security policy (filter policy, URL filter policy and SSL filter policy) must be reviewed after the firewall is updated. During this adjustment phase, users may notice that filtering does not function optimally.

The review of the security policy requires the following considerations to be taken into account:

- The EWC URL categories have changed: former and new categories do not fully match, as some have been removed while others have been added;
- The classification logic has changed: the new URL/SSL filter policy must now be in blacklist mode;
- The new filter policy must be adapted to assign profiles from the new URL/SSL filter policy to rules;

The impact of changing the database is explained in the section Understanding the impact of changing the EWC URL database.

To limit the impact of changing the database, follow the Recommendations to limit the impact of changing the EWC URL database.

NOTE

The following information is presented in the Appendices of this document:

- The list of new EWC URL categories and their descriptions,
- Tables to map former and new URL categories,
- Recommended URL/SSL filter profiles.

Understanding the impact of changing the EWC URL database

This section explains the impact of changing the EWC URL database, and how to view changes that are automatically made after the database is installed. **We strongly advise you to read this section.**

Impact on the classification logic and construction of the URL/SSL policy

The classification logic has changed after the installation of the new database: the URL/SSL filter policy must now be in blacklist mode. This requires the following considerations to be taken into account:

- The URL categories to be prohibited must be placed above rules that allow other categories,
- You are strongly advised to build the URL/SSL filter policy in several sections and by following a particular order. We recommend these sections:

Section	Description
1 - Compromised URLs	Category that groups malicious URLs, and which Stormshield's security teams continuously update
2 - Always block	Illegal, dangerous and violent content
3 - Always pass, never decrypt (GDPR)	Content that requires the protection of user data (banking, healthcare, etc.)
4 - Always pass, can be decrypted	Content relating to the organization's business sector and which users require for work
5 - Block recommended	Content that should be blocked, but without preventing users from visiting websites that fall under "Always pass" sections
6 - Pass recommended	Content that should be allowed, so that users are not prevented from browsing the Internet (in particular, the URL categories *unknown*, *misc*, *hosting* and *computersandsoftware*). Some categories can also be allowed only during specific time slots (social media during lunch break, for example)
7 - Pass (Any)	Equivalent to a *pass all* rule. Action applied to any website that has not been categorized in previous sections

- In section *6 - Pass recommended*, you are strongly advised to allow the URL categories *unknown*, *misc*, *hosting* and *computersandsoftware*. If these categories are blocked, the display of websites that use external resources (images, .css, .js, write policies, etc.) may be affected, even if the visited website is in an allowed category.

Impact on URL/SSL filter rules

The way URL/SSL filter rules are processed when the database is changed depends on whether the former and new URL categories match. There are several possible matches:

- Categories exactly match;
- Categories partially match;

- Categories do not match, the former category has no equivalent;
- Categories do not match, the new category has no equivalent.

After the database is changed, **administrator intervention is required in some scenarios to fix inconsistencies or errors in the configuration**. Warning messages appear in the firewall's administration interface to identify such inconsistencies:

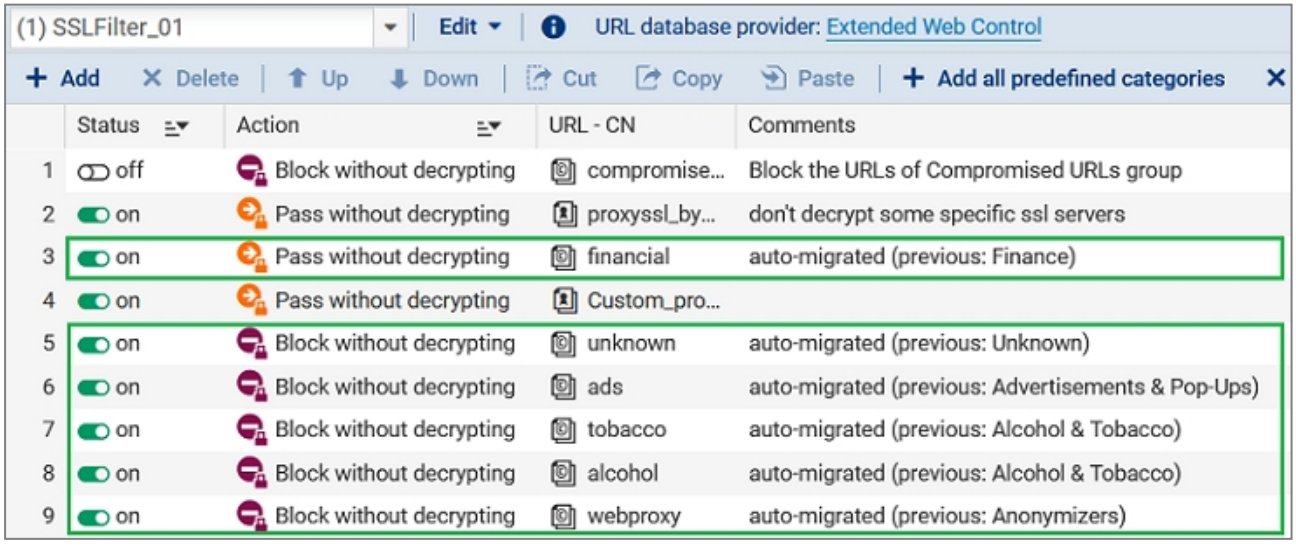
- In the menu on the left, in front of the **URL filtering** and **SSL filtering** modules,
- In the **Dashboard**, in the **Messages** section.

Categories exactly match

The Former EWC URL categories that are exact matches of new categories are automatically replaced in the URL/SSL filter rules in question.

The rule is processed as follows during migration:

- The former category is replaced with the new equivalent category,
- The rule keeps the status (enabled/disabled) and action that it had before it was migrated,
- An "auto-migrated (previous: *name_former_category*)" comment will be associated with it.



Categories partially match

The Former EWC URL categories that partially match new categories may have been grouped under a single new category.

EXAMPLES
The categories *Child abuse* and *Criminal activity* fall under the new category *illegal*.
The categories *Religion* and *Cults* fall under the new category *religion*.

Separate former categories may have been used in different rules. There are two situations in which rules would apply the same or different actions (pass, block, decrypt, etc.). In each case, rules are processed differently when they are migrated.

Category appearing in rules that apply the same action

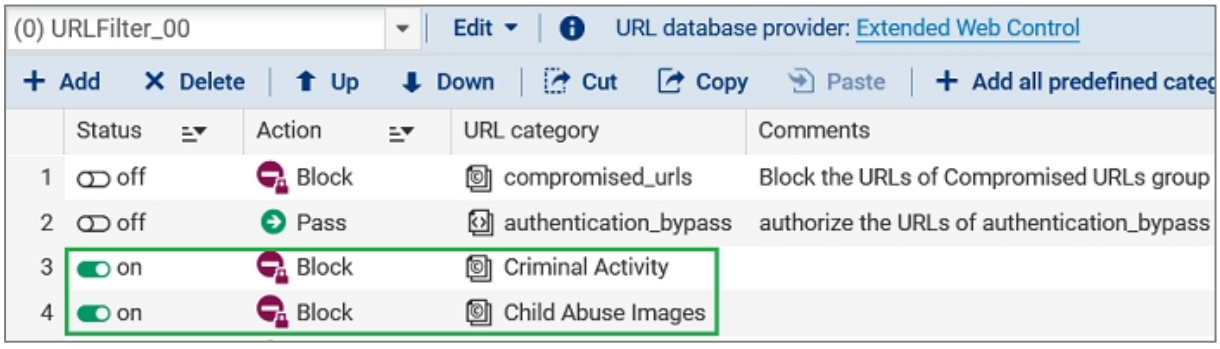
In the first filter rule encountered that uses the former category:

- The former category is replaced with the new equivalent category,
- An "auto-migrated (previous: *name_former_category*)" comment will be associated with it.

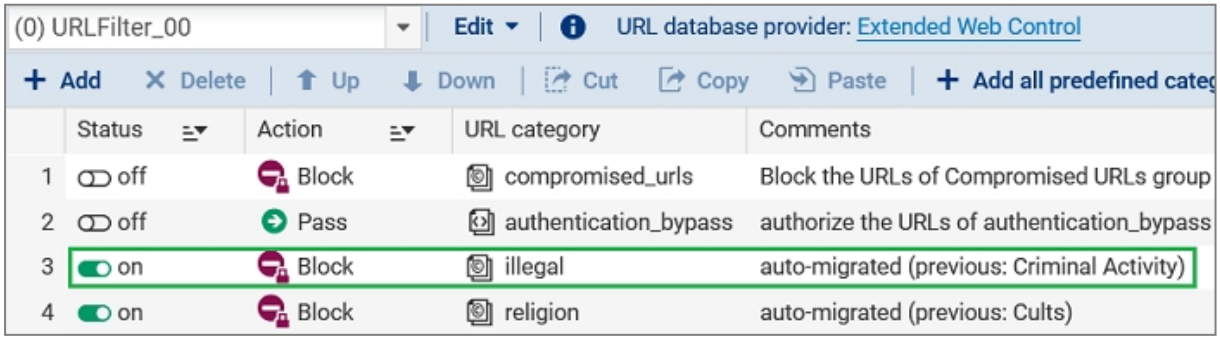
The following rules that used the former category will be deleted from the URL/SSL filter profile to avoid creating duplicate rules.

EXAMPLE
The first rule that blocks the former category *Child abuse*, which now falls under the new category *illegal*, will be retained. The second rule that blocks the former category *Criminal activity*, which now falls under the new category *illegal*, will be deleted since the first rule already blocks the category.

Before migration:



After migration:



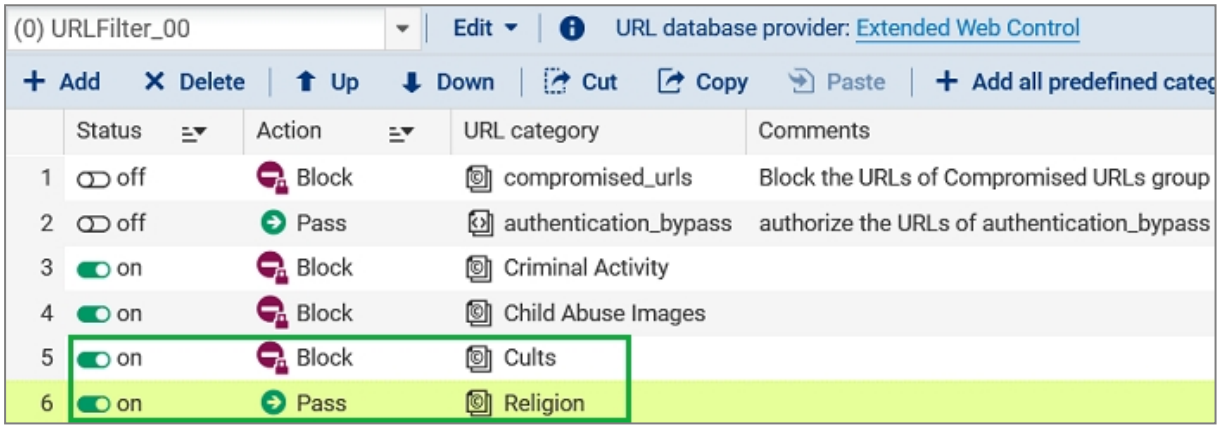
Category appearing in rules that apply different actions

For each rule:

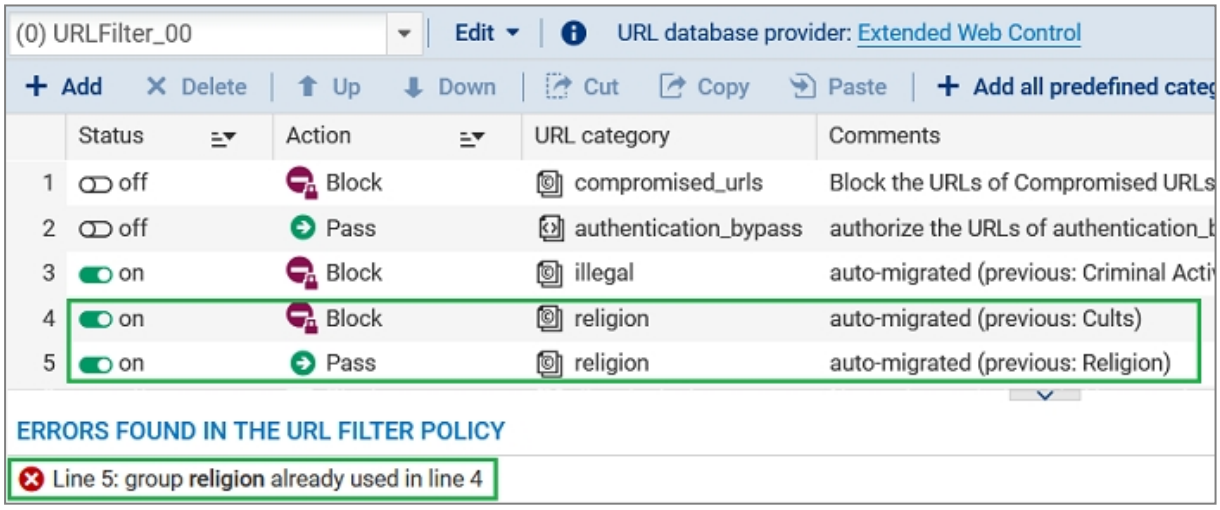
- The former category is replaced with the new equivalent category,
- An "auto-migrated (previous: *name_former_category*)" comment will be associated with each rule.

These rules will generate a warning in the consistency checker: **administrator intervention is required to fix this situation and validate the policy.**

Before migration:



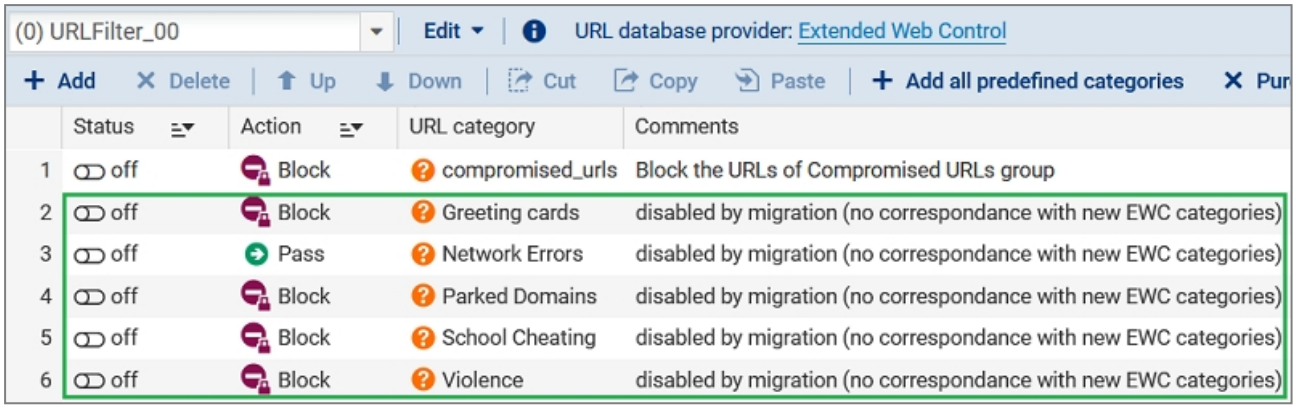
After migration:



Categories do not match, the former category has no equivalent

A rule that uses Former EWC URL categories without any equivalence with new categories is processed as follows:

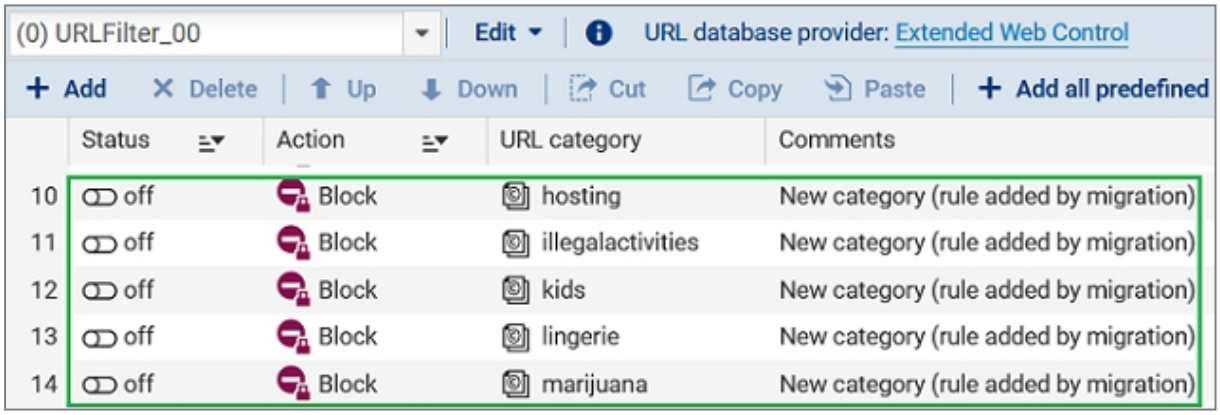
- The rule is retained with the former URL category, but is disabled,
- A "disabled by migration (no correspondence with new EWC categories)" comment will be associated with it.



Categories do not match, the new category has no equivalent

The new provider's URL database introduces New EWC URL categories without any equivalence with former categories. For each of these categories:

- A disabled rule with a block action is added right at the end of the URL/SSL filter profile,
- A "New category (rule added by migration)" comment is associated with it.



Impact on URL category groups

The way URL category groups are processed when the database is changed depends on whether the former and new URL categories match. There are two possible situations.

Exact or partial category match

The Former EWC URL categories that are exact matches of new categories and Former EWC URL categories that partially match new categories, are automatically replaced with the new equivalent category(ies) in the URL category groups that may have been created before the migration.

EXAMPLES
The category *Finance* has been replaced with the new category *financial*. The categories *Child abuse* and *Criminal activity* have been replaced with the new category *illegal*.

Categories do not match, the former category has no equivalent

The Former EWC URL categories without any equivalence with new categories are deleted from URL category groups that may have been created before the migration.

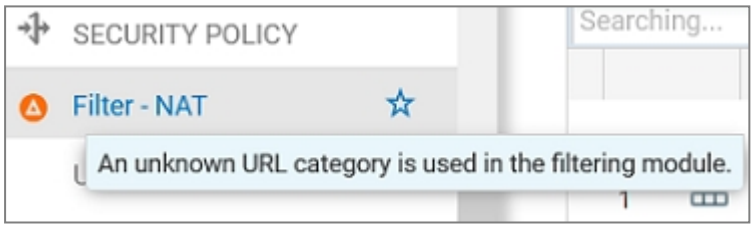
In this case, no warnings will be displayed in the firewall's administration interface: **administrator intervention is required to check this situation and fix the groups**.

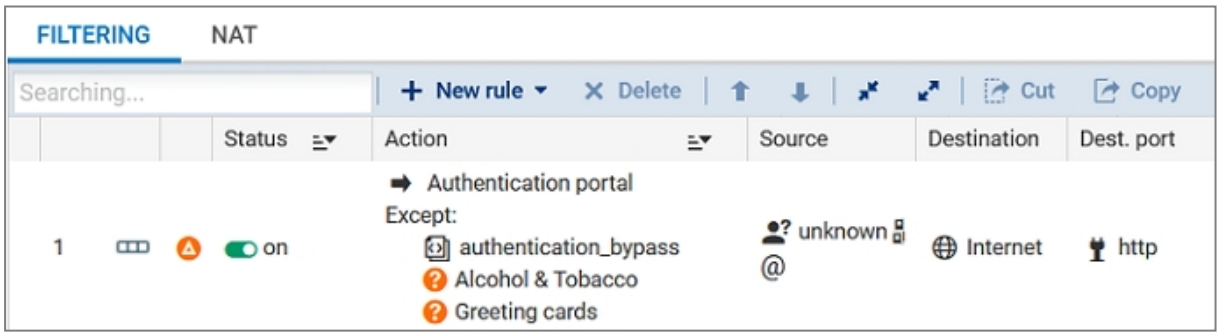
Impact on authentication exception rules in the filter policy

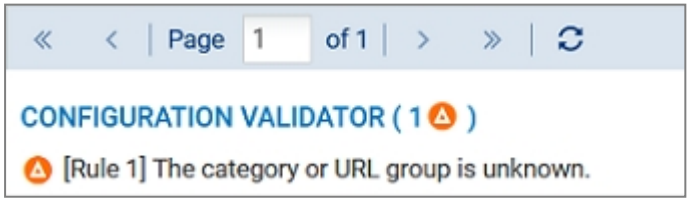
Former categories **will not be replaced** in authentication exception rules in the filter policy.

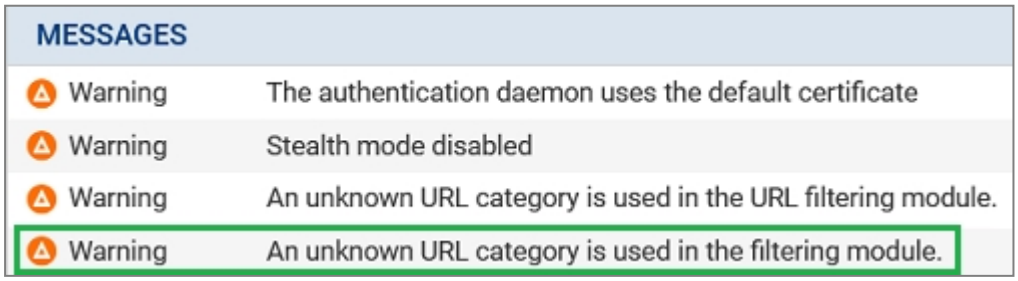
After the database is changed, **administrator intervention is required to fix errors and validate the policy.** Warning messages appear in the firewall's administration interface to identify such inconsistencies:

- In the menu on the left, in front of the name of the **Filter - NAT** module,
- In the **Filter - NAT** module, in the filter policy rules,
- In the **Filter - NAT** module, in the filter consistency checker,
- In the **Dashboard**, in the **Messages** section.





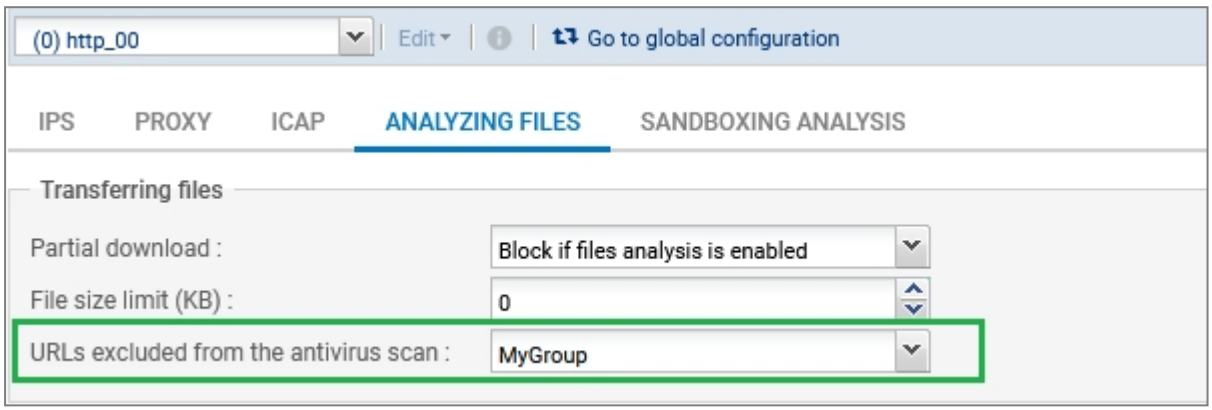




Impact on URLs excluded from the HTTP protocol antivirus scan

Check that the content of groups/URLs specified in the URLs excluded from the HTTP protocol antivirus scan (**Protocols** > **HTTP** > **File scan** tab) still complies with the desired policy.

No warnings will be displayed in the firewall's administration interface: **administrator intervention is required to check this situation and fix it.**



Recommendations to limit the impact of changing the EWC URL database

The steps below serve to limit the impact of changing the EWC URL database, as described in the section Understanding the impact of changing the EWC URL database.

You are strongly advised to carry out these steps before updating the firewall to an SNS version that uses the new database. If the firewall has already been updated, go to the section Checking and adapting the security policy after the EWC URL database has been changed.

IMPORTANT
Before updating the firewall, we strongly recommend backing up the current configuration of your firewall so that you can restore it whenever necessary.

For every URL filter policy profile used:

1. Disable all rules with a Block action, excluding the rules under section "2 - Always block", which match your environment (see appendix Recommended URL/SSL filter profiles).
2. Create a rule with a **Pass** action applied to the **Any** URL category and placed in the last position of the URL filter profile.

For every SSL filter policy profile used:

1. Disable all rules with a **Block without decrypting** action, excluding the rules under section "2 - Always block", which match your environment (see appendix Recommended URL/SSL filter profiles).
2. Create a rule with a **Pass without decrypting** action applied to the **Any** URL category and placed in the last position of the SSL filter profile.

You can then proceed to update the firewall. The modified policy is not the optimal version but will not block commonly encountered and legitimate traffic for your users. Next, continue to the section Checking and adapting the security policy after the EWC URL database has been changed.

Checking and adapting the security policy after the EWC URL database has been changed

After the EWC URL database has been changed, the administrator has two ways to rebuild a security policy that complies with the one in place before the change:

- Import the URL/SSL filter profiles recommended by Stormshield (faster solution),
- Manually fix the security policy (longer solution).

Solution 1: Import the URL/SSL filter profiles recommended by Stormshield

Stormshield offers a backup file (.na format) that contains 3 recommended URL/SSL filter profiles that the administrator can restore on the firewall. These profiles will automatically be placed in the first 3 SSL/URL filter profiles:

- 00: "permissive" profile,
- 01: "standard" profile,
- 02: "restrictive" profile.

The recommended URL/SSL filter profiles are explained in the appendix Recommended URL/SSL filter profiles.

IMPORTANT
By importing these profiles, all URL/SSL filter profiles configured earlier on the firewall will be lost.

Backing up the firewall's configuration

Back up the firewall's current configuration so that you can restore it whenever necessary.

1. In **System** > **Maintenance** > **Backup**, fill in the field **Backup filename**.
   In the **Advanced properties** section, you can set a password to protect the backup file.
2. Click on **Download the configuration backup** and save the backup file (.na format) on your administration workstation.

Importing the recommended URL/SSL filter profiles

1. Retrieve the *templates_Extended_Web_Control.na* file from your MyStormshield personal area in **Downloads** > **Downloads** > **Stormshield Network Security** > **Tools**.
2. In **System > Maintenance > Restore**, select the file *templates_Extended_Web_Control.na*.
3. In the **Advanced properties** section:
   - Unselect **Restore the configuration from the file**,
   - Select **URL filtering** and **SSL filtering**.
4. Click on **Restore the configuration from the file**.
   The recommended profiles will automatically be imported in the SSL/URL filter profiles 00, 01 and 02.
   All other URL/SSL filter profiles (profiles 03 to 09) will be reinitialized.

Adapting the security policy

1. In **Configuration > Security Policy > URL filtering** and **SSL filtering**, adapt the profiles so that they match your organization's activity and policy.

   > **TIP**
   > You can copy one policy to another by clicking on **Edit > Copy to** on the right side of its name, and by selecting the destination policy.
   > If this policy is the one used in the filter policy, you can skip the next step.

2. In **Configuration > Security policy > Filter - NAT > Filtering** tab, ensure that the rules in the filter policy use profiles from the new URL/SSL filter policy. Adapt the filter policy if necessary.
3. If you use authentication exception rules in the filter policy, you must fix them by replacing the former categories with the new ones. The tables that map former and new URL categories are shown in the Appendices.

Checking and fixing URL category groups

If you use URL category groups in the firewall's configuration, check that they still contain the desired URL categories. Reminder: these groups can be used in the following modules:

- URL filtering,
- SSL filtering,
- Filter - NAT, in authentication exception rules,
- HTTP protocol, in the configuration of the antivirus scan that targets excluded URLs.

Solution 2: Manually fix the security policy

> **IMPORTANT**
> Before continuing, if you have not already done so, we strongly recommend backing up the current configuration of your firewall so that you can restore it whenever necessary.

Fixing the URL/SSL filter policy

In **Configuration > Security Policy > URL filtering** and **SSL filtering**, for each URL/SSL filter profile used:

1. Click on **Add all predefined categories** to add new unused categories that match former categories. These new categories are imported and placed at the end of profiles in enabled rules and with an action to show block pages *BlockPage_00*.

> **TIP**
> Block pages can be customized in **Configuration > Notifications > Block messages > Block page** tab. For more information, refer to the **Block pages** section in the SNS user manual:
> - HTTP block page tab for SNS 4.3 versions,
> - Block page tab for SNS 4.8 versions and higher.

   Reminder: the new categories without any equivalence with former categories were automatically imported during migration and placed in disabled rules with a block action.
2. Select the categories to allow/block, then rebuild and gather the corresponding rules by sections. Reminder: the recommended URL/SSL filter profiles are explained in the appendix Recommended URL/SSL filter profiles.
3. Click on **Purge rules** to delete rules that detect unknown categories. The list of categories in question is provided in the appendix Former EWC URL categories without any equivalence with new categories.
4. Apply blacklist mode by creating a rule that allows **Any** category in the last position of the URL/SSL filter profile.

Fixing the filter policy

1. Go to **Configuration > Security policy > Filter - NAT, Filtering** tab.
2. Adapt the filter policy to assign profiles from the new URL/SSL filter policy to rules.
3. If you use authentication exception rules in the filter policy, you must fix them by replacing the former categories with the new ones. The tables that map former and new URL categories are shown in the Appendices.

Checking and fixing URL category groups

If you use URL category groups in the firewall's configuration, check that they still contain the desired URL categories. Reminder: these groups can be used in the following modules:

- URL filtering,
- SSL filtering,
- Filter - NAT, in authentication exception rules,
- HTTP protocol, in the configuration of the antivirus scan that targets excluded URLs.

SNS firewall pools

The way URL/SSL filter policies are updated on an SNS firewall pool varies, depending on whether the pool is managed by an SMC server.

Firewall pools managed by an SMC server

The update of the URL/SSL filter policy requires five steps.

Rebuilding a compliant security policy on an SNS firewall in the pool

Follow the method described in the section Checking and adapting the security policy after the EWC URL database has been changed.

Exporting the configuration of the reference firewall (.na format file)

Follow the method described in the section Backing up the firewall's configuration to export the configuration of the reference firewall.

Importing the backup of the reference firewall's configuration on the SMC server

Follow the method described in the section Attaching files to a script and receiving files generated by script in the SMC administration guide to import the configuration backup file exported earlier.

Creating the CLI command script

Follow the method described in the paragraph Creating the CLI command script in the SMC administration guide.

The CLI/Serverd commands to be inserted in the script will be the following:

```
CONFIG OBJECT URLGROUP SETBASE base=CLOUDURL
CONFIG RESTORE list=urlfiltering,sslfiltering $FROM_DATA_FILE("backup_
file_name.na")
```

Replace *backup_file_name*.na with the name of the file exported from the reference firewall. Ensure that you use the *urlfiltering,sslfiltering* values for the *list* parameter to restore only the URL/SSL filter policy.

Running the script from the SMC server on the firewall pool

Follow the method described in the section Running the SNS CLI script from the web interface in the SMC administration guide.

Firewall pools not managed by an SMC server

The update of the URL/SSL filter policy requires three steps.

Rebuilding a compliant security policy on an SNS firewall in the pool

Follow the method described in the section Checking and adapting the security policy after the EWC URL database has been changed.

Exporting the configuration of the reference firewall (.na format file)

Follow the method described in the section Backing up the firewall's configuration to export the configuration of the reference firewall.

Importing the backup of the firewall's configuration on every SNS firewall in the pool

IMPORTANT
By importing the backup, all URL/SSL filter profiles configured earlier on the destination firewall will be lost.

1. In **System** > **Maintenance** > **Restore**, select the configuration backup file of the reference firewall (*.na*).
2. In the **Advanced properties** section:
   - Unselect **Restore the configuration from the file**,
   - Select **URL filtering** and **SSL filtering**.
3. Click on **Restore the configuration from the file**.
   The profiles will automatically be imported in the SSL/URL filter profiles.

Appendices

This section groups the following appendices:

- List of new EWC URL categories,
- Former EWC URL categories that are exact matches of new categories,
- Former EWC URL categories that partially match new categories,
- Former EWC URL categories without any equivalence with new categories,
- New EWC URL categories without any equivalence with former categories,
- Recommended URL/SSL filter profiles.

List of new EWC URL categories

New URL category	Description
ads (Advertisements and ad content)	Sites that provide advertising graphics or other ad content files that appear on Web pages.
advice (Forums, discussion groups and FAQs)	Sites for sharing information in the form of forums, discussion groups and FAQ websites on which users chat and receive answers to the questions that they ask. This category does not include the specific sections of corporate websites on which customer queries are answered (FAQ).
alcohol	Sites that offer the sale of alcoholic products, or which contain information on alcoholic products, such as alcohol brands.
astrology	Sites that promote, provide or share information on beliefs relating to astrology such as horoscopes, zodiac signs, etc. This category also includes similar beliefs not related to astrology, such as numerology, fortune telling, etc., but does not include organized religions or cults.
auto (Motorized vehicles)	Sites containing information on motorized road vehicles such as cars, motorcycles, go-karts, etc.
blogs (Personal websites)	Sites about individuals, either hosted by them or by commercial websites (such as *Blogger*, AOL, etc.).
business (Business activity)	Sites that obtain sales information such as corporate websites, that help organizations of all sizes to conduct their daily business activity.
c&c (Malware command and control websites)	Websites that generally exploit malware already installed on the user's host. A malware download may sometimes be in progress when the user connects to the website, if the site both hosts and exploits the malware.
computersandsoftware (Software download websites)	Sites that contain downloadable software, whether shareware, freeware, or for a charge. This category may also cover some online app stores.
drugs (Pharmaceuticals, alcohol and tobacco)	Sites that obtain information on the use or sale of legal pharmaceuticals, medical accessories, alcohol or tobacco products. This category includes the categories alcohol, tobacco and pharmacy (Pharmaceuticals). Illegal drugs are covered by the category narcotics (Drugs and narcotics).
education (Teaching and learning)	Sites sponsored by educational institutions and schools of all types including distance education. This category includes educational and reference materials, such as dictionaries, encyclopedias, online courses, teaching aids and discussion guides.
entertainment	Sites containing programming guides to television, movies, music and video (including video on demand), celebrity sites, and entertainment news.

New URL category	Description
filesharing (Peer-to-peer)	Sites that enable files to be directly exchanged and downloaded between users without dependence on a central server. This category also includes some torrent sharing websites and torrent trackers.
financial	Sites related to banking, finance, payment or investment, including banks, brokerages, online stock trading, stock quotes, fund management, insurance companies, credit unions, credit card companies, and so on. Some local banks may not be covered by this category.
food	Sites with content relating to food and non-alcoholic beverages, such as recipes, ingredients, amount of calories, etc.
fraud (Fraudulent websites)	Known fraudulent websites that aim to obtain information, payments and credentials from users through false declarations or fraudulent means. For example, online stores that offer very low prices for popular products that will never be sent. This category does not include phishing websites.
gambling (Online betting and gambling)	Sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance. In general, such websites require users to pay before they can start placing bets. While some of these websites are legitimate (prizes and jackpots can be won), others are fraudulent (no chances of winning anything). This category includes websites that provide tips and tricks that describe effective methods to earn money from gambling, as well as online lottery websites.
games (Computer games and consoles)	Websites that provide, promote or sell games, including online games, computer games and board games, either for free or with a subscription. This category also includes game discussion forums, guides, cheats, etc.
government (Government departments or agencies)	Sites run by governmental or military organizations, departments, embassies or agencies, including police departments, fire departments, customs bureaus, emergency services, civil defense, counterterrorism organizations and hospitals.
hacking	Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information, perpetrating fraud, creating viruses, or committing other illegal activity related to theft of digital inform.
hate (Hate, racism and discrimination)	Sites that promote any form of supremacy (political, religious, racial, etc.). This category includes websites that encourage oppression of people or groups of people based on their race, religion, gender, age, disability, sexual orientation or nationality. It also includes websites belonging to terrorist organizations and websites discussing aggressive sports and/or promoting violence.
health (Health care)	Sites that contain information relating to healthcare institutions, and preventing and treating illnesses. Websites that offer information or products for weight loss, dieting, steroids, anabolic products or human growth hormones, as well as information on aesthetic surgery.
hobbies	Sites that offer information relating to leisure activities and pastimes such as collecting, art and crafts, etc.

New URL category	Description
homograph (Homographic websites)	Websites with domain names that visually resemble legitimate domain names, but which use different character sets, such as Cyrillic characters that match Latin characters, e.g., 'a', 'p' and 'e'. Although these domain names are visually identical to the original domain names, they are generally used for malicious purposes.
hosting (Website hosting)	Free or commercial website hosting services that allow individuals or organizations to create and publish websites.
illegal (Illegal software activities)	Sites relating to software piracy and associated forums, that illegally distribute or help to distribute copyrighted content and software, pirated software, key generators and serial numbers to facilitate the illegal use of software programs. Some of these websites may also be detected as pornographic or relating to alcohol/cigarettes if they publish ads in these industries to earn money.
illegalactivities (Illegal activities)	Sites with content that would be considered illegal in most countries, including, for example, content relating to the sexual exploitation of minors. This category does not include computer hacking or narcotics.
im (Instant messaging/chat)	Instant messaging and chat websites that allow users to chat in real time (such as ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, etc.). This category also includes yahoo.com and gmail.com, which both embed instant messaging services.
jobsearch	Sites containing job listings, career information, assistance with job searches (such as resume writing, interview tips, etc.). This category includes job offer aggregators, but does not contain recruitment agencies or the career pages of corporate websites.
kids (Children's websites)	SItes designed for use by children, with content such as children's stories, games and media.
lifestyle (Fashion, beauty and lifestyles)	Sites devoted to fashion, beauty products and tattoos.
lingerie (Lingerie and swimwear)	Sites that promote or sell lingerie, undergarments and bathing suits.
malware (Malicious software)	Sites that contain or provide malicious software in the form of executable files, vulnerability exploitation tools, JavaScript or any other malicious programs.
malware-hd (Probable malicious software)	Sites that are deemed to potentially contain or provide malicious software, but may also not contain any. As this status is stricter than the "Malware" status, it may generate false positives. For a strict inspection, this status should raise an alert on websites. For a normal inspection, this status can be ignored.
marijuana (Marijuana and derived products)	Sites that sell marijuana and associated products, as well as sites that provide information and forums on growing marijuana and its effects.

New URL category	Description
maturecontent (Content for adults only)	Sites targeting an adult audience. This category includes a wide array of websites, ranging from the Kama Sutra, sex education websites to hardcore porn. It groups the categories lingerie (Lingerie and swimwear), nudity, sextoys (Erotic gadgets), sexualeducation and sexualcontent (Other sexual content).
miners (Cryptocurrency miners)	Sites that attempt to mine cryptocurrency in the user's web browser by using the computer's resources. In general, such sites hide this from the user, but may sometimes inform the user.
misc (Miscellaneous)	Websites that do not present any danger, but which may have been classified under one or several other categories.
narcotics (Drugs and narcotics)	Sites with information on the purchase, manufacture, and use of illegal or recreational drugs and their paraphernalia, and misuse of prescription drugs and other compounds. This category contains the categories marijuana (Marijuana and derived products) and narcoticsgeneral (Drugs other than marijuana).
narcoticsgeneral (Drugs other than marijuana)	Sites that offer information on illegal narcotics other than marijuana (which is included in the category marijuana [Marijuana and derived products]) This category also includes websites that explain the ingredients, use and manufacture of drugs, or which offer them for sale or exchange.
news	Sites covering news and current events such as newspapers, newswire services, personalized news services, broadcasting sites, and magazines. This category aims to cover local and international information websites, but some specifically local websites may not be covered.
nudity	Websites that discuss and promote nudism, and other non-pornographic websites on which human nudity is the main topic, generally in the form of a documentary or an art. This category does not include websites that fall under the category porn (Erotic content and pornography).
occult (Occult and supernatural)	Websites that discuss and promote supernatural occult or "magic" practices such as witchcraft, voodoo, Satanism, etc. This category does not include websites that fall under astrology and religion (Religious and sectarian proselytizing).
onlinedating (Dating websites)	Sites that promote networking for interpersonal relationships such as dating and marriage. This category includes sites for match-making, online dating, spousal introduction, escort services, either paid or free. As most popular social media can be used as online dating websites, some such as Facebook are also detected under this category.
onlinepay (Online payment)	Sites that offer online payment or money transfers. This category includes popular payment websites such as *PayPal* and *Moneybookers*. It also heuristically includes pages on websites that request credit card information, which makes it possible to detect hidden, unknown or illegal online stores.
onlineshop (Online shopping)	Sites for online shopping, catalogues, online sales, auctions or classified ads.

New URL category	Description
pets	Websites that sell pets and accessories for pets, or which provide information and discussion forums on owning and caring for pets.
pharmacy (Pharmaceuticals)	Websites that offer medical information on pharmaceuticals, or which offer medical advice and sell pharmaceuticals.
phishing	Sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials.
photosonline (Images and photos)	Sites that host digital photographs and images, online photo albums and digital photo exchanges.
piracy (Software and hacked content)	Websites that promote or offer content for distribution without the consent of the copyright owner.
porn (Erotic content and pornography)	Sites that share erotic content and pornography. Includes subscription websites and free websites that provide images, stories and videos, and also covers pornographic content on mixed-content websites.
portals	Sites that aggregate information from multiple sources and various domains and which generally offer features such as search engines, electronic mail, news and to information on leisure activities.
privateipaddress (Private IP addresses)	Sites that are private IP addresses as defined in RFC 1918, i.e., hosts that do not require access to hosts in other organizations (or require just limited access).
pua (Potentially undesirable applications)	Sites that host potentially undesirable applications, often installed and used by third parties for malicious purposes without the user's consent. This category includes software programs such as web proxies or socks proxies, remote administration tools, location tracking tools, etc.
radiomusic (Radio and music websites)	Sites that offer online music streaming services: from online radio stations to websites that provide on-demand audio content (free or paid).
realestate	Websites that offer the sale and rent of real estate properties such as real estate agencies.
religion (Religious and sectarian proselytizing)	Sites that promote a religion or sect. This category also includes discussion forums linked to one or more religions.
searchengines	Sites enabling the searching of the Web, newsgroups, images, directories, and other online content. This category includes portal and directory websites such as white pages/yellow pages.
sextoys (Erotic gadgets)	Websites that offer the sale of erotic products and accessories.
sexualcontent (Other sexual content)	Websites with sexual content that do not correspond to any other category that deals with eroticism or pornography.

New URL category	Description
sexualeducation	Websites offering content intended for sex education, and which is not of a pornographic nature.
socialnetworks	Sites that enable social networking for online communities of various topics, for friendship, dating, or professional reasons. Specialized social media as *YouTube* are listed in the videos (Video/photo) category.
society (NGOs or political parties)	Websites dedicated to specific social functions such as NGOs, political parties, etc.
spam (Sites referenced as spam)	Sites that have been promoted through spam techniques.
sports	Sites relating to sports teams, fan clubs, scores and sports news. This category includes sports that are practiced on a professional or recreational basis.
suicide	Websites that promote suicide. This category does not include suicide prevention clinics.
tabloids (Sensational media)	Soft porn and celebrity gossip websites. Many information websites that publish such content may have sub-categories listed under this category via heuristic detection.
timewasters	Websites on which users tend to spend a lot of time. These may be websites belonging to other categories such as social media, entertainment websites, etc.
tobacco	Websites that sell or advertise tobacco products, or which encourage smoking.
travel	Sites that provide travel and tourism information or online booking or travel services such as airlines, accommodations, car rentals.
unknown	Resources on a website required for it to be displayed properly (images, css, js, etc.) or uncategorized websites.
untrusted (Compromised URLs)	Compromised URLs with particular features, which give the impression that they are not reliable.
videos (Videos/photos)	Sites that host videos or photos downloaded by users or provided by various content providers (e.g., *Youtube*, *Metacafe*, *Google Video*, *Picasa* or *Flickr*). This category also includes videos embedded on other websites and blogs.
weapons	Sites that depict, sell, review or describe guns and weapons, including for sport.
webmail (Online messaging)	Sites that enables users to send and receive email through a web-accessible email.
webproxy (Anonymizers and proxies)	Sites and proxy servers that act as an intermediary to enable browsing other sites anonymously, spoofing an address, bypassing web filtering and attempting to access forbidden content.

Former EWC URL categories that are exact matches of new categories

Former URL category	New URL category	Description of the new URL category
Advertisements & Pop-Ups	ads (Advertisements and ad content)	Sites that provide advertising graphics or other ad content files that appear on Web pages.
Alcohol & Tobacco	alcohol tobacco	alcohol: Sites that offer the sale of alcoholic products, or which contain information on alcoholic products, such as alcohol brands. tobacco: Websites that sell or advertise tobacco products, or which encourage smoking.
Anonymizers	webproxy (Anonymizers and proxies)	Sites and proxy servers that act as an intermediary to enable browsing other sites anonymously, spoofing an address, bypassing web filtering and attempting to access forbidden content.
Botnets	malware (Malicious software)	Sites that contain or provide malicious software in the form of executable files, vulnerability exploitation tools, JavaScript or any other malicious programs.
Business	business (Business activity)	Sites that obtain sales information such as corporate websites, that help organizations of all sizes to conduct their daily business activity.
Compromised	untrusted (Compromised URLs)	Compromised URLs with particular features, which give the impression that they are not reliable.
Computers & Technology	computersandsoftware (Software download websites)	Sites that contain downloadable software, whether shareware, freeware, or for a charge. This category may also cover some online app stores.
Dating & Personals	onlinedating (Dating websites)	Sites that promote networking for interpersonal relationships such as dating and marriage. This category includes sites for match-making, online dating, spousal introduction, escort services, either paid or free. As most popular social media can be used as online dating websites, some such as Facebook are also detected under this category.
Education	education (Teaching and learning)	Sites sponsored by educational institutions and schools of all types including distance education. This category includes educational and reference materials, such as dictionaries, encyclopedias, online courses, teaching aids and discussion guides.
Entertainment	entertainment	Sites containing programming guides to television, movies, music and video (including video on demand), celebrity sites, and entertainment news.

Former URL category	New URL category	Description of the new URL category
Fashion & Beauty	lifestyle (Fashion, beauty and lifestyles)	Sites devoted to fashion, beauty products and tattoos.
Finance	financial	Sites related to banking, finance, payment or investment, including banks, brokerages, online stock trading, stock quotes, fund management, insurance companies, credit unions, credit card companies, and so on. Some local banks may not be covered by this category.
Gambling	gambling (Online betting and gambling)	Sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance. In general, such websites require users to pay before they can start placing bets. While some of these websites are legitimate (prizes and jackpots can be won), others are fraudulent (no chances of winning anything). This category includes websites that provide tips and tricks that describe effective methods to earn money from gambling, as well as online lottery websites.
Games	games (Computer games and consoles)	Websites that provide, promote or sell games, including online games, computer games and board games, either for free or with a subscription. This category also includes game discussion forums, guides, cheats, etc.
General	misc (Miscellaneous)	Websites that do not present any danger, but which may have been classified under one or several other categories.
Government	government (Government departments or agencies)	Sites run by governmental or military organizations, departments, embassies or agencies, including police departments, fire departments, customs bureaus, emergency services, civil defense, counterterrorism organizations and hospitals.
Hacking	hacking	Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information, perpetrating fraud, creating viruses, or committing other illegal activity related to theft of digital inform.
Hate & Intolerance	hate (Hate, racism and discrimination)	Sites that promote any form of supremacy (political, religious, racial, etc.). This category includes websites that encourage oppression of people or groups of people based on their race, religion, gender, age, disability, sexual orientation or nationality. It also includes websites belonging to terrorist organizations and websites discussing aggressive sports and/or promoting violence.
Health & Medicine	health (Health care)	Sites that contain information relating to healthcare institutions, and preventing and treating illnesses. Websites that offer information or products for weight loss, dieting, steroids, anabolic products or human growth hormones, as well as information on aesthetic surgery.

Former URL category	New URL category	Description of the new URL category
Illegal Drug	narcotics (Drugs and narcotics)	Sites with information on the purchase, manufacture, and use of illegal or recreational drugs and their paraphernalia, and misuse of prescription drugs and other compounds. This category contains the categories marijuana (Marijuana and derived products) and narcoticsgeneral (Drugs other than marijuana).
Illegal Software	piracy (Software and hacked content)	Websites that promote or offer content for distribution without the consent of the copyright owner.
Image Sharing	photosonline (Images and photos)	Sites that host digital photographs and images, online photo albums and digital photo exchanges.
Job Search	jobsearch	Sites containing job listings, career information, assistance with job searches (such as resume writing, interview tips, etc.). This category includes job offer aggregators, but does not contain recruitment agencies or the career pages of corporate websites.
Leisure & Recreation	hobbies	Sites that offer information relating to leisure activities and pastimes such as collecting, art and crafts, etc.
Malware	malware (Malicious software)	Sites that contain or provide malicious software in the form of executable files, vulnerability exploitation tools, JavaScript or any other malicious programs.
News	news	Sites covering news and current events such as newspapers, newswire services, personalized news services, broadcasting sites, and magazines. This category aims to cover local and international information websites, but some specifically local websites may not be covered.
Personal Sites	blogs (Personal websites)	Sites about individuals, either hosted by them or by commercial websites (such as *Blogger*, AOL, etc.).
Phishing & Fraud	phishing fraud (Fraudulent websites)	phishing: Sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials. fraud: Known fraudulent websites that aim to obtain information, payments and credentials from users through false declarations or fraudulent means. For example, online stores that offer very low prices for popular products that will never be sent. This category does not include phishing websites.
Pornography/Sexually Explicit	porn (Erotic content and pornography)	Sites that share erotic content and pornography. Includes subscription websites and free websites that provide images, stories and videos, and also covers pornographic content on mixed-content websites.
Private IP Addresses	privateipaddress (Private IP addresses)	Sites that are private IP addresses as defined in RFC 1918, i.e., hosts that do not require access to hosts in other organizations (or require just limited access).

Former URL category	New URL category	Description of the new URL category
Real Estate	realestate	Websites that offer the sale and rent of real estate properties such as real estate agencies.
Restaurants & Dining	food	Sites with content relating to food and non-alcoholic beverages, such as recipes, ingredients, amount of calories, etc.
Search Engines & Portals	searchengines portals	searchengines: Sites enabling the searching of the Web, newsgroups, images, directories, and other online content. This category includes portal and directory websites such as white pages/yellow pages. portals: Sites that aggregate information from multiple sources and various domains and which generally offer features such as search engines, electronic mail, news and to information on leisure activities.
Sex Education	sexualeducation	Websites offering content intended for sex education, and which is not of a pornographic nature.
Shopping	onlineshop (Online shopping)	Sites for online shopping, catalogues, online sales, auctions or classified ads.
Social Networking	socialnetworks	Sites that enable social networking for online communities of various topics, for friendship, dating, or professional reasons. Specialized social media as *YouTube* are listed in the videos (Video/photo) category.
Spam Sites	spam (Sites referenced as spam)	Sites that have been promoted through spam techniques.
Sports	sports	Sites relating to sports teams, fan clubs, scores and sports news. This category includes sports that are practiced on a professional or recreational basis.
Tasteless	timewasters	Websites on which users tend to spend a lot of time. These may be websites belonging to other categories such as social media, entertainment websites, etc.
Transportation	auto (Motorized vehicles)	Sites containing information on motorized road vehicles such as cars, motorcycles, go-karts, etc.
Travel	travel	Sites that provide travel and tourism information or online booking or travel services such as airlines, accommodations, car rentals.
Unknown	unknown	Resources on a website required for it to be displayed properly (images, css, js, etc.) or uncategorized websites.
Weapons	weapons	Sites that depict, sell, review or describe guns and weapons, including for sport.
Web-based Email	webmail (Online messaging)	Sites that enables users to send and receive email through a web-accessible email.

Former EWC URL categories that partially match new categories

Former URL category	New URL category	Description of the new URL category
Arts	entertainment	Sites containing programming guides to television, movies, music and video (including video on demand), celebrity sites, and entertainment news.
Chat	im (Instant messaging/chat)	Instant messaging and chat websites that allow users to chat in real time (such as ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, etc.). This category also includes yahoo.com and gmail.com, which both embed instant messaging services.
Child Abuse images	illegalactivities (Illegal activities)	Sites with content that would be considered illegal in most countries, including, for example, content relating to the sexual exploitation of minors. This category does not include computer hacking or narcotics.
Criminal Activity	illegal (Illegal software activities)	Sites relating to software piracy and associated forums, that illegally distribute or help to distribute copyrighted content and software, pirated software, key generators and serial numbers to facilitate the illegal use of software programs. Some of these websites may also be detected as pornographic or relating to alcohol/cigarettes if they publish ads in these industries to earn money.
Cults	religion (Religious and sectarian proselytizing)	Sites that promote a religion or sect. This category also includes discussion forums linked to one or more religions.
Download sites	filesharing (Peer-to-Peer)	Sites that enable files to be directly exchanged and downloaded between users without dependence on a central server. This category also includes some torrent sharing websites and torrent trackers.
Forums & Newsgroups	advice (Forums, discussion groups and FAQs)	Sites for sharing information in the form of forums, discussion groups and FAQ websites on which users chat and receive answers to the questions that they ask. This category does not include the specific sections of corporate websites on which customer queries are answered (FAQ).
Information Security	computersandsoftware (Software download websites)	Sites that contain downloadable software, whether shareware, freeware, or for a charge. This category may also cover some online app stores.
Instant messaging	im (Instant messaging/chat)	Instant messaging and chat websites that allow users to chat in real time (such as ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, etc.). This category also includes yahoo.com and gmail.com, which both embed instant messaging services.
Non-profits & NGOs	society (NGOs or political parties)	Websites dedicated to specific social functions such as NGOs, political parties, etc.

Former URL category	New URL category	Description of the new URL category
Nudity	maturecontent (Content for adults only)	Sites targeting an adult audience. This category includes a wide array of websites, ranging from the Kama Sutra, sex education websites to hardcore porn. It groups the categories lingerie (Lingerie and swimwear), nudity, sextoys (Erotic gadgets), sexualeducation and sexualcontent (Other sexual content).
Peer-to-peer	filesharing (Peer-to-Peer)	Sites that enable files to be directly exchanged and downloaded between users without dependence on a central server. This category also includes some torrent sharing websites and torrent trackers.
Politics	society (NGOs or political parties)	Websites dedicated to specific social functions such as NGOs, political parties, etc.
Religion	religion (Religious and sectarian proselytizing)	Sites that promote a religion or sect. This category also includes discussion forums linked to one or more religions.
Streaming Media & Downloads	videos (Videos/photos) radiomusic (Radio and music websites)	videos: Sites that host videos or photos downloaded by users or provided by various content providers (e.g., *Youtube*, *Metacafe*, *Google Video*, *Picasa* or *Flickr*). This category also includes videos embedded on other websites and blogs. radiomusic: Sites that offer online music streaming services: from online radio stations to websites that provide on-demand audio content (free or paid).
Translators	education (Teaching and learning)	Sites sponsored by educational institutions and schools of all types including distance education. This category includes educational and reference materials, such as dictionaries, encyclopedias, online courses, teaching aids and discussion guides.

Former EWC URL categories without any equivalence with new categories

Former URL category	New URL category
Greeting cards	No matching category
Network Errors	No matching category
Parked Domains	No matching category
School Cheating	No matching category
Violence	No matching category

New EWC URL categories without any equivalence with former categories

New URL category	Description of the new URL category
astrology	Sites that promote, provide or share information on beliefs relating to astrology such as horoscopes, zodiac signs, etc. This category also includes similar beliefs not related to astrology, such as numerology, fortune telling, etc., but does not include organized religions or cults.
c&c (Malware command and control websites)	Websites that generally exploit malware already installed on the user's host. A malware download may sometimes be in progress when the user connects to the website, if the site both hosts and exploits the malware.
homograph (Homographic websites)	Websites with domain names that visually resemble legitimate domain names, but which use different character sets, such as Cyrillic characters that match Latin characters, e.g., 'a', 'p' and 'e'. Although these domain names are visually identical to the original domain names, they are generally used for malicious purposes.
hosting (Website hosting)	Free or commercial website hosting services that allow individuals or organizations to create and publish websites.
illegalactivities (Illegal activities)	Sites with content that would be considered illegal in most countries, including, for example, content relating to the sexual exploitation of minors. This category does not include computer hacking or narcotics.
kids (Children's websites)	SItes designed for use by children, with content such as children's stories, games and media.
lingerie (Lingerie and swimwear)	Sites that promote or sell lingerie, undergarments and bathing suits.
malware-hd (Probable malicious software)	Sites that are deemed to potentially contain or provide malicious software, but may also not contain any. As this status is stricter than the "Malware" status, it may generate false positives. For a strict inspection, this status should raise an alert on websites. For a normal inspection, this status can be ignored.
marijuana (Marijuana and derived products)	Sites that sell marijuana and associated products, as well as sites that provide information and forums on growing marijuana and its effects.
miners (Cryptocurrency miners)	Sites that attempt to mine cryptocurrency in the user's web browser by using the computer's resources. In general, such sites hide this from the user, but may sometimes inform the user.
narcoticsgeneral (Drugs other than marijuana)	Sites that offer information on illegal narcotics other than marijuana (which is included in the category marijuana [Marijuana and derived products]) This category also includes websites that explain the ingredients, use and manufacture of drugs, or which offer them for sale or exchange.

New URL category	Description of the new URL category
nudity	Websites that discuss and promote nudism, and other non-pornographic websites on which human nudity is the main topic, generally in the form of a documentary or an art. This category does not include websites that fall under the category porn (Erotic content and pornography).
occult (Occult and supernatural)	Websites that discuss and promote supernatural occult or "magic" practices such as witchcraft, voodoo, Satanism, etc. This category does not include websites that fall under astrology and religion (Religious and sectarian proselytizing).
onlinepay (Online payment)	Sites that offer online payment or money transfers. This category includes popular payment websites such as *PayPal* and *Moneybookers*. It also heuristically includes pages on websites that request credit card information, which makes it possible to detect hidden, unknown or illegal online stores.
pets	Websites that sell pets and accessories for pets, or which provide information and discussion forums on owning and caring for pets.
pharmacy (Pharmaceuticals)	Websites that offer medical information on pharmaceuticals, or which offer medical advice and sell pharmaceuticals.
pua (Potentially undesirable applications)	Sites that host potentially undesirable applications, often installed and used by third parties for malicious purposes without the user's consent. This category includes software programs such as web proxies or socks proxies, remote administration tools, location tracking tools, etc.
sextoys (Erotic gadgets)	Websites that offer the sale of erotic products and accessories.
sexualcontent (Other sexual content)	Websites with sexual content that do not correspond to any other category that deals with eroticism or pornography.
suicide	Websites that promote suicide. This category does not include suicide prevention clinics.
tabloids (Sensational media)	Soft porn and celebrity gossip websites. Many information websites that publish such content may have sub-categories listed under this category via heuristic detection.

Recommended URL/SSL filter profiles

Policy section	Description	URL categories			Recommended operations	
		"permissive" profile	"standard" profile	"restrictive" profile	URL filtering	SSL filtering
1 - Compromised URLs	Category that groups malicious URLs, and which Stormshield's security teams continuously update.	compromised_urls			Block	Block without decrypting
2 - Always block	Illegal, dangerous and violent content	phishing malware untrusted fraud spam pua miner c&c homograph drugs hacking hate illegal illegalactivities narcotics narcoticsgeneral marijuana maturecontent piracy porn sexualcontent suicide weapons	"permissive" + profile malware-hd gambling nudity sextoys sexualeducation onlinedating occult	"standard" + profile tabloids timewasters alcohol tobacco webproxy ads im lingerie games astrology filesharing travel religion hobbies entertainment	Block	Block without decrypting

Policy section	Description	URL categories			Recommended operations	
		"permissive" profile	"standard" profile	"restrictive" profile	URL filtering	SSL filtering
3 - Always pass, never decrypt (GDPR)	Content that requires the protection of user data (banking, healthcare, etc.)	pharmacy health financial webmail portals	pharmacy health financial webmail		Pass	Pass without decrypting
4 - Always pass, can be decrypted	Content relating to the organization's business sector and which users require for work	privateipaddress searchengines government education business + according to business sector (examples): auto news food travel ...	privateipaddress searchengines government business	privateipaddress	Pass	Decrypt
5 - Block recommended	Content that should be blocked, but without preventing users from visiting websites that fall under "Always pass" sections	alcohol tobacco malware-hd gambling nudity sextoys timewasters webproxy sexualeducation onlinedating occult	tabloids timewasters alcohol tobacco webproxy ads im lingerie games astrology filesharing travel religion hobbies entertainment		Block	Block without decrypting

Policy section	Description	URL categories			Recommended operations	
		"permissive" profile	"standard" profile	"restrictive" profile	URL filtering	SSL filtering
6 - Pass recommended	Content that should be allowed, so that users are not prevented from browsing the Internet. Some categories can also be allowed only during specific time slots (social media during lunch break, for example).	unknown misc computerandsoftware hosting videos advice blogs tabloids ads socialnetworks society sports realestate	unknown misc computerandsoftware hosting	unknown misc computerandsoftware hosting government searchengines business	Pass	Decrypt
7 - Pass (Any)	Action applied to any website that has not been categorized by previous rules	Any	Any	Any	Pass except for the "restrictive" profile: Block	Decrypt except for the "restrictive" profile: Block without decrypting

Policy section	Description	URL categories			Recommended operations	
		"permissive" profile	"standard" profile	"restrictive" profile	URL filtering	SSL filtering
-	Other available categories	astrology entertainment filesharing travel games hobbies im jobsearch kids lifestyle lingerie onlinepay photosonline onlineshop pets radiomusic religion	advice blogs auto food education news jobsearch kids lifestyle onlinepay photosonline onlineshop pets portals radiomusic realestate socialnetworks society sports videos	advice blogs auto food education news jobsearch kids lifestyle onlinepay photosonline onlineshop pets portals radiomusic realestate socialnetworks society sports videos pharmacy health financial webmail	-	-

Further reading

Additional information and answers to questions you may have are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu