Configuring IPSec with CLI

This section provides information to configure IPSec using the command line interface.

Topics in this section include:

Provisioning an IPSec ISA

An IPSec ISA can only be provisioned on an IOM2. The following output displays a card and ISA configuration.

```
*A:ALA-49>config# info
----------------------------------------------
...
    card 1
        card-type iom2-20g
        mda 1
            mda-type m10-1gb-sfp
        exit
        mda 2
            mda-type isa-ipsec
        exit
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring IPSec ISA

The following output displays an IPSec group configuration in the ISA context. The **primary** command identifies the card/slot number where the IPSec ISA is the primary module for the IPSec group.

```
*A:ALA-49>config# info
----------------------------------------------
...
    isa
        ipsec-group 1 create
            primary 1/2
            no shutdown
        exit
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring Router Interfaces for IPSec

The following output displays an interface “internet” configured using the network port (1/1/1).

```
*A:ALA-49>config# info
----------------------------------------------
...
    router
        interface "internet"
            address 10.10.7.118/24
            port 1/1/1
        exit
        interface "system"
            address 10.20.1.118/32
        exit
        autonomous-system 123
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring IPSec Parameters

The following output displays an IPSec configuration example.

```
*A:ALA-49>config# info
----------------------------------------------
...
    ipsec
        ike-policy 1 create
            ipsec-lifetime 300
            isakmp-lifetime 600
            pfs
            auth-algorithm md5
            dpd interval 10 max-retries 5
        exit
        ipsec-transform 1 create
            esp-auth-algorithm sha1
            esp-encryption-algorithm aes128
        exit
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring IPSec in Services

The following output displays an IES and VPRN service with IPSec parameters configured.

```
*A:ALA-49>config# info
----------------------------------------------
...
    service
        ies 100 customer 1 create
            interface "ipsec-public" create
                address 10.10.10.1/24
                sap ipsec-1.public:1 create
                exit
            exit
            no shutdown
        exit
       vprn 200 customer 1 create
            ipsec
                security-policy 1 create
                    entry 1 create
                        local-ip 172.17.118.0/24
                        remote-ip 172.16.91.0/24
                    exit
                exit
            exit
           route-distinguisher 1:1
            ipsec-interface "ipsec-private" create
                sap ipsec-1.private:1 create
                tunnel "remote-office" create
                    security-policy 1
                  local-gateway-address 10.10.10.118 peer 10.10.7.91 delivery-service
100
                    dynamic-keying
                        ike-policy 1
                        pre-shared-key "humptydumpty"
                        transform 1
                    exit
                    no shutdown
                exit
            exit
            interface "corporate-network" create
                address 172.17.118.118/24
                sap 1/1/2 create
                exit
            exit
          static-route 172.16.91.0/24 ipsec-tunnel "remote-office"
            no shutdown
        exit
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring X.509v3 Certificate Parameters

The following displays steps to configure certificate enrollment.

1. Generate a key.

```
admin certificate gen-keypair cf3:/key_plain_rsa2048 size 2048 type rsa
```

2. Generate a certificate request.

```
admin certificate gen-local-cert-req keypair cf3:/key_plain_rsa2048 subject-dn
"C=US,ST=CA,CN=7750" file 7750_req.csr
```

3. Send the certificate request to CA-1 to sign and get the signed certificate.

4. Import the key.

```
admin certificate import type key input cf3:/key_plain_rsa2048 output key1_rsa2048
format der
```

5. Import the signed certificate.

```
admin certificate import type cert input cf3:/7750_cert.pem output 7750cert format pem
```

The following displays steps to configure CA certificate/CRL import.

1. Import the CA certificate.

```
admin certificate import type cert input cf3:/CA_1_cert.pem output ca_cert format pem
```

2. Import the CA's CRL.

```
admin certificate import type crl input cf3:/CA_1_crl.pem output ca_crl format pem
```

The following displays a certificate authentication for IKEv2 static LAN-to-LAN tunnel configuration.

```
config>system>security>pki
-----------------------------------------------
                ca-profile "CA-1" create
                    shutdown
                    cert-file "ca_cert"
                    crl-file "ca_crl"
             no shutdown
                exit

config>ipsec
-----------------------------------------------
        ike-policy 1 create
            ike-version 2
            auth-method cert-auth
            own-auth-method cert
        exit

config>service>vprn>if>sap
-----------------------------------------------
                    ipsec-tunnel "t50" create
                        security-policy 1
                        local-gateway-address 192.168.55.30 peer 192.168.33.100 delivery-
service 300
                        dynamic-keying
                            ike-policy 1
                            transform 1
                            cert
                                trust-anchor "CA-1"
                                cert "7750cert"
                                key "key1_rsa2048"
                            exit
                        exit
                        no shutdown
                    exit
```

The following displays an example of the syntax to import a certificate from the pem format.

```
*A:SR-7/Dut-A# admin certificate import type cert input cf3:/pre-import/R1-0cert.pem out-
put R1-0cert.der format pem
```

The following displays and example of the syntax to export a certificate to the pem format.

```
*A:SR-7/Dut-A#  admin certificate export type cert input R1-0cert.der output cf3:/R1-
0cert.pem format pem
```

Configuring MC-IPSec

Configuring MIMP

The following is an MIMP configuration example.

```
config>redundancy>multi-chassis
-----------------------------------------------
            peer 2.2.2.2 create
                mc-ipsec
                    bfd-enable
                    tunnel-group 1 create
                        peer-group 2
                        priority 120
                        no shutdown
                    exit
                exit
                no shutdown
            exit
```

The peer's tunnel-group id is not necessarily the same as the local tunnel-group id With **bfd-enable**, the BFD parameters are specified under the interface that the MIMP source address resides on, which must be a loopback interface in the base routing instance. The default source address of MIMP is the system address.

The **keep-alive-interval** and **hold-on-neighbor-failure** define the MIMP alive parameter, however, BFD could be used for faster chassis failure detection.

The SR-OS also provides a **tool** command to manually trigger the switchover such as:

```
tools perform redundancy multi-chassis mc-ipsec force-switchover tunnel-group 1
```

Configuring Multi-Chassis Synchronization

The following displays an MCS for MC-IPSec configuration.

```
config>redundancy>multi-chassis>
-----------------------------------------------
            peer 2.2.2.2 create
                sync
                    ipsec
                    tunnel-group 1 sync-tag "sync_tag_1" create
                    no shutdown
                exit
```

The **sync-tag** must matched on both chassis for the corresponding tunnel-groups.

Configuring Routing for MC-IPSec

The following configuration is an example using a route policy to export /32 local tunnel address route:

```
config>router>policy-options>
-----------------------------------------------
            policy-statement "exportOSPF"
                entry 10
                    from
                        protocol ipsec
                        state ipsec-master-with-peer
                    exit
                    action accept
                        metric set 500
                    exit
                exit
                entry 20
                    from
                        protocol ipsec
                        state ipsec-non-master
                    exit
                    action accept
                        metric set 1000
                    exit
                exit
                entry 30
                    from
                        protocol ipsec
                        state ipsec-master-without-peer
                    exit
                    action accept
                        metric set 1000
                    exit
                exit
            exit
```

The following configuration shows shunting in public and private service.

Shunting in public service:

```
config>service>ies>
            interface "ipsec-pub" create
                address 172.16.100.254/24
                sap tunnel-1.public:100 create
                exit
                static-tunnel-redundant-next-hop 1.1.1.1
            exit
```

Shunting in private service:

```
config>service>vprn>
 interface "ipsec-priv" tunnel create
    …
                static-tunnel-redundant-next-hop 7.7.7.1
            exit
```

Shunting is enabled by configuring redundant next-hop on a public or private IPsec interface

static-tunnel-redundant-next-hop — Shunting nexthop for a static tunnel.

dynamic-tunnel-redundant-next-hop — Shunting next-hop for a dynamic tunnel.