=> Conceptos Teóricos Breves:

Tecnología simple de filtrado del tráfico spam de entrada en el protocolo SMTP. Se basa simplemente en la reputación IP ofrecida a traves de 'Sophos Cloud'. Las opciones de configuración son simples.

==> Opciones de Configuración:

- ↘ → **Address Blacklist**: Lista de hosts bloqueados por la solución antispam.
- ↘ → **Address Whitelist**: Lista de hosts permitidos por la solución antispam.
- ↘ → **SBL**: Parte principal del perfil que definirá las acciones a adoptar.
  - → **Custom Tag String**: String que etiqueta la cabecera del emisor cuando se detecta spam, para marcarlo o eliminarlo. Puede ser configurado en el servidor antispam, o en la parte cliente.
  - → **NO / SBL Default Server**: Usar o no el Servidor '**Blacklist**', por defecto → **SI**.

  - → **Spam Action**: Acciones a realizar cuando se detecta spam. Pueden ser:
    - → Bloquear mensaje.
    - → Etiquetar cabecera SMTP.
    - → Etiquetar línea '**Subject**' del mensaje.

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

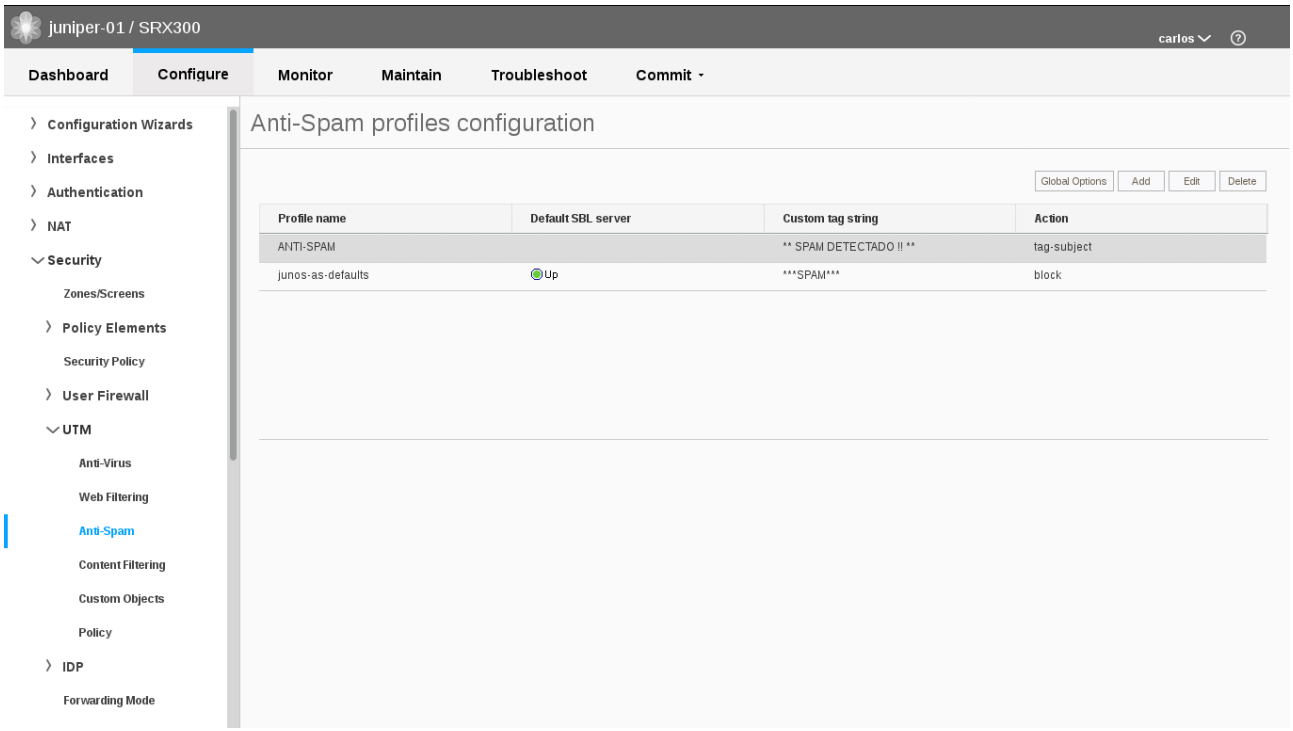
root@juniper-01> request system autorecovery state save
Saving config recovery information
Saving license recovery information
Saving BSD label recovery information

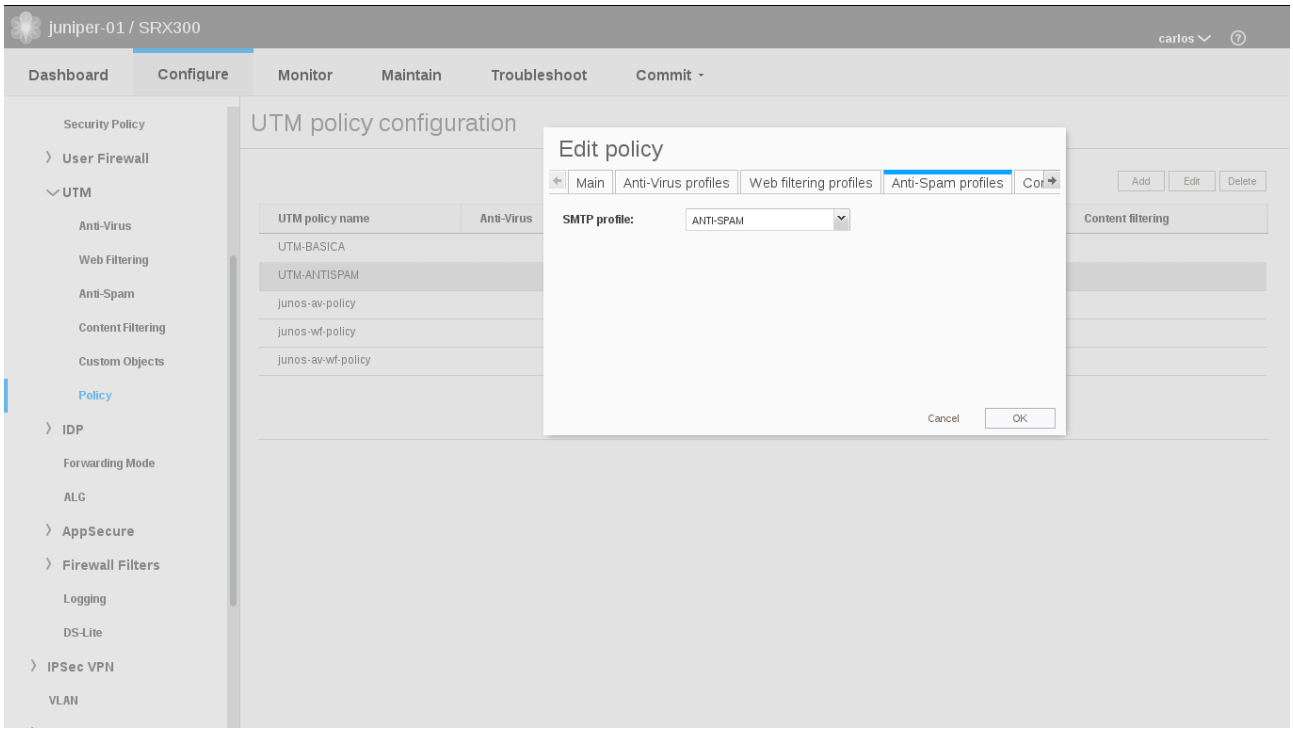
root@juniper-01> request system configuration rescue save

↘↘==> Configuración de 'Antispam con un Perfil Personalizado'.

root@juniper-01# set security utm feature-profile anti-spam sbl profile **ANTI-SPAM** custom-tag-string "**** SPAM DETECTADO !! ****" spam-action tag-subject

[edit security utm]
root@juniper-01# set utm-policy **UTM-ANTISPAM** anti-spam smtp-profile **ANTI-SPAM**


juniper-01 / SRX300
carlos
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Commit
Configuration Wizards
Interfaces
Authentication
NAT
Security
Zones/Screens
Policy Elements
Security Policy
User Firewall
UTM
Anti-Virus
Web Filtering
Anti-Spam
Content Filtering
Custom Objects
Policy
IDP
Forwarding Mode
Anti-Spam profiles configuration
Global Options
Add
Edit
Delete
Profile name
Default SBL server
Custom tag string
Action
ANTI-SPAM
** SPAM DETECTADO !! **
tag-subject
junos-as-defaults
Up
SPAM
block


juniper-01 / SRX300
carlos
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Commit
Security Policy
User Firewall
UTM
Anti-Virus
Web Filtering
Anti-Spam
Content Filtering
Custom Objects
Policy
IDP
Forwarding Mode
ALG
AppSecure
Firewall Filters
Logging
DS-Lite
IPSec VPN
VLAN
UTM policy configuration
Edit policy
Main
Anti-Virus profiles
Web filtering profiles
Anti-Spam profiles
SMTP profile:
ANTI-SPAM
Cancel
OK
Add
Edit
Delete
UTM policy name
Anti-Virus
Content filtering
UTM-BASICA
UTM-ANTISPAM
junos-av-policy
junos-wf-policy
junos-av-wf-policy

→ Zona 'Internet'→ 'Internal':

[edit]
root@juniper-01# set security policies from-zone **Internet** to-zone **Internal** policy **MAIL-INBOUND** match source-address any destination-address any application junos-smtp

[edit]
root@juniper-01# set security policies from-zone **Internet** to-zone **Internal** policy **MAIL-INBOUND** then permit application-services utm-policy **UTM-ANTISPAM**

[edit]
root@juniper-01# set security policies from-zone **Internet** to-zone **Internal** policy **MAIL-INBOUND** then log session-close

→ Zona 'Internet'→ 'OFICINA-100':

[edit]
root@juniper-01# set security policies from-zone **Internet** to-zone **OFICINA-100** policy **MAIL-INBOUND** match source-address any destination-address any application junos-smtp

[edit]
root@juniper-01# set security policies from-zone **Internet** to-zone **OFICINA-100** policy **MAIL-INBOUND** then permit application-services utm-policy UTM-ANTISPAM

[edit]
root@juniper-01# set security policies from-zone **Internet** to-zone **OFICINA-100** policy **MAIL-INBOUND** then log session-close

==> 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	**1**	**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 policies from-zone **Internet** to-zone **Internal**

```
policy MAIL-INBOUND {
    match {
        source-address any;
        destination-address any;
        application junos-smtp;
    }
    then {
        permit {
            application-services {
                utm-policy UTM-ANTISPAM;
            }
        }
        log {
            session-close;
        }
    }
}
```

root@juniper-01# show security policies from-zone **Internet** to-zone **OFICINA-100**

```
policy MAIL-INBOUND {
    match {
        source-address any;
        destination-address any;
        application junos-smtp;
    }
    then {
        permit {
            application-services {
                utm-policy UTM-ANTISPAM;
            }
        }
        log {
            session-close;
        }
    }
}
```

root@juniper-01# show security utm feature-profile anti-spam

```
sbl {
    profile ANTI-SPAM {
        spam-action tag-subject;
        custom-tag-string "** SPAM DETECTADO !! **";
    }
}
```

BIBLIOGRAFÍA Y DOCUMENTACIÓN:

→ **Juniper SRX Series. O'Reilly (Brad Woodberg & Rob Cameron) – Junio 2013.**