Configuring IPSec with CLI

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

Topics in this section include:

Provisioning a Tunnel 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-tunnel
        exit
    exit
...
----------------------------------------------
*A:ALA-49>config#
```

Configuring a Tunnel Group

The following output displays a tunnel 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
        tunnel-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 tunnel-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" tunnel create
                sap tunnel-1.private:1 create
                ipsec-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

note: since 12.0R1, the system encodes the common name field as UTF8 instead of a
printable string format. If a printable string is required for compatibility add the option
"use-printable" to the request for legacy behavior.
```

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# info
----------------------------------------------
                ca-profile "alu-root" create
                    cert-file "alu_root.cert"
                    crl-file "alu_root.crl"
                    no shutdown
                exit
----------------------------------------------
config>ipsec# info
----------------------------------------------
        ike-policy 1 create
            ike-version 2
            auth-method cert-auth
        exit
        ipsec-transform 1 create
        exit
       cert-profile "segw" create
            entry 1 create
                cert segw.cert
                key segw.key
            exit
            no shutdown
        exit
        trust-anchor-profile "alu" create
            trust-anchor "alu-root"
        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-profile "alu"
                                cert-profile "segw"
                            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.

Configuring and Using CMPv2

CMPv2 server information is configured under corresponding ca-profile by using following key commands:

```
config>system>security>pki>ca-profile
     cmpv2
          url <url-string> [service-id <service-id>]
          response-signing-cert <filename>
          key-list
               key <password> reference <reference-number>
```

The **url** command specifies the HTTP URL of the CMPv2 server, the service specifies the routing instance that the system used to access the CMPv2 server (if omitted, then system will use base routing instance).

Also note that the service ID is only needed for inband connections to the server via VPRN services. IES services are not to be referenced by the service ID as any of those are considered base routing instance.

The **response-signing-cert** command specifies a imported certificate that is used to verify the CMP response message if they are protected by signature. If this command is not configured, then CA's certificate will be used.

The **keylist** specifies a list of pre-shared-key used for CMPv2 initial registration message protection.

For example:

```
config>system>security>pki>ca-profile>
     cmpv2
          url "http://cmp.example.com/request" service-id 100
          key-list
              key passwordToBeUsed reference "1"
```

All CMPv2 operations are invoked by using the **admin certificate cmpv2** command.

If there is no **key-list** defined under the **cmpv2** configuration, the system will default to the **cmpv2** transaction input for the command line in regards to authenticating a message without a senderID. Also, if there is no senderID in the response message, and there IS a key-list defined, it will choose the lexicographical first entry only, if that fails, it will have a fail result for the transaction.

Refer to the command reference section for details about syntax and usage. The system supports optional commands (such as, **always-set-sender-ir**) to support inter-op with CMPv2 servers. Refer to CMPv2 Commands on page 505 for details.

Configuring OCSP

OCSP server information is configured under the corresponding ca-profile:

```
config>system>security>pki>ca-profile>
     ocsp
          responder-url <url-string>
          service <service-id>
```

The **responder-url** command specifies the HTTP URL of the OCSP responder. The **service** command specifies the routing instance that system used to access the OCSP responder.

Example:

```
config>system>security>pki>ca-profile>
     ocsp
          responder-url "http://ocsp.example.com/request"
          service 100
```

For a given ipsec-tunnel or ipsec-gw, the user can configure a primary method, a secondary method and a default result.

```
config>service>ies>if>sap>ipsec-gw>
config>service>vprn>if>sap>ipsec-gw>
config>service>vprn>if>sap>ipsec-tun>
     cert
          status-verify
               primary {ocsp|crl}
               secondary {ocsp|crl}
               default-result {revoked|good}
```

Example:

```
config>service>ies>if>sap>ipsec-gw>
     cert
          status-verify
               primary ocsp
               secondary crl
```

Configuring IKEv2 Remote-Access Tunnel

The following are configuration tasks for an IKEv2 remote-access tunnel:

- Create an ike-policy with one of the auth-methods that enabled the remote-access tunnel.
- Configure a tunnel-template/ipsec-transform This is the same as configuring a dynamic LAN-to-LAN tunnel.
- Create a radius-authentication-policy and optionally, a radius-accounting-policy (a radius-server-policy and a radius-server must be preconfigured)
- Configure a private VPRN service and private tunnel interface with an address on the interface. The internal address assigned to the client must come from the subnet on the private interface.
- Configure a public IES/VPRN service and an ipsec-gw under the public tunnel SAP.
- Configure the radius-authentication-policy and radius-accounting-policy (optional) under the ipsec-gw.
- Certificate the related configuration if cert-radius is used.

The following shows an example using cert-radius:

```
config>system>security>pki# info
----------------------------------------------
                ca-profile "ALU-ROOT" create
                    cert-file "ALU-ROOT.cert"
                    crl-file "ALU-ROOT.crl"
                    no shutdown
                exit
----------------------------------------------
A:SeGW>config>aaa# info
----------------------------------------------
        radius-server-policy "femto-aaa" create
            servers
                router "management"
                server 1 name "svr-1"
            exit
        exit
----------------------------------------------
A:SeGW>config>router# info
----------------------------------------------
        radius-server
            server "svr-1" address 10.10.10.1 secret "KR35xB3W4aUXtL8o3WzPD." hash2 create
            exit
        exit
----------------------------------------------

config>ipsec# info
----------------------------------------------
        ike-policy 1 create
            ike-version 2
            auth-method cert-radius
        exit
        ipsec-transform 1 create
```

```
        exit
        tunnel-template 1 create
            transform 1
        exit
        cert-profile "c1" create
            entry 1 create
                cert SeGW2.cert
                key SeGW2.key
            exit
            no shutdown
        exit
        trust-anchor-profile "tap-1" create
            trust-anchor "ALU-ROOT"
        exit
        radius-authentication-policy "femto-auth" create
            include-radius-attribute
                calling-station-id
                called-station-id
            exit
            password "DJzlyYKCefyhomnFcFSBuLZovSemMKde" hash2
            radius-server-policy "femto-aaa"
        exit
        radius-accounting-policy "femto-acct" create
            include-radius-attribute
                calling-station-id
                framed-ip-addr
            exit
            radius-server-policy "femto-aaa"
        exit

-----------------------------------------------
config>service>ies# info
-----------------------------------------------
            interface "pub" create
                address 172.16.100.0/31
                tos-marking-state untrusted
                sap tunnel-1.public:100 create
                    ipsec-gw "rw"
                        cert
                            trust-anchor-profile "tap-1"
                            cert-profile "c1"
                        exit
                        default-secure-service 400 interface "priv"
                        default-tunnel-template 1
                        ike-policy 1
                        local-gateway-address 172.16.100.1
                        radius-accounting-policy "femto-acct"
                        radius-authentication-policy "femto-auth"
                        no shutdown
                    exit
                exit
            exit
            no shutdown
-----------------------------------------------
A:SeGW>config>service>vprn# info
-----------------------------------------------
            route-distinguisher 400:11
            interface "priv" tunnel create
                address 20.20.20.1/24
                sap tunnel-1.private:200 create
                exit
```

```
            exit
            interface "l1" create
                address 9.9.9.9/32
                loopback
            exit
            no shutdown
-------------------------------------------
```

Configuring IKEv2 Remote — Access Tunnel with Local Address Assignment

The following are configuration tasks of IKEv2 remote-access tunnel:

- Create an **ike-policy** with any **auth-method.**
- Configure the **tunnel-template** or **ipsec-transform**. (This is the same as configuring a dynamic LAN-to-LAN tunnel.)
- Configure a private VPRN service and a private tunnel interface with an address on the interface. The internal address assigned to the client must come from the subnet on the private interface.
- Configure a local DHCPv4 or DHCPv6 server with address pool that from which the internal address to be assigned from.
- Configure public IES/VPRN service and **ipsec-gw** under public tunnel SAP.
- Configure the local address assignment under **ipsec-gw**.

The following output shows an example using cert-auth:

```
config>system>security>pki# info
----------------------------------------------
                ca-profile "smallcell-root" create
                    cert-file "smallcell-root-ca.cert"
                    revocation-check crl-optional
                    no shutdown
                exit
----------------------------------------------
config>ipsec# info
----------------------------------------------
        ike-policy 3 create
            ike-version 2
            auth-method cert-auth
            nat-traversal
        exit
        ipsec-transform 1 create
        exit
        cert-profile "segw-mlab" create
            entry 1 create
                cert SeGW-MLAB.cert
                key SeGW-MLAB.key
            exit
            no shutdown
        exit
        trust-anchor-profile "sc-root" create
            trust-anchor "smallcell-root"
        exit
        tunnel-template 1 create
            transform 1
        exit
----------------------------------------------
config>service>ies# info
----------------------------------------------
            interface "pub" create
```

```
                address 172.16.100.253/24
                tos-marking-state untrusted
                sap tunnel-1.public:100 create
                    ipsec-gw "rw"
                        default-secure-service 400 interface "priv"
                        default-tunnel-template 1
                        ike-policy 3
                        local-address-assignment
                            ipv6
                                address-source router 400 dhcp-server "d6" pool "1"
                            exit
                            no shutdown
                        exit
                        local-gateway-address 172.16.100.1
                        cert
                            trust-anchor-profile "sc-root"
                            cert-profile "segw-mlab"
                            status-verify
                                default-result good
                            exit
                        exit
                        local-id type fqdn value segwmobilelab.alu.com
                        no shutdown
                    exit
                exit
            exit
            no shutdown
-----------------------------------------------
config>service>vprn# info
-----------------------------------------------
            dhcp6
                local-dhcp-server "d6" create
                    use-pool-from-client
                    pool "1" create
                        options
                            dns-server 2001::808:808
                        exit
                        exclude-prefix 2001:beef::101/128
                        prefix 2001:beef::/96 failover access-driven pd wan-host create
                        exit
                    exit
                    no shutdown
                exit
            exit
            route-distinguisher 400:1
            interface "priv" tunnel create
                ipv6
                    address 2001:beef::101/96
                exit
                sap tunnel-1.private:200 create
                exit
            exit
            no shutdown
-----------------------------------------------
```