root@juniper-01% cli
root@juniper-01> configure
Entering configuration mode
[edit]
root@juniper-01#

==> Comprobamos el modo global. (Comportamiento por Defecto):

root@juniper-01# run show ethernet-switching global-information
Global Configuration:

MAC aging interval : 300
MAC learning : Enabled
MAC statistics : Disabled
MAC limit Count : 16383
MAC limit hit : Disabled
MAC packet action drop: Disabled
LE aging time : 1200
LE VLAN aging time : 1200
Global Mode : **Switching**

Si no tenemos esta configuración por defecto, debemos configurar de la forma:
root@juniper-01# set protocols l2-learning global-mode switching

Y reiniciar, ...

==> OBJETIVO: → Configurar las interfaces de la forma:

ge-0/0/0	↘ WAN.	
ge-0/0/1	↘ Estrictamente Administrativo.	→ 192.168.1.1/24
ge-0/0/2-ge-0/0/5	↘ VLAN → vlan.100	→ 192.168.100.100/24
ge-0/0/5	↘ VLAN → vlan.99 (‘**TRUNK**’)	→ 192.168.99.99/24
ge-0/0/6-ge-0/0/7	↘ VLAN → vlan.100 (**‘FIBRA’**)	→ 192.168.100.100/24

ge-0/0/0

ge-0/0/1

==> ge-0/0/2 a ge-0/0/4.

root@juniper-01# set interfaces ge-0/0/2 unit 0 description "**To vlan.100 LAN**"
root@juniper-01# set interfaces ge-0/0/2 description "**vlan.100**"
root@juniper-01# set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
root@juniper-01# **delete** interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members vlan0
root@juniper-01# set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members vlan.100

root@juniper-01# set interfaces ge-0/0/3 unit 0 description "To vlan.100 LAN"
root@juniper-01# set interfaces ge-0/0/3 description "**vlan.100**"
root@juniper-01# set interfaces ge-0/0/3 unit 0 family ethernet-switching interface-mode access
root@juniper-01# **delete** interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members vlan0
root@juniper-01# set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members vlan.100

root@juniper-01# set interfaces ge-0/0/4 unit 0 description "To vlan.100 LAN"
root@juniper-01# set interfaces ge-0/0/4 description "**vlan.100**"
root@juniper-01# set interfaces ge-0/0/4 unit 0 family ethernet-switching interface-mode access
root@juniper-01# **delete** interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members vlan0
root@juniper-01# set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members vlan.100

==> Integrated Routing and Bridging, y Definición de VLAN's.

root@juniper-01# set interfaces **irb unit 100** family inet address **192.168.100.100/24**
root@juniper-01# set vlans vlan.100 vlan-id 100
root@juniper-01# **set vlans vlan.100 l3-interface irb.100**

root@juniper-01# set interfaces **irb unit 99** family inet address **192.168.99.99/24**
root@juniper-01# set vlans vlan.99 vlan-id 99
root@juniper-01# **set vlans vlan.99 l3-interface irb.99**

==> Trunking.

ge-0/0/5 → TRUNK.

root@juniper-01# set interfaces ge-0/0/5 native-vlan-id 99

(Esto ayuda a reclasificar paquetes '**untagged'** en el puerto Trunk).

root@juniper-01# run show ethernet-switching interface ge-0/0/5
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
LH - MAC limit hit, DN - interface down,
MMAS - Mac-move action shutdown,
SCTL - shutdown by Storm-control)

Logical interface	Vlan members	TAG	MAC limit	STP state	Logical interface flags	Tagging
ge-0/0/5.0			16383		DN	tagged
	default	1	16383	Discarding		tagged

vlan.100	100	16383	Discarding	tagged
vlan.99	**99**	**16383**	**Discarding**	**untagged**
vlan0	2	16383	Discarding	tagged

root@juniper-01# set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
root@juniper-01# set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members vlan.100
root@juniper-01# set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members vlan.99

==> Zonas de Seguridad:

root@juniper-01# set security zones security-zone **OFICINA-100** interfaces irb.100
root@juniper-01# set security zones security-zone **Nativa-99** interfaces irb.99

→ Permitir tráfico **bidireccional** entre las zonas '**Internal**' y '**OFICINA-100**'.

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internal** policy **Permitir_HTTP** match source-address any

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internal** policy **Permitir_HTTP** match destination-address any

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internal** policy **Permitir_HTTP** match application junos-http

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internal** policy **Permitir_HTTP** then permit

→ Permitir **ICMP** → pings.

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internal** policy **Permitir_ICMP** match application junos-icmp-all

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internal** policy **Permitir_ICMP** then permit

→ Definición de Políticas en las Zonas Definidas.

root@juniper-01# set security policies from-zone **Internal** to-zone **OFICINA-100** policy **Permitir_HTTP** match source-address any

root@juniper-01# set security policies from-zone **Internal** to-zone **OFICINA-100** policy **Permitir_HTTP** match destination-address any

root@juniper-01# set security policies from-zone **Internal** to-zone **OFICINA-100** policy **Permitir_HTTP** match application junos-http

root@juniper-01# set security policies from-zone **Internal** to-zone **OFICINA-100** policy **Permitir_HTTP** then permit

→ Permitir ICMP → pings

root@juniper-01# set security policies from-zone **Internal** to-zone **OFICINA-100** policy **Permitir_ICMP** match application junos-icmp-all

root@juniper-01# set security policies from-zone **Internal** to-zone **OFICINA-100** policy **Permitir_ICMP** then permit

→ Permitir **Internet** para zonas: '**Internal**' y '**OFICINA-100**'.

root@juniper-01# set security policies from-zone **Internal** to-zone **Internet** policy **Permitir_Internet** match source-address any

root@juniper-01# set security policies from-zone **Internal** to-zone **Internet** policy **Permitir_Internet** match destination-address any

root@juniper-01# set security policies from-zone **Internal** to-zone **Internet** policy **Permitir_Internet** match application any

root@juniper-01# set security policies from-zone **Internal** to-zone **Internet** policy **Permitir_Internet** then permit

---

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internet** policy **Permitir_Internet** match source-address any

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internet** policy **Permitir_Internet** match destination-address any

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internet** policy **Permitir_Internet** match application any

root@juniper-01# set security policies from-zone **OFICINA-100** to-zone **Internet** policy **Permitir_Internet** then permit

→ Permitir **NAT**.

root@juniper-01# set security nat source rule-set **NAT-Internet** from zone **Internal**
root@juniper-01# set security nat source rule-set **NAT-Internet** from zone **OFICINA-100**

root@juniper-01# set security nat source rule-set **NAT-Internet** to zone **Internet**
root@juniper-01# set security nat source rule-set **NAT-Internet** rule **NAT-interfaz** match source-address 0.0.0.0/0

root@juniper-01# set security nat source rule-set **NAT-Internet** rule **NAT-interfaz** then source-nat interface

→ Zonas para IRB.

↘ De Confianza:

root@juniper-01# set security zones security-zone **Internal** interfaces irb.0
root@juniper-01# set security zones security-zone **OFICINA-100** interfaces irb.100
root@juniper-01# set security zones security-zone **Nativa-99** interfaces irb.99

root@juniper-01# set security zones security-zone **Internal** host-inbound-traffic system-services ping
root@juniper-01# set security zones security-zone **OFICINA-100** host-inbound-traffic system-services ping

root@juniper-01# set security zones security-zone **Internal** host-inbound-traffic system-services ssh
root@juniper-01# set security zones security-zone **OFICINA-100** host-inbound-traffic system-services ssh

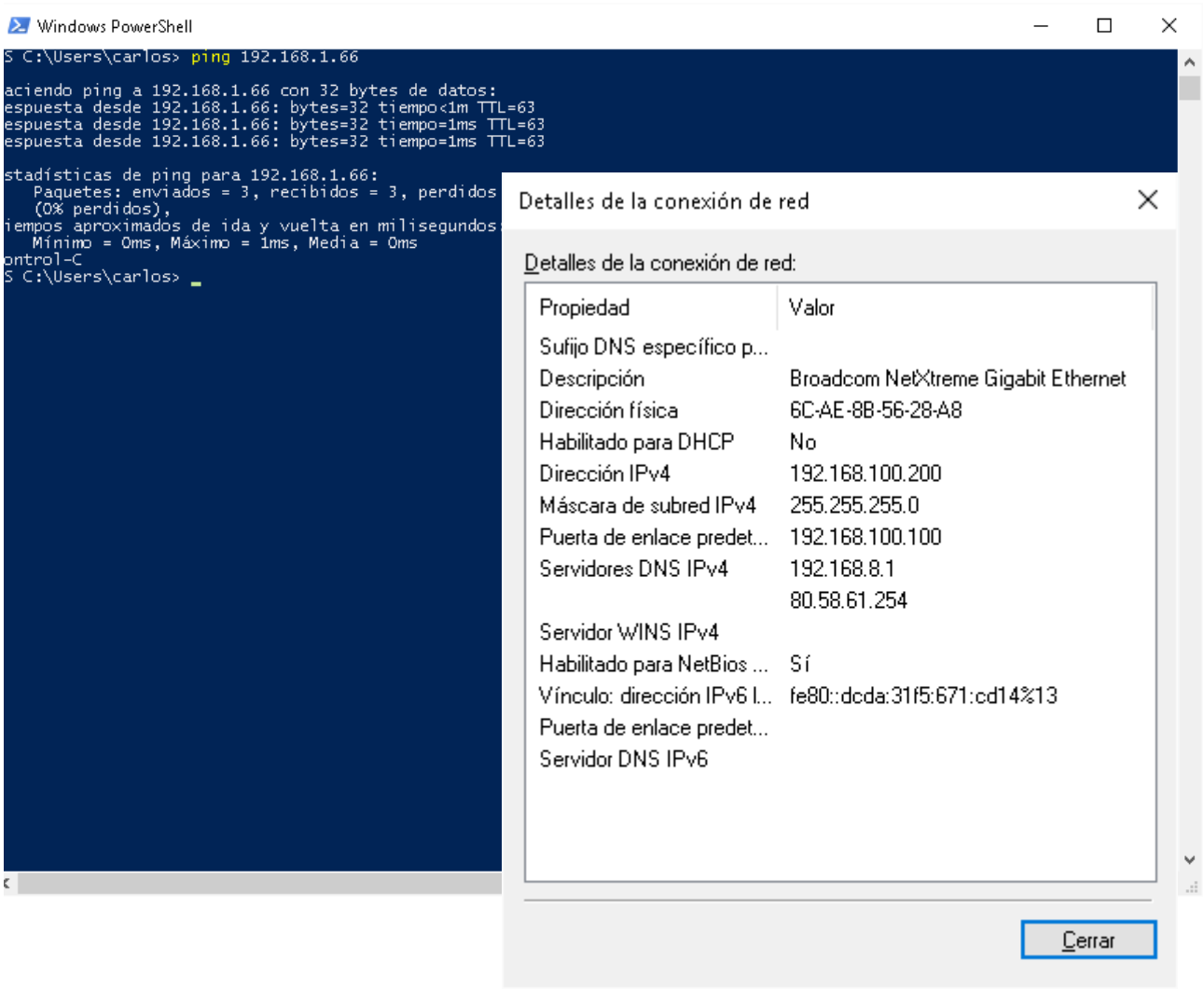
root@juniper-01# set security zones security-zone **Internal** host-inbound-traffic system-services http
root@juniper-01# set security zones security-zone **OFICINA-100** host-inbound-traffic system-services http

root@juniper-01# set security zones security-zone **Internal** host-inbound-traffic system-services https
root@juniper-01# set security zones security-zone **OFICINA-100** host-inbound-traffic system-services https

↘ De 'NO' Confianza:

root@juniper-01# set security zones security-zone **Internet** interfaces ge-0/0/0.0
root@juniper-01# set security zones security-zone **Internet** host-inbound-traffic system-services ping

==> Comprobación de tráfico entre VLAN's (Layer 3):



[carlos@centos-pavilion ~]$ ifconfig eno1

eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.66 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::5bed:a371:be30:9366 prefixlen 64 scopeid 0x20<link>
ether 38:ea:a7:f8:3d:7a txqueuelen 1000 (Ethernet)
RX packets 69878 bytes 57932142 (55.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 67566 bytes 9701369 (9.2 MiB)
TX errors 9 dropped 0 overruns 0 carrier 0 collisions 0

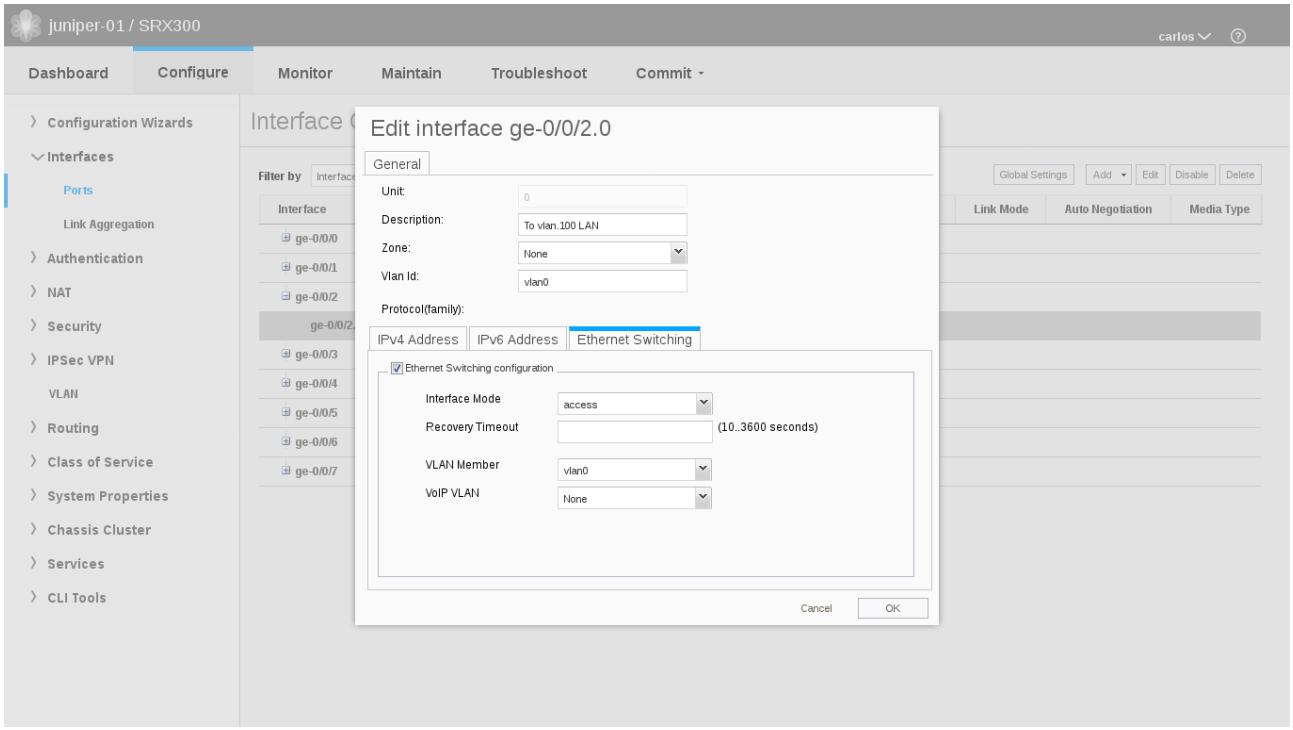
[carlos@centos-pavilion ~]$ ping -c3 192.168.100.200

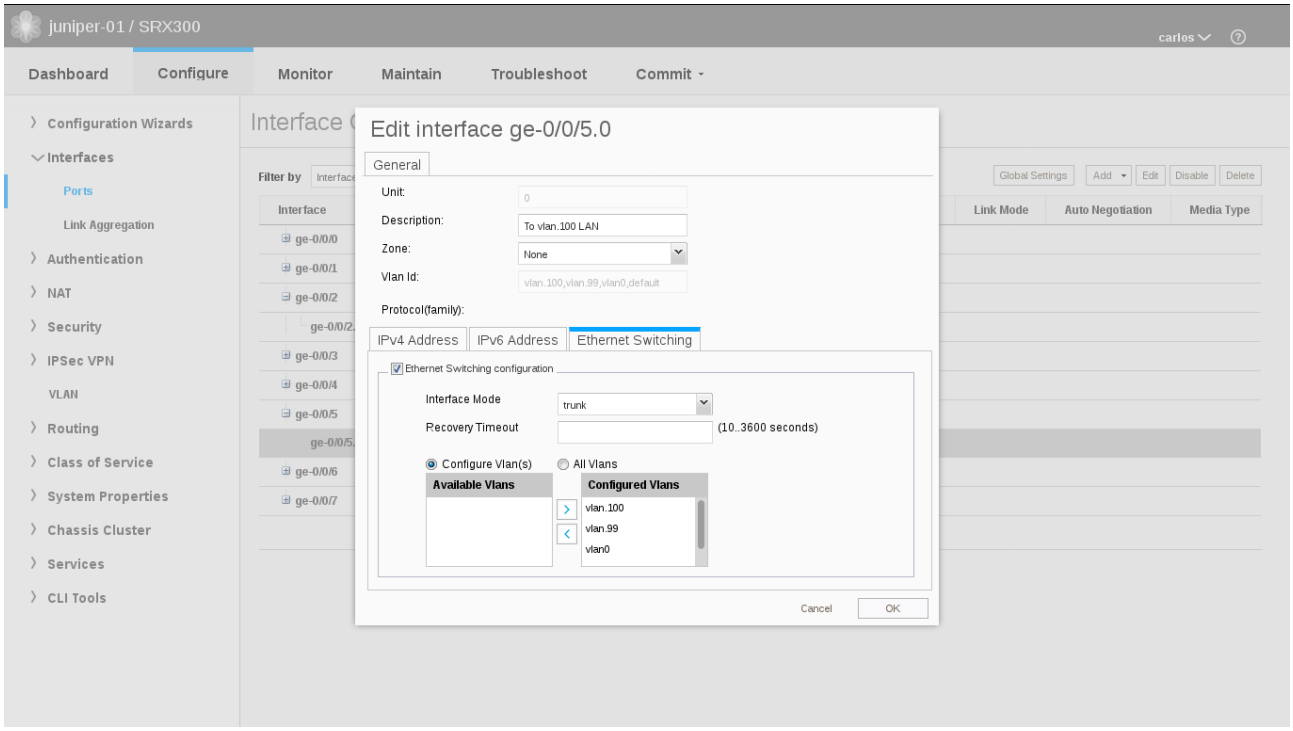
PING 192.168.100.200 (192.168.100.200) 56(84) bytes of data.
64 bytes from 192.168.100.200: icmp_seq=1 ttl=127 time=1.20 ms
64 bytes from 192.168.100.200: icmp_seq=2 ttl=127 time=1.35 ms

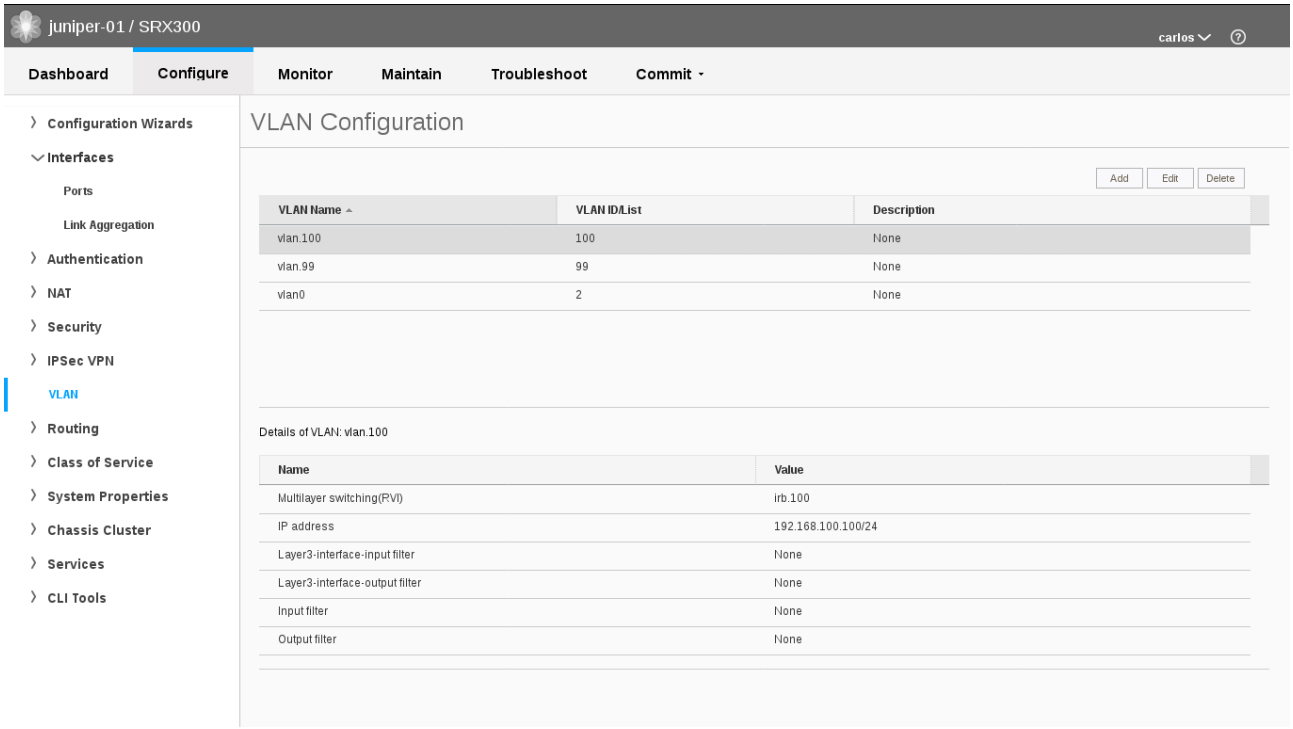
64 bytes from 192.168.100.200: icmp_seq=3 ttl=127 time=1.34 ms

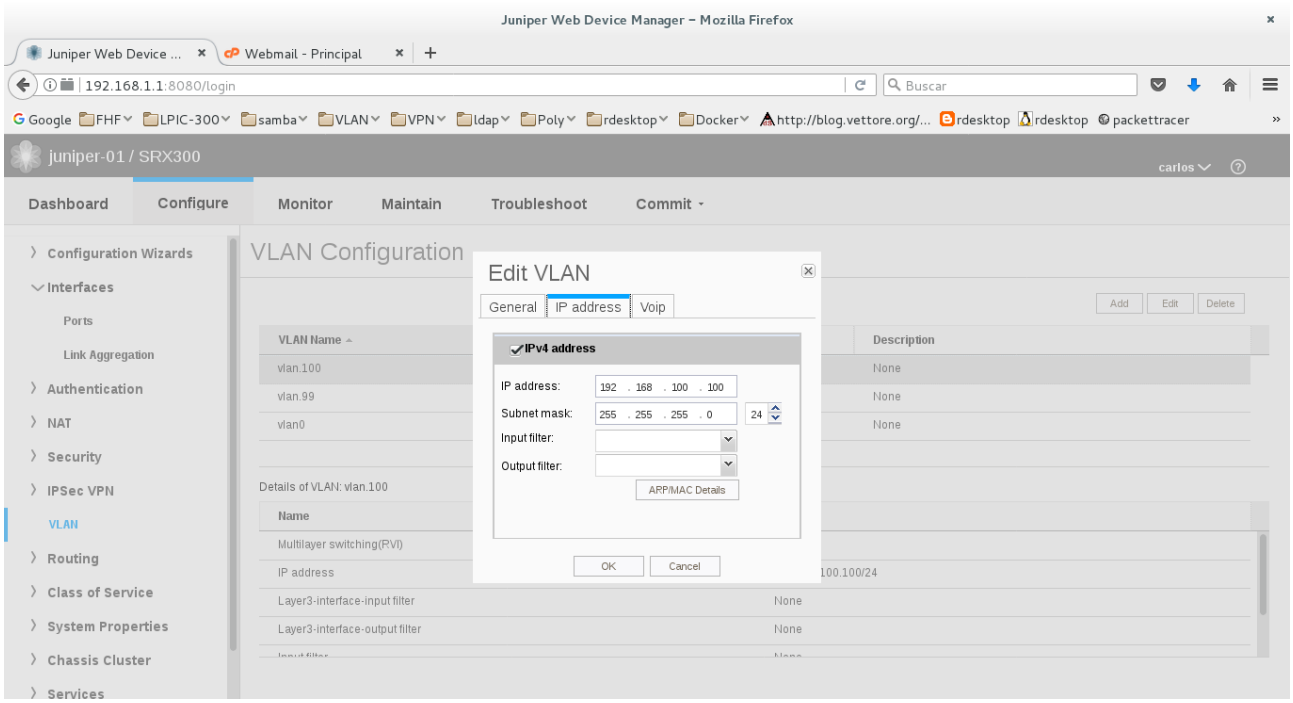
--- 192.168.100.200 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.208/1.303/1.359/0.067 ms

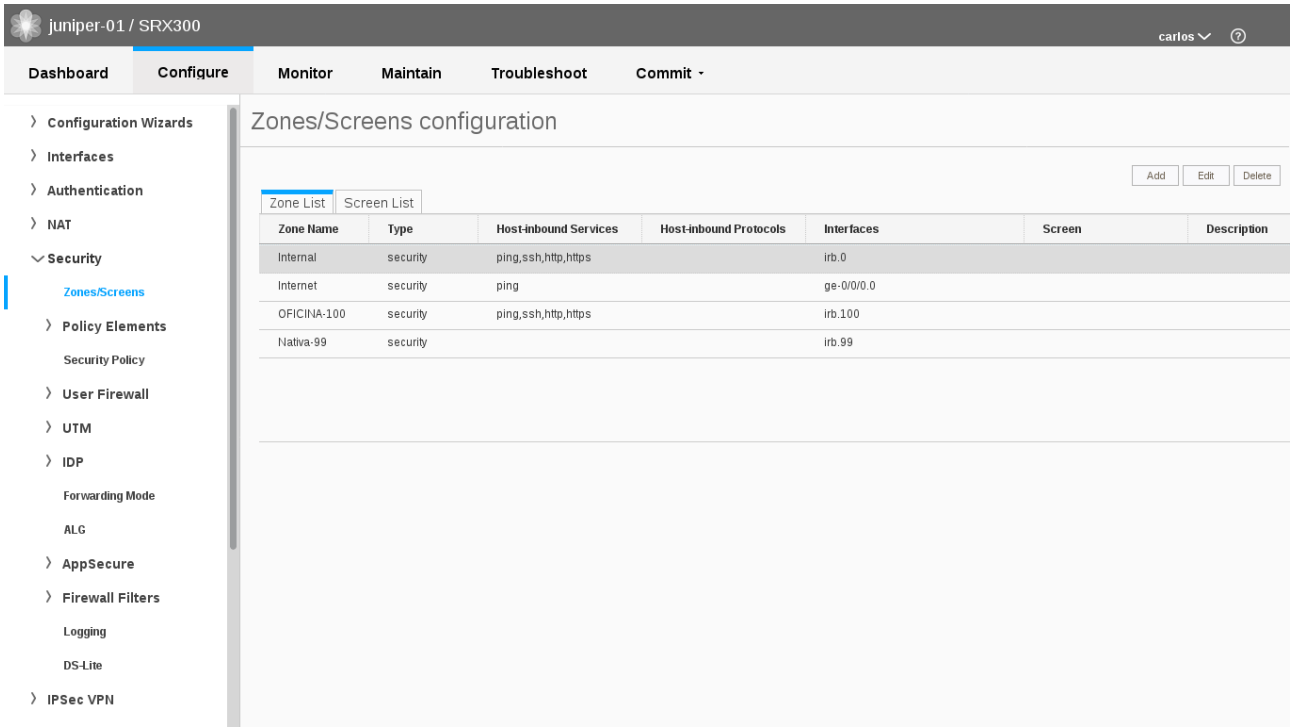
==> Comprobación en J-Web:

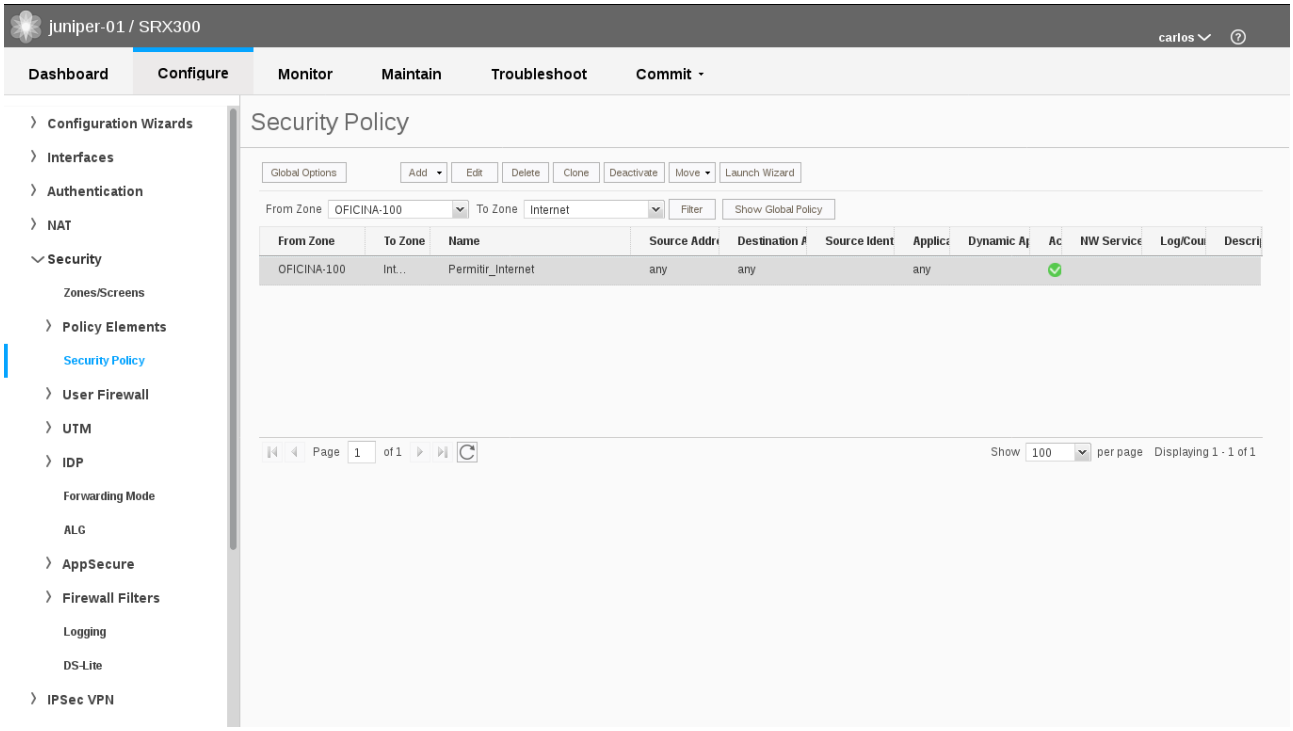


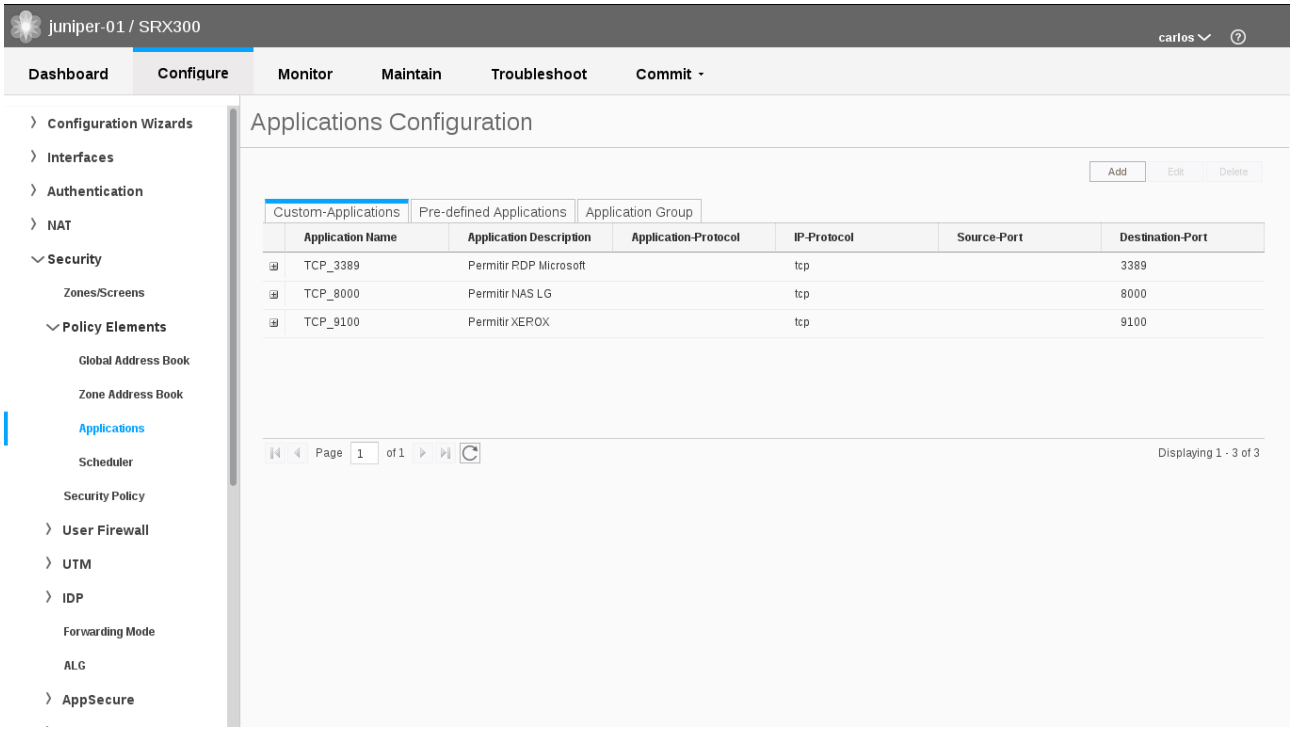

juniper-01 / SRX300
carlos
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Commit
Configuration Wizards
Interfaces
Ports
Link Aggregation
Authentication
NAT
Security
IPSec VPN
VLAN
Routing
Class of Service
System Properties
Chassis Cluster
Services
CLI Tools
Edit interface ge-0/0/5.0
General
Unit:
Description:
To vlan.100 LAN
Zone:
None
Vlan Id:
vlan.100,vlan.99,vlan0,default
Protocol(family):
IPv4 Address
IPv6 Address
Ethernet Switching
Ethernet Switching configuration
Interface Mode
trunk
Recovery Timeout
(10..3600 seconds)
Configure Vlan(s)
All Vlans
Available Vlans
Configured Vlans
vlan.100
vlan.99
vlan0
Cancel
OK


juniper-01 / SRX300
carlos
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Commit
Configuration Wizards
Interfaces
Ports
Link Aggregation
Authentication
NAT
Security
IPSec VPN
VLAN
Routing
Class of Service
System Properties
Chassis Cluster
Services
CLI Tools
VLAN Configuration
Add
Edit
Delete
VLAN Name
VLAN ID/List
Description
vlan.100
100
None
vlan.99
99
None
vlan0
2
None
Details of VLAN: vlan.100
Name
Value
Multilayer switching(PVI)
irb.100
IP address
192.168.100.100/24
Layer3-interface-input filter
None
Layer3-interface-output filter
None
Input filter
None
Output filter
None


Juniper Web Device Manager – Mozilla Firefox
Juniper Web Device ...
Webmail - Principal
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
Configuration Wizards
Interfaces
Ports
Link Aggregation
Authentication
NAT
Security
IPSec VPN
VLAN
Routing
Class of Service
System Properties
Chassis Cluster
Services
VLAN Configuration
Add Edit Delete
VLAN Name
Description
vlan.100
vlan.99
vlan0
None
Details of VLAN: vlan.100
Name
Multilayer switching(RVI)
IP address
100.100/24
Layer3-interface-input filter
Layer3-interface-output filter
Edit VLAN
General IP address Voip
IPv4 address
IP address: 192 . 168 . 100 . 100
Subnet mask: 255 . 255 . 255 . 0 24
Input filter:
Output filter:
ARP/MAC Details
OK Cancel


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
Firewall Filters
Logging
DS-Lite
IPSec VPN
Zones/Screens configuration
Add Edit Delete
Zone List Screen List
Zone Name Type Host-inbound Services Host-inbound Protocols Interfaces Screen Description
Internal security ping,ssh,http,https irb.0
Internet security ping ge-0/0/0.0
OFICINA-100 security ping,ssh,http,https irb.100
Nativa-99 security irb.99


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
Firewall Filters
Logging
DS-Lite
IPSec VPN
Security Policy
Global Options
Add
Edit
Delete
Clone
Deactivate
Move
Launch Wizard
From Zone
OFICINA-100
To Zone
Internet
Filter
Show Global Policy
From Zone
To Zone
Name
Source Addr
Destination A
Source Ident
Applica
Dynamic Ap
Ac
NW Service
Log/Cour
Descrip
OFICINA-100
Int...
Permitir_Internet
any
any
any
Page
1
of 1
Show
100
per page
Displaying 1 - 1 of 1


juniper-01 / SRX300
carlos
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Commit
Configuration Wizards
Interfaces
Authentication
NAT
Security
Zones/Screens
Policy Elements
Global Address Book
Zone Address Book
Applications
Scheduler
Security Policy
User Firewall
UTM
IDP
Forwarding Mode
ALG
AppSecure
Applications Configuration
Add
Edit
Delete
Custom-Applications
Pre-defined Applications
Application Group
Application Name
Application Description
Application-Protocol
IP-Protocol
Source-Port
Destination-Port
TCP_3389
Permitir RDP Microsoft
tcp
3389
TCP_8000
Permitir NAS LG
tcp
8000
TCP_9100
Permitir XEROX
tcp
9100
Page
1
of 1
Displaying 1 - 3 of 3

==> Fichero General de Configuración:

```
## Last changed: 2017-04-26 08:55:05 CEST
version 15.1X49-D80.4;
system {
    host-name juniper-01;
    time-zone Europe/Madrid;
    root-authentication {
        encrypted-password "$5$1Uvcmi3G0JVtopGHSOYrW9n4"; ## SECRET-DATA
    }
    name-server {
        80.58.61.254;
        80.58.61.250;
        8.8.8.8;
    }
    name-resolution {
        no-resolve-on-input;
    }
    login {
        user carlos {
            uid 100;
            class super-user;
            authentication {
                encrypted-password "$5$uVMMh5MI$Mgsffgffjjfgjgjgj"; ## SECRET-DATA
            }
        }
    }
    services {
        ftp;
        ssh;
        telnet;
        xnm-clear-text;
        dhcp-local-server {
            group jweb-default-group {
                interface irb.0;
            }
        }
        web-management {
            http {
                port 8080;
            }
            https {
                port 8443;
                system-generated-certificate;
            }
            session {
```

```
            idle-timeout 60;
        }
    }
}
syslog {
    archive size 100k files 3;
    user * {
        any emergency;
    }
    file messages {
        any notice;
        authorization info;
    }
    file interactive-commands {
        interactive-commands any;
    }
}
max-configurations-on-flash 49;
max-configuration-rollbacks 49;
license {
    autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
    }
}
ntp {
    server hora.roa.es;
}
}
security {
    screen {
        ids-option untrust-screen {
            icmp {
                ping-death;
            }
            ip {
                source-route-option;
                tear-drop;
            }
            tcp {
                syn-flood {
                    alarm-threshold 1024;
                    attack-threshold 200;
                    source-threshold 1024;
                    destination-threshold 2048;
                    timeout 20;
                }
                land;
```

```
        }
    }
}
nat {
    source {
        rule-set nsw_srcnat {
            from zone Internal;
            to zone Internet;
            rule nsw-src-interface {
                match {
                    source-address 0.0.0.0/0;
                    destination-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
        rule-set NAT-Internet {
            from zone [ Internal OFICINA-100 ];
            to zone Internet;
            rule NAT-interfaz {
                match {
                    source-address 0.0.0.0/0;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
}
policies {
    from-zone Internal to-zone Internet {
        policy Permitir_Internet {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
```

```
    }
  }
  from-zone OFICINA-100 to-zone Internal {
    policy Permitir_HTTP {
      match {
        source-address any;
        destination-address any;
        application junos-http;
      }
      then {
        permit;
      }
    }
    policy Permitir_ICMP {
      match {
        source-address any;
        destination-address any;
        application junos-icmp-all;
      }
      then {
        permit;
      }
    }
  }
  from-zone Internal to-zone OFICINA-100 {
    policy Permitir_HTTP {
      match {
        source-address any;
        destination-address any;
        application [ junos-http junos-https TCP_8000 ];
      }
      then {
        permit;
      }
    }
    policy Permitir_ICMP {
      match {
        source-address any;
        destination-address any;
        application junos-icmp-all;
      }
      then {
        permit;
      }
    }
    policy Permitir_RDP {
      description "Permitir RDP Microsoft";
```

```
            match {
                source-address any;
                destination-address any;
                application TCP_3389;
            }
            then {
                permit;
            }
        }
        policy Permitir_FTP {
            description "Permitir FTP";
            match {
                source-address any;
                destination-address any;
                application junos-ftp;
            }
            then {
                permit;
            }
        }
        policy Permitir_XEROX {
            description "Permitir XEROX";
            match {
                source-address any;
                destination-address any;
                application TCP_9100;
            }
            then {
                permit;
            }
        }
    }
    from-zone OFICINA-100 to-zone Internet {
        policy Permitir_Internet {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
zones {
    security-zone Internal {
```

```
        host-inbound-traffic {
            system-services {
                ping;
                ssh;
                http;
                https;
            }
        }
        interfaces {
            irb.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        dhcp;
                        http;
                        https;
                        ssh;
                        telnet;
                    }
                }
            }
        }
    }
    security-zone Internet {
        host-inbound-traffic {
            system-services {
                ping;
            }
        }
        interfaces {
            ge-0/0/0.0 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        dhcp;
                    }
                }
            }
        }
    }
    security-zone OFICINA-100 {
        host-inbound-traffic {
            system-services {
                ping;
                ssh;
                http;
                https;
```

```
            }
        }
        interfaces {
            irb.100 {
                host-inbound-traffic {
                    system-services {
                        ping;
                        ssh;
                    }
                }
            }
        }
    }
    security-zone Nativa-99 {
        interfaces {
            irb.99;
        }
    }
}
}
interfaces {
    ge-0/0/0 {
        description WAN;
        unit 0 {
            description "To Internet";
            family inet {
                dhcp-client;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan0;
                }
            }
        }
    }
    ge-0/0/2 {
        description vlan.100;
        unit 0 {
            description "To vlan.100 LAN";
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members vlan0;
```

```
            }
        }
    }
}
ge-0/0/3 {
    description vlan.100;
    unit 0 {
        description "To vlan.100 LAN";
        family ethernet-switching {
            interface-mode access;
            vlan {
                members vlan.100;
            }
        }
    }
}
ge-0/0/4 {
    description vlan.100;
    unit 0 {
        description "To vlan.100 LAN";
        family ethernet-switching {
            interface-mode access;
            vlan {
                members vlan.100;
            }
        }
    }
}
ge-0/0/5 {
    description vlan.100;
    native-vlan-id 99;
    unit 0 {
        description "To vlan.100 LAN";
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members [ vlan.100 vlan.99 vlan0 default ];
            }
        }
    }
}
ge-0/0/6 {
    unit 0 {
        family ethernet-switching {
            interface-mode access;
            vlan {
                members vlan.100;
```

```
            }
        }
    }
    ge-0/0/7 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members vlan.100;
                }
            }
        }
    }
    irb {
        unit 0 {
            family inet {
                address 192.168.1.1/24;
            }
        }
        unit 99 {
            family inet {
                address 192.168.99.99/24;
            }
        }
        unit 100 {
            family inet {
                address 192.168.100.100/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 192.168.8.1;
    }
}
protocols {
    l2-learning {
        global-mode switching;
    }
}
access {
    address-assignment {
        pool jweb-default-pool {
            family inet {
                network 192.168.1.0/24;
```

```
            range jweb-default-range {
               low 192.168.1.2;
               high 192.168.1.254;
            }
            dhcp-attributes {
               router {
                  192.168.1.1;
               }
            }
         }
      }
   }
}
applications {
   application TCP_3389 {
      protocol tcp;
      destination-port 3389;
      description "Permitir RDP Microsoft";
   }
   application TCP_8000 {
      protocol tcp;
      destination-port 8000;
      description "Permitir NAS LG";
   }
   application TCP_9100 {
      protocol tcp;
      destination-port 9100;
      description "Permitir XEROX";
   }
}
vlans {
   vlan.100 {
      vlan-id 100;
      l3-interface irb.100;
   }
   vlan.99 {
      vlan-id 99;
      l3-interface irb.99;
   }
   vlan0 {
      vlan-id 2;
      l3-interface irb.0;
   }
}
```

BIBLIOGRAFÍA Y DOCUMENTACIÓN:

→ **Ethernet Switching Configuration Guide. (Rahul Ramachandran).**
http://cdn2.hubspot.net/hubfs/213747/Juniper/Assets/Ethernet_Switching_Configuration_Guide_for_SRX_Series_-_App_Note.pdf?t=1472249094610

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

→ https://kb.juniper.net/InfoCenter/index?page=content&id=KB31081&actp=RSS