==> Conceptos Teóricos Breves:

→ '**URL Filtering**' posee 2 características importantes para los administradores de redes:

→↘ Control de los recursos web que los usuarios pueden tener acceso basados en categorías o listas específicas: '**White List**' o '**Black List**'.

→↘ Capa adicional de seguridad para prevenir que el usuario utilice sitios maliciosos.

↘↘==> URL Filtering → Flavours:

→ Local.
→ Websense Redirect.
→ Surfcontrol (Websense).
→ 'Websense Enhanced'. ← Configuraremos este tipo.

↘↘==> Configuración de URL Filtering con un perfil por defecto.

→ Respaldar Configuración Inicial → 'rescue' y 'autorecovery':

root@juniper-01> request system autorecovery state save
Saving config recovery information
Saving license recovery information
Saving BSD label recovery information

root@juniper-01> request system configuration rescue save

→ Establecer perfil → 'junos-wf-enhanced-default':

root@juniper-01# set security utm utm-policy **UTM-BASICA** web-filtering http-profile junos-wf-enhanced-default

root@juniper-01# show security utm utm-policy **UTM-BASICA**
anti-virus {
    http-profile **SOPHOS-PERFIL-01**;
    ftp {
        upload-profile **SOPHOS-PERFIL-01**;
        download-profile **SOPHOS-PERFIL-01**;
    }
}
web-filtering {

http-profile junos-wf-enhanced-default;
}

→ Definimos políticas entre ZONAS:
ZONA 'Internal':

root@juniper-01# edit security policies from-zone Internal to-zone Internet policy **INTERNAL-OUTBOUND**

[edit security policies from-zone Internal to-zone Internet policy **INTERNAL-OUTBOUND**]

root@juniper-01# set match source-address any destination-address any application [junos-http junos-ftp]

[edit security policies from-zone Internal to-zone Internet policy **INTERNAL-OUTBOUND**]

root@juniper-01# set then permit application-services utm-policy **UTM-BASICA**

[edit security policies from-zone Internal to-zone Internet policy **INTERNAL-OUTBOUND**]

root@juniper-01# set then log session-close

[edit security policies from-zone Internal to-zone Internet policy **INTERNAL-OUTBOUND**]

```
root@juniper-01# show
match {
    source-address any;
    destination-address any;
    application [ junos-http junos-ftp ];
}
then {
    permit {
        application-services {
            utm-policy UTM-BASICA;
        }
    }
    log {
        session-close;
    }
}
```

ZONA 'OFICINA-100':

root@juniper-01# edit security policies from-zone OFICINA-100 to-zone Internet policy **OFICINA-100-OUTBOUND**

[edit security policies from-zone **OFICINA-100** to-zone Internet policy **OFICINA-100-OUTBOUND**]

root@juniper-01# set match source-address any destination-address any application [junos-http junos-ftp]

[edit security policies from-zone **OFICINA-100** to-zone Internet policy **OFICINA-100-OUTBOUND**]

root@juniper-01# set then permit application-services utm-policy **UTM-BASICA**

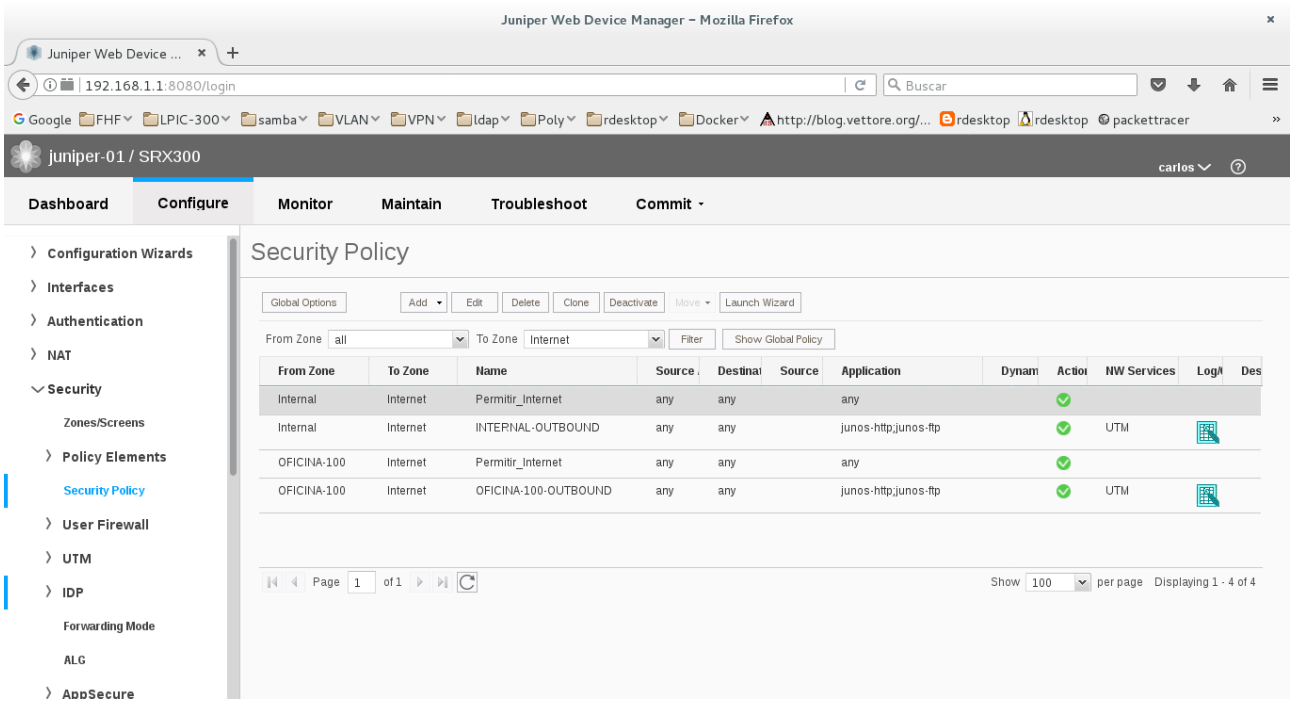
[edit security policies from-zone **OFICINA-100** to-zone Internet policy OFICINA-100-OUTBOUND]

root@juniper-01# set then log session-close

[edit security policies from-zone **OFICINA-100** to-zone Internet policy **OFICINA-100-OUTBOUND**]

root@juniper-01# show

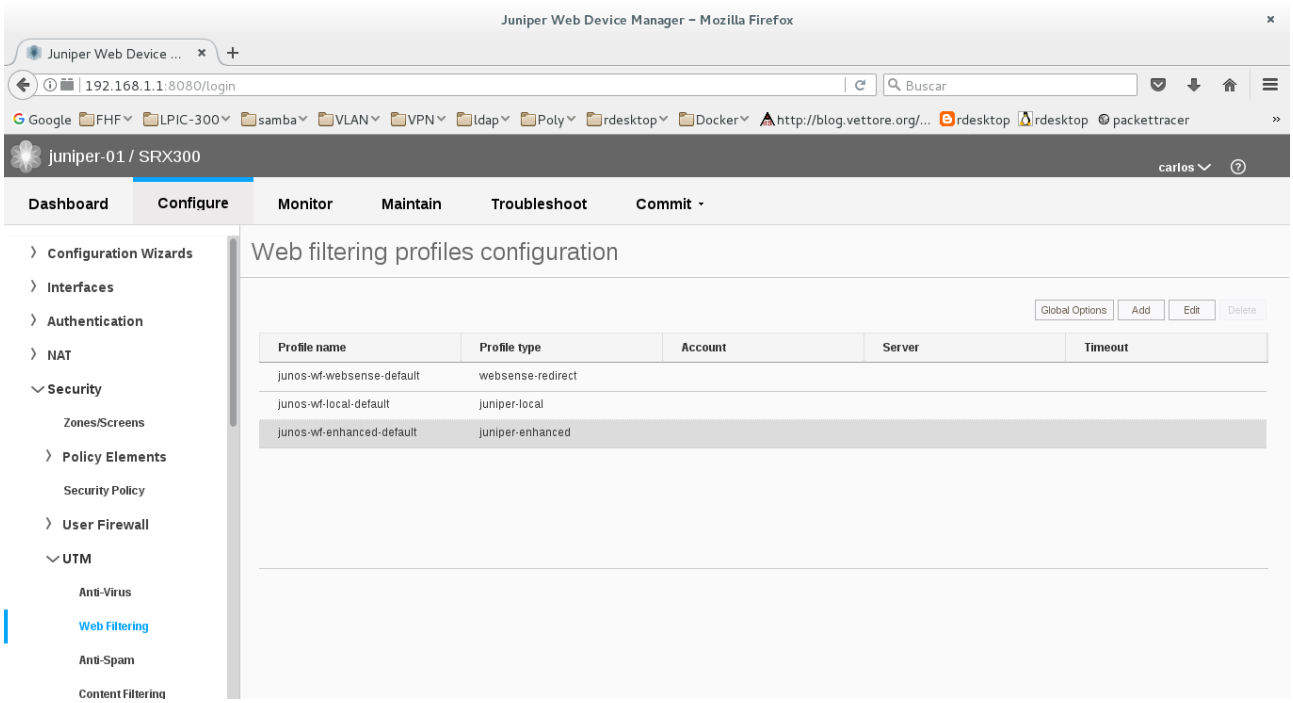
```
match {
    source-address any;
    destination-address any;
    application [ junos-http junos-ftp ];
}
then {
    permit {
        application-services {
            utm-policy UTM-BASICA;
        }
    }
    log {
        session-close;
    }
}
```



==> 'Websense Enhanced Filtering' -perfil por defecto-:

↘ Conceptos Teóricos Breves:

→ Cache:
→ Server: Permite definir diferentes servidores de búsqueda en cloud.
→ Profile:
    → Block Message:
→ Category:
→ Custom Block Message:
→ Default:
→ No-Safe-Search:
→ Site Reputation Action:
→ Timeout:
→ Fallback Settings:



→ Comprobamos Uso de Licencia:

root@juniper-01# run show system license
License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
anti_spam_key_sbl	0	1	0	2018-05-25 02:00:00 CEST
idp-sig	0	1	0	2018-05-25 02:00:00 CEST
dynamic-vpn	0	2	0	permanent
av_key_sophos_engine	**1**	**1**	**0**	**2018-05-25 02:00:00 CEST**
wf_key_websense_ewf	**0**	**1**	**0**	**2018-05-25 02:00:00 CEST**
remote-access-ipsec-vpn-client	0	2	0	permanent

→ Parámetros Generales de 'web-filtering':

root@juniper-01# set security utm feature-profile web-filtering type juniper-enhanced
root@juniper-01# set security utm feature-profile web-filtering juniper-enhanced cache timeout 1800
root@juniper-01# set security utm feature-profile web-filtering juniper-enhanced cache size **1500**
root@juniper-01# set security utm application-proxy traceoptions flag all

→ Parámetros → 'host cloud':

root@juniper-01# set security utm feature-profile web-filtering juniper-enhanced server host **rp.cloud.threatseeker.com**
root@juniper-01# set security utm feature-profile web-filtering juniper-enhanced server port **80**

→ Categorias Añadidas:

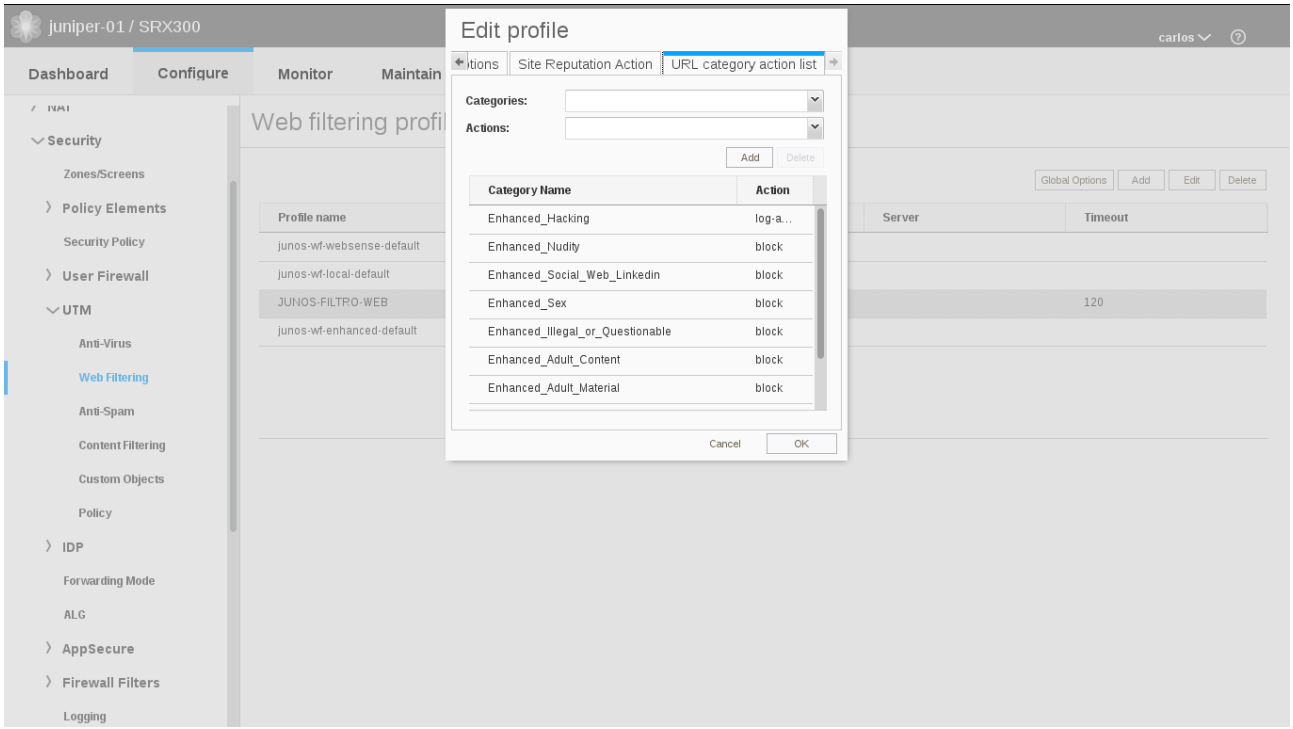
root@juniper-01# set security utm feature-profile web-filtering juniper-enhanced profile **JUNOS-FILTRO-WEB** category Enhanced_Hacking action log-and-permit

root@juniper-01# edit security utm feature-profile web-filtering juniper-enhanced profile **JUNOS-FILTRO-WEB**

[edit security utm feature-profile web-filtering juniper-enhanced profile **JUNOS-FILTRO-WEB**]
[edit security utm feature-profile web-filtering juniper-enhanced profile **JUNOS-FILTRO-WEB**]
root@juniper-01# set category Enhanced_Illegal_or_Questionable action block

[edit security utm feature-profile web-filtering juniper-enhanced profile JUNOS-FILTRO-WEB]
…

Mejor indicar las categorias a través de J-Web, ...



→ Configurar Acción de Reputación de los Sitios.

root@juniper-01# edit security utm feature-profile web-filtering

[edit security utm feature-profile web-filtering]
root@juniper-01# set juniper-enhanced profile **JUNOS-FILTRO-WEB** site-reputation-action **very-safe permit**

[edit security utm feature-profile web-filtering]
root@juniper-01# set juniper-enhanced profile **JUNOS-FILTRO-WEB** site-reputation-action **moderately-safe** log-and-permit

[edit security utm feature-profile web-filtering]
root@juniper-01# set juniper-enhanced profile **JUNOS-FILTRO-WEB** site-reputation-action **fairly-safe** log-and-permit

[edit security utm feature-profile web-filtering]
root@juniper-01# set juniper-enhanced profile **JUNOS-FILTRO-WEB** site-reputation-action **suspicious** log-and-permit

[edit security utm feature-profile web-filtering]
root@juniper-01# set juniper-enhanced profile JUNOS-FILTRO-WEB site-reputation-action **harmful** block

[edit security utm feature-profile web-filtering]
root@juniper-01# set juniper-enhanced profile **JUNOS-FILTRO-WEB** custom-block-message "**** **NO PERMITIDO - Bloqueo Juniper ****"

[edit security utm feature-profile web-filtering]
root@juniper-01# set juniper-enhanced profile **JUNOS-FILTRO-WEB** default log-and-permit

[edit security utm feature-profile web-filtering juniper-enhanced profile **JUNOS-FILTRO-WEB**]
root@juniper-01# set fallback-settings default log-and-permit

[edit security utm feature-profile web-filtering juniper-enhanced profile **JUNOS-FILTRO-WEB**]
root@juniper-01# set fallback-settings server-connectivity log-and-permit

[edit security utm feature-profile web-filtering juniper-enhanced profile **JUNOS-FILTRO-WEB**]
root@juniper-01# set fallback-settings timeout log-and-permit

[edit security utm feature-profile web-filtering juniper-enhanced profile **JUNOS-FILTRO-WEB**]
root@juniper-01# set fallback-settings too-many-requests log-and-permit

→ Aplicación de Políticas:

root@juniper-01# set security utm utm-policy **UTM-BASICA** web-filtering http-profile **JUNOS-FILTRO-WEB**

→ Comprobaciones:

root@juniper-01> show security utm web-filtering status
UTM web-filtering status:
Server status: Juniper Enhanced using Websense server **UP**

→ Opciones Troubleshooting:

root@juniper-01# set security utm traceoptions flag all
root@juniper-01# set security utm feature-profile web-filtering traceoptions flag all

→ Problemas:

root@juniper-01> ping rp.cloud.threatseeker.com
PING rp.cloud.threatseeker.com (85.115.52.140): 56 data bytes
64 bytes from 85.115.52.140: icmp_seq=0 ttl=52 time=85.504 ms
64 bytes from 85.115.52.140: icmp_seq=1 ttl=52 time=97.929 ms
64 bytes from 85.115.52.140: icmp_seq=2 ttl=52 time=87.935 ms

--- rp.cloud.threatseeker.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 85.504/90.456/97.929/5.377 ms

root@juniper-01> show security utm web-filtering status
UTM web-filtering status:
Server status: Juniper Enhanced using Websense server **UP**

==> Comprobación de Uso de Licencias:

root@juniper-01# run show system license
License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
anti_spam_key_sbl	0	1	0	2018-05-25 02:00:00 CEST
idp-sig	0	1	0	2018-05-25 02:00:00 CEST
dynamic-vpn	0	2	0	permanent
av_key_sophos_engine	**1**	**1**	**0**	**2018-05-25 02:00:00 CEST**
wf_key_websense_ewf	**1**	**1**	**0**	**2018-05-25 02:00:00 CEST**
remote-access-ipsec-vpn-client	0	2	0	permanent

→ Comprobar y salvar Configuración:

root@juniper-01# commit check
configuration check succeeds

root@juniper-01# commit
commit complete

→ Código:

root@juniper-01# show security utm feature-profile web-filtering

```
type juniper-enhanced;
traceoptions {
    flag all;
}
juniper-enhanced {
    cache {
        timeout 1800;
        size 1500;
    }
    server {
        host rp.cloud.threatseeker.com;
        port 80;
    }
    profile JUNOS-FILTRO-WEB {
        category {
            Enhanced_Hacking {
                action log-and-permit;
            }
            Enhanced_Nudity {
                action block;
            }
            Enhanced_Social_Web_Linkedin {
                action block;
            }
            Enhanced_Sex {
                action block;
            }
            Enhanced_Illegal_or_Questionable {
                action block;
            }
            Enhanced_Adult_Content {
                action block;
            }
            Enhanced_Adult_Material {
                action block;
            }
            Enhanced_Gay_or_Lesbian_or_Bisexual_Interest {
                action block;
```

```
            }
            Enhanced_Sex_Education {
                action block;
            }
        }
        site-reputation-action {
            very-safe permit;
            moderately-safe log-and-permit;
            fairly-safe log-and-permit;
            suspicious log-and-permit;
            harmful block;
        }
        default log-and-permit;
        custom-block-message "** NO PERMITIDO - Bloqueo Juniper **";
        fallback-settings {
            default log-and-permit;
            server-connectivity log-and-permit;
            timeout log-and-permit;
            too-many-requests log-and-permit;
        }
        timeout 120;
    }
}
```

[edit]

BIBLIOGRAFÍA Y DOCUMENTACIÓN:

→ **Juniper SRX Series. O'Reilly (Brad Woodberg & Rob Cameron) – Junio 2013.**
→ **http://www.juniper.net/documentation/en_US/junos12.1x46/topics/example/security-utm-enhanced-web-filtering-configuring.html**
→ **https://kb.juniper.net/InfoCenter/index?page=content&id=KB22483&actp=METADATA**