IPSec Design

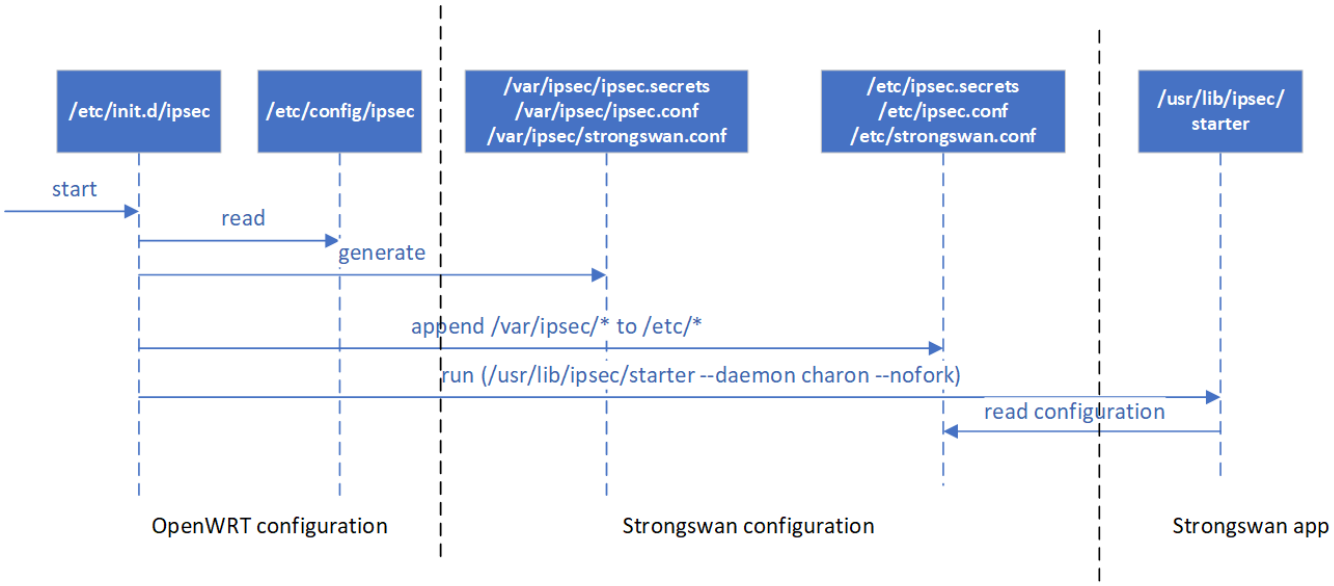
Introduction

ICN SDEWAN solution leverages IPSec functionality in SD-EWAN CNF to setup security tunnel to enable communication between ONAP4K8S/APPX Manager with Edge cluster or Edge cluster with Edge cluster. There are several solutions in OpenWRT to implement IPSec, include: Openswan, Racoon, and StrongSwan. ICN will use StrongSwan solution.

OpenWRT StrongSwan Basic

Service Start Flow:

StrongSwan application is run by command: "/etc/init.d/ipsec start", this command will generate StrongSwan's configuration (e.g. /etc/ipsec/*) based on openwrt configuration (e.g. /etc/config/ipsec) then start ipsec application as daemon, below diagram shows its flow



Configuration: OpenWRT's IPSec Configuration is defined in /etc/config/ipsec, the detail configuration content and map to StrongSwan configuration are described in below table

Section	Option	Type	StrongSwan configuration file	StrongSwan configuration option	Validated values	Description
ipsec						Global configuration
	debug	int	strongswan.conf	charon.syslog		whether to enable log information
	rtinstall_enabled	boolean	strongswan.conf	charon.install_routes		Install routes into a separate routing table for established IPsec tunnels.
	ignore_routing_tables	list	strongswan.conf	charon.ignore_routing_tables		A space-separated list of routing tables to be excluded from route lookup.
	interface	list	strongswan.conf	charon.interfaces_use		A comma-separated list of network interfaces that should be used by charon. All other interfaces are ignored.
remote						Define a group remote tunnels with same security configuration
	tunnel	list				
	transport	list				
	enabled	boolean				whether this configuration is enabled

	gateway	String	ipsec.secrets ipsec.conf	local_gateway/remote_gateway right	192.168.0.5	Defines the counter party ip address here
	pre_shared_key	String	ipsec.secrets	PSK		Add the PSK inside the secrets file
	authentication_method	String	ipsec.conf	leftauth/rightauth	pubkey, psk, eap, xauth	Defines the auth method that going to be used by two counter parties.
	local_identifier	String	ipsec.secrets ipsec.conf	local_identifier leftid	"C=CH, O=strongSwan, CN=peer"	Assigns a specific identifier for the itself (This identity will be send to the counter party inside the request)
	remote_identifier	String	ipsec.secrets ipsec.conf	remote_identifier rightid	"C=CH, O=strongSwan, CN=peerB"	Assigns a specific identifier for the counter party
	crypto_proposal	list	ipsec.conf	ike	default: aes128-sha256-modp3072	Defines list of IKE/ISAKMP SA encryption/authentication algorithms to be used
	force_crypto_proposal	boolean				
tunnel /transport						Define configuration for a tunnel or transport
	mode	String	ipsec.conf	auto	add/start/route	Sets the operation for the connection while starts.
	local_subnet	String	ipsec.conf	leftsubnet	192.168.1.1/24	Mostly used in site-to-site case. Sets the local subnet
	local_nat	String	ipsec.conf	leftsubnet	192.168.1.1/24	Mostly used in site-to-site case. Sets the local subnet
	local_sourceip	String	ipsec.conf	leftsourceip	192.168.1.2, %config	Sets the ip address of local site. The value can be set to '%config' if the site is going to request a dynamic ip from the counter party
	local_updown	String	ipsec.conf	leftupdown	<path_to_script>	The Updown plugin can be used to set custom firewall rules.
	local_firewall	String	ipsec.conf	leftfirewall	yes, no(default)	Whether the local site is doing forwarding-firewalling (including masquerading) using iptables for traffic from left|rightsubnet
	remote_subnet	String	ipsec.conf	rightsubnet	192.168.0.1/24	Mostly used in site-to-site case. Sets the subnet of the counter party
	remote_sourceip	String	ipsec.conf	rightsourceip	192.168.0.2, 192.168.0.3-192.168.0.15	Sets the ip address of the remote site. An ip pool can also be assigned when using the virtual ip
	remote_updown	String	ipsec.conf	rightupdown	<path_to_script>	The path to the updown script to run to adjust routing and/or firewalling when the status of the connection changes
	remote_firewall	String	ipsec.conf	rightfirewall	yes, no(default)	Whether the remote site is doing forwarding-firewalling (including masquerading) using iptables for traffic from left|rightsubnet
	*ikelifetime	String	ipsec.conf	ikelifetime	3h(default)	Sets the life time of the ike process before its re-negotiation. (Currently using default value)
	*lifetime	String	ipsec.conf	lifetime	1h(default)	Set the life time of a particular instance would last. (Currently using default value)
	*margintime	String	ipsec.conf	margintime	9m(default)	Sets how long before connection expiry or keying-channel expiry should attempts to negotiate a replacement begin. (Currently using default value)
	*keyingtries	String	ipsec.conf	keyingtries	3(default)	Sets the maxium attempts to negotiate for a connection. (Currently using default value)
	*dpdaction	String	ipsec.conf	dpdaction	clear, hold, restart, none (default)	Sets the action against peer timeout, validated through Dead Peer Protection Protocol. (Currently using default value)
	*dpddelay	String	ipsec.conf	dpddelay	30s(default)	Defines the time interval for the informational exchange sent to peer. (Currently using default value)

	*inactivity	boolean	ipsec.conf	inactivity	30m	Defines the timeout interval, after which a CHILD_SA is closed if it did not send or receive any traffic. (Currently using default value)
	*keyexchange	String	ipsec.conf	keyexchange	ikev2, ikev1, ike (default, same as ikev2)	Defines the protocol being used to initialize the connection. (Currently using default value)
	crypto_proposal	list	ipsec.conf	esp	aes128-sha256 (default)	Defines the comma-separated list of ESP encryption/authentication algorithms to be used for the connection
	*local_public_cert	String	ipsec.conf	leftcert	peer.der/peer.pem	Sets the path of the local certificate used for authentication **NOTE: This is a key that currently not supported by OpenWrt**
	*remote_public_cert	String	ipsec.conf	rightcert	peerB.der /peerB.pem	Sets the path of the remote certificate used for authentication **NOTE: This is a key that currently not supported by OpenWrt**
	*local_private_cert	String	/etc/ipsec.d /private			Puts the path of private key for the certificate. Maybe not needed for the CRD. But need to upload the file. **NOTE: This is a key that currently not supported by OpenWrt**
	*shared_ca	String	/etc/ipsec.d /cacerts			Puts the shared CA for auth. Maybe not needed for CRD, but need to upload the file. **NOTE: This is a key that currently not supported by OpenWrt**
proposal						Define configuration for a proposal
	encryption_algorithm	String	ipsec.conf	ike/esp	aes128	Defines the encryption algorithm(together in ike)
	hash_algorithm	String	ipsec.conf	ike/esp	sha256	Defines the hash algorithm(together in ike)
	dh_group	String	ipsec.conf	ike/esp	modp3072	Define the Diffie-Hellman group(together in ike)
	*proposal_name	String				Define the proposal name.

IPSec CRD

IPSec CRD will be created by EWAN config Agent to configurate a remote configuration. it is defined as below, with filed map to ipsec configuration.

SDEWAN IPSec Proposal CR

```
apiVersion: sdewan.akraino.org/v1alpha1
kind: IpsecProposal
metadata:
  name: test_proposal_1
  namespace: default
  labels:
    sdewanPurpose: cnf-1
spec:
  encryption_algorithm: aes128
  hash_algorithm: sha256
  dh_group: modp3072
status:
  appliedVersion: "1"
  appliedTime: "2020-04-12T09:28:38Z"
  inSync: True
```

SDEWAN IPSec Site CR

```
apiVersion: sdewan.akraino.org/v1alpha1
kind: IpsecSite
metadata:
  name: ipsecsite-sample
  namespace: default
  labels:
    sdewanPurpose: cnf-1
spec:
  type: route-based/policy-based
  remote: xx.xx.xx.xx
  authentication_method: psk
  pre_shared_key: xxx
  local_public_cert:
  local_private_cert:
  shared_ca:
  local_identifier:
  remote_identifier:
  crypto_proposal:
    - test_proposal_1
  connections:
    - connection_name: connection_A
      type: tunnel
      mode: start
      local_subnet: 172.12.0.0/24, 10.239.160.22
      remote_sourceip: 172.12.0.30-172.12.0.45
      remote_subnet:
      mark: xxx
      crypto_proposal:
        - test_proposal_1
status:
  appliedVersion: "1"
  appliedTime: "2020-04-12T09:28:38Z"
  inSync: True
```

SDEWAN IPSec Host CR

```
apiVersion: sdewan.akraino.org/v1alpha1
kind: IpsecHost
metadata:
  name: ipsechost-sample
  namespace: default
  labels:
    sdewanPurpose: cnf-1
spec:
  type: route-based/policy-based
  remote: xx.xx.xx.xx/%any
  authentication_method: psk
  pre_shared_key: xxx
  local_public_cert:
  local_private_cert:
  shared_ca:
  local_identifier:
  remote_identifier:
  crypto_proposal:
    - test_proposal_1
  connections:
    - connection_name: connection_A
      type: tunnel
      mode: start
      local_sourceip: %config
      remote_sourceip: xx.xx.xx.xx
      remote_subnet: xx.xx.xx.xx/xx
      mark: xxx
      crypto_proposal:
        - test_proposal_1
status:
  appliedVersion: "1"
  appliedTime: "2020-04-12T09:28:38Z"
  inSync: True
```

Draft for route based tunnel

```
ip tunnel add vti0 local 192.168.0.1 remote 192.168.0.2 mode vti key 0x01000201
sysctl -w net.ipv4.conf.vti0.disable_policy=1
ip link set vti0 up
ip route add 10.1.0.0/16 dev vti0
```

SDEWAN IPSec Route based

```
apiVersion: sdewan.akraino.org/v1alpha1
kind: IpsecHost
metadata:
  name: ipsec-route-based
  namespace: default
  labels:
    sdewanPurpose: cnf-1
spec:
  remote: xx.xx.xx.xx/%any
  authentication_method: psk
  pre_shared_key: xxx
  local_public_cert:
  local_private_cert:
  shared_ca:
  local_identifier:
  remote_identifier:
  crypto_proposal:
    - test_proposal_1
  connections:
    - connection_name: connection_A
      type: tunnel
      mode: start
      local_sourceip: %config
      remote_sourceip: xx.xx.xx.xx
      local_subnet: xx.xx.xx.xx/xx
      remote_subnet: xx.xx.xx.xx/xx
      mark_in: 0xffffffff
      mark_out: 0xffffffff
      crypto_proposal:
        - test_proposal_1
status:
  appliedVersion: "1"
  appliedTime: "2020-04-12T09:28:38Z"
  inSync: True
```

IPSec Rest API

SD-EWAN IPSec Restful API provides support to get/create/update/delete IPSec Site, Proposal.

IPSec Proposal

POST /cgi-bin/luci/sdewan/ipsec/v1/proposals

create a new proposal

Request:

- Request Parameters: same with PUT's request
- Request Example: same with PUT's example

Response

- Normal response codes: 201
- Error response codes: 400, 401

PUT /cgi-bin/luci/sdewan/ipsec/v1/proposals/{proposal-name}

update a proposal

Request:

- Request Parameters:

Name	In	Type	Description

proposal-name	path	string	proposal name
encryption_algorithm	body	string	encryption algorithm
hash_algorithm	body	string	hash algorithm
dh_group	body	string	Diffie-Hellman group

- Request Example
  PUT /cgi-bin/luci/sdewan/ipsec/proposals/proposal1

```
{
    "encryption_algorithm": "aes256",
    "hash_algorithm": "sha256",
    "dh_group": "modp4096"
}
```

Response

- Normal response codes: 204
- Error response codes: 400, 401, 404

GET /cgi-bin/luci/sdewan/ipsec/v1/proposals

Lists all defined proposals

Request: N/A

Response

- Normal response codes: 200
- Response Parameters

Name	In	Type	Description
proposals	body	array	a dict of defined proposals

- Response Example

```
{
  "proposals": [
    {
      "name": "proposal1",
      "encryption_algorithm": "aes128",
      "hash_algorithm": "sha256",
      "dh_group": "modp3072"
    }
  ]
}
```

GET /cgi-bin/luci/sdewan/ipsec/v1/proposals/{proposal-name}

Get a proposal

Request: N/A

- Request Parameters

Name	In	Type	Description
proposal-name	path	string	proposal name

Response

- Normal response codes: 200
- Error response code: 404
- Response Parameters

Name	In	Type	Description
name	body	string	proposal name
encryption_algorithm	body	string	encryption algorithm
hash_algorithm	body	string	hash algorithm
dh_group	body	string	Diffie-Hellman group

- Response Example

```
{
    "name": "proposal1",
    "encryption_algorithm": "aes128",
    "hash_algorithm": "sha256",
    "dh_group": "modp3072"
}
```

DELETE /cgi-bin/luci/sdewan/ipsec/v1/proposals/{proposal-name}

delete a proposal

Request:

- Request Parameters

Name	In	Type	Description
proposal-name	path	string	proposal name

Response

- Normal response codes: 200
- Error response codes: 401, 404

IPSec Site

POST /cgi-bin/luci/sdewan/ipsec/v1/sites

create a new site

Request:

- Request Parameters: same with PUT's request
- Request Example: same with PUT's example

Response

- Normal response codes: 201
- Error response codes: 400, 401

PUT /cgi-bin/luci/sdewan/ipsec/v1/sites/{site-name}

update a site

Request:

- Request Parameters:

Name	In	Type	Required	Description
site-name	path	string	Y	Site name
gateway	body	string	Y	The corresponding responder
pre_shared_key	body	string	N	Optional, only if using the PSK authentication mode

local_public_cert	body	string	N	Optional, only if using the public key authentication mode. Public key used for auth.
local_private_cert	body	string	N	Optional, only if using the public key authentication mode. Private key used for auth.
shared_ca	body	string	N	Optional, only if using the public key authentication mode. CA information
authentication_method	body	string	Y	Either 'psk' or 'pubkey' as the authentication method.
local_identifier	body	string	N	The identifier for localhost
remote_identifier	body	string	N	The identifier for remote counter party
crypto_proposal	body	list	Y	Proposal names used for ike process
force_crypto_proposal	body	boolean	N	The flag on forcing the proposal or not
connections	body	list	Y	List of connectionArray

connectionArray:

Name	In	Type	Required	Description
name	body	string	Y	Connection name
type	body	string	Y	Type of connection. Either "tunnel" or "transport"
mode	body	string	Y	Mode used for connection. Either 'add', 'route' or 'start'
local_subnet	body	string	N	Defines the local subnet.
local_nat	body	string	N	Defines the local nat, if exists, replace the local_subnet
local_sourceip	body	string	N	Defines the local source ip
local_updown	body	string	N	Defines the local iptable rules.
local_firewall	body	string	N	Flag used to determine whether to enable the local firewall rules or not
remote_subnet	body	string	N	Defines the subnet of the counter party
remote_sourceip	body	string	N	Defines the source ip of the counter party
remote_updown	body	string	N	Defines the iptable rules applied for the counter party
remote_firewall	body	string	N	Flag used to determine whether to enable the remote firewall rules or not
crypto_proposal	body	string	N	Crypto proposal used for ESP

- Request Example
  PUT /cgi-bin/luci/sdewan/ipsec/v1/sites/sites

```
{
    "gateway": "10.1.0.2",
    "name": "site1",
    "crypto_proposal": "proposal1"
    "connections": [
     {
       "name": "site_to_site",
       "type": "tunnel"
       "local_subnet":
       "remote_subnet":
        "crypto_proposal": "proposal1"
     }
}
```

Response

- Normal response codes: 204
- Error response codes: 400, 401, 404

GET /cgi-bin/luci/sdewan/ipsec/v1/sites

Lists all defined sites

Request: N/A

Response

- Normal response codes: 200
- Response Parameters

Name	In	Type	Description
sites	body	array	a list of defined sites

- Response Example


```
{
   "sites": [
     {   "name": "site1",
         "gateway":"10.0.1.2",
         "authentication_method": "psk",
         "crypto_proposal": "proposal1",
         "connections": [
          {
            "name": "connA"
            "type": "tunnel"
            "local_subnet": "192.168.1.1/24",
            "remote_subnet": "192.168.0.1/24",
            "crypto_proposal": "proposal1"
          }
        ]
     }
   ]
}
```


GET /cgi-bin/luci/sdewan/ipsec/v1/sites/{site-name}

Get a site

Request: N/A

- Request Parameters

Name	In	Type	Description
site-name	path	string	remote site name

Response

- Normal response codes: 200
- Error response code: 404
- Response Parameters

Name	In	Type	Required	Description
name	body	string	Y	Site name
gateway	body	string	Y	The corresponding responder
pre_shared_key	body	string	N	Optional, only if using the PSK authentication mode

local_public_cert	body	string	N	Optional, only if using the public key authentication mode. Public key used for auth.
local_private_cert	body	string	N	Optional, only if using the public key authentication mode. Private key used for auth.
shared_ca	body	string	N	Optional, only if using the public key authentication mode. CA information
authentication_method	body	string	Y	Either 'psk' or 'pubkey' as the authentication method.
local_identifier	body	string	N	The identifier for localhost
remote_identifier	body	string	N	The identifier for remote counter party
crypto_proposal	body	list	Y	Proposal names used for ike process
force_crypto_proposal	body	boolean	N	The flag on forcing the proposal or not
connections	body	list	Y	List of connectionArray

connectionArray:

Name	In	Type	Required	Description
name	body	string	Y	Connection name
type	body	string	Y	Type of connection. Either "tunnel" or "transport"
mode	body	string	Y	Mode used for connection. Either 'add', 'route' or 'start'
local_subnet	body	string	N	Defines the local subnet.
local_nat	body	string	N	Defines the local nat, if exists, replace the local_subnet
local_sourceip	body	string	N	Defines the local source ip
local_updown	body	string	N	Defines the local iptable rules.
local_firewall	body	string	N	Flag used to determine whether to enable the local firewall rules or not
remote_subnet	body	string	N	Defines the subnet of the counter party
remote_sourceip	body	string	N	Defines the source ip of the counter party
remote_updown	body	string	N	Defines the iptable rules applied for the counter party
remote_firewall	body	string	N	Flag used to determine whether to enable the remote firewall rules or not
crypto_proposal	body	string	N	Crypto proposal used for ESP

- Response Example

```
{
    "name": "site1",
    "gateway":"10.1.0.2",
    "crypto_proposal": "proposal1"
    "connections": [
     {
       "name": "site_to_site",
       "type": "tunnel",
       "local_subnet":
       "remote_subnet":
        "crypto_proposal": "proposal2"
     }
   ]
}
```

DELETE /cgi-bin/luci/sdewan/ipsec/v1/sites/{site-name}

delete a site

Request:

- Request Parameters

Name	In	Type	Description
site-name	path	string	remote site name

Response

- Normal response codes: 200
- Error response codes: 401, 404