IKEv2 RFC 5996 Compliance

This chapter describes how StarOS complies with RFC 5996 – Internet Key Exchange Protocol Version 2 (IKEv2).

The following topics are discussed:

RFC 5996 Compliance

Overview

StarOS currently complies with RFC 4306 – *Internet Key Exchange (IKEv2) Protocol*. StarOS IKEv2 has been enhanced to comply with RFC 5996 – *Internet Key Exchange Protocol Version 2 (IKEv2)*.

RFC 5996 introduces two new notification payloads using which certain conditions of the sender can be notified to the receiver. The IANA assigned numbers for these payloads are as follows:

- TEMPORARY_FAILURE – IANA Assigned Number = 43
- CHILD_SA_NOT_FOUND – IANA Assigned Number = 44

StarOS sends the above payloads only in collision scenarios as mentioned in RFC 5996 Section 2.25.

TEMPORARY_FAILURE

A TEMPORARY_FAILURE notification should be sent when a peer receives a request that cannot be completed due to a temporary condition. When StarOS receives this notification type, it waits (50% of the remaining time of the IKESA/Child SA) and then retries a maximum of eight times until the hard lifetimer expires. A retry is initiated only if 50% of the remaining time is greater than or equal to two minutes. If it continues to receive TEMPORARY_FAILURE for all the retries initiated, no further retry is done and the IKESA/Child SA is deleted after its hard lifetime expiry.

When TEMPORARY_FAILURE is received, retry is done only for an exchange corresponding to REKEYS. If temporary failure is received for a non-rekey exchange, the temporary failure is considered as failed for the exchange.

CHILD_SA_NOT_FOUND

A CHILD_SA_NOT_FOUND notification should be sent when a peer receives a request to rekey a Child SA that does not exist. If StarOS receives this notification, it silently deletes the Child SA.

On receipt of CHILD_SA_NOT_FOUND, the CHILDSA for which REKEY was initiated is terminated. If the CHILDSA is the only CHILDSA under the IKESA, the IKESA is terminated and a DELETE request is sent to the peer for the same.

Exchange Collisions

In IKEv2 exchange collisions may happen when both peers start an exchange for an IKE SA at the same time. For example UE starts CHILDSA REKEY using CREATE_CHILD_SA and a security gateway also starts CHILDSA REKEY when SA soft lifetime has expired in both at the same time.

RFC 5996 defines a framework to resolve this collision so that only one of the exchanges succeeds. The collision handling mechanism supported in StarOS complies with the mechanism defined in RFC 5996.

Integrity with Combined Mode Ciphers

RFC 5996 makes changes in specifications to allow negotiation of combined mode ciphers. Combined mode ciphers are algorithms that support integrity and encryption in a single encryption algorithm. RFC 5996 makes negotiation for the integrity algorithm optional if combined mode cipher is used. In RFC 4306 the integrity algorithm was mandatory in the SA payload.

StarOS does not support the combined mode cipher. Staros IKEv2 has been enhanced to identify a currently defined combined cipher. If a proposal for combined mode cipher is received, StarOS responds with NO_PROPOSAL_CHOSEN if no other proposal matches.

Negotiation Parameters in CHILDSA REKEY

On rekeying of a CHILD SA the traffic selectors and algorithms match the ones negotiated during the set up of the child SA. StarOS IKEv2 does not send any new parameters in CREATE_CHILD_SA for a child SA being rekeyed.

Certificates

StarOS supports a CLI command to enable sending and receiving HTTP method for hash-and-URL lookup with CERT/CERTREQ payloads.

If configured and if a peer requests CERT using encoding type as "Hash and URL of X.509 certificate" and send HTTP_CERT_LOOKUP_SUPPORTED using notify payload in the first IKE_AUTH, StarOS sends the URL in the CERT payload instead of sending the entire certificate in the payload.

If not configured and CERTREQ is received with encoding type as "Hash and URL for X.509 certificate", StarOS responds with entire certificate as it in release 14.1, even if peer had sent HTTP_CERT_LOOKUP_SUPPORTED.

If configured for Hash and URL while sending the CERTREQ request, StarOS sends the request with encoding type as "Hash and URL of X.509 certificate" and sends notify payload HTTP_CERT_LOOKUP_SUPPORTED. However, also sends another CERTREQ with encoding type as X.509 certificate (as in release 14.1) and accepts the entire certificate coming in the CERT payload. If CERT payload is received with encoding type as hash and URL, StarOS fetches the certificate using the URL.

Multiple Traffic Selectors

During traffic selector negotiation, the gateway should be able to narrow down the UE's request for a range of traffic selectors in accordance with RFC 5996.

CLI Commands

Important The commands and new keywords described below appear in the CLI for this release. However, they have not been qualified for use with any current Cisco StarOS gateway products.

Context Configuration Mode

Enable Notification Payloads

To enable the sending and receiving of TEMPORARY_FAILURE and CHILD_SA_NOT_FOUND notifications, use one of the following configuration sequences.

For a crypto map the configuration sequence is:

```
configure
  context ctxt_name
    crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
      ikev2-ikesa
        policy use-rfc5996-notification
```

For a crypto template the configuration sequence is:

```
configure
  context ctxt_name
    crypto template template_name ikev2-dynamic
      ikev2-ikesa
        policy use-rfc5996-notification
```

Refer to the *Command Line Interface Reference* for a complete description of these commands and their keywords.

Add Hash and URL Encoding to Certificates

Use the following configuration to add Hash and URl encoding of certificates.

For a crypto map the configuration sequence is:

```
configure
  context ctxt_name
    crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
      certificate name
        pem url url
        cert-enc cert-hash-url url url url
```

For a crypto template the configuration sequence is:

```
configure
   context ctxt_name
      crypto template template_name ikev2-dynamic
           pem url url
           cert-enc cert-hash-url url url url
```

Refer to the *Command Line Interface Reference* for a complete description of these commands and their keywords.

Enable Hash and URL Certificate Encoding

Hash and URL encoding must be enabled in a crypto map or crypto template.

For a crypto map the configuration sequence is:

```
configure
   context ctxt_name
      crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
        allow-cert-enc cert-hash-url
```

For a crypto template the configuration sequence is:

```
configure
   context ctxt_name
      crypto template template_name ikev2-dynamic
        allow-cert-enc cert-hash-url
```

Refer to the *Command Line Interface Reference* for a complete description of these commands and their keywords.

Disable Change in Rekey Parameters in CHILDSA REKEY

Disabling of rekey parameters must be enabled in a crypto map or crypto template.

For a crypto map the configuration sequence is:

```
configure
   context ctxt_name
      crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
        ikev2-ikesa
          rekey disallow-param-change
```

For a crypto template the configuration sequence is:

```
configure
   context ctxt_name
      crypto template template_name ikev2-dynamic
        ikev2-ikesa
          rekey disallow-param-change
```

Refer to the *Command Line Interface Reference* for a complete description of these commands and their keywords.

Enable TSr Ranges

To support multiple traffic selectors, the **tsr start-address** command has been modified to process both IPv4 and IPv6 addresses.

```
configure
   context context_name
      crypto templatetnplt_name ikev2-dynamic
         payload payload_name match childsa match any
            tsr start-address ipv4v6_address end-address ipv4v6_address
          end
```

Notes:

- The configuration is restricted to a maximum of four TSrs per payload and per childsa.
- Overlapping TSrs are not allowed either inside the same payload or across different payloads.
- When a TSr is configured via this command, only the configured TSr will be considered for narrowing-down. For example, if one IPv4 TSr is configured, and the gateway receives an IPv6 TSr, the gateway will reject the call with a TS_UNACCEPTABLE notification.
- The UE must send both INTERNAL_IP4_ADDRESS and INTERNAL_IP6_ADDRESS in the Configuration Payload, whenever it needs both IPv4 and IPv6 addresses in TSrs. Otherwise, the gateway will respond back with only one type depending upon the type of address received in the Configuration Payload. For example,.if the gateway receives only INTERNAL_IP4_ADDRESS in the Configuration Payload but both IPv4 and IPv6 addresses are in the TSrs, the gateway will narrow down only the IPv4 address, and ignore the IPv6 TSrs.
- IPv4 TSrs are not allowed inside IPv6 payloads.
- IPv6 TSrs are not allowed inside IPv4 payloads.

show commands

The following **show** commands display configuration parameters associated with support of RFC 5996:

- Statistics for notification payloads
  - **show crypto statistics ikev2**
  - **show crypto ikev2-ikesa security-associations**
  - **show crypto ipsec security-associations**
  - **show crypto statistics ikev2**
- Send and receive statistics for hash-url encrypted certificates
  - **show crypto statistics ikev2**
- RFC 5996 configuration options
  - **show configuration**