Crypto Templates

This chapter describes how to configure and use StarOS crypto templates.

The CLI Crypto Template Configuration Mode is used to configure an IKEv2 IPSec policy. It includes most of the IPSec parameters and IKEv2 dynamic parameters for cryptographic and authentication algorithms. A security gateway service will not function without a configured crypto template. Only one crypto template can be configured per service.

The following topics are discussed:

Crypto Template Parameters

A crypto template requires the configuration of the following parameters:

- **allow-cert-enc cert-hash-url** – Enables support for certificate enclosure type other than default.
- **allow-custom-fqdn-idr** – Allows non-standard FQDN (Fully Qualified Domain Name) strings in the IDr (Identification - Responder) payload of IKE_AUTH messages received from the UE with the payload type as FQDN.
- **authentication** – Configures the gateway and subscriber authentication methods to be used by this crypto template.
- **blacklist** – Enables use of a blacklist file
- **ca-certificate list** – Binds an X.509 Certificate Authority (CA) root certificate to a crypto template.
- **ca-crl list** – Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto template.
- **certificate** – Binds a single X.509 trusted certificate to a crypto template.
- **control-dont-fragment** – Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.
- **dns-handling** – Adds a custom option to define the ways a DNS address is returned based on proscribed circumstances described below.

- **dos cookie-challenge notify-payload** – Configures the cookie challenge parameters for IKEv2 INFO Exchange notify payloads for the given crypto template.
- **identity local** – Configures the identity of the local IPSec Client (IKE ID).
- **ikev2-ikesa** – Configures parameters for the IKEv2 IKE Security Associations within this crypto template.
- **ip mtu** – Configures the MTU (Maximum Transmission Unit) of the user payload for IPv4 tunnels in bytes.
- **ipv6 mtu** – Configures the MTU of the user payload for IPv6 tunnels in bytes.
- **keepalive** – Configures keepalive or dead peer detection for security associations used within this crypto template.
- **max-childsa** – Defines a soft limit for the number of child Security Associations (SAs) per IKEv2 policy.
- **nai** – Configures the Network Access Identifier (NAI) parameters to be used for the crypto template IDr (recipient's identity).
- **natt** – Configures Network Address Translation - Traversal (NAT-T) for all security associations associated with this crypto template. This feature is disabled by default.
- **ocsp** – Enables Online Certificate Store Protocol (OCSP) requests from the crypto map/template.
- **payload** – Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.
- **peer network** – Configures a list of allowed peer addresses on this crypto template.
- **remote-secret-list** – Configures Remote Secret List.
- **whitelist** – Enables use of a whitelist file.

Crypto Template IKEv2-Dynamic Payload Parameters

The Crypto Template IKEv2-Dynamic Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses. There should be two payloads configured. The first must have a dynamic addressing scheme from which the ChildSA gets a TIA address. The second payload supplies the ChildSA with a HoA, which is the default setting for ip-address-allocation.

Crypto template payloads include the following parameters:

- **ignore-rekeying-requests** – Ignores CHILD SA rekey requests from the Packet Data Interworking Function (PDIF).
- **ip-address-allocation** – Configures IP address allocation for subscribers using this crypto template payload. Configure two payloads per crypto template. The first must have a dynamic address to assign a tunnel inner address (TIA) to the ChildSA. The second payload is configured after a successful MAnaged IP (MIP) initiation and can use the default Home Address (HoA) option.
- **ipsec transform set** -–Configures the IPSec transform set to be used for this crypto template payload.
- **lifetime** – Configures the number of seconds for IPSec Child SAs derived from this crypto template payload to exist.

- **maximum-child-sa** – Configures the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association.
- **rekey [disallow-param-change]** – Configures IPSec Child Security Association rekeying.
- **tsi** – Configures the IKEv2 Traffic Selector initiator (TSi) payload address options.
- **tsr** – Configures the IKEv2 Traffic Selector responder (TSr) payload address options.

Configuring a Crypto Template

The general command sequence for configuring a crypto template is as follows.

```
configure
   context ctxt_name
      crypto template template_name ikev2-dynamic
         allow-cert-enc cert-hash-url
         allow-custom-fqdn-idr
         authentication { eap-profile name [ second-phase eap-profile name ]
 | local { certificate | pre-shared-key { encrypted key value | key clear_text
 } } |  pre-shared-key { encrypted key value | key clear_text [ second-phase
 eap-profile name ] } | remote { certificate | eap-profile name [
second-phase eap-profile name ] | pre-shared-key { encrypted key value | key
 clear_text [ second-phase eap-profile name ] } } }
         blacklist
         ca-certificate list ca-cert-name name [ ca-cert-name name ]
         ca-crl list ca-crl-name name [ ca-crl-name name ]
         certificate name
         control-dont-fragment { clear-bit | copy-bit | set-bit }
         dns-handling { custom | normal }
        dos cookie-challenge notify-payload [ half-open-sess-count { start
 integer | stop integer } ]
         identity local id-type type id name
         ikev2-ikesa { allow-empty-ikesa | cert-sign { pkcs1.5 | pkcs2.0 }
 | ignore-notify-protocol-id | ignore-rekeying-requests |
keepalive-user-activity | max-retransmissions number | policy {
congestion-rejection [notify-status-value] | error-notification
[invalid-major-version] [invalid-message-id
[invalid-major-version|invalid-syntax]] | invalid-syntax
[invalid-major-version] } | rekey | retransmission-timeout msec |
setup-timer sec | transform-set list name1 name2 name3 name4 name5 name6 }
         keepalive [ interval sec ]
         max-childsa numbr [ overload action { ignore | terminate } ]
        nai { idr name [ id-type { der-asn1-dn | der-asn1-gn | fqdn | ip-addr
 | key-id | rfc822-addr } ] | use-received-idr }
         natt [ include-header ] [ send-keepalive [ idle-interval idle_secs
] [ interval interval_secs ]
         ocsp [ nonce ]
         payload payload_namee match childsa
            ignore-rekeying-requests
            ip-address-allocation { dynamic | home-address }
```

```
          ipsec transform-set list name
          lifetime { sec [ kilo-bytes kbytes ] | kilo-bytes kbytes }
          maximum-child-sa num
          rekey [ keepalive ]
          tsi start-address { any { end-address any } | endpoint {
end-address endpoint } }
       peer network ip_address {/mask | mask ip_mask } [ encrypted
pre-shared-key key | pre-shared-key key ]
       remote-secret-list list_name
       whitelist
       end
```

Notes:

- You can enable **blacklist** or **whitelist**, but not both. For additional information, refer to the *Access Control via Blacklist or Whitelist* section of the *Access Control* chapter of this guide.
- For more information on the above commands and keywords, see the *Crypto Template Configuration Mode Commands* and *Crypto Template IKEv2 Dynamic Payload Configuration Mode Commands* chapters of the *Command Line Interface Reference*.

Verifying a Crypto Template Configuration

Enter the following Exec mode command for the appropriate context to display and verify your crypto template:

show crypto template tag *map_name*

This command outputs configuration information for the specified template.

The following is a sample output for a crypto template named *wsg-01*.

```
Map Name: wsg01
=======================================

  Map Status: Complete

  Crypto Map Type: IPSEC IKEv2 Template

  IKE SA Transform 1/1

    Transform Set: ikesa-wsg-01
      Encryption Cipher: aes-chc-128
      Pseudo Random Function: sha1
      Hashed Message Authentication Code: sha1-96
      Diffie-Hellman Group: 2
  IKE SA Rekey: Disabled
  Blacklist/Whitelist : None

  OCSP Status:        : Disabled
  OCSP Nounce Status  : Enabled

  NAI: 92.99.99.30

  Remote-secret-list: <not configured>

  Authetication Local:
         Phase 1 - Pre-Shared Key (Size = 3)
```

```
Self-certificate Validation: Diabled


IPSec SA Payload 1/1 (Generic)
  Name : wsg-sa0
  Payload Local
    Protocol 255 Port 0-0 Address Range 76.67.0.1-76.67.0.1
  Payload Remote
    Protocol 255 Port 0-0 Address Range 54.45.0.1-54.45.0.1
  IPSec SA Transform 1/1
    Transform Set: tselsa-wsg
      Protocol: esp
      Encryption Cipher: aes-cbc-128
      Hashed Message Authentication Code: sha1-96
      Diffie-Hellman Group: none
  IPSec SA Rekey: Enabled

Dead Peer Detection: Disabled

Maximum CHILD_SA: 2 Overload Action: Ignore

DOS Cookie Challenge: Disabled
Dont Fragment: Copy bit from inner header

Local Gateway: Not Set
Remote Gateway: Not Set
```