The purpose of this document is to provide users with a quick reference for configuring interfaces, routing, firewall filters, security zones, security policies, schedulers, logging, VPN, NAT, clustering and IDP on a SRX device.

Overview
INTERFACE

Set single vlan or point to point

```
set interfaces ge-0/0/4
unit 0 family inet address 10.1.1.9/24
```

Set multiple vlans sub interfaces

```
set interfaces ge-0/0/1
unit 101
vlan-id 101
family inet address 172.1.101.9/24

set interfaces ge-0/0/1
unit 201
vlan-id 201
family inet address 172.1.201.9/24
```

Repeat for other interfaces

ROUTING

Static routing

```
set routing-options route 0/0 next hop 10.1.1.1
```

OSPF add interfaces to area

```
set protocols ospf area 0
interface ge-0/0/1.0

set protocols ospf area 0
interface ge-0/0/2.0

set protocols ospf area 0
interface ge-0/0/4.101
```

Export routes into OSPF

```
set policy-options policy-statement some-policy-name

term name-of-match from protocol static

set policy-options policy-statement some-policy-name

term name-of-match from route-filter 10.1.1.0/24 exact

set policy-options policy-statement some-policy-name

term name-of-match then accept
```

FIREWALL FILTERS

(Stateless)

Create filter

```
create filter
edit firewall family inet filter some-filter-name
```

Edit firewall filter

```
set term rule-name from protocol icmp

set term rule-name from source-address 1.1.1.1/24

set term rule-name then accept
```

Apply filter to an interface

```
set interfaces lo0 unit 0 family inet filter input some-filter-name
```

ZONES

Add interfaces into a named zone

```
set security zones security-zone zone-name interfaces
```

Add interfaces into a named zone (functional)

```
set security zones security-zone management interfaces ge-0/0/0.0

set security zones security-zone management host-inbound-traffic system-services ssh

set security zones security-zone management host-inbound-traffic system-services ping

set security zones security-zone management host-inbound-traffic system-services traceroute

set security zones security-zone management host-inbound-traffic system-services https

set security zones security-zone management host-inbound-traffic system-services snmp
```

Set up functional zone management services - high-end SRX with fxp0 port

```
set system system-services ssh

set system system-services ping

set system system-services traceroute

set system system-services https

set system system-services snmp
```

Set up functional zone management services - low-end SRX without fxp0 ports

```
set security zones functional-zone management interfaces ge-0/0/0.0

set security zones functional-zone management host-inbound-traffic system-services ssh

set security zones functional-zone management host-inbound-traffic system-services ping

set security zones functional-zone management host-inbound-traffic system-services traceroute

set security zones functional-zone management host-inbound-traffic system-services https

set security zones functional-zone management host-inbound-traffic system-services snmp
```

BLOCKING

```
set security policies policy-definition allow-unknown hosts block
```

INTERFACE
SECURITY POLICIES

create address objects

set address-book address host_name 192.168.1.10/32

set address-book address network_name 192.168.100.0/24

create custom application objects

set source-port any

set destination-port 5001

set protocol tcp

create zone to zone policy

set match source-address any

(set an address object like host_name above)

set match destination-address any

(set an address object like network_name above)

set match application any

(set an application object like app_name above)

set then permit (or deny)

SCHEDULERS

times when policies are allowed

set daily start-time 07:00:00

stop-time 18:00:00

set saturday exclude

set sunday exclude

apply to security policy

set security policies from-zone zone_name1 to-zone zone_name2 policy zonepolicy_name scheduler-name sched_name

move a policy in case order is an issue (policy is evaluated top down)

insert policy zonepolicy_name1 before policy zonepolicy_name2

VPN

time is important to see the output of show security ike commands

set ntp server n.n.n.n (ntp server ip is n.n.n.n)

route based ipsec

set interfaces st0 unit 0 family inet address 192.168.100.10

(set ike parameters auth method, dh-group, auth algorithm, encrypt alg, lifetime)

edit security ike set proposal prop_name authentication-method pre-shared-keys (or rsa-signatures)

set proposal prop_name dh-group group2 (can be group1, group2 or group5)

set proposal prop_name authentication-algorithm md5 (can be md5 or sha1 or sha-256)

set proposal prop_name encryption-algorithm 3des-cbc (can be aes-128-cbc, aes-192-cbc, aes-256-cbc, des-cbc)

set proposal prop_name lifetime-seconds 600 (in seconds)

(set ike policy mode and pre-shared key)

edit security ike set policy policy_name mode main (can be main or aggressive – for dynamic ip endpoints)

set policy policy_name proposals prop_name

set policy policy_name pre-shared-key ascii-text your_password

(set gateway and timeouts for peer)

edit security ike set gateway phase1_gateway ike-policy policy_name

set gateway phase1_gateway address remote_peer_ip_address

set gateway phase1_gateway dead-peer-detection interval 20

set gateway phase1_gateway dead-peer-detection threshold 5

(set gateway the peer's firewall interface)

set external-interface ge-0/0/3.0

(set IPSEC/phase2 encap protocol, auth algorithm, encrypt algorithm, lifetime)

edit security ipsec

set security zones security-zone untrust interfaces st0.0

(set ike parameters auth method, dh-group, auth algorithm, encrypt alg, lifetime)
set proposal
phase2_name
protocol esp
(can be esp or ah – ah has no encryption)
set proposal
phase2_name
authentication-algorithm hmac-md5-96
(or hmac-sha1-96)
set proposal
phase2_name
encryption-algorithm 3des-cbc
(or aes-128-cbc, aes-192-cbc, aes-256-cbc, des-cbc)
set proposal
phase2_name
lifetime-seconds
3200
(in seconds)
(set ipsec policy for PFS, which dh group)
edit security ipsec set policy
policy2_name
perfect-forward-secrecy keys group2
set policy
policy2_name
proposals
phase2_name
(setup vpn tunnel, bind st interface, set ike gateway, set ipsec policy)
edit security ipsec set vpn
tunnel_name
bind-interface st0.0
(your st tunnel name from beginning)
set vpn
tunnel_name
ike gateway
phase1_gateway
set vpn
tunnel_name
ike ipsec-policy
policy2_name
set vpn
tunnel_name
establish tunnels immediately
(start vpn w/out traffic)
(set static route)
set routing-options static route
10.10.10.0/24
next-hop st0.0
(you need to create security policy to allow traffic in BOTH directions)
edit from-zone
untrust
to-zone
zone-name
set policy
sec-policy_name
match source-address
ip_source
set policy
sec-policy_name
match destination-address
ip_dest
set policy
sec-policy_name
match application
tcp-udp_port
set policy
sec-policy_name
then permit
** policy based vpn
tunnel config (all of the above steps, no need to create interface st0.0)
edit security ipsec set vpn
tunnel_name
ike gateway
phase1_gateway
set vpn
tunnel_name
ike ipsec-policy
policy2_name
set vpn
tunnel_name
establish tunnels immediately
(start vpn w/out traffic)
(set create the policy)
edit security policies from-zone
source_zone_name
to-zone
dest_zone_name
set policy
pol_name
match source-address
some_ips
set policy
pol_name
match destination-address
public_ips
set policy
pol_name
match any
set policy
pol_name
then permit tunnel ipsec-vpn
tunnel_name
an adjustment of MTU might be needed for large packets
(set you view ipsec detail you can check mtu for overhead)
set security flow tcp-mss ipsec-vpn mss 1350
NAT
Interface Source Nat (usually outbound traffic)
edit security nat source set rule-set
nat_name
from interface
ge-0/0/4.100
(intf or zone  traffic comes into fw on)
set rule-set
nat_name
from interface
ge-0/0/4.200
(add optional interfaces)
set rule-set
nat_name
from zone
untrust
(can be zone or interface)
set rule-set
nat_name
rule 1 match destination-address
4.2.2.1/32
set rule-set
nat_name
rule 1 then source-nat interface
set security flow tcp-mss ipsec-vpn mss 1350
NAT
Pool Based Destination NAT (usually inbound traffic)
edit security nat destination set pool
webservers
address
172.20.201.10/32
(can be any address)
set rule-set
from_internet
from zone
untrust
(interface or zone)
set rule-set
from_internet
rule 1 match source-address
4.2.0.0/16
set rule-set
from_internet
rule 1 match destination-address
200.1.1.1
(your external address)
set then destination-nat pool
webservers
(you need to create security policy to allow traffic in BOTH directions)
Pool Based Source NAT with Overflow Pool (setting ip's on out interface network)

```plaintext
edit security nat source set pool
vr_name
port no-translation
set pool
vr_name
overflow-pool interface
set pool
vr_name
address
172.20.200.2 to 172.20.200.9
(* ip's you want the destination to see)
set rule-set
vr_name
from zone
zone_name-from
set rule-set
vr_name
to zone
zone_name-to
set rule-set
vr_name
rule
vr_name-to-name
match source-address
172.20.100.0/24
(source IP)
set rule-set
vr_name
rule
vr_name-to-name
then source-nat pool
vr_name
(you need to create security policy to allow traffic in BOTH directions – see policy section)
set proxy arp if your pool is in same network as your interface
edit security nat proxy arp interface
ge-0/0/4.100
(interface with pool ip's on it's net)
set address
172.20.200.2
to
172.20.200.9
(addresses of your pool vr_name)
```

CLUSTERING

On primary firewall
rename interfaces
ge-0/0/0
to
fxp0
(Set management port (if no fxp0))
set chassis cluster cluster-id 1 node 0 reboot
On secondary firewall
set chassis cluster cluster-id 1 node 1 reboot
Set fabric link interfaces
set interfaces fab0 fabric-options member-interfaces
ge-0/0/2
(intf connected to other firewall)
set interfaces fab1 fabric-options member-interfaces
ge-0/0/5
(intf connected to other firewall)
Set backup router routes (to get to secondary fw mgmt port)
set system backup-router
10.210.1.1
destination
10.210.0.0/16
(change ips to your mgmt network)

IDP

Copy IDP license to firewall
> start shell
% cd /var/tmp
% scp user@server:dir1/licensefile.txt .
% cd /var/db/idpd
% scp user@server:/dir1/idp.tar.tgz
% tar xzvf idp.tar.tgz
% exit
```

SETUP REDUNDANCY GROUPS

```plaintext
edit chassis cluster set redundancy-group 0 node 0 priority 200
(control plane node 0 as primary)
set redundancy-group 0 node 1 priority 100
(control plane node 1 as secondary)
set redundancy-group 1 node 0 priority 200
(data plane node 0 as primary)
set redundancy-group 1 node 1 priority 100
(data plane node 1 as secondary)
set redundancy-group 1 preempt
(optional)
set redundancy-group 1 interface-monitor
ge-0/0/3
(weight 255)
… repeat for other interfaces to monitor
setup reth interfaces for data traffic
set interfaces ge-0/0/4
gigether-options redundant-parent reth
0
set interfaces ge-5/0/4
gigether-options redundant-parent reth
0
set interfaces reth
0
redundant-ether-options redundancy-group 1
set interfaces unit 0 family inet address
172.20.1.1/24
(set reth ip address)
```

```plaintext
set security zones security
zone
set interfaces reth
0
security_zone
… repeat for other reth interfaces
```

```plaintext
SETUP REDUNDANCY GROUPS
```

```
set security zones security
zone
set security zones security
zone
set interfaces reth
0
security_zone
… repeat for other reth interfaces
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```
**LOGGING**

define what to log

edit security policies from-zone

set policy zone1-to-zone2-log then log session-init

set policy zone1-to-zone2-log then log session-close

branch srx default logging is local in /var/log for both control and data logs

to set branch srx to log to nsm

set system syslog host x.x.x.x

set system syslog file default-log-messages any any

set system syslog file default-log-messages structured-data

(high-end or branch srx data-plane logging to strm (you have limited local logging due to #sess/sec from pfe to re))

set security log source-address y.y.y.y

set security log format sd-syslog

set security log stream strm_feed severity debug

set security log stream strm_feed category all

set security log stream strm_feed host x.x.x.x

(set security log source-address y.y.y.y, set security log format sd-syslog, set security log stream strm_feed severity debug, set security log stream strm_feed category all, set security log stream strm_feed host x.x.x.x, then commit)

set security log stream strm_feed category content-security

(set security log source-address y.y.y.y, set security log format sd-syslog, set security log stream strm_feed severity debug, set security log stream strm_feed category content-security, then commit)

(set security log source-address y.y.y.y, set security log format sd-syslog, set security log stream strm_feed severity debug, set security log stream strm_feed category content-security, then commit)

(set security log source-address y.y.y.y, set security log format sd-syslog, set security log stream strm_feed severity debug, set security log stream strm_feed category content-security, then commit)

(set security log source-address y.y.y.y, set security log format sd-syslog, set security log stream strm_feed severity debug, set security log stream strm_feed category content-security, then commit)

(set security log source-address y.y.y.y, set security log format sd-syslog, set security log stream strm_feed severity debug, set security log stream strm_feed category content-security, then commit)

(set security log source-address y.y.y.y, set security log format sd-syslog, set security log stream strm_feed severity debug, set security log stream strm_feed category content-security, then commit)

(set security log source-address y.y.y.y, set security log format sd-syslog, set security log stream strm_feed severity debug, set security log stream strm_feed category content-security, then commit)

(set security log source-address y.y.y.y, set security log format sd-syslog, set security log stream strm_feed severity debug, set security log stream strm_feed category content-security, then commit)
**SHOW COMMANDS and TROUBLESHOOTING**

* checking system
  - show system uptime
  - show system alarms
  - show chassis alarms
  - show system processes

* checking schedules – make sure flow is allowed in schedule
  - show schedulers

* checking interfaces
  - show interfaces terse | detail | extensive
  - show interface ge-0/0/1 media | match mtu (see mtu setting)

* checking for security policies
  - show security zones
  - show security policies
  - show security flow session
  - show security flow session session-identifier xx
  - show log messages | match RT_FLOW (only if firewall is logging locally)

* show interfaces extensive
  - ge-0/0/3 | find “Flow Statistics”

* screen settings
  - show security screen statistics zone untrust
  - show log messages | match RT_SCREEN (only if firewall is logging locally)

* view natting
  - show security flow session (make sure return:out address is to the natted address)
  - show security nat source rule all | summary
  - show security nat destination pool all | summary
  - show security nat source summary | pool all

* view VPN
  - show interfaces st0 terse
  - show security ike security-associations
  - show security ipsec security-associations
  - show security ipsec security-associations index xx (xx is the index number from the previous cmd)
  - show security ipsec statistics
  - clear security ike security associations peer-address x.x.x.x (clear SA’s if you are having vpn issues)
  - clear security ipsec security associations index_number (clear specific ipsec, index is from show command)

To view vpn debug logs (does not work in Cluster mode)
  - > request security ike debug-enable local <local IKE IP> remote <IKE GATEWAY IP> level 15
  - > show log kmd (The unit will start to log to the default debug KMD log)

To disable:
  - > request security ike debug-disable

* clustering
  - show chassis cluster status
  - show interface terse (make sure fxp0, fxp1, fab0 and fab1 are up)
  - show interfaces terse | match reth (see status of reth addresses)

* idp
  - show system license
  - show security policies policy-name some-name detail
  - show security idp memory
  - show security idp security-package-version
Trace options to verify flow

- set security flow traceoptions file DEBUG (create a file to store debug)
- set security flow traceoptions flag basic-datapath (flag all paths in flow)
- set security flow traceoptions packet-filter match-outgoing source-prefix 192.168.2.0/24
- set security flow traceoptions packet-filter match-outgoing destination-prefix 0.0.0.0/0
- set security flow traceoptions packet-filter match-reverse source-prefix 0.0.0.0/0
- set security flow traceoptions packet-filter match-reverse destination-prefix 192.168.2.0/24

(match-reverse is needed to capture the entire flow since Junos only captures uni-flow)

- show log DEBUG | trim 42 (shows the traces that match your filter and removes the date and time)

When complete deactivate the trace options – CPU overhead

- deactivate security flow traceoptions