==> Conceptos Teóricos Breves:

→ **UTM** (Unified Threat Management) → **Gestión Unificada de Amenazas**.
→ **UTM** opera en la capa '**7**' del modelo OSI (**Aplicación**). ↘'(**APSTREF**)'.
→ Componentes de **UTM**:
- → Antivirus.
- → URL Filtering.
- → AntiSpam.
- → Content Filtering.

==> URI versus URL → (URI=URL+URN):

→ Concepto Fundamental en UTM's Sophos.
→ 'URI versus URL'.

https://es.wikipedia.org/wiki/Identificador_de_recursos_uniforme

==> Flavours Antivirus SRX:

- → Sophos. (Reino Unido).
- → Kaspersky Full. (Rusia).
- → Kasperskt Express. (Rusia).

==> 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

root@juniper-01# rollback ?
Possible completions:

<[Enter]>	Execute this command
0	2017-04-26 08:55:26 CEST by carlos via junoscript
1	2017-04-26 08:53:54 CEST by carlos via junoscript
...	
rescue	**2017-04-27 09:46:21 CEST by root via cli**

==> Comprobación de Licencias (Previamente Instaladas via 'J-Web/CLI'):

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	**0**	**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

Configuración Sophos AV.

→ Utiliza 2 técnicas de inspección de malware:

→ De hash tradicional.
→ Inspección de reputación por niveles chequeadas a traves de la URI.

→ Envio de mensajes codificados a '**Sophos Cloud**' a traves de DNS. Sophos responde analizando la **URI**.

→ Es importante acceder a '**Sophos Cloud**' para chequear reputación **URI**. Importante DNS y NTP.

A ==> Configuración de Sophos con un perfil por defecto:

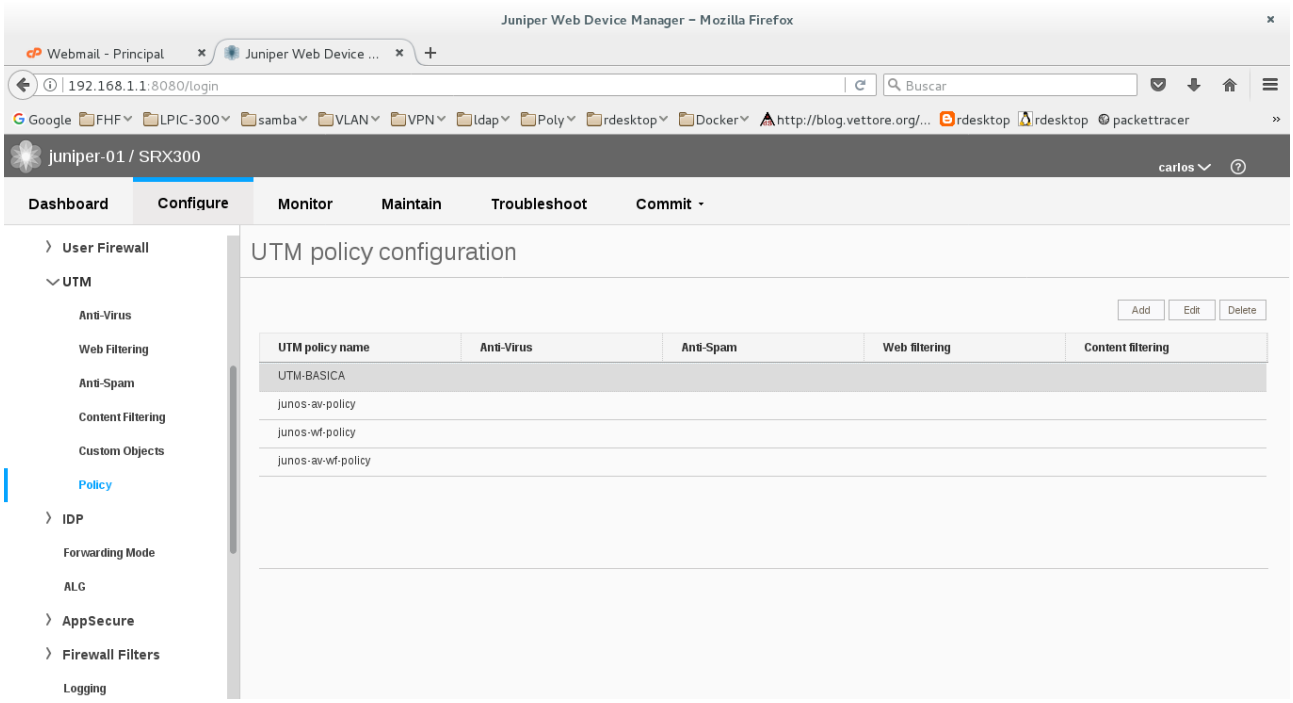
↘ Protocolos:

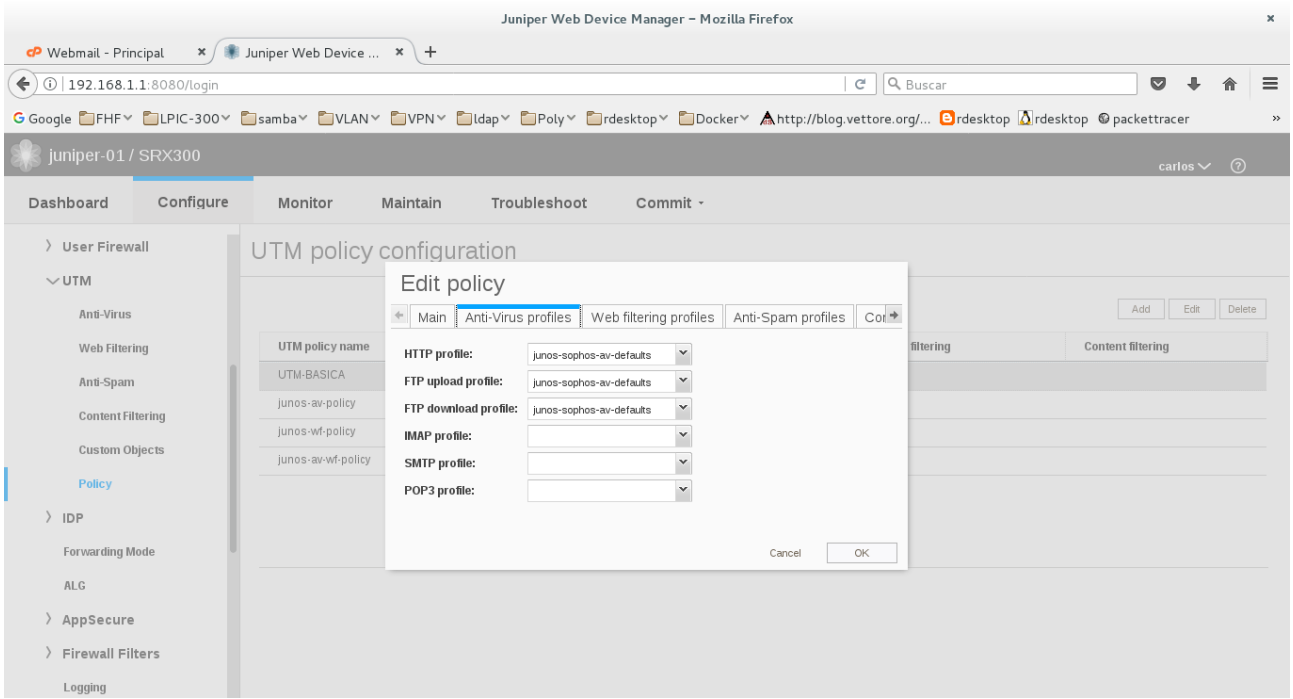
Utilizamos 'HTTP y FTP' (carga/descarga). Puertos 'TCP 80,20 y 21'.

root@juniper-01# set security utm utm-policy **UTM-BASICA** anti-virus **http-profile** junos-sophos-av-defaults **ftp** upload-profile junos-sophos-av-defaults download-profile junos-sophos-av-defaults

root@juniper-01# show security utm

```
utm-policy UTM-BASICA {
    anti-virus {
        http-profile junos-sophos-av-defaults;
        ftp {
            upload-profile junos-sophos-av-defaults;
            download-profile junos-sophos-av-defaults;
        }
    }
}
```


Juniper Web Device Manager – Mozilla Firefox
Webmail - Principal
Juniper Web Device ...
192.168.1.1:8080/login
Buscar
Google FHF LPIC-300 samba VLAN VPN ldap Poly rdesktop Docker http://blog.vettore.org/... rdesktop rdesktop packettracer
juniper-01 / SRX300
carlos
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Commit
User Firewall
UTM
Anti-Virus
Web Filtering
Anti-Spam
Content Filtering
Custom Objects
Policy
IDP
Forwarding Mode
ALG
AppSecure
Firewall Filters
Logging
UTM policy configuration
Add
Edit
Delete
UTM policy name
Anti-Virus
Anti-Spam
Web filtering
Content filtering
UTM-BASICA
junos-av-policy
junos-wf-policy
junos-av-wf-policy


Juniper Web Device Manager – Mozilla Firefox
Webmail - Principal
Juniper Web Device ...
192.168.1.1:8080/login
Buscar
Google FHF LPIC-300 samba VLAN VPN ldap Poly rdesktop Docker http://blog.vettore.org/... rdesktop rdesktop packettracer
juniper-01 / SRX300
carlos
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Commit
User Firewall
UTM
Anti-Virus
Web Filtering
Anti-Spam
Content Filtering
Custom Objects
Policy
IDP
Forwarding Mode
ALG
AppSecure
Firewall Filters
Logging
UTM policy configuration
Edit policy
Main
Anti-Virus profiles
Web filtering profiles
Anti-Spam profiles
HTTP profile:
junos-sophos-av-defaults
FTP upload profile:
junos-sophos-av-defaults
FTP download profile:
junos-sophos-av-defaults
IMAP profile:
SMTP profile:
POP3 profile:
Cancel
OK
Add
Edit
Delete
UTM policy name
Content filtering
UTM-BASICA
junos-av-policy
junos-wf-policy
junos-av-wf-policy

↘ Red 'Internal':

root@juniper-01# 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]
root@juniper-01# set then permit application-services utm-policy **UTM-BASICA**
root@juniper-01# set then log session-close
root@juniper-01# show

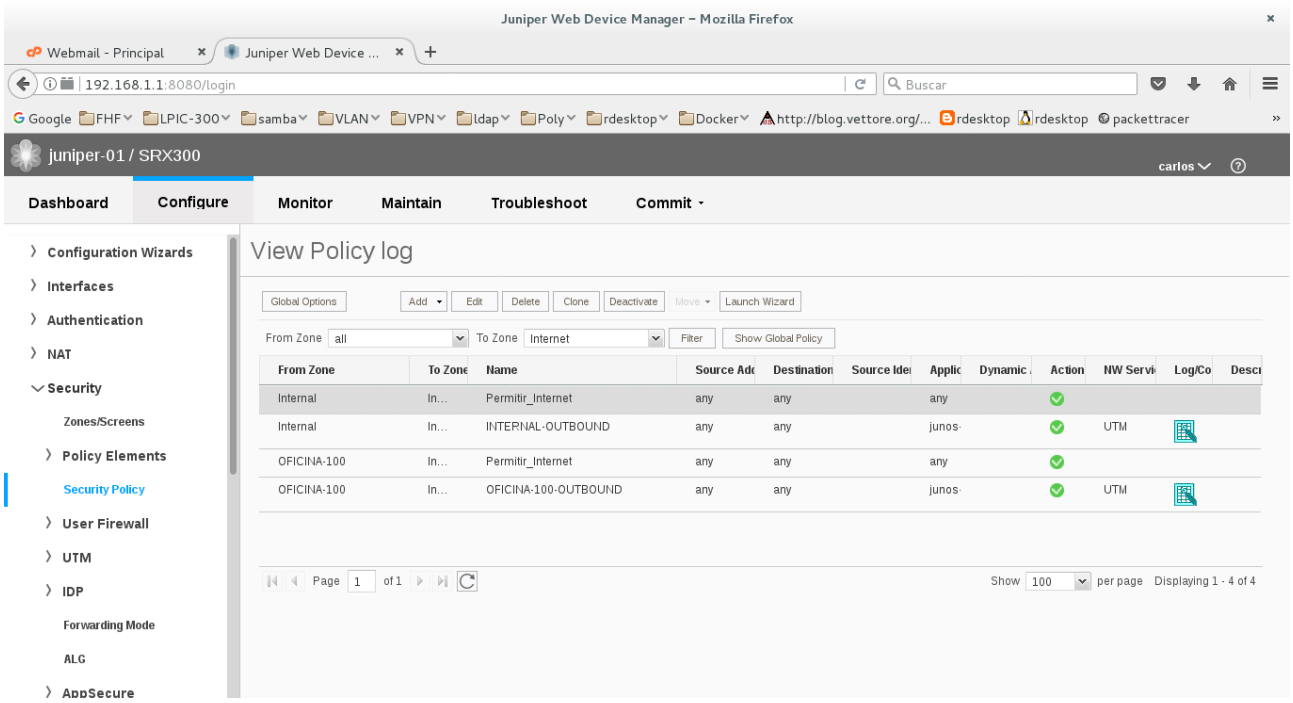
```
match {
    source-address any;
    destination-address any;
    application [ junos-http junos-ftp ];
}
then {
    permit {
        application-services {
            utm-policy UTM-BASICA;
        }
    }
    log {
        session-close;
    }
}
```

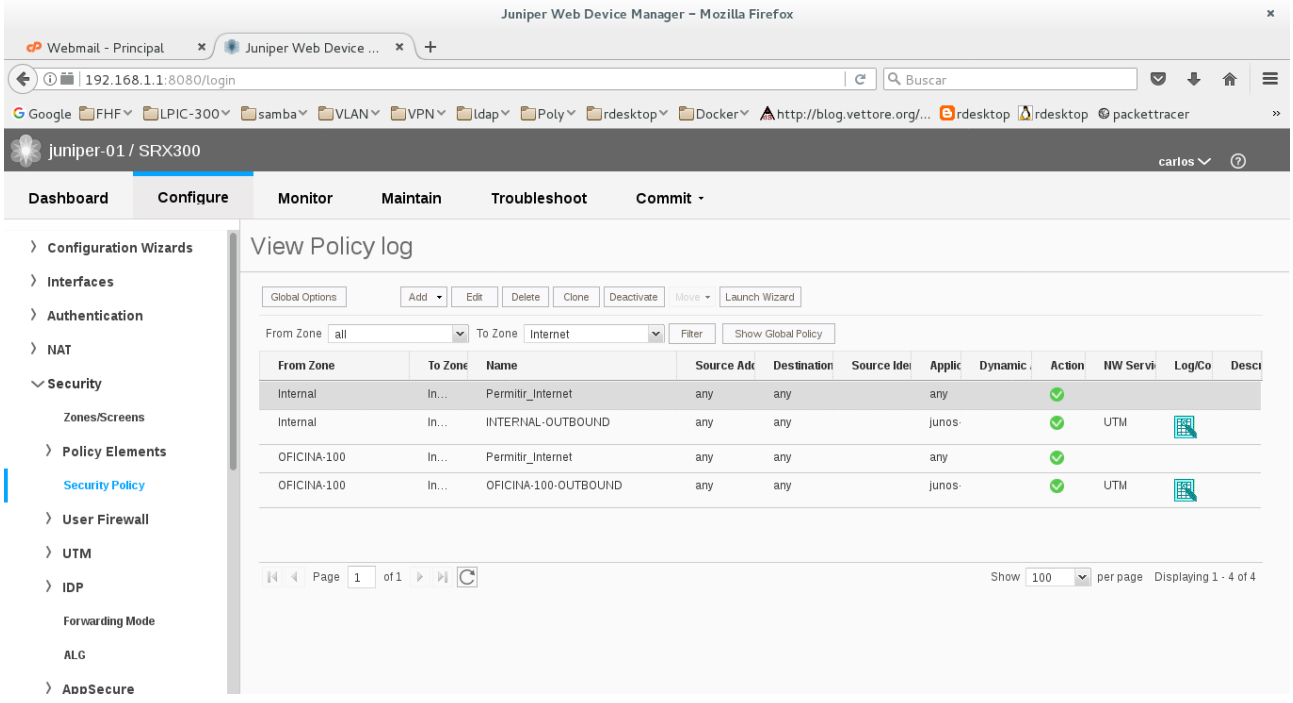
↘ Red 'OFICINA-100':

root@juniper-01# 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]
root@juniper-01# set then permit application-services utm-policy **UTM-BASICA**
root@juniper-01# set then log session-close
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;
```

```
    }
}
```


Juniper Web Device Manager – Mozilla Firefox
Webmail - Principal
Juniper Web Device ...
192.168.1.1:8080/login
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
IDP
Forwarding Mode
ALG
AppSecure
View Policy log
Global Options
Add
Edit
Delete
Clone
Deactivate
Move
Launch Wizard
From Zone
all
To Zone
Internet
Filter
Show Global Policy
From Zone
To Zone
Name
Source Ad
Destination
Source Ide
Applic
Dynamic
Action
NW Servi
Log/Co
Descr
Internal
In...
Permitir_Internet
any
any
any
Internal
In...
INTERNAL-OUTBOUND
any
any
junos-
UTM
OFICINA-100
In...
Permitir_Internet
any
any
any
OFICINA-100
In...
OFICINA-100-OUTBOUND
any
any
junos-
UTM
Page
1
of 1
Show
100
per page
Displaying 1 - 4 of 4


Juniper Web Device Manager – Mozilla Firefox
Webmail - Principal
Juniper Web Device ...
192.168.1.1:8080/login
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
IDP
Forwarding Mode
ALG
AppSecure
View Policy log
Global Options
Add
Edit
Delete
Clone
Deactivate
Move
Launch Wizard
From Zone
all
To Zone
Internet
Filter
Show Global Policy
From Zone
To Zone
Name
Source Ad
Destination
Source Ide
Applic
Dynamic
Action
NW Servi
Log/Co
Descr
Internal
In...
Permitir_Internet
any
any
any
Internal
In...
INTERNAL-OUTBOUND
any
any
junos-
UTM
OFICINA-100
In...
Permitir_Internet
any
any
any
OFICINA-100
In...
OFICINA-100-OUTBOUND
any
any
junos-
UTM
Page
1
of 1
Show
100
per page
Displaying 1 - 4 of 4

↘ Asignación del -engine- : → 'sophos-engine':

root@juniper-01# set security utm feature-profile anti-virus type sophos-engine
root@juniper-01# run show security utm anti-virus status

```
UTM anti-virus status:

  Anti-virus key expire date: 2018-05-25 02:00:00
  Update server: https://update.juniper-updates.net/SAV/
      Interval: 1440 minutes
      Pattern update status: next update in 1439 minutes
      Last result: already have latest database
  Anti-virus signature version: 1.13 (1.02)
  Scan engine type: sophos-engine
  Scan engine information: last action result: No error
```

root@juniper-01# run show security utm anti-virus statistics

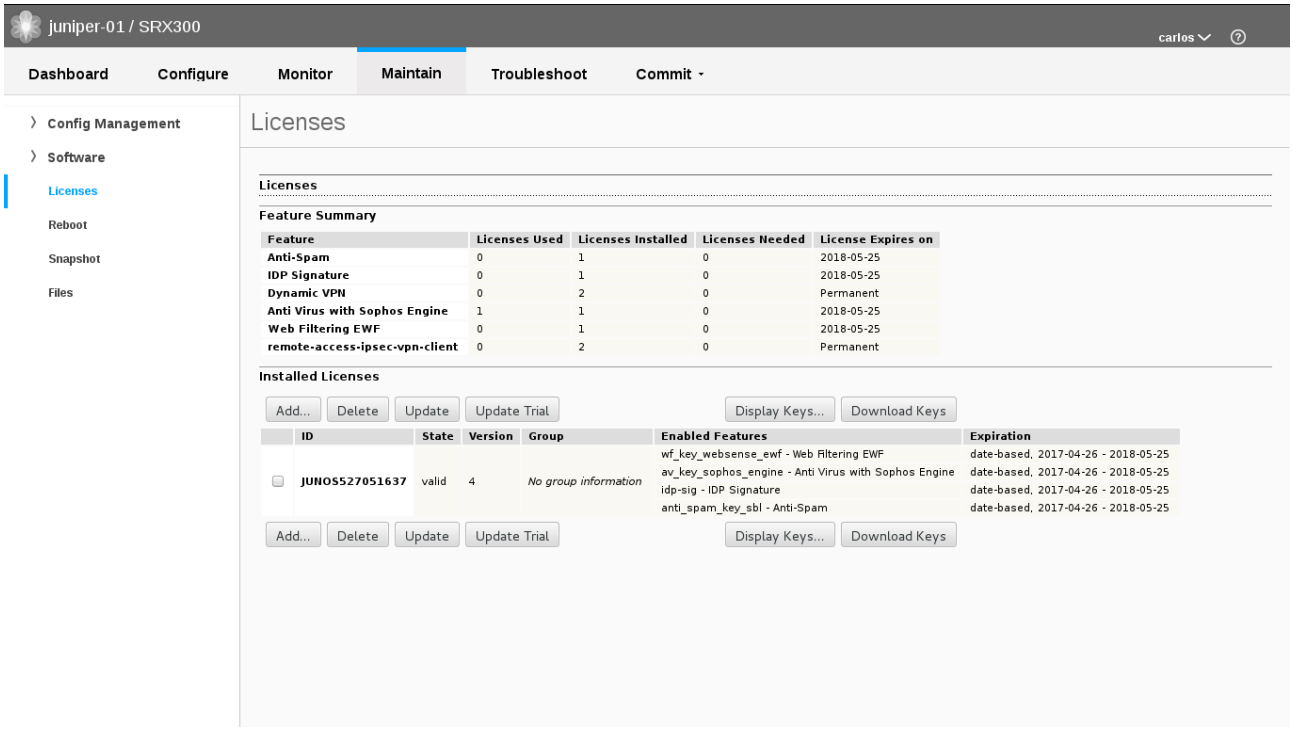
```
UTM Anti Virus statistics:
MIME-whitelist passed:          0
URL-whitelist passed:           0
Session abort:                  0
Scan Request:

 Total        Clean        Threat-found   Fallback
   0            0            0              0

Fallback:
                        Log-and-Permit   Block        Permit
Engine not ready:       0                0            0
Out of resources:       0                0            0
Timeout:                0                0            0
Maximum content size:   0                0            0
Too many requests:      0                0            0
Others:                 0                0            0
```

root@juniper-01# run show system license

```
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                  used         installed   needed
  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
```



B ==> Configuración de -Sophos- con un 'perfil' → '-Mas Personalizado-':

↘ Buenas prácticas, antes de, …

root@juniper-01% cli
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

↘ Teoría Básica :

→ 'fallback-options':

→ 'scan-options':

→ 'notification-options':

root@juniper-01# edit security utm feature-profile anti-virus sophos-engine profile SOPHOS-PERFIL-01
root@juniper-01# set fallback-options content-size block default log-and-permit out-of-resources block too-many-requests block
root@juniper-01# set notification-options fallback-block type message no-notify-mail-sender

root@juniper-01# set scan-options content-size-limit 20000
root@juniper-01# set notification-options virus-detection type message no-notify-mail-sender custom-message "* VIRUS ATENCION ***"**

root@juniper-01# up 4
root@juniper-01# set utm-policy UTM-BASICA anti-virus http-profile SOPHOS-PERFIL-01 ftp download-profile SOPHOS-PERFIL-01 upload-profile SOPHOS-PERFIL-01

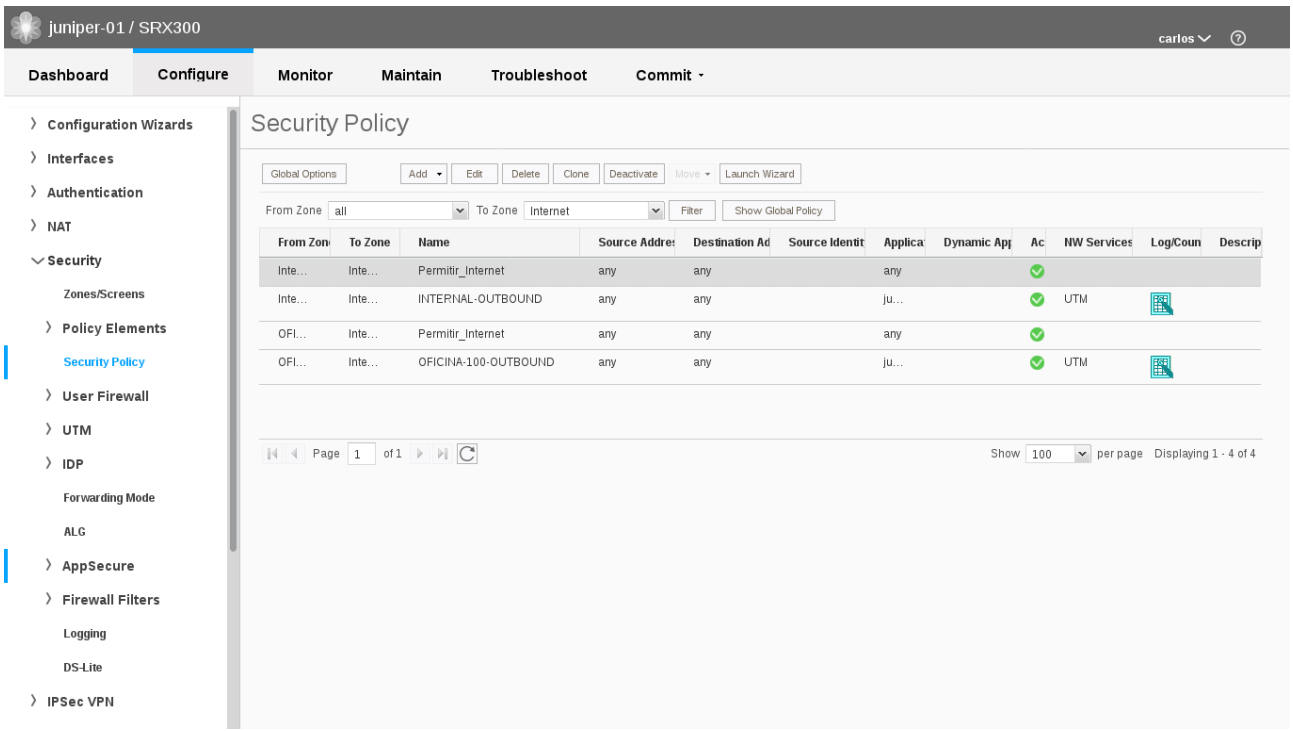
root@juniper-01# show

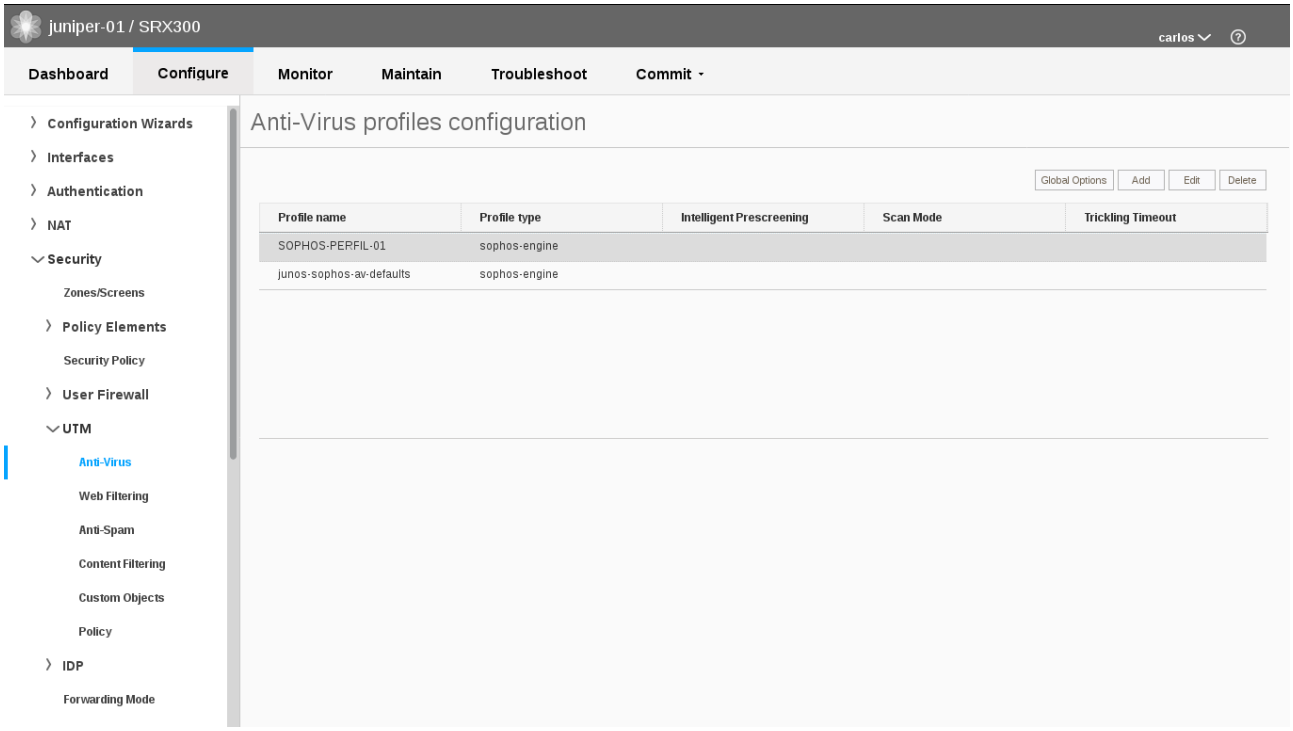
```
feature-profile {
    anti-virus {
        type sophos-engine;
        sophos-engine {
            profile SOPHOS-PERFIL-01 {
                fallback-options {
                    default log-and-permit;
                    content-size block;
                    out-of-resources block;
                    too-many-requests block;
                }
                scan-options {
                    content-size-limit 20000;
                }
                notification-options {
                    virus-detection {
                        type message;
                        no-notify-mail-sender;
                        custom-message "*** VIRUS ATENCION ***";
                    }
                    fallback-block {
                        type message;
                        no-notify-mail-sender;
                    }
                }
            }
        }
    }
}
utm-policy UTM-BASICA {
    anti-virus {
        http-profile SOPHOS-PERFIL-01;
```

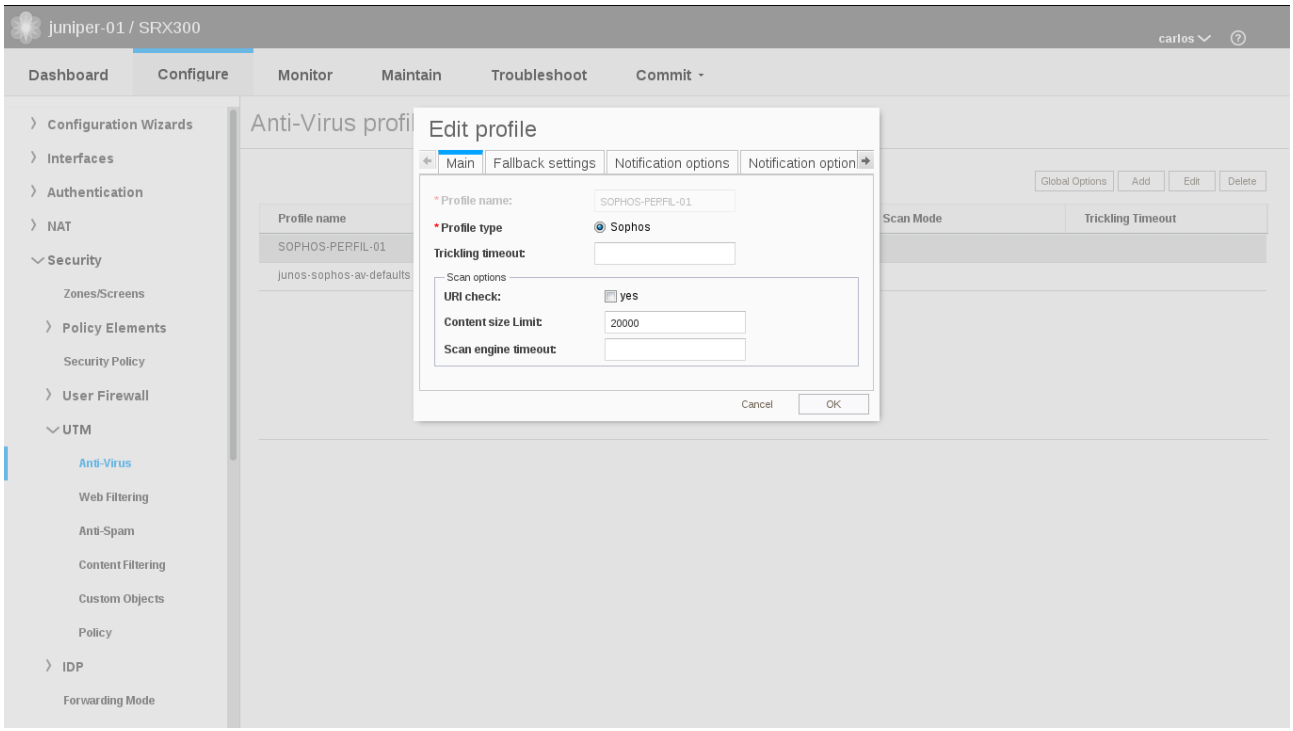
```
        ftp {
            upload-profile SOPHOS-PERFIL-01;
            download-profile SOPHOS-PERFIL-01;
        }
    }
}
```

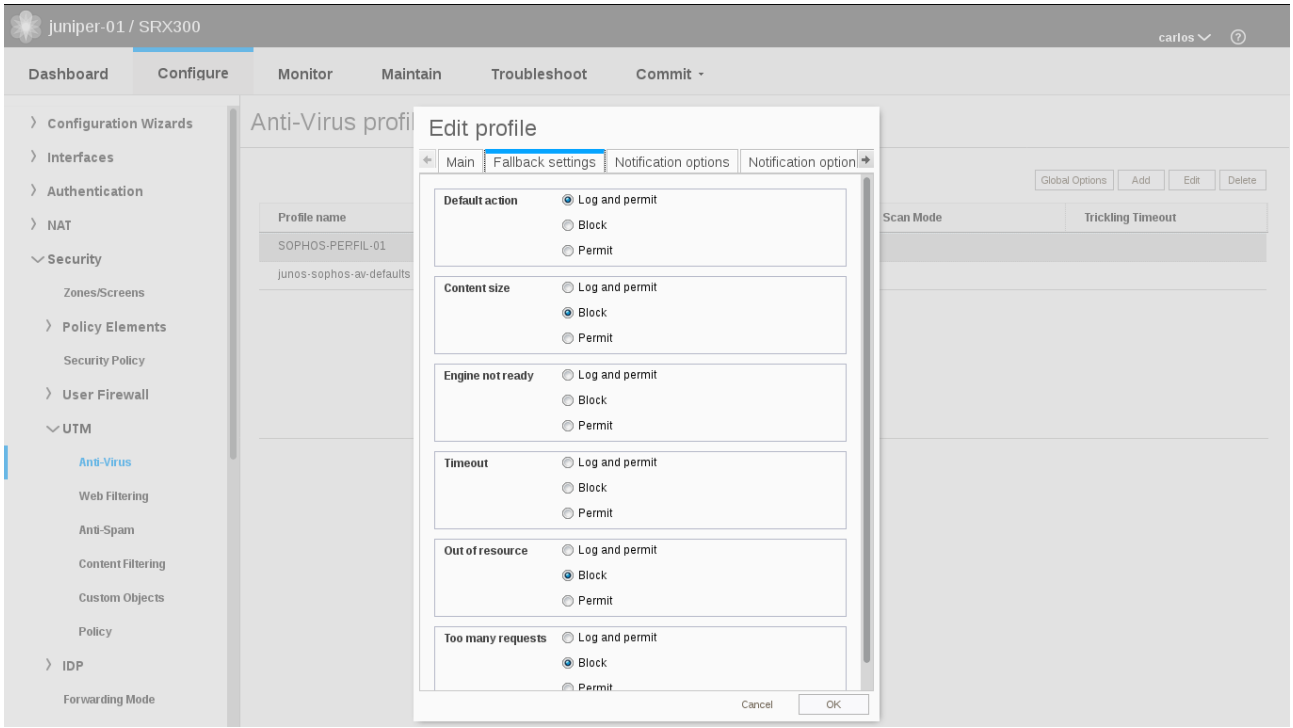
root@juniper-01# commit check
configuration check succeeds

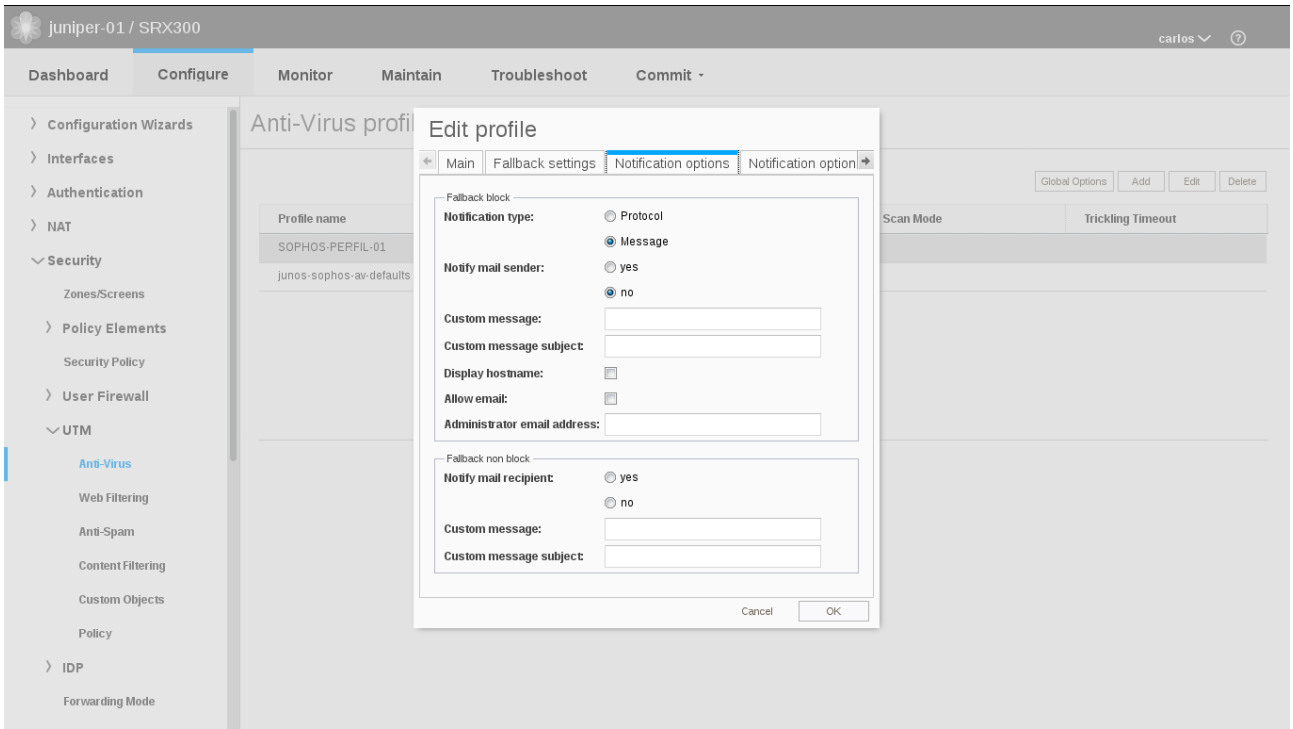
root@juniper-01# commit

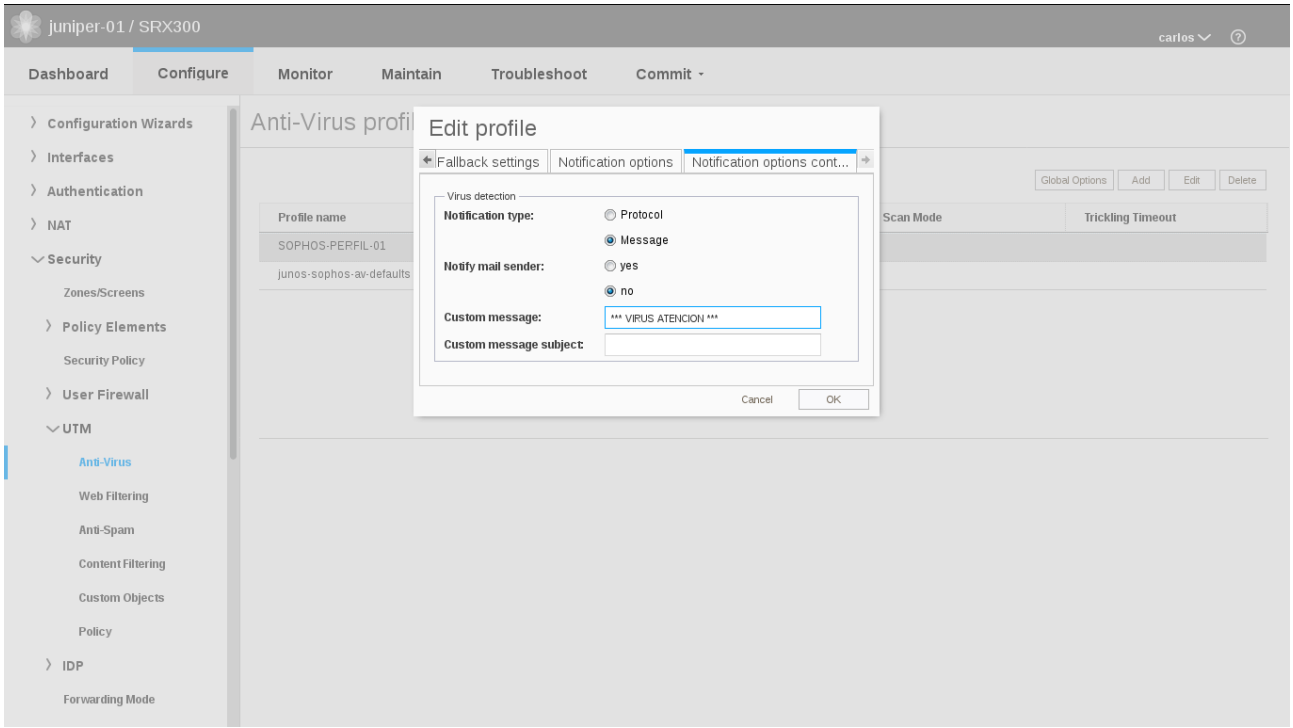



juniper-01 / SRX300
carlos
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Commit
Configuration Wizards
Interfaces
Authentication
NAT
Security
Zones/Screens
Policy Elements
Security Policy
User Firewall
UTM
Anti-Virus
Web Filtering
Anti-Spam
Content Filtering
Custom Objects
Policy
IDP
Forwarding Mode
Anti-Virus profiles configuration
Global Options
Add
Edit
Delete
Profile name
Profile type
Intelligent Prescreening
Scan Mode
Trickling Timeout
SOPHOS-PERFIL-01
sophos-engine
junos-sophos-av-defaults
sophos-engine


juniper-01 / SRX300
carlos
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Commit
Edit profile
Main
Fallback settings
Notification options
Profile name:
SOPHOS-PERFIL-01
Profile type
Sophos
Trickling timeout:
Scan options
URI check:
yes
Content size Limit:
20000
Scan engine timeout:
Cancel
OK


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-Virus profi
Edit profile
Main
Fallback settings
Notification options
Notification option
Default action
Log and permit
Block
Permit
Content size
Engine not ready
Timeout
Out of resource
Too many requests
Cancel
OK
Global Options
Add
Edit
Delete
Profile name
SOPHOS-PERFIL-01
junos-sophos-av-defaults
Scan Mode
Trickling Timeout


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-Virus profi
Edit profile
Main
Fallback settings
Notification options
Notification option
Fallback block
Notification type:
Protocol
Message
Notify mail sender:
yes
no
Custom message:
Custom message subject:
Display hostname:
Allow email:
Administrator email address:
Fallback non block
Notify mail recipient:
yes
no
Custom message:
Custom message subject:
Cancel
OK
Global Options
Add
Edit
Delete
Profile name
SOPHOS-PERFIL-01
junos-sophos-av-defaults
Scan Mode
Trickling Timeout



BIBLIOGRAFÍA Y DOCUMENTACIÓN:

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